UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

VINÍCIUS FRANCO VASCONCELOS

TEORIA DOS CONJUNTOS – UM ESTUDO INTRODUTÓRIO

TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO
2018

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM
MATEMÁTICA**

VINÍCIUS FRANCO VASCONCELOS

TEORIA DOS CONJUNTOS – UM ESTUDO INTRODUTÓRIO

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná, Câmpus Toledo, como requisito parcial à obtenção do título de Licenciado em Matemática.

Orientador: Adriano Gomes de Santana

TOLEDO
2018

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM
MATEMÁTICA**

TERMO DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado "TEORIA DOS CONJUNTOS – UM ESTUDO INTRODUTÓRIO" foi considerado **APROVADO** de acordo com a ata nº __ de __/__/____

Fizeram parte da banca examinadora os professores:

Adriano Gomes de Santana

Wilian Francisco de Araujo

Ana Cláudia Golzio

Robson Willians Vinciguerra

TOLEDO
2018

RESUMO

Este texto apresenta a Teoria Axiomática dos Conjuntos de Zermelo-Fraenkel com o Axioma da Escolha. A Teoria dos Conjuntos serve de fundamento a diversas áreas da Matemática. Partindo dos axiomas e construções básicas tais como relações, funções e partições, definimos o conjunto dos números naturais, desenvolvemos as noções de números ordinais e números cardinais, bem como suas aritméticas, construímos a hierarquia cumulativa de conjuntos e abordamos alguns conceitos de Teoria dos Modelos. Trata-se de um trabalho introdutório, sem a pretensão de ser completo, mas com o intuito de servir de estudo a interessados em Teoria dos Conjuntos.

Palavras-chave: Teoria dos Conjuntos. Fundamentos da Matemática. Números Ordinais. Números Cardinais. Teoria dos Modelos.

ABSTRACT

The present text introduces Axiomatic Set Theory of Zermelo-Fraenkel with Axiom of Choice. Set Theory serves as a foundation for several areas of Mathematics. From axioms and basic constructions like relations, functions and partitions, we define the set of natural numbers, we develop the notions of ordinal numbers and cardinal numbers, as well as their arithmetics, we construct the cumulative hierarchy of sets and we approach some concepts of Model Theory. It is an introductory development, without pretension to be a complete work, but with the purpose to help studies of people attracted by Set Theory.

Keywords: Set Theory. Foundations of Mathematics. Ordinal Numbers. Cardinal Numbers. Model Theory.

LISTA DE SÍMBOLOS

$\{k \in x : P(k)\}$, descrição de um conjunto por separação

$\{F(k) : k \in x\}$, descrição de um conjunto por substituição

$x = y$, x é igual a y

$x \in y$, x pertence a y

$x \Subset y$, x pertence ou é igual a y

$x \subseteq y$, x contido em y

$x \subsetneq y$, x contido propriamente em y

$\varnothing$, conjunto vazio

$\{x\}$, conjunto unitário de x

$\{x, y\}$, par não-ordenado x y

(x, y), par ordenado x y

$x \cup y$, união de x e y

$x \cap y$, intersecção de x e y

$x \smallsetminus y$, diferença de x e y

$x \bigtriangleup y$, diferença simétrica de x e y

$x \mathbin{\dot\cup} y$, união disjunta de x e y

$x \times y$, produto cartesiano de x e y

$\bigcup x$, união de x

$\bigcap x$, intersecção de x

$\dot{\bigcup} x$, união disjunta de x

$\mathcal{P}(x)$, conjunto das partes de x

$\mathcal{P}_{<\omega}(x)$, conjunto das partes finitas de x

$\mathcal{S}(x)$, sucessor de x

$\bigcup_{k \in \lambda} x_k$, união dos x_k

$\bigcap_{k \in \lambda} x_k$, intersecção dos x_k

Id_x, identidade de x

$\in_x$, pertinência em x

$\subseteq_x$, inclusão em x

$\mathrm{Dom}\, r$, domínio de r

$\mathrm{Ran}\, r$, contradomínio de r

$\mathrm{Im}\, r$, imagem de r

$r[x]$, imagem de r por x

r^{-1}, relação inversa de r

$s \circ r$, composição de r e s

$f : x \to y$, função f de x em y

χ_x, função característica de x

π_1, projeção na primeira coordenada

π_2, projeção na segunda coordenada

$f \restriction x$, restrição de f a x

$\mathcal{F}(x, y)$, conjunto das funções de x em y

y^x, conjunto das funções de x em y

$\prod_{k \in \lambda} x_k$, produto cartesiano dos x_k

$[x]_r$, classe de equivalência de x em r

$x \,/\, r$, quociente de x por r

$\mathcal{T}(x)$, fecho transitivo de x

ω, conjunto dos números naturais

$\leq_+$, ordem usual dos naturais

$\leq_\bullet$, ordem da divisibilidade dos naturais

$\leq_\cup$, ordem união

$\leq_\times$, ordem lexicográfica

$\min x$, mínimo de x

$\max x$, máximo de x

$\sup x$, supremo de x

$\inf x$, ínfimo de x

$\langle f_\xi : \xi < \vartheta \rangle$, sequência f de comprimento ϑ

$f \frown g$, concatenação de f e g

$\lim f$, limite de f

$\mathrm{cof}\, \alpha$, cofinalidade de α

$|x| = |y|$, x é equipotente a y

$|x|$, cardinalidade de x

$\mathcal{H}(x)$, número de Hartogs de x

ω, menor ordinal infinito

ω_1, menor ordinal não-enumerável

ε, ordinal limite da sequência ω, ω^ω, ω^{ω^ω}, ...

$\mathfrak{c}$, potência do continuum

κ^+, cardinal sucessor de κ

$\aleph_0$, cardinal infinito enumerável

$\aleph_\alpha$, α-ésimo cardinal infinito

$\mathcal{V}_\alpha$, α-ésimo nível da hierarquia cumulativa

$\operatorname{rank} x$, ranque de x

$\mathcal{V}$, classe universal

Ord, classe dos números ordinais

Card, classe dos números cardinais

$\neg\varphi$, não φ

$\varphi \to \psi$, se φ então ψ

$\varphi \leftrightarrow \psi$, φ se e somente se ψ

$\varphi \vee \psi$, φ ou ψ

$\varphi \wedge \psi$, φ e ψ

$\varphi \veebar \psi$, φ ou ψ mas não ambos

$\forall x\ \varphi$, para todo x temos φ

$\exists x\ \varphi$, existe x tal que φ

$\exists! x\ \varphi$, existe um único x tal que φ

$\Gamma \vdash \varphi$, Γ deduz φ

$\Gamma \models \varphi$, Γ satisfaz φ

$\mathfrak{M} \models \Gamma$, $\mathfrak{M}$ é um modelo de Γ

$\varphi^{\mathfrak{M}}$, interpretação de φ em $\mathfrak{M}$

$\mathrm{Con}(\Gamma)$, Γ é consistente

SUMÁRIO

INTRODUÇÃO

Nesse trabalho estudamos especificamente a Teoria Axiomática de Conjuntos de Zermelo-Fraenkel com o Axioma da Escolha, abreviada como ZFC, mas não nos restringimos a ela, tratando também de classes e modelos.

Assumimos que o leitor já teve um primeiro contato com Lógica Proposicional e Lógica de Predicatos, bem como já tem uma noção intuitiva sobre o que é um conjunto. O texto foi escrito tendo em mente ser acessível a alunos de graduação de cursos de Matemática, particularmente alunos dos últimos períodos da Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná campus Toledo, que já cursaram ou estão cursando disciplinas de Análise e Álgebra, não sendo estas, no entanto, disciplinas indispensáveis para a leitura.

Trata-se de um trabalho introdutório, sem a pretensão de ser completo, mas com o intuito de servir de estudo a interessados em Teoria dos Conjuntos, visto a carência de livros-texto em português na área a nível de graduação. Temos a pretensão de futuramente transformar esse trabalho em livro, e o desejo de que seja uma área mais difundida pelas universidades brasileiras.

A referência principal foi o livro (JECH, 2002), sendo também utilizados os livros (HRBACEK; JECH, 1999), (HALBEISEN, 2012) e (KUNEN, 1980), bem como as notas de aula (CONIGLIO, 1999).

Como dito anteriormente, assumimos que o leitor já teve um primeiro contato com Lógica, de maneira que já conhece tabelas-verdade e sabe o que são tautologias, pois usaremos tautologias recorrentemente. Também assumimos que o leitor já tem certa familiaridade com algumas técnicas de demonstração tais como demonstração direta, demonstração pela contrapositiva, demonstração por redução ao absurdo, demonstração por divisão em casos, etc.

Logo no início do Capítulo 1 falamos brevemente sobre a linguagem de Teoria dos Conjuntos, porém sem nos aprofundar (abordamos de maneira mais profunda no Capítulo 9). Os conectivos considerados são: negação ($\neg p$, "não p"), implicação ($p \to q$, "se p então q"), biimplicação ($p \leftrightarrow q$, "p se e somente se q"), disjunção ($p \vee q$, "p ou q"), conjunção ($p \wedge q$, "p e q") e disjunção exclusiva ($p \veebar q$, "p ou q mas não ambos"). Os quantificadores considerados são: universal ($\forall x$, "para todo x"), existencial ($\exists x$, "existe algum x") e de unicidade ($\exists! x$, "existe um único x"). Além desses símbolos lógicos, também temos a igualdade ($x = y$, "x é igual a y"). Apesar de considerarmos todos esses conectivos e quantificadores, observamos que poderíamos reduzir nossa lista para somente $\neg$, $\to$, $\forall$ e $=$, e definir os demais a partir destes.

No Capítulo 1 apresentamos todos os axiomas de ZFC, bem como algumas consequências e construções iniciais, tais como união, intersecção, produto cartesiano, etc. No Capítulo 2 fazemos mais construções, sendo elas de objetos que acreditamos que o leitor já tem certa familiaridade, tais como relações e funções, porém com uma roupagem possivelmente nova, isto é, sendo apresentados como conjuntos.

No Capítulo 3 tratamos dos números naturais, construindo o conjunto a partir do Axioma da Infinitude. Falamos essencialmente o básico sobre os números naturais, e acreditamos que a partir do que foi apresentado o leitor não deve ter dificuldades para definir por conta própria os demais conceitos, tais como subtração, divisão, múltiplo, divisor, número primo, etc. Apresentamos também uma formulação da Aritmética de Peano.

No Capítulo 4 abordamos classes de uma maneira um tanto ingênua, mas suficiente para os propósitos do trabalho, sendo essencialmente uma outra maneira de lidar com fórmulas. Também generalizamos alguns conceitos de conjuntos para classes.

No Capítulo 5 aparecem efetivamente conceitos que podem ser inéditos para a maioria dos alunos de graduação. Começamos o capítulo falando de relações de ordem e conceitos relacionados. Introduzimos a noção de número ordinal e generalizamos os teoremas de indução e de recursão.

No Capítulo 6 introduzimos o conceito de cardinalidade e formalizamos a ideia de conjuntos finitos e conjuntos infinitos. Aprofundamos o estudo de ordinais e apresentamos os números cardinais, bem como os álefs. Falamos também de alguns problemas que são independentes de ZFC, tais como a Hipótese do Continuum e a existência de um cardinal fortemente inacessível.

No Capítulo 7 trabalhamos com filtros e apresentamos alguns resultados envolvendo sequências. No Capítulo 8 trazemos outra generalização dos teoremas de indução e de recursão, bem como uma construção de um modelo de ZFC.

No Capítulo 9 apresentamos algumas ideias e resultados de Teoria dos Modelos, dentre eles os Teoremas de Gödel (sem demonstração), e concluímos exibindo a construção de um modelo de ZFC.

Ademais, esperamos que esse trabalho seja útil e interessante para os que o lerem.

1 AXIOMAS DA TEORIA

1.1 LINGUAGEM DA TEORIA

Neste trabalho desenvolveremos a Teoria dos Conjuntos numa linguagem de primeira ordem. Além do símbolo de predicato $=$, a linguagem da Teoria dos Conjuntos consiste do símbolo de predicato binário $\in$, que dá a noção de "ser elemento de". A teoria possui somente um tipo de objeto: *conjuntos*.

As fórmulas atômicas em Teoria dos Conjuntos são:

- $x = y$
- $x \in y$

Se φ e ψ são fórmulas, então também são fórmulas:

- $(\neg\,\varphi)$
- $(\varphi \to \psi)$
- $(\varphi \leftrightarrow \psi)$
- $(\varphi \vee \psi)$
- $(\varphi \wedge \psi)$
- $(\varphi \veebar \psi)$
- $\forall x\ (\varphi)$
- $\exists x\ (\varphi)$
- $\exists! x\ (\varphi)$

Sendo que nas três últimas a variável x não pode aparecer quantificada em φ. Os parênteses podem ser omitidos se não houver ambiguidade.

De fato, utilizamos outros símbolos quando nos referimos a fórmulas em teoria dos conjuntos, mas são símbolos definidos a partir destes, de forma que qualquer fórmula pode ser escrita em termos de $=$, $\in$, conectivos, quantificadores, parênteses e variáveis. Como exemplo, escrevemos todos os axiomas de ZFC dessa forma.

Uma variável x é dita *livre* em φ quando aparece não quantificada em φ. Se φ não tiver variáveis livres, então φ é chamada de *sentença*.

Algumas abreviações recorrentes são:

- $\forall u \in x\ (\varphi)$ para $\forall u\ (u \in x \to \varphi)$;
- $\exists u \in x\ (\varphi)$ para $\exists u\ (u \in x \wedge \varphi)$;
- $\exists! u \in x\ (\varphi)$ para $\exists! u\ (u \in x \wedge \varphi)$;
- $x \neq y$ para $\neg\,(x = y)$;
- $x \notin y$ para $\neg\,(x \in y)$.

Definição 1.1. Quando $a \in b$, dizemos que a *pertence* a b, ou que a é um *elemento* de b, ou que a *está* em b, e também é usual escrever $b \ni a$. Se $a \in b$ ou $a = b$, escrevemos $a \underline{\in} b$. O símbolo $\in$ é chamado de *pertinência*.

1.2 AXIOMA DA EXTENSÃO

Definição 1.2. Dados dois conjuntos a e b, dizemos que a está *contido* em b, ou que b *contém* a, ou que a está *incluso* em b, ou que a é um *subconjunto* de b, ou que a é uma *parte* de b, se todo elemento de a é elemento de b, e escrevemos $a \subseteq b$ ou $b \supseteq a$. Caso contrário, escrevemos $a \nsubseteq b$ ou $b \nsupseteq a$. Além disso, dizemos que a está *contido propriamente* em b, ou que b *contém propriamente* a, ou que a está *incluso propriamente* em b, ou que a é um *subconjunto próprio* de b, se $a \subseteq b$ e $a \neq b$, e escrevemos $a \subsetneq b$ ou $b \supsetneq a$. Os símbolos $\subseteq$ e $\subsetneq$ são chamados respectivamente de *inclusão* e de *inclusão própria*.

Axioma da Extensão. Dois conjuntos x e y são iguais se e somente se eles têm os mesmos elementos, isto é, $x = y$ se e somente se $x \subseteq y$ e $x \supseteq y$.
Na linguagem da Teoria dos Conjuntos:

$$\forall x \; \forall y \; (\forall u \; (u \in x \; \leftrightarrow \; u \in y) \; \rightarrow \; x = y) \tag{1.1}$$

1.3 AXIOMAS DA SEPARAÇÃO

Esquema de Axiomas da Separação. Dado um conjunto x, para cada fórmula φ (possivelmente com parâmetros) que expressa uma propriedade, existe o conjunto y cujos elementos são os elementos de x que satisfazem φ.
Na linguagem da Teoria dos Conjuntos:

$$\forall x \; \forall p \; \exists y \; (\forall u \; (u \in y \; \leftrightarrow \; (u \in x \; \wedge \; \varphi(u,p)))) \tag{1.2}$$

Note aqui que não se trata somente de um axioma, mas infinitos, uma vez que para cada fórmula φ temos um axioma. Por isso dizemos que se trata de um *esquema*.

Definição 1.3. Dado um conjunto a, chamando a propriedade expressa por $\varphi(u,p)$ de $P(u)$, o conjunto cujos elementos são os elementos $k \in a$ que satisfazem a propriedade $P(k)$ é denotado por $\{k \in a : P(k)\}$. Tal conjunto é um subconjunto de a.

Definição 1.4. Um conjunto a é chamado de *conjunto vazio*, ou simplesmente de *vazio*, se a não possui elementos, isto é, não existe u tal que $u \in a$. Um conjunto diferente do vazio é chamado de *conjunto não-vazio*, ou simplesmente de *não-vazio*.

Teorema 1.1. Se existe algum conjunto, então existe um único conjunto vazio.

Demonstração. Considere um conjunto t, e tome $a = \{k \in t : k \neq k\}$. Como todo conjunto u satisfaz $u = u$, segue que $u \notin a$, isto é, a é vazio. Seja b um conjunto vazio. Como $u \in a \; \leftrightarrow \; u \in b$ se trata de uma tautologia para todo u, segue que $a = b$. □

Uma vez que existe um único conjunto vazio, ele é denotado por $\varnothing$. A existência de ao menos um conjunto é garantida pelo Axioma da Infinitude, que será visto mais adiante.

Um esquema de axiomas que era considerado anteriormente era o dos Axiomas da Compreensão. Esse esquema é mais forte do que o dos Aximas da Separação, entretanto tais axiomas conduzem a contradições dentro da teoria, como por exemplo o Paradoxo de Russel, visto a seguir.

Esquema de Axiomas da Compreensão (Falso)**.** Para cada fórmula φ (possivelmente com parâmetros) que expressa uma propriedade, existe o conjunto x cujos elementos são os conjuntos que satisfazem φ.
Na linguagem da Teoria dos Conjuntos:

$$\forall p\ \exists x\ (\forall u\ (u \in x\ \leftrightarrow\ \varphi(u,p)))$$

Paradoxo de Russel. Considere o conjunto x dos conjuntos que não pertencem a si mesmos, isto é, para cada u, segue que $u \in x$ se e somente se $u \notin u$. Se $x \in x$, então $x \notin x$, mas se $x \notin x$, então $x \in x$, absurdo. Logo, não existe um conjunto definido pela propriedade "$u \notin u$".

Teorema 1.2. Não existe o conjunto de todos os conjuntos.

Demonstração. Suponha que exista o conjunto U de todos os conjuntos. Seja $x = \{k \in U : k \notin k\}$. Pelo Paradoxo de Russel, o conjunto x não existe, absurdo. Portanto não existe o conjunto de todos os conjuntos. $\square$

1.4 AXIOMA DO PAR

Axioma do Par. Dados dois conjuntos x e y, existe o conjunto z cujos elementos são x e y.
Na linguagem da Teoria dos Conjuntos:

$$\forall x\ \forall y\ \exists z\ (\forall u\ (u \in z\ \leftrightarrow\ (u = x\ \vee\ u = y))) \tag{1.3}$$

Definição 1.5. Dados dois conjuntos a e b, o conjunto cujos elementos são a e b é chamado de *par não-ordenado* a b, ou simplesmente de *par* a b, e é denotado por $\{a,b\}$. Quando $a = b$, o par não-ordenado é denotado simplesmente por $\{a\}$ e é chamado de conjunto *unitário* de a. A unicidade do par não-ordenado decorre do Axioma da Extensão.

Definição 1.6. Dados dois conjuntos a e b, o conjunto $\{\{a\},\{a,b\}\}$ é chamado de *par ordenado* a b, e é denotado por (a,b). Os conjuntos a e b são chamados respectivamente de *primeira coordenada* e de *segunda coordenada* de (a,b).

A motivação para definir par ordenado consiste no fato de que dois pares ordenados são iguais se e somente se suas respectivas coordenadas são iguais. Isso é o que garante o Teorema 1.3.

Teorema 1.3. Dados quatro conjuntos a, b, c e d, temos $(a, b) = (c, d)$ se e somente se $a = c$ e $b = d$.

Demonstração. ($\Rightarrow$) Suponha que $a \neq c$. Assim, temos $\{a\} \neq \{c\}$, e como $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, segue que $\{a\} = \{c, d\}$, logo $a = c$, absurdo. Portando $a = c$. Suponha agora que $b \neq d$. Como $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, devemos ter $\{a, b\} = \{c\}$ ou $\{a, b\} = \{c, d\}$. Se $\{a, b\} = \{c\}$, então $a = c = b$, e $\{\{c\}, \{c, d\}\} = \{\{a\}\}$, o que implica $\{c, d\} = \{a\}$, logo $d = a = b$, absurdo. Se $\{a, b\} = \{c, d\}$, devemos ter $d = a = c$, logo $\{a, b\} = \{d\}$, e $b = d$, aburso. Portanto $b = d$.
($\Leftarrow$) É imediato. $\square$

1.5 AXIOMA DA UNIÃO

Axioma da União. Dado um conjunto x, existe o conjunto y cujos elementos são os que pertencem a algum elemento de x.
Na linguagem da Teoria dos Conjuntos:

$$\forall x \; \exists y \; (\forall u \; (u \in y \leftrightarrow \exists v \; (v \in x \wedge u \in v))) \tag{1.4}$$

Definição 1.7. Dado um conjunto a, o conjunto cujos elementos são os que pertencem a algum elemento de a é chamado de *união* de a, e é denotado por $\bigcup a$. A unicidade da união decorre do Axioma da Extensão.

Definição 1.8. Dado um conjunto não-vazio a, o conjunto cujos elementos são os que pertencem a todos os elemento de a é chamado de *intersecção* de a, e é denotado por $\bigcap a$. A existência da intersecção decorre dos Axiomas da Separação. Em símbolos:

$$\bigcap a = \left\{ k \in \bigcup a : \forall u \in a \; (k \in u) \right\}$$

É imediato da definição que se a é um conjunto não-vazio então $\bigcap a \subseteq \bigcup a$.

Definição 1.9. Dados dois conjuntos a e b, definimos:

- a *união* de a e b como $a \cup b = \bigcup \{a, b\}$;
- a *intersecção* de a e b como $a \cap b = \bigcap \{a, b\}$;
- a *diferença* de a e b como $a \smallsetminus b = \{k \in a : k \notin b\}$;

- a *diferença simétrica* de a e b como $a \triangle b = (a \cup b) \setminus (a \cap b)$.

Quando $b \subseteq a$, a diferença $a \setminus b$ também é chamada de *complementar* de b em relação a a.

Note as seguintes equivalências, para cada x, y e u:

- $u \in x \cup y$ se e somente se $u \in x \ \vee \ u \in y$;
- $u \in x \cap y$ se e somente se $u \in x \ \wedge \ u \in y$;
- $u \in x \setminus y$ se e somente se $u \in x \ \wedge \ u \notin y$;
- $u \in x \triangle y$ se e somente se $u \in x \ \veebar \ u \in y$.

Teorema 1.4. Para quaisquer conjuntos a, b e c, as seguintes propriedades são válidas:

(i) $a \cup a = a$;

(ii) $a \cap a = a$;

(iii) $a \cup b = b \cup a$;

(iv) $a \cap b = b \cap a$;

(v) $a \triangle b = b \triangle a$;

(vi) $(a \cup b) \cup c = a \cup (b \cup c)$;

(vii) $(a \cap b) \cap c = a \cap (b \cap c)$;

(viii) $(a \triangle b) \triangle c = a \triangle (b \triangle c)$;

(ix) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$;

(x) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$;

(xi) $a \cap (b \triangle c) = (a \cap b) \triangle (a \cap c)$;

(xii) $a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c)$;

(xiii) $a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)$;

(xiv) $(a \cup b) \setminus (a \cap b) = (a \setminus b) \cup (b \setminus a)$.

Demonstração. Sejam φ, ψ e χ respectivamente as fórmulas $u \in a$, $u \in b$ e $u \in c$. Os itens decorrem das seguintes tautologias:
(i) $(\varphi \vee \varphi) \leftrightarrow \varphi$
(ii) $(\varphi \wedge \varphi) \leftrightarrow \varphi$
(iii) $(\varphi \vee \psi) \leftrightarrow (\psi \vee \varphi)$
(iv) $(\varphi \wedge \psi) \leftrightarrow (\psi \wedge \varphi)$
(v) $(\varphi \veebar \psi) \leftrightarrow (\psi \veebar \varphi)$
(vi) $((\varphi \vee \psi) \vee \chi) \leftrightarrow (\varphi \vee (\psi \vee \chi))$
(vii) $((\varphi \wedge \psi) \wedge \chi) \leftrightarrow (\varphi \wedge (\psi \wedge \chi))$
(viii) $((\varphi \veebar \psi) \veebar \chi) \leftrightarrow (\varphi \veebar (\psi \veebar \chi))$
(ix) $(\varphi \vee (\psi \wedge \chi)) \leftrightarrow ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$
(x) $(\varphi \wedge (\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$
(xi) $(\varphi \wedge (\psi \veebar \chi)) \leftrightarrow ((\varphi \wedge \psi) \veebar (\varphi \wedge \chi))$
(xii) $(\varphi \wedge \neg(\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \neg\psi) \wedge (\varphi \wedge \neg\chi))$
(xiii) $(\varphi \wedge \neg(\psi \wedge \chi)) \leftrightarrow ((\varphi \wedge \neg\psi) \vee (\varphi \wedge \neg\chi))$
(xiv) $((\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)) \leftrightarrow ((\varphi \wedge \neg\psi) \vee (\psi \wedge \neg\varphi))$ $\square$

Teorema 1.5. Para qualquer conjunto a, as seguintes propriedades são válidas:

(i) $a \cup \varnothing = a$;

(ii) $a \cap \varnothing = \varnothing$;

(iii) $a \smallsetminus \varnothing = a$;

(iv) $a \bigtriangleup \varnothing = a$;

(v) $\varnothing \smallsetminus a = \varnothing$;

(vi) $a \smallsetminus a = \varnothing$;

(vii) $a \bigtriangleup a = \varnothing$.

Demonstração. Seja φ a fórmula $u \in a$. Como $u \in \varnothing$ é sempre falso, os itens decorrem das seguintes tautologias ($\perp$ representa uma fórmula falsa):
(i) $(\varphi \vee \perp) \leftrightarrow \varphi$
(ii) $(\varphi \wedge \perp) \leftrightarrow \perp$
(iii) $(\varphi \wedge \neg\perp) \leftrightarrow \varphi$
(iv) $(\varphi \veebar \perp) \leftrightarrow \varphi$
(v) $(\perp \wedge \neg\varphi) \leftrightarrow \perp$
(vi) $(\varphi \wedge \neg\varphi) \leftrightarrow \perp$
(vii) $(\varphi \veebar \varphi) \leftrightarrow \perp$ □

Teorema 1.6. Para quaisquer conjuntos a, b e c, as seguintes propriedades são válidas:

(i) $a \cup b = b$ se e somente se $a \subseteq b$;

(ii) $a \cap b = b$ se e somente se $a \supseteq b$;

(iii) $a \cup b \subseteq c$ se e somente se $a \subseteq c$ e $b \subseteq c$;

(iv) $a \cap b \supseteq c$ se e somente se $a \supseteq c$ e $b \supseteq c$.

Demonstração. Sejam φ, ψ e χ respectivamente as fórmulas $u \in a$, $u \in b$ e $u \in c$. Os itens decorrem das seguintes tautologias:
(i) $((\varphi \vee \psi) \leftrightarrow \psi) \leftrightarrow (\varphi \to \psi)$
(ii) $((\varphi \wedge \psi) \leftrightarrow \psi) \leftrightarrow (\psi \to \varphi)$
(iii) $((\varphi \vee \psi) \to \chi) \leftrightarrow ((\varphi \to \chi) \wedge (\psi \to \chi))$
(iv) $(\chi \to (\varphi \wedge \psi)) \leftrightarrow ((\chi \to \varphi) \wedge (\chi \to \psi))$ □

Definição 1.10. Dados dois conjuntos a e b, dizemos que eles são *disjuntos* se eles não têm elementos em comum, isto é, se $a \cap b = \varnothing$. Dizemos que os elementos de a são *dois a dois disjuntos* se para quaisquer $u, v \in a$ com $u \neq v$ tivermos que u e v são disjuntos.

Dois conjuntos são disjuntos se não possuem elementos em comum. Essa noção é bem útil em diversos contextos.

Definição 1.11. Dado um conjunto a, se os elementos de a são dois a dois disjuntos, então a união $\bigcup a$ é chamada de *união disjunta*, e denotamos por $\dot{\bigcup} a$. Dado um outro conjunto b, se a e b forem disjuntos, denotamos $a \cup b$ como $a \mathbin{\dot\cup} b$.

1.6 AXIOMA DA POTÊNCIA

Axioma da Potência. Dado um conjunto x, existe o conjunto y cujos elementos são os subconjuntos de x.
Na linguagem da Teoria dos Conjuntos:

$$\forall x\ \exists y\ (\forall u\ (u \in y\ \leftrightarrow\ \forall v\ (v \in u\ \rightarrow\ v \in x))) \tag{1.5}$$

Definição 1.12. Dado um conjunto a, o conjunto cujos elementos são os subconjuntos de a é chamado de *conjunto das partes* de a, ou de *conjunto potência* de a, e é denotado por $\mathcal{P}(a)$. A unicidade do conjunto das partes decorre do Axioma da Extensão.

Note que para qualquer conjunto a temos $\mathcal{P}(a) \neq \varnothing$. De fato, como $a \subseteq a$ e $\varnothing \subseteq a$, segue que $a \in \mathcal{P}(a)$ e $\varnothing \in \mathcal{P}(a)$. Em particular, se $\mathcal{P}(a)$ é unitário, então $a = \varnothing$.

Teorema 1.7. Dados dois conjuntos a e b, temos $a \subseteq b$ se e somente se $\mathcal{P}(a) \subseteq \mathcal{P}(b)$.

Demonstração. ($\Rightarrow$) Seja $u \in \mathcal{P}(a)$, isto é, $u \subseteq a$. Como $a \subseteq b$, segue que $u \subseteq b$, logo $u \in \mathcal{P}(b)$. Portanto, $\mathcal{P}(a) \subseteq \mathcal{P}(b)$.
($\Leftarrow$) Seja $v \in a$. Temos $\{v\} \subseteq a$, logo $\{v\} \in \mathcal{P}(a)$, e assim $\{v\} \in \mathcal{P}(b)$, logo $\{v\} \subseteq b$ e segue que $v \in b$. Portanto, $a \subseteq b$. $\square$

Teorema 1.8. Dados dois conjuntos a e b e elementos $c \in a$ e $d \in b$, temos $(c, d) \in \mathcal{P}(\mathcal{P}(a \cup b))$.

Demonstração. Como $c \in a$ e $d \in b$, temos $c \in a \cup b$ e $d \in a \cup b$ e segue que $\{c\} \subseteq a \cup b$ e $\{c, d\} \subseteq a \cup b$, isto é, $\{c\} \in \mathcal{P}(a \cup b)$ e $\{c, d\} \in \mathcal{P}(a \cup b)$. Deste modo, $\{\{c\}, \{c, d\}\} \subseteq \mathcal{P}(a \cup b)$, e portanto $(c, d) = \{\{c\}, \{c, d\}\} \in \mathcal{P}(\mathcal{P}(a \cup b))$. $\square$

Definição 1.13. Dados dois conjuntos a e b, o conjunto dos pares ordenados cuja primeira coordenada pertence a a e a segunda coordenada pertence a b é chamado de *produto cartesiano* de a e b, e é denotado por $a \times b$. Em símbolos:

$$a \times b = \{k \in \mathcal{P}(\mathcal{P}(a \cup b)) : \exists u \in a\ \exists v \in b\ (k = (u, v))\}$$

Teorema 1.9. Para quaisquer conjuntos a, b e c, as seguintes propriedades são válidas:

(i) $a \times (b \cup c) = (a \times b) \cup (a \times c)$;

(ii) $a \times (b \cap c) = (a \times b) \cap (a \times c)$;

(iii) $a \times (b \smallsetminus c) = (a \times b) \smallsetminus (a \times c)$;

(iv) $a \times (b \mathbin{\triangle} c) = (a \times b) \mathbin{\triangle} (a \times c)$.

Demonstração. Sejam φ, ψ e χ respectivamente as fórmulas $u \in a$, $v \in b$ e $v \in c$. Os itens decorrem das seguintes tautologias:
(i) $(\varphi\ \wedge\ (\psi\ \vee\ \chi))\ \leftrightarrow\ ((\varphi\ \wedge\ \psi)\ \vee\ (\varphi\ \wedge\ \chi))$

(ii) $(\varphi \wedge (\psi \wedge \chi)) \leftrightarrow ((\varphi \wedge \psi) \wedge (\varphi \wedge \chi))$
(iii) $(\varphi \wedge (\psi \wedge \neg\chi)) \leftrightarrow ((\varphi \wedge \psi) \wedge \neg(\varphi \wedge \chi))$
(iv) $(\varphi \wedge (\psi \veebar \chi)) \leftrightarrow ((\varphi \wedge \psi) \veebar (\varphi \wedge \chi))$ $\square$

Teorema 1.10. Dados dois conjuntos a e b, temos $a \times b = \varnothing$ se e somente se $a = \varnothing$ ou $b = \varnothing$.

Demonstração. ($\Rightarrow$) Se $a \neq \varnothing$ e $b \neq \varnothing$, então existem $u \in a$ e $v \in b$, de forma que $(u, v) \in a \times b$, logo $a \times b \neq \varnothing$. O resultado segue da contrapositiva.
($\Leftarrow$) Se $a \times b \neq \varnothing$, então existe $(u, v) \in a \times b$ tal que $u \in a$ e $v \in b$, isto é, $a \neq \varnothing$ e $b \neq \varnothing$. O resultado segue da contrapositiva. $\square$

Teorema 1.11. As seguintes propriedades **não** são válidas para quaisquer conjuntos a, b e c:

(i) $a \times b = b \times a$;

(ii) $a \times (b \times c) = (a \times b) \times c$.

Demonstração. Contraexemplos, sendo u, v e w conjuntos unitários distintos:
(i) $\{u\} \times \{v\} = \{(u, v)\} \neq \{(v, u)\} = \{v\} \times \{u\}$
(ii) $\{u\} \times (\{v\} \times \{w\}) = \{(u, (v, w))\} \neq \{((u, v), w)\} = (\{u\} \times \{v\}) \times \{w\}$ $\square$

1.7 AXIOMAS DA SUBSTITUIÇÃO

Esquema de Axiomas da Substituição. Dado um conjunto x, para cada fórmula φ (possivelmente com parâmetros) que expressa a ideia de uma função, isto é, para cada $u \in x$ existe um único v_u que torna φ verdadeira, existe o conjunto y cujos elementos são os v_u tais que $u \in x$.
Na linguagem da Teoria dos Conjuntos:

$$\begin{gathered} \forall x\ \forall p\ (\forall u\ (u \in x\ \rightarrow\ \exists! v\ (\varphi(u, v, p)))\ \rightarrow \\ \exists y\ \forall u\ (u \in y\ \leftrightarrow\ \exists v\ (v \in x\ \wedge\ \varphi(v, u, p)))) \end{gathered} \tag{1.6}$$

Definição 1.14. Dado um conjunto a, se para cada $k \in a$ existe um único ℓ tal que $\varphi(k, \ell, p)$ é verificada, escrevendo ℓ como $F(k)$, o conjunto cujos elementos são os ℓ tais que $k \in a$ é denotado por $\{F(k) : k \in a\}$. Um conjunto da forma $\{F(k) : k \in a\}$ é chamado de *família* indexada por a, e a é chamado de conjunto de *índices*. Note que todo conjunto b é, a rigor, uma família, uma vez que $b = \{k : k \in b\}$.

Algumas fórmulas que expressam a ideia de função são "$\{x\} = y$", "$(x, x) = y$", "$\bigcup x = y$", "$\mathcal{P}(x) = y$", pois para cada x existe um único y que torna cada uma delas verdadeira.

Intuitivamente, os Axiomas da Separação falam da existência de subconjuntos, ao passo que os Axiomas da Substituição falam da existência da imagem de funções (conforme apresentado no Capítulo 2 e no Teorema 4.4).

Definição 1.15. Dada uma família não-vazia $a = \{a_k : k \in \lambda\}$, a união e a intersecção de a são comumente escritas como seguem:

$$\bigcup \{a_k : k \in \lambda\} = \bigcup_{k \in \lambda} a_k \qquad\qquad \bigcap \{a_k : k \in \lambda\} = \bigcap_{k \in \lambda} a_k$$

Teorema 1.12. Para quaisquer conjunto a e família não-vazia $\{b_k : k \in \lambda\}$, as seguintes propriedades são válidas:

(i) $a \cup \bigcap_{k \in \lambda} b_k = \bigcap_{k \in \lambda} (a \cup b_k)$;

(ii) $a \cap \bigcup_{k \in \lambda} b_k = \bigcup_{k \in \lambda} (a \cap b_k)$;

(iii) $a \setminus \bigcup_{k \in \lambda} b_k = \bigcap_{k \in \lambda} (a \setminus b_k)$;

(iv) $a \setminus \bigcap_{k \in \lambda} b_k = \bigcup_{k \in \lambda} (a \setminus b_k)$;

Demonstração. (i) Seja $u \in a \cup \bigcap_{k \in \lambda} b_k$. Temos $u \in a$ ou $u \in b_k$ para todo $k \in \lambda$, logo $u \in a \cup b_k$ para todo $k \in \lambda$, e segue que $u \in \bigcap_{k \in \lambda}(a \cup b_k)$. Portanto $a \cup \bigcap_{k \in \lambda} b_k \subseteq \bigcap_{k \in \lambda}(a \cup b_k)$. Seja $v \in \bigcap_{k \in \lambda}(a \cup b_k)$. Como $v \in a \cup b_k$ para todo $k \in \lambda$, segue que $v \in a$ ou $v \in b_k$ para todo $k \in \lambda$, e assim $v \in a \cup \bigcap_{k \in \lambda} b_k$. Portanto $a \cup \bigcap_{k \in \lambda} b_k \supseteq \bigcap_{k \in \lambda}(a \cup b_k)$.
(ii) Análogo ao item (i).
(iii) Seja $u \in a \setminus \bigcup_{k \in \lambda} b_k$. Temos $u \in a$ e não existe $k \in \lambda$ tal que $u \in b_k$, isto é, $u \notin b_k$ para todo $k \in \lambda$, logo $u \in a \setminus b_k$ para todo $k \in \lambda$, e segue que $u \in \bigcap_{k \in \lambda}(a \setminus b_k)$. Portanto $a \setminus \bigcup_{k \in \lambda} b_k \subseteq \bigcap_{k \in \lambda}(a \setminus b_k)$. Seja $v \in \bigcap_{k \in \lambda}(a \setminus b_k)$. Como $v \in a \setminus b_k$ para todo $k \in \lambda$, segue que $v \in a$ e $v \notin b_k$ para todo $k \in \lambda$, de forma que não existe $k \in \lambda$ tal que $v \in b_k$, e assim $v \in a \setminus \bigcup_{k \in \lambda} b_k$. Portanto $a \setminus \bigcup_{k \in \lambda} b_k \supseteq \bigcap_{k \in \lambda}(a \setminus b_k)$.
(iv) Análogo ao item (iii). □

1.8 AXIOMA DA INFINITUDE

Definição 1.16. Dado um conjunto a, o conjunto $\mathcal{S}(a) = a \cup \{a\}$ é chamado de *sucessor* de a.

Definição 1.17. Dado um conjunto s, dizemos que s é *indutivo* se $\varnothing \in s$ e para todo $u \in s$ temos $\mathcal{S}(u) \in s$.

Axioma da Infinitude. Existe um conjunto indutivo.
Na linguagem da Teoria dos Conjuntos:

$$\begin{gathered} \exists x \ (\forall u \ (\neg \exists v \ (v \in u) \ \to \ u \in x) \ \wedge \\ \forall u \ (u \in x \ \to \ \forall v \ (\forall w \ (w \in v \ \leftrightarrow \ (w \in u \ \vee \ w = u)) \ \to \ v \in x))) \end{gathered} \tag{1.7}$$

O Axioma da Infinitude, além de garantir a existência de um conjunto, permite construir o conjunto dos números naturais dentro de ZFC conforme veremos no Capítulo 3. Embora na definição de conjunto indutivo utilizemos o conjunto vazio, cuja existência depende do Axioma da Infinitude, não dependemos do vazio para enunciar o axioma, como pode ser visto na Fórmula (1.7).

1.9 AXIOMA DA REGULARIDADE

Definição 1.18. Dado um conjunto não-vazio a, dizemos que a é *regular* se existe $u \in a$ tal que $a \cap u = \varnothing$.

Exemplo 1.1. Dado um conjunto a, se $\varnothing \in a$ então a é regular, uma vez que $a \cap \varnothing = \varnothing$.

Exemplo 1.2. Dado um conjunto a, dizemos que a é *reflexivo* se $a = \{a\}$. Seja x um conjunto reflexivo. Como o único elemento de x é o próprio x, e $x \cap x = x \neq \varnothing$, segue que x não é regular.

Axioma da Regularidade. Todo conjunto não-vazio é regular.
Na linguagem da Teoria dos Conjuntos:

$$\forall x \; (\exists u \; (u \in x) \; \rightarrow \; \exists u \; (u \in x \; \wedge \; \neg \exists v \; (v \in x \; \wedge \; v \in u))) \tag{1.8}$$

Uma das consequências do Axioma da Regularidade é que não existem conjuntos reflexivos. De fato, vale um resultado mais geral do que esse, apresentado no Teorema 1.13.

Teorema 1.13. Não existe um conjunto a tal que $a \in a$.

Demonstração. Suponha que exista um a tal que $a \in a$. Seja $u = \{a\}$. Como o único elemento de u é a e $a \cap u = u \neq \varnothing$, segue que u não é regular, absurdo. □

Corolário 1.13.1. Dado um conjunto a, temos $a \neq \mathcal{S}(a)$.

Demonstração. Como $a \in \mathcal{S}(a)$, segue que $a \neq \mathcal{S}(a)$. □

Teorema 1.14. Não existem conjuntos a e b tais que $a \in b$ e $b \in a$.

Demonstração. Suponha que existam conjuntos a e b tais que $a \in b$ e $b \in a$. Seja $u = \{a, b\}$. Temos $a \cap u = \{b\} \neq \varnothing$ e $b \cap u = \{a\} \neq \varnothing$, logo u não é regular, absurdo. □

O Teorema 5.17 generaliza os teoremas 1.13 e 1.14.

Definição 1.19. Dado um conjunto a, dizemos que $x \in a$ é um $\in$-*minimal* elemento de a se para todo $t \in a$ temos $t \notin x$.

Teorema 1.15. Dado um conjunto a, se a é não-vazio então a tem um $\in$-minimal elemento.

Demonstração. Suponha que a não tem um $\in$-minimal elemento, isto é, para cada $u \in a$ existe $t \in a$ tal que $t \in u$, logo $t \in a \cap u \neq \varnothing$, e portanto a não é regular, absurdo. $\square$

O Axioma da Regularidade desempenha um papel essencial no Capítulo 8.

1.10 AXIOMA DA ESCOLHA

Axioma da Escolha. Toda família x de conjuntos não-vazios admite um conjunto minimal de representantes, isto é, um conjunto y tal que para cada $u \in x$ existe um único $v \in u$ tal que $v \in y$.
Na linguagem da Teoria dos Conjuntos:

$$\forall x \ (\forall u \ (u \in x \ \rightarrow \ \exists v \ (v \in u)) \ \rightarrow \ \exists y \ (\forall u \ (u \in x \ \rightarrow \ \exists! v \ (v \in u \ \wedge \ v \in y)))) \tag{1.9}$$

O Axioma da Escolha é abreviado por AC (*Axiom of Choice*). ZFC sem o Axioma da Escolha é abreviado como ZF. No decorrer do trabalho, os teoremas que forem consequência do Axioma da Escolha serão apresentados com uma estrela ($\bigstar$).

2 RELAÇÕES E FUNÇÕES

2.1 RELAÇÕES

Definição 2.1. Dado um conjunto r, dizemos que r é uma *relação binária*, ou simplesmente uma *relação*, se os elementos de r forem pares ordenados. Dados dois conjuntos a e b, dizemos que r é uma relação de a em b se $r \subseteq a \times b$. Se r é uma relação de a em a, então dizemos simplesmente que r é uma relação em a. Se $(x, y) \in r$, é usual escrevermos $x \, r \, y$.

Exemplo 2.1. Como não existe $u \in \varnothing$ que não seja um par ordenado, temos que $\varnothing$ é uma relação.

Exemplo 2.2. Dados dois conjuntos a e b, o produto cartesiano $a \times b$ é uma relação de a em b.

Definição 2.2. Dado um conjunto a, a relação $\mathrm{Id}_a = \{(k, k) : k \in a\}$ é chamada de *identidade* em a, ou de *diagonal* de a, ou de *igualdade* em a.

Definição 2.3. Dado um conjunto a, a relação $\in_a = \{(k, \ell) \in a \times a : k \in \ell\}$ é chamada de *pertinência* em a. Além disso, as relações $\subseteq_a = \{(k, \ell) \in a \times a : k \subseteq \ell\}$ e $\subsetneq_a = \{(k, \ell) \in a \times a : k \subsetneq \ell\}$ são chamadas respectivamente de *inclusão* e de *inclusão própria* em a. Definimos ainda a relação $\underline{\in}_a = \{(k, \ell) \in a \times a : k \in \ell \vee k = \ell\}$.

Definição 2.4. Dada uma relação $r \subseteq a \times b$, a é chamado de *domínio* de r e b é chamado de *contradomínio* de r. Se a e b não forem explicitados, definimos o *domínio* de r como $\operatorname{Dom} r = \{k \in \bigcup\bigcup r : \exists u \; ((k, u) \in r)\}$ e o *contradomínio* de r como $\operatorname{Ran} r = \{k \in \bigcup\bigcup r : \exists u \; ((u, k) \in r)\}$.

Exemplo 2.3. Dado um conjunto a, temos $\operatorname{Dom} \mathrm{Id}_a = \operatorname{Ran} \mathrm{Id}_a = a$.

Exemplo 2.4. Dados dois conjuntos a e b, temos $\operatorname{Dom}(a \times b) = a$ e $\operatorname{Ran}(a \times b) = b$.

Definição 2.5. Dada uma relação r, definimos a *relação inversa* de r como $r^{-1} = \{(k, \ell) : (\ell, k) \in r\}$.

Definição 2.6. Dada uma relação $r \subseteq a \times b$ e um subconjunto $c \subseteq a$, definimos a *imagem* de r em c, ou *imagem* de c por r, como $r[c] = \{k \in b : \exists u \in c \; ((u, k) \in r)\}$. Dado um subconjunto $d \subseteq b$, o conjunto $r^{-1}[d] = \{k \in a : \exists u \in d \; ((k, u) \in r)\}$ é chamado de *imagem inversa* de d por r, ou de *pré-imagem* de d por r. Em particular, o conjunto $r[a]$ é chamado de *imagem* de r e escrevemos $r[a] = \operatorname{Im} r$.

Teorema 2.1. Dados uma relação $r \subseteq a \times b$ e dois subconjuntos $c, d \subseteq a$, temos:

(i) $r[c \cup d] = r[c] \cup r[d]$; (ii) $r[c \cap d] \subseteq r[c] \cap r[d]$; (iii) $r[c \smallsetminus d] \supseteq r[c] \smallsetminus r[d]$.

Demonstração. (i) Seja $x \in b$. Temos $x \in r[c \cup d]$ se e somente se existe $u \in c \cup d$ tal que $(u, x) \in r$, isto é, existe $v \in c$ tal que $(v, x) \in r$ ou existe $w \in d$ tal que $(w, x) \in r$, que é equivalente a $x \in r[c]$ ou $x \in r[d]$, isto é, $x \in r[c] \cup r[d]$. Portanto $r[c \cup d] = r[c] \cup r[d]$.
(ii) Seja $x \in r[c \cap d]$. Temos que existe $u \in c \cap d$ tal que $(u, x) \in r$, logo $x \in r[c]$ e $x \in r[d]$, isto é, $x \in r[c] \cap r[d]$. Portanto $r[c \cap d] \subseteq r[c] \cap r[d]$.
(iii) Seja $x \in r[c] \smallsetminus r[d]$. Temos que existe $u \in c$ tal que $(u, x) \in r$ e não existe $v \in d$ tal que $(v, x) \in r$, o que implica $u \notin d$, logo $u \in c \smallsetminus d$ e segue que $x \in r[c \smallsetminus d]$. Portanto $r[c \smallsetminus d] \supseteq r[c] \smallsetminus r[d]$. $\square$

Definição 2.7. Dadas duas relações $r \subseteq a \times b$ e $s \subseteq c \times d$, definimos a *composição* de r e s como $s \circ r = \{(k, \ell) \in a \times d : \exists u\ ((k, u) \in r \wedge (u, \ell) \in s)\}$.

Teorema 2.2. Para quaisquer relações r, s e t, as seguintes propriedades são válidas:

(i) $(r^{-1})^{-1} = r$;

(ii) $r \circ \mathrm{Id}_{\mathrm{Dom}\, r} = \mathrm{Id}_{\mathrm{Ran}\, r} \circ r = r$;

(iii) $t \circ (s \circ r) = (t \circ s) \circ r$;

(iv) $(s \circ r)^{-1} = r^{-1} \circ s^{-1}$.

Demonstração. (i) É imediato.
(ii) Sejam $a = \mathrm{Dom}\, r$ e $b = \mathrm{Ran}\, r$. Temos:

$$\begin{aligned}
r \circ \mathrm{Id}_a &= \{(k, \ell) \in a \times b : \exists u\ ((k, u) \in \mathrm{Id}_a \wedge (u, \ell) \in r)\} \\
&= \{(k, \ell) \in a \times b : \exists u\ (k = u \wedge (u, \ell) \in r)\} \\
&= \{(k, \ell) \in a \times b : (k, \ell) \in r)\} \\
&= \{(k, \ell) \in a \times b : \exists u\ ((k, u) \in r \wedge u = \ell)\} \\
&= \{(k, \ell) \in a \times b : \exists u\ ((k, u) \in r \wedge (u, \ell) \in \mathrm{Id}_b)\} \\
&= \mathrm{Id}_b \circ r
\end{aligned}$$

Além disso, $r = \{(k, \ell) \in a \times b : (k, \ell) \in r)\}$.
(iii) Sejam $a = \mathrm{Dom}\, r$ e $b = \mathrm{Ran}\, t$. Temos:

$$\begin{aligned}
t \circ (s \circ r) &= \{(k, \ell) \in a \times b : \exists u\ ((k, u) \in s \circ r \wedge (u, \ell) \in t)\} \\
&= \{(k, \ell) \in a \times b : \exists u\ (\exists v\ ((k, v) \in r \wedge (v, u) \in s) \wedge (u, \ell) \in t)\} \\
&= \{(k, \ell) \in a \times b : \exists v\ ((k, v) \in r \wedge \exists u\ ((v, u) \in s \wedge (u, \ell) \in t))\} \\
&= \{(k, \ell) \in a \times b : \exists v\ ((k, v) \in r \wedge (v, \ell) \in t \circ s))\} \\
&= (t \circ s) \circ r
\end{aligned}$$

(iv) Sejam $a = \mathrm{Dom}\, r$ e $b = \mathrm{Ran}\, s$. Temos:

$$\begin{aligned}
(s \circ r)^{-1} &= \{(k, \ell) \in b \times a : \exists u\ ((\ell, u) \in r \wedge (u, k) \in s)\} \\
&= \{(k, \ell) \in b \times a : \exists u\ ((k, u) \in s^{-1} \wedge (u, \ell) \in r^{-1})\} \\
&= r^{-1} \circ s^{-1}
\end{aligned}$$

$\square$

Definição 2.8. Dada uma relação r em a, dizemos que:

- r é *reflexiva* se $(x, x) \in r$ para todo $x \in a$;
- r é *simétrica* se $(x, y) \in r$ implica $(y, x) \in r$ para todos $x, y \in a$;
- r é *antissimétrica* se $(x, y) \in r$ e $(y, x) \in r$ implica $x = y$ para todos $x, y \in a$;
- r é *transitiva* se $(x, y) \in r$ e $(y, z) \in r$ implica $(x, z) \in r$ para todos $x, y, z \in a$.

Definição 2.9. Dada uma relação r, se r for reflexiva, simétrica e transitiva, dizemos que r é uma *relação de equivalência*.

Definição 2.10. Dada uma relação r, se r for reflexiva, antissimétrica e transitiva, dizemos que r é uma *relação de ordem*.

Exemplo 2.5. Dado um conjunto a, a identidade Id_a é uma relação de equivalência em a e uma relação de ordem em a.

Exemplo 2.6. Dado um conjunto a, o produto cartesiano $a \times a$ é uma relação de equivalência em a.

Exemplo 2.7. Dado um conjunto a, a inclusão $\subseteq_a$ é uma relação de ordem em a.

Teorema 2.3. Para quaisquer conjunto a e relação r em a, as seguintes equivalências são válidas:

(i) r é reflexiva se e somente se $\mathrm{Id}_a \subseteq r$;

(ii) r é simétrica se e somente se $r^{-1} \subseteq r$;

(iii) r é antissimétrica se e somente se $r \cap r^{-1} \subseteq \mathrm{Id}_a$;

(iv) r é transitiva se e somente se $r \circ r \subseteq r$.

Demonstração. É imediato das definições. □

2.2 FUNÇÕES

Definição 2.11. Dada uma relação $f \subseteq a \times b$, se para cada $x \in a$ existe um único $y \in b$ tal que $(x, y) \in f$, dizemos que f é uma *função* de a em b, e denotamos por $f : a \to b$. Quando $(x, y) \in f$, é usual escrevermos $f(x) = y$ ou $x \overset{f}{\longmapsto} y$.

Exemplo 2.8. A identidade Id_a é uma função de a em a.

Exemplo 2.9. Dados dois conjuntos a e b, a relação $a \times \{b\}$ é uma função, chamada de *função constante* b.

Exemplo 2.10. Dados dois conjuntos a e b com $b \subseteq a$, a relação χ_b dada por $(b \times \{\{\varnothing\}\}) \uplus ((a \setminus b) \times \{\varnothing\})$ é uma função, chamada de *função característica* de b.

A função característica é uma função $\chi_b : a \to \{\varnothing, \{\varnothing\}\}$ tal que $\chi_b(x) = \{\varnothing\}$ se $x \in b$ e $\chi_b(x) = \varnothing$ se $x \in a \setminus b$. É comum descrevermos funções assim.

Definição 2.12. Dada uma relação r, definimos a *projeção* de r na *primeira coordenada* como $\pi_1 = \{((k, \ell), k) : (k, \ell) \in r\}$. Analogamente, definimos a *projeção* de r na *segunda coordenada* como $\pi_2 = \{((k, \ell), \ell) : (k, \ell) \in r\}$. As projeções são funções $\pi_1 : r \to \operatorname{Dom} r$ e $\pi_2 : r \to \operatorname{Ran} r$.

Definição 2.13. Dados uma função $f : a \to b$ e um subconjunto $c \subseteq a$, definimos a *restrição* de f a c, ou a função f *restrita* a c, como $f \restriction c = f \cap (c \times b)$. Se existir uma função g tal que $f = g \restriction a$, dizemos que g é uma *extensão* de f, ou que g *estende* f.

Teorema 2.4. Dada uma família de funções $\{f_k : k \in \lambda\}$, se para quaisquer $u, v \in \lambda$ existir uma função $g_{u,v}$ que estende ambas f_u e f_v, então $f = \bigcup_{k \in \lambda} f_k$ é uma função. Além disso, $\operatorname{Dom} f = \bigcup_{k \in \lambda} \operatorname{Dom} f_k$.

Demonstração. Como $f \subseteq \bigcup_{k \in \lambda}(\operatorname{Dom} f_k \times \operatorname{Ran} f_k)$, temos $\operatorname{Dom} f \subseteq \bigcup_{k \in \lambda} \operatorname{Dom} f_k$. Seja $x \in \bigcup_{k \in \lambda} \operatorname{Dom} f_k$. Sejam $u, v \in \lambda$ tais que $x \in \operatorname{Dom} f_u \cap \operatorname{Dom} f_v$ quaisquer. Temos $f_u(x) = g_{u,v}(x) = f_v(x)$, logo existe um único y tal que $(x, y) \in f$. Portanto f é uma função e $\operatorname{Dom} f = \bigcup_{k \in \lambda} \operatorname{Dom} f_k$. □

Definição 2.14. Dado uma família a de conjuntos não-vazios, uma função $f : a \to \bigcup a$ tal que $f(x) \in x$ para todo $x \in a$ é chamada de *função escolha* de a.

Teorema* 2.5. Dado uma família a de conjuntos não-vazios, existe uma função escolha $f : a \to \bigcup a$.

Demonstração. Pelo Axioma da Escolha, existe um conjunto c tal que para cada $x \in a$ existe um único $y \in x$ tal que $y \in c$. Como os elementos de c são elementos de elementos de a, segue que $c \subseteq \bigcup a$. Portanto, $f = \{(k, \ell) \in a \times c : \ell \in k\}$ é uma função escolha de a. □

Teorema 2.6. Dadas duas funções $f : a \to b$ e $g : b \to c$, temos que $g \circ f$ é uma função de a em c. Além disso, dado $x \in a$, temos $(g \circ f)(x) = g(f(x))$.

Demonstração. Seja $u \in a$. Como f é uma função, existe um único $v \in b$ tal que $(u, v) \in f$. Além disso, como g é uma função, existe um único $w \in c$ tal que $(v, w) \in g$. Logo, $(u, w) \in g \circ f$. Seja $w' \in c$ tal que $(u, w') \in g \circ f$. Existe $v' \in b$ tal que $(u, v') \in f$ e $(v', w') \in g$. De $(u, v') \in f$ concluímos que $v' = v$, e de $(v, w') \in g$ concluímos que $w' = w$. Portanto $g \circ f$ é uma função de a em c, e $(g \circ f)(u) = w = g(v) = g(f(u))$. □

Definição 2.15. Dada uma função $f : a \to b$, dizemos que f é *injetora* se para todos $u, v \in a$, $f(u) = f(v)$ implica $u = v$. Dizemos que f é *sobrejetora* se para todo $w \in b$ existe $x \in a$ tal que $f(x) = w$. Se f for injetora e sobrejetora, dizemos que f é *bijetora*, ou que f é uma *bijeção*, ou que f é uma *correspondência biunívoca*. Se f for bijetora e $a = b$, dizemos que f é uma *permutação*. É comum nos referirmos à *injetividade* de uma função injetora, à *sobrejetividade* de uma função sobrejetora e à *bijetividade* de uma função bijetora.

Note que, enquanto a injetividade de uma função f depende somente de f, a sobrejetividade (e consequentemente a bijetividade) também depende do contradomínio de f. Por exemplo, se $f = \{(\varnothing, \varnothing)\}$, então $f : \{\varnothing\} \to \{\varnothing\}$ é sobrejetora, entretanto $f : \{\varnothing\} \to \{\varnothing, \{\varnothing\}\}$ não é sobrejetora.

Teorema 2.7. Dadas duas funções $f : a \to b$ e $g : b \to c$, temos:

(i) Se f e g são injetoras, então $g \circ f$ é injetora;

(ii) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora;

(iii) Se f e g são bijetoras, então $g \circ f$ é bijetora.

Demonstração. (i) Sejam $x, y \in a$. Se $g(f(x)) = g(f(y))$, como g é injetora, temos $f(x) = f(y)$, e como f é injetora, segue que $x = y$. Portanto $g \circ f$ é injetora.
(ii) Seja $x \in c$. Como g é sobrejetora, existe $u \in b$ tal que $g(u) = x$, e como f é sobrejetora, existe $v \in a$ tal que $f(v) = u$, logo $x = g(u) = g(f(v))$. Portanto $g \circ f$ é sobrejetora.
(iii) É imediato dos itens (i) e (ii). □

Teorema 2.8. Dadas duas funções $f : a \to b$ e $g : b \to c$, temos:

(i) Se $g \circ f$ é injetora, então f é injetora;

(ii) Se $g \circ f$ é sobrejetora, então g é sobrejetora.

Demonstração. (i) Suponha que f não é injetora, isto é, existem $u, v \in a$ distintos tais que $f(u) = f(v)$, logo $g(f(u)) = g(f(v))$, e portanto $g \circ f$ não é injetora. O resultado segue da contrapositiva.
(ii) Suponha que g não é sobrejetora, isto é, existe $u \in c$ tal que $g(x) \neq u$ para todo $x \in b$. Ora, para todo $y \in a$, temos $f(y) \in b$, logo $g(f(y)) \neq u$, e portanto $g \circ f$ não é sobrejetora. O resultado segue da contrapositiva. □

Teorema 2.9. Dada uma função $f : a \to b$, temos que f é bijetora se e somente se $f^{-1} : b \to a$ é uma função.

Demonstração. ($\Rightarrow$) Como f é sobrejetora, para cada $u \in b$ existe um $v \in a$ tal que $(v, u) \in f$, isto é, tal que $(u, v) \in f^{-1}$. Além disso, como f é injetora, dado $w \in a$ tal que

$(w, u) \in f$, temos $v = w$, em outras palavras, o v é único, e portanto $f^{-1} : b \to a$ é uma função.
($\Leftarrow$) Como $f^{-1} : b \to a$ é uma função, para cada $x \in b$ existe um único $y \in a$ tal que $(x, y) \in f^{-1}$, isto é, tal que $(y, x) \in f$. O resultado segue. □

Corolário 2.9.1. Dada uma função bijetora $f : a \to b$, temos que $f^{-1} : b \to a$ é bijetora.

Demonstração. Como f^{-1} é uma função tal que $(f^{-1})^{-1} = f$ também é uma função, segue que f^{-1} é bijetora. □

Teorema 2.10. Dada uma função bijetora $f : a \to b$, temos $f^{-1} \circ f = \mathrm{Id}_a$ e $f \circ f^{-1} = \mathrm{Id}_b$.

Demonstração. Como dado $(x, y) \in f$ qualquer temos $(y, x) \in f^{-1}$, segue que $f^{-1}(f(x)) = f^{-1}(y) = x$ para todo $x \in a$ e $f(f^{-1}(y)) = f(x) = y$ para todo $y \in b$, logo $f^{-1} \circ f = \mathrm{Id}_a$ e $f \circ f^{-1} = \mathrm{Id}_b$. □

Definição 2.16. Dadas duas funções $f : a \to b$ e $g : b \to a$, se $g \circ f = \mathrm{Id}_a$, dizemos que g é uma *inversa à esquerda* de f, ou que f é uma *inversa à direita* de g.

Teorema★ 2.11. Dada uma função $f : a \to b$, temos:

(i) f é injetora se e somente se existe $g : b \to a$ tal que $g \circ f = \mathrm{Id}_a$;

(ii) f é sobrejetora se e somente se existe $g : b \to a$ tal que $f \circ g = \mathrm{Id}_b$.

Demonstração. (i) ($\Rightarrow$) Se $a = \varnothing$, então $f = \varnothing$, logo f é injetora. Se $a \neq \varnothing$, fixe um $t \in a$. Considere a função $u : b \to a$ dada por:

$$u(x) = \begin{cases} y & \text{se } x \in \operatorname{Im} f \text{ e } f(y) = x \\ t & \text{caso contrário} \end{cases}$$

A função u assim definida é tal que $u \circ f = \mathrm{Id}_a$.
($\Leftarrow$) Como Id_a é bijetora, decorre do Teorema 2.8 que f é injetora.
(ii) ($\Rightarrow$) Como f é sobrejetora, para cada $x \in b$, temos $f^{-1}[\{x\}] \neq \varnothing$. Deste modo, existe uma função escolha $c : \{f^{-1}[\{k\}] : k \in b\} \to a$. Assim, considere a função $v : b \to a$ dada por $v(x) = c(f^{-1}[\{x\}])$. A função v assim definida é tal que $f \circ v = \mathrm{Id}_b$.
($\Leftarrow$) Como Id_b é bijetora, decorre do Teorema 2.8 que f é sobrejetora. □

Corolário★ 2.11.1. Dados dois conjuntos não-vazios a e b, existe uma função injetora $f : a \to b$ se e somente se existe uma função sobrejetora $g : b \to a$.

Demonstração. ($\Rightarrow$) Pelo item (i) do Teorema 2.11, existe $g : b \to a$ tal que $g \circ f = \mathrm{Id}_a$, e pelo Teorema 2.8 temos que g é sobrejetora.
($\Leftarrow$) Pelo item (ii) do Teorema 2.11, existe $f : a \to b$ tal que $g \circ f = \mathrm{Id}_a$, e pelo Teorema 2.8 temos que f é injetora. □

Teorema 2.12. Dados uma função $f : a \to b$ e dois subconjuntos $c, d \subseteq b$, temos:

(i) $f^{-1}[c \cap d] = f^{-1}[c] \cap f^{-1}[d]$; (ii) $f^{-1}[c \smallsetminus d] = f^{-1}[c] \smallsetminus f^{-1}[d]$.

Além disso, se f é injetora, então dados dois subconjuntos $c', d' \subseteq a$, temos:

(iii) $f[c' \cap d'] = f[c'] \cap f[d']$; (iv) $f[c' \smallsetminus d'] = f[c'] \smallsetminus f[d']$.

Demonstração. (i) Seja $x \in f^{-1}[c] \cap f^{-1}[d]$. Temos que existem $u \in c$ e $v \in d$ tais que $(u, x), (v, x) \in f^{-1}$, isto é, tais que $f(x) = u$ e $f(x) = v$, logo $u = v \in c \cap d$ e $x \in f^{-1}[c \cap d]$. Portanto $f^{-1}[c \cap d] \supseteq f^{-1}[c] \cap f^{-1}[d]$. Segue do Teorema 2.1 que $f^{-1}[c \cap d] = f^{-1}[c] \cap f^{-1}[d]$.
(ii) Seja $x \in f^{-1}[c \smallsetminus d]$. Temos que existe $u \in c \smallsetminus d$ tal que $(u, x) \in f^{-1}$, isto é, tal que $f(x) = u$. Como $u \in c$ e $u \notin d$, segue que $x \in f^{-1}[c]$ e $x \notin f^{-1}[d]$, isto é, $x \in f^{-1}[c] \smallsetminus f^{-1}[d]$. Portanto $f^{-1}[c \smallsetminus d] \subseteq f^{-1}[c] \smallsetminus f^{-1}[d]$. Segue do Teorema 2.1 que $f^{-1}[c \smallsetminus d] = f^{-1}[c] \smallsetminus f^{-1}[d]$.
(iii) e (iv) Se f é injetora, então $f : a \to \operatorname{Im} f$ é bijetora, e $f^{-1} : \operatorname{Im} f \to a$ é uma função. Os resultados seguem dos itens (i) e (ii). □

Definição 2.17. Dados dois conjuntos a e b, definimos o *conjunto das funções* de a em b como $\mathcal{F}(a, b) = \{f \in \mathcal{P}(a \times b) : f \text{ é uma função de } a \text{ em } b\}$. Por vezes o conjunto $\mathcal{F}(a, b)$ também é denotado por b^a.

Definição 2.18. Dada uma família $a = \{a_k : k \in \lambda\}$, definimos o *produtório* de a como:

$$\prod_{k \in \lambda} a_k = \left\{ f \in \mathcal{F}\left(\lambda, \textstyle\bigcup_{k \in \lambda} a_k\right) : \forall \ell \in \lambda \ (f(\ell) \in a_\ell) \right\}$$

Teorema* 2.13. Dada uma família não-vazia $a = \{a_k : k \in \lambda\}$, temos $\prod_{k \in \lambda} a_k = \varnothing$ se e somente se $a_k = \varnothing$ para algum $k \in \lambda$.

Demonstração. ($\Rightarrow$) Suponha que $a_k \neq \varnothing$ para todo $k \in \lambda$. Existe uma função escolha $c : a \to \bigcup_{k \in \lambda} a_k$. Seja $f : \lambda \to \bigcup_{k \in \lambda} a_k$ dada por $f(x) = c(a_x)$. Como $f(x) = c(a_x) \in a_x$ para todo $x \in \lambda$, segue que $f \in \prod_{k \in \lambda} a_k$, logo $\prod_{k \in \lambda} a_k \neq \varnothing$. O resultado segue da contrapositiva.
($\Leftarrow$) Suponha que $\prod_{k \in \lambda} a_k \neq \varnothing$ e tome $g \in \prod_{k \in \lambda} a_k$. Como $g(x) \in a_x$ para todo $x \in \lambda$, segue $a_x \neq \varnothing$ para todo $x \in \lambda$. O resultado segue da contrapositiva. □

2.3 PARTIÇÕES

Definição 2.19. Dado um conjunto $p \subseteq \mathcal{P}(a)$, dizemos que p é uma *partição* de a se $\varnothing \notin p$, os elementos de p são dois a dois disjuntos e $\dot\bigcup p = a$.

Exemplo 2.11. Dado um conjunto a, o conjunto $\{a\}$ é uma partição de a.

Exemplo 2.12. Dado um conjunto a, o conjunto $\{\{k\} : k \in a\}$ é uma partição de a.

Teorema 2.14. Dada uma partição p de a, a relação $r = \{(k, \ell) \in a \times a : \exists u \in p\ (k \in u \wedge \ell \in u)\}$ é uma relação de equivalência em a.

Demonstração. É imediato de $\bigcup p = a$ e da idempotência de $\wedge$ que r é reflexiva, e imediato da comutatividade de $\wedge$ que r é simétrica.
Dados $x, y, z \in a$ tais que $(x, y) \in r$ e $(y, z) \in r$, existem $u, v \in p$ tais que $x, y \in u$ e $y, z \in v$, logo $y \in u \cap v$. Mas como os elementos de p são dois a dois disjuntos, segue que $u = v$, e portanto $(x, z) \in r$, isto é, r é transitiva. Portanto r é uma relação de equivalência em a. $\square$

Definição 2.20. Dada uma relação de equivalência r em a, para cada $u \in a$ definimos a *classe de equivalência* de u em r como $[u]_r = \{k \in a : (k, u) \in r\}$, e dizemos que u é um *representante* da classe $[u]_r$.

Teorema 2.15. Dada uma relação de equivalência r em a, o conjunto $p = \{[k]_r : k \in a\}$ é uma partição de a.

Demonstração. Dado $x \in p$, existe $u \in a$ tal que $x = [u]_r$, logo $u \in x$, e segue que x é não-vazio. Portanto $\varnothing \notin p$. Dados $y, z \in p$, existem $v, w \in a$ tais que $y = [v]_r$ e $z = [w]_r$. Se $y \cap z \neq \varnothing$, então existe $t \in a$ tal que $(t, v) \in r$ e $(t, w) \in r$. Logo, como r é de equivalência, temos $(v, w) \in r$, isto é, $y = [v]_r = [w]_r = z$. Como dado $s \in a$ temos $s \in [s]_r \in p$, segue que $\bigcup p \supseteq a$, e como os elementos de p são subconjuntos de a, segue que $\bigcup p \subseteq a$, o que implica $\bigcup p = a$. Portanto p é uma partição de a. $\square$

Definição 2.21. Dados um conjunto a e uma relação de equivalência r em a, definimos o *quociente* de a por r como a partição das classes de equivalência em r, e denotamos por $a \,/\, r$.

Teorema* 2.16. Dada uma partição p de a, existe uma função $f : p \to a$ tal que $f(x) \in x$ para todo $x \in p$.

Demonstração. Como p é uma família de conjuntos não-vazios, existe uma função escolha $f : p \to \bigcup p$. $\square$

3 NÚMEROS NATURAIS

Assumimos que o leitor já tem certa familiaridade com o conjunto dos números naturais, não sendo este o primeiro contato com o conjunto. Não definiremos *subtração*, *divisão*, *números primos*, dentre outros conceitos que podem aparecer nos exemplos posteriores.

3.1 CONJUNTO DOS NÚMEROS NATURAIS

Definição 3.1. Seja $\mathcal{I}$ um conjunto indutivo. Definimos o *conjunto dos números naturais* como:

$$\omega = \{k \in \mathcal{I} : \forall x \ (x \text{ é indutivo } \rightarrow \ k \in x)\}$$

Os elementos de ω são chamados de *números naturais*. Outra notação usual para o conjunto dos números naturais é $\mathbb{N}$.

Teorema 3.1. O conjunto ω é indutivo.

Demonstração. É imediato que $\varnothing \in \omega$. Seja $u \in \omega$. Para cada conjunto x, temos que se x é indutivo então $u \in x$, o que implica $\mathcal{S}(u) \in x$, inclusive para o caso particular $x = \mathcal{I}$, logo $\mathcal{S}(u) \in \omega$. Portanto ω é indutivo. □

Teorema 3.2. Dados dois conjuntos a e b, temos que se $\mathcal{S}(a) \subseteq \mathcal{S}(b)$, então $a \subseteq b$.

Demonstração. Se $a = b$, então $a \subseteq b$. Suponha que $a \neq b$. Seja $u \in a$. Como $a \subseteq \mathcal{S}(a) \subseteq \mathcal{S}(b)$, temos $u = b$ ou $u \in b$. Se $u = b$, então $b \in a$, e como $a \in \mathcal{S}(a) \subseteq \mathcal{S}(b)$ e $a \neq b$, segue que $a \in b$. Logo, como $a \in b$ e $b \in a$ é um absurdo, devemos ter $u \in b$, e portanto $a \subseteq b$. □

Corolário 3.2.1. Dados dois conjuntos a e b, temos que se $\mathcal{S}(a) = \mathcal{S}(b)$, então $a = b$.

Demonstração. Como $\mathcal{S}(a) \subseteq \mathcal{S}(b)$, temos $a \subseteq b$. Além disso, como $\mathcal{S}(a) \supseteq \mathcal{S}(b)$, temos $a \supseteq b$. Portanto $a = b$. □

Corolário 3.2.2. A relação $\mathcal{S}_\omega = \{(k, \mathcal{S}(k)) : k \in \omega\}$ é uma função injetora de ω em ω.

Demonstração. O fato de $\mathcal{S}_\omega : \omega \rightarrow \omega$ ser uma função decorre de ω ser indutivo. A injetividade de $\mathcal{S}_\omega$ é imediata do corolário anterior. □

Definição 3.2. Denotamos os números naturais por

- $0 = \varnothing$,

- $1 = \mathcal{S}(0) = \{0\} = \{\varnothing\}$,
- $2 = \mathcal{S}(1) = \{0, 1\} = \{\varnothing, \{\varnothing\}\}$,
- $3 = \mathcal{S}(2) = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$,
- $4 = \mathcal{S}(3) = \{0, 1, 2, 3\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}$,

e assim sucessivamente.

Definição 3.3. Dados um número natural n e uma família $\{a_k : k \in n\}$ indexada por n, dizemos que um subconjunto $r \subseteq \prod_{k \in n} a_k$ é uma *relação n-ária*, ou que r é uma *relação de n argumentos*. Dada uma função f, se $\operatorname{Dom} f$ é uma relação n-ária, dizemos que f é uma *função n-ária*, ou que f é uma *função de n argumentos*, ou que f é uma *função de n variáveis*. Em ambos os casos, n é chamado de *aridade*.

Note que, a rigor, uma relação binária e uma relação 2-ária são coisas distintas, mas não faremos distinção nos tratamentos desses dois casos.

3.2 INDUÇÃO E RECURSÃO FINITAS

Teorema 3.3 (Indução Finita)**.** Se uma propriedade $\varphi(x, p)$ (com parâmetro p) é tal que

(i) $\varphi(0, p)$ é verificada e

(ii) para cada número natural n, temos que $\varphi(n, p)$ implica $\varphi(\mathcal{S}(n), p)$,

então $\varphi(x, p)$ é satisfeita por todos os números naturais.

Demonstração. Seja φ uma fórmula que satisfaça (i) e (ii). Seja $s = \{k \in \omega : \varphi(k, p)\}$. Por (i), temos que $\varnothing \in s$. Por (ii), temos que $n \in s$ implica $\mathcal{S}(n) \in s$. Logo, s é indutivo, e portanto $\omega \subseteq s$, e como $s \subseteq \omega$, segue que $s = \omega$, isto é, $\varphi(x, p)$ é satisfeita para todo $x \in \omega$. □

Teorema 3.4. O único número natural que não pertence à imagem de $\mathcal{S}_\omega$ é o 0.

Demonstração. Claro que $\varnothing \notin \operatorname{Im} \mathcal{S}_\omega$, uma vez que $x \in \mathcal{S}(x)$ para todo x. Seja $\varphi(x)$ a fórmula "$x = \varnothing \lor x \in \operatorname{Im} \mathcal{S}_\omega$". Claramente $\varphi(\varnothing)$ é satisfeita e $\varphi(\mathcal{S}(n))$ é satisfeita para todo $n \in \omega$. O resultado segue por indução finita. □

Teorema 3.5. Dados dois números naturais m e n, temos $m \subseteq n$ ou $m \supseteq n$.

Demonstração. Seja $\varphi(x)$ a fórmula "$\forall m \in \omega\ (m \subseteq x \lor m \supseteq x)$". É claro que $m \supseteq \varnothing$ para todo $m \in \omega$, logo $\varphi(\varnothing)$ é satisfeita. Suponha que $\varphi(n)$ é satisfeita. Se $m = \varnothing$, claro que $m \subseteq \mathcal{S}(n)$ ou $m \supseteq \mathcal{S}(n)$. Se $m \neq \varnothing$, existe $\ell \in \omega$ tal que $\mathcal{S}(\ell) = m$, logo $\ell \subseteq n$ ou $\ell \supseteq n$, e portanto $\mathcal{S}(\ell) \subseteq \mathcal{S}(n)$ ou $\mathcal{S}(\ell) \supseteq \mathcal{S}(n)$, isto é, $m \subseteq \mathcal{S}(n)$ ou $m \supseteq \mathcal{S}(n)$. Portanto $\varphi(\mathcal{S}(n))$ é satisfeita. O resultado segue por indução finita. □

Teorema 3.6 (Recursão Finita)**.** Dados um conjunto a, um elemento $t \in a$ e uma função $g : a \times \omega \to a$, existe uma única função $f : \omega \to a$ tal que

(i) $f(0) = t$ e

(ii) $f(\mathcal{S}(n)) = g((f(n), n))$ para todo $n \in \omega$.

Demonstração. Para cada $n \in \omega$, considere as funções $f_n : \mathcal{S}(n) \to a$ definidas como $f_0 = \{(0, t)\}$ e, como $\mathcal{S}(n) \notin \operatorname{Dom} f_n$, existe a função $f_{\mathcal{S}(n)} = \{(\mathcal{S}(n), g((f_n(n), n)))\} \cup f_n$. Por indução, segue que f_n está definido para todo $n \in \omega$. Como dados $u, v \in \omega$, temos $u \subseteq v$ ou $u \supseteq v$, segue que $f_{u \cup v}$ estende f_u e f_v. Logo, pelo Teorema 2.4, temos que $f = \bigcup_{n \in \omega} f_n$ é uma função e $\operatorname{Dom} f = \bigcup_{n \in \omega} \mathcal{S}(n) = \omega$. $\square$

3.3 ARITMÉTICA NATURAL

Definição 3.4. Definimos a *adição* de números naturais via recursão finita, para cada $m \in \omega$:

$$\begin{cases} m + 0 = m \\ m + \mathcal{S}(n) = \mathcal{S}(m + n) & \text{para cada } n \in \omega \end{cases}$$

Definição 3.5. Definimos a *multiplicação* de números naturais via recursão finita, para cada $m \in \omega$:

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot \mathcal{S}(n) = m \cdot n + m & \text{para cada } n \in \omega \end{cases}$$

Definição 3.6. Definimos a *exponenciação* de números naturais via recursão finita, para cada $m \in \omega$:

$$\begin{cases} m^0 = 1 \\ m^{\mathcal{S}(n)} = m^n \cdot m & \text{para cada } n \in \omega \end{cases}$$

Na ausência de parênteses, a multiplicação tem prioridade sobre a adição, a exponenciação tem prioridade sobre a adição e a multiplicação.

Teorema 3.7. Para quaisquer números naturais a, b e c, as seguintes propriedades são válidas:

(i) $(a + b) + c = a + (b + c)$;

(ii) $a + b = b + a$;

(iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

(iv) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(v) $a \cdot b = b \cdot a$;

(vi) $a^{b+c} = a^b \cdot a^c$;

(vii) $(a \cdot b)^c = a^c \cdot b^c$;

(viii) $(a^b)^c = a^{b \cdot c}$.

Demonstração. Por indução finita.

(i) $(a+b)+0 = a+b = a+(b+0)$

$(a+b)+\mathcal{S}(n) = \mathcal{S}((a+b)+n) = \mathcal{S}(a+(b+n)) = a+\mathcal{S}(b+n) = a+(b+\mathcal{S}(n))$

(ii) $0+0 = 0+0$

$\mathcal{S}(m)+0 = \mathcal{S}(m) = \mathcal{S}(m+0) = \mathcal{S}(0+m) = 0+\mathcal{S}(m)$

$0+\mathcal{S}(n) = \mathcal{S}(n)+0$

$\mathcal{S}(m) + \mathcal{S}(n) = \mathcal{S}(\mathcal{S}(m)+n) = \mathcal{S}(n+\mathcal{S}(m)) = \mathcal{S}(\mathcal{S}(n+m)) = \mathcal{S}(\mathcal{S}(m+n)) =$
$= \mathcal{S}(m+\mathcal{S}(n)) = \mathcal{S}(\mathcal{S}(n)+m) = \mathcal{S}(n)+\mathcal{S}(m)$

(iii) $a\cdot(b+0) = a\cdot b = a\cdot b+0 = a\cdot b + a\cdot 0$

$a\cdot(b+\mathcal{S}(n)) = a\cdot\mathcal{S}(b+n) = a\cdot(b+n)+a = (a\cdot b+a\cdot n)+a = a\cdot b+(a\cdot n+a) =$
$= a\cdot b + a\cdot\mathcal{S}(n)$

(iv) $(a\cdot b)\cdot 0 = 0 = a\cdot 0 = a\cdot(b\cdot 0)$

$(a\cdot b)\cdot\mathcal{S}(n) = (a\cdot b)\cdot n + a\cdot b = a\cdot(b\cdot n)+a\cdot b = a\cdot(b\cdot n+b) = a\cdot(b\cdot\mathcal{S}(n))$

(v) $0\cdot 0 = 0\cdot 0$

$\mathcal{S}(m)\cdot 0 = 0 = m\cdot 0 = 0\cdot m = 0\cdot m+0 = 0\cdot\mathcal{S}(m)$

$0\cdot\mathcal{S}(n) = \mathcal{S}(n)\cdot 0$

$\mathcal{S}(m)\cdot\mathcal{S}(n) = \mathcal{S}(m)\cdot n+\mathcal{S}(m) = n\cdot\mathcal{S}(m)+\mathcal{S}(m) = (n\cdot m+n)+\mathcal{S}(m) =$
$= \mathcal{S}((n\cdot m+n)+m) = \mathcal{S}(n\cdot m+(n+m)) = \mathcal{S}(n\cdot m+(m+n)) = \mathcal{S}(m\cdot n+(m+n)) =$
$= m\cdot n+\mathcal{S}(m+n) = m\cdot n+(m+\mathcal{S}(n)) = (m\cdot n+m)+\mathcal{S}(n) = m\cdot\mathcal{S}(n)+\mathcal{S}(n) =$
$= \mathcal{S}(n)\cdot m+\mathcal{S}(n) = \mathcal{S}(n)\cdot\mathcal{S}(m)$

(vi) $a^{b+0} = a^b = a^b+0 = 0+a^b = a^b\cdot 0+a^b = a^b\cdot\mathcal{S}(0) = a^b\cdot 1 = a^b\cdot a^0$

$a^{b+\mathcal{S}(n)} = a^{\mathcal{S}(b+n)} = a^{b+n}\cdot a = (a^b\cdot a^n)\cdot a = a^b\cdot(a^n\cdot a) = a^b\cdot a^{\mathcal{S}(n)}$

(vii) $(a\cdot b)^0 = 1 = 1+0 = 0+1 = 1\cdot 0+1 = 1\cdot\mathcal{S}(0) = 1\cdot 1 = a^0\cdot b^0$

$(a\cdot b)^{\mathcal{S}(n)} = (a\cdot b)^n\cdot(a\cdot b) = (a^n\cdot b^n)\cdot(a\cdot b) = a^n\cdot(b^n\cdot(a\cdot b)) = a^n\cdot((a\cdot b)\cdot b^n) =$
$= a^n\cdot(a\cdot(b\cdot b^n)) = (a^n\cdot a)\cdot(b\cdot b^n) = (a^n\cdot a)\cdot(b^n\cdot b) = a^{\mathcal{S}(n)}\cdot b^{\mathcal{S}(n)}$

(viii) $(a^b)^0 = 1 = a^0 = a^{b\cdot 0}$

$(a^b)^{\mathcal{S}(n)} = (a^b)^n\cdot a^b = a^{b\cdot n}\cdot a^b = a^{b\cdot n+b} = a^{b\cdot\mathcal{S}(n)}$ □

Teorema 3.8. Para quaisquer números naturais a e b, temos que $a\cdot b = 0$ se e somente se $a = 0$ ou $b = 0$.

Demonstração. ($\Rightarrow$) Se $a \neq 0$ e $b \neq 0$, então existem $u, v \in \omega$ tais que $a = \mathcal{S}(u)$ e $b = \mathcal{S}(v)$, logo $a\cdot b = \mathcal{S}(u)\cdot\mathcal{S}(v) = \mathcal{S}(u)\cdot v+\mathcal{S}(u) = \mathcal{S}(\mathcal{S}(u)\cdot v+u) \neq 0$. O resultado segue da contrapositiva.

($\Leftarrow$) Imediato do item (v) do Teorema 3.7. □

3.4 AXIOMAS DE PEANO

A Aritmética de Peano, abreviada como PA (*Peano Arithmetic*), é uma teoria que descreve o conjunto dos números naturais. Há mais de uma maneira de formular a

Aritmética de Peano. A que apresentamos utiliza lógica de primeira ordem e possui um número infinito de axiomas, pois a Fórmula (3.3) trata-se de um esquema.

Aritmética de Peano. A teoria é formada por apenas um tipo de objeto, que são chamados *números*. A linguagem é composta por dois símbolos: s e θ. O s é um símbolo de função 1-ário chamado *sucessor*, e o θ é um símbolo de constante chamado *zero*. Os axiomas da teoria são os seguintes:

1. A constante θ não pertence à imagem de s. Na linguagem da teoria:

$$\neg\exists x\ (s(x) = \theta) \tag{3.1}$$

2. A função s é injetora. Na linguagem da teoria:

$$\forall x\ \forall y\ (s(x) = s(y)\ \rightarrow\ x = y) \tag{3.2}$$

3. Se uma propriedade φ é satisfeita por θ e sempre que φ é satisfeita por um número n também é satisfeita por $s(n)$, então a propriedade φ é satisfeita por todos os números. Na linguagem da teoria:

$$\forall p\ ((\varphi(\theta, p)\ \wedge\ \forall x\ (\varphi(x, p)\ \rightarrow\ \varphi(s(x), p)))\ \rightarrow\ \forall x\ \varphi(x, p)) \tag{3.3}$$

A partir de ω obtemos uma estrutura $\mathfrak{N} = (\omega, s^{\mathfrak{N}}, \theta^{\mathfrak{N}})$ em que $s^{\mathfrak{N}} = \{(k, \mathcal{S}(k)) : k \in \omega\}$ e $\theta^{\mathfrak{N}} = \varnothing$, tal que $\mathfrak{N}$ satisfaz a Aritmética de Peano. Dizemos que essa estrutura é um *modelo* para a teoria. Estudaremos modelos de maneira mais detalhada no Capítulo 9.

4 CLASSES

Neste trabalho não nos aprofundaremos em Teoria das Classes, abordando somente o básico. Uma axiomatização da Teoria das Classes pode ser vista em (JECH, 2002, p. 70).

4.1 CLASSES E CONJUNTOS

Definição 4.1. Para cada fórmula $\varphi(x,p)$, definimos a *classe* C dos conjuntos x que satisfazem $\varphi(x,p)$, isto é, $x \in C$ é uma abreviação da fórmula $\varphi(x,p)$, e escrevemos $C = \{x : \varphi(x,p)\}$. Se $x \in C$, dizemos que x *pertence* a C, ou que x é um *elemento* de C. Também escrevemos $x \notin C$ como uma abreviação da fórmula $\neg\varphi(x,p)$. É usual denotar classes com letras maiúsculas.

Definição 4.2. De forma análoga a conjuntos, dadas duas classes $A = \{x : \varphi(x,p)\}$ e $B = \{x : \psi(x,p)\}$, dizemos que A e B são *iguais*, e escrevemos $A = B$, se e somente se $\varphi(x,p) \leftrightarrow \psi(x,p)$ para todo conjunto x. Caso contrário, dizemos que A e B são *diferentes* e escrevemos $A \neq B$. Dizemos que A está *contida* em B, ou que B *contém* A, ou que A está *inclusa* em B, ou que A é uma *subclasse* de B, e escrevemos $A \subseteq B$, se e somente se $\varphi(x,p) \rightarrow \psi(x,p)$ para todo conjunto x. Caso contrário, escrevemos $A \nsubseteq B$. Se $A \subseteq B$ e $A \neq B$, escrevemos $A \subsetneq B$.

Definição 4.3. Dadas duas classes $A = \{x : \varphi(x,p)\}$ e $B = \{x : \psi(x,p)\}$, definimos:

- $A \cup B = \{x : x \in A \lor x \in B\}$;
- $A \cap B = \{x : x \in A \land x \in B\}$;
- $A \setminus B = \{x : x \in A \land x \notin B\}$;
- $A \triangle B = \{x : x \in A \veebar x \in B\}$;
- $\complement_A = \{x : x \notin A\}$;
- $\bigcup A = \{x : \exists u\ (u \in A \land x \in u)\}$;
- $\bigcap A = \{x : \forall u\ (u \in A \rightarrow x \in u)\}$;
- $A \times B = \{x : \exists u\ \exists v\ (x = (u,v) \land u \in A \land v \in B)\}$.

Definição 4.4. Dado um conjunto a, identificamos a com a classe $A = \{x : x \in a\}$, e escrevemos $a \simeq A$. A classe identificada com o conjunto vazio é chamada *classe vazia.* Uma classe diferente da classe vazia é chamada *classe não-vazia.* Se uma classe A está identificada com um conjunto, dizemos que A *é* um conjunto, caso contrário dizemos que A é uma *classe própria.* Essa identificação entre conjuntos e classes, quando existe, é única.

Teorema 4.1. As noções de igualdade, inclusão, união, intersecção, diferença, diferença simétrica e produto cartesiano coincidem entre os conjuntos e as classes que os identificam, isto é, dados dois conjuntos a e b e duas classes A e B tais que $a \simeq A$ e $b \simeq B$, temos:

(i) $a = b$ se e somente se $A = B$;

(ii) $a \subseteq b$ se e somente se $A \subseteq B$;

(iii) $a \cup b \simeq A \cup B$;

(iv) $a \cap b \simeq A \cap B$;

(v) $a \smallsetminus b \simeq A \smallsetminus B$;

(vi) $a \triangle b \simeq A \triangle B$;

(vii) $\bigcup a \simeq \bigcup A$;

(viii) se $a \neq \varnothing$, então $\bigcap a \simeq \bigcap A$;

(ix) $a \times b \simeq A \times B$.

Demonstração. É imediato. □

Definição 4.5. Definimos a *classe universal* como a classe de todos os conjuntos, $\mathcal{V} = \{x : x = x\}$. O Teorema 1.2 nos diz que $\mathcal{V}$ é uma classe própria.

Teorema 4.2. Dadas duas classes A e B tais que $A \subseteq B$, se existe um conjunto b tal que $b \simeq B$ então existe um conjunto a tal que $a \simeq A$.

Demonstração. Seja $s = \{k \in b : k \in a\}$, temos $s \simeq A$. □

Teorema 4.3. Dada uma classe não-vazia A, existe um conjunto x tal que $x \simeq \bigcap A$.

Demonstração. Tome um $a \in A$. Seja $s = \{k \in a : k \in \bigcap A\}$, temos $s \simeq \bigcap A$. □

Exemplo 4.1. Temos $\omega \simeq \bigcap\{x : x \text{ é indutivo}\}$.

Utilizaremos o símbolo $^\blacklozenge$ para distinguir quando nos referimos a uma classe própria de quando nos referimos a um conjunto, já que conceitos como relações, funções e sequências aparecem em ambos os contextos.

Definição 4.6. Dada uma classe R, dizemos que R é uma *relação*$^\blacklozenge$ se todos os elementos de R são pares ordenados, e escrevemos $R = \{(x, y) : (x, y) \in R\}$. A classe $\{t : \exists w\ ((t, w) \in R)\}$ é chamada de *domínio* de R, e denotada por $\operatorname{Dom} R$.

Exemplo 4.2. As classes próprias $\mathrm{Id}_{\mathcal{V}} = \{(x, y) : x = y\}$, $\in_{\mathcal{V}} = \{(x, y) : x \in y\}$, $\subseteqq_{\mathcal{V}} = \{(x, y) : x \subseteqq y\}$, $\subseteq_{\mathcal{V}} = \{(x, y) : x \subseteq y\}$ e $\subsetneq_{\mathcal{V}} = \{(x, y) : x \subsetneq y\}$ são relações$^\blacklozenge$ com domínio $\mathcal{V}$.

Definição 4.7. Dada uma relação♦ F, dizemos que F é uma *função*♦ se para quaisquer x, y e z tais que $(x, y) \in F$ e $(x, z) \in F$ temos $y = z$. Se $(u, v) \in F$, escrevemos $v = F(u)$.

Exemplo 4.3. As classes próprias $\{(x, y) : y = \bigcup x\}$ e $\{(x, y) : y = \bigcap x\}$ são funções♦ com domínios $\mathcal{V}$ e $\{k : k \neq \varnothing\}$, respectivamente.

Exemplo 4.4. A classe própria $\mathcal{P} = \{(x, y) : y = \mathcal{P}(x)\}$ é uma função♦ com domínio $\mathcal{V}$.

Exemplo 4.5. A classe própria $\mathcal{S} = \{(x, y) : y = \mathcal{S}(x)\}$ é uma função♦ com domínio $\mathcal{V}$.

Definição 4.8. Dados uma classe A e uma função♦ F cujo domínio contém A, definimos a *restrição* de F a A como $F \restriction A = \{(x, y) : x \in A \wedge (x, y) \in F\}$.

Teorema 4.4. Dados uma classe A e uma função♦ F cujo domínio contém A, se existir um conjunto a tal que $a \simeq A$, então existe uma função f tal que $f \simeq F \restriction A$. Neste caso, escrevemos $f = F \restriction a$.

Demonstração. Seja $f = \{(k, F(k)) : k \in a\}$, temos $f \simeq F \restriction A$. $\square$

5 NÚMEROS ORDINAIS

5.1 RELAÇÕES DE ORDEM

Definição 5.1. Dados um conjunto a e uma relação de ordem $\leq$ em a, a estrutura $(a, \leq)$ é chamada de *conjunto ordenado*. É comum dizermos simplesmente que a é um conjunto ordenado quando está claro a que ordem nos referimos.

Definição 5.2. Dado um conjunto ordenado $(a, \leq)$, definimos a *ordem estrita* em a como segue: para cada $u, v \in a$, escrevemos $u < v$ se $u \leq v$ e $u \neq v$.

Exemplo 5.1. Dado um conjunto x, como a inclusão é uma ordem em x, a estrutura $(x, \subseteq_x)$ é um conjunto ordenado.

Exemplo 5.2. Dado um conjunto x, como a identidade é uma ordem em x, a estrutura (x, Id_x) é um conjunto ordenado.

Exemplo 5.3. Dados dois conjuntos x e y, seja $z = \bigcup_{k \in \mathcal{P}(x)} \mathcal{F}(k, y)$, a restrição é uma ordem em z, isto é, sendo $\restriction_z = \{(f, g) \in z \times z : f = g \restriction \mathrm{Dom}\, f\}$, a estrutura $(z, \restriction_z)$ é um conjunto ordenado.

Exemplo 5.4. Em ω, defina $\leq_+ = \{(m, n) \in \omega \times \omega : \exists k \in \omega\ (m + k = n)\}$ e $\leq_\bullet = \{(m, n) \in \omega \times \omega : \exists k \in \omega\ (m \cdot k = n)\}$. As relações $\leq_+$ e $\leq_\bullet$ são ordens em ω, sendo que $\leq_+$ é a ordem usual e $\leq_\bullet$ é a relação de divisibilidade.

Definição 5.3. Dados um conjunto ordenado $(a, \leq)$ e um subconjunto $s \subseteq a$, dizemos que $x \in s$ é o *mínimo* de s se para todo $u \in s$ temos $x \leq u$. Analogamente, dizemos que $y \in s$ é o *máximo* de s se para todo $u \in s$ temos $u \leq y$.

O mínimo e o máximo de s, caso existam, são únicos. De fato, se x e x' são mínimos de s, então $x \leq x'$ e $x' \leq x$, o que implica $x = x'$. A unicidade do máximo segue de forma análoga. O mínimo e o máximo de s são denotados respectivamente por $\min s$ e por $\max s$.

Definição 5.4. Dados um conjunto ordenado $(a, \leq)$ e um subconjunto $s \subseteq a$, dizemos que $x \in s$ é um *elemento minimal* de s se não existe $u \in s$ tal que $u < x$. Analogamente, dizemos que $y \in s$ é um *elemento maximal* de s se não existe $u \in s$ tal que $y < u$.

Dado um conjunto a, se $\underline{\in}_a$ é uma ordem em a então os elementos minimais coincidem com os elementos $\in$-minimais.

Exemplo 5.5. Em $(\mathcal{P}(x), \subseteq_{\mathcal{P}(x)})$, considere o subconjunto $\mathcal{P}(x) \smallsetminus \{\varnothing, x\} \subseteq \mathcal{P}(x)$. Os elementos minimais de $\mathcal{P}(x) \smallsetminus \{\varnothing, x\}$ são os subconjuntos unitários de x e os elementos maximais de $\mathcal{P}(x) \smallsetminus \{\varnothing, x\}$ são os subconjuntos $y \subseteq x$ tais que $x \smallsetminus y$ é unitário.

Exemplo 5.6. Em $(\omega, \leq_\bullet)$, considere o subconjunto $\omega \smallsetminus \{1\} \subseteq \omega$. Os elementos minimais de $\omega \smallsetminus \{1\}$ são os números primos.

Definição 5.5. Dados um conjunto ordenado $(a, \leq)$ e um subconjunto $s \subseteq a$, dizemos que $x \in a$ é um *limitante inferior* de s se para todo $u \in s$ temos $x \leq u$. Analogamente, dizemos que $y \in a$ é um *limitante superior* de s se para todo $u \in s$ temos $u \leq y$. Se existir um limitante inferior de s, dizemos que s é *limitado inferiormente*, e se existir um limitante superior de s, dizemos que s é *limitado superiormente*. Se s for limitado inferiormente e limitado superiormente, dizemos que s é *limitado*.

Definição 5.6. Dados um conjunto ordenado $(a, \leq)$ e um subconjunto $s \subseteq a$, dizemos que $x \in a$ é o *supremo* de s se $x = \min\{k \in a : k \text{ é limitante superior de } s\}$. Analogamente, dizemos que $y \in a$ é o *ínfimo* de s se $y = \max\{k \in a : k \text{ é limitante inferior de } s\}$.

O supremo e o ínfimo de s, caso existam, são únicos, uma vez que são definimos como o mínimo e o máximo de um conjunto. O supremo e o ínfimo de s são denotados respectivamente por $\sup s$ e por $\inf s$.

Exemplo 5.7. Em $(\mathcal{P}(x), \subseteq_{\mathcal{P}(x)})$, dado um subconjunto $s \subseteq \mathcal{P}(x)$ qualquer, temos:

$$\sup s = \bigcup s \qquad \qquad \inf s = \begin{cases} \bigcap s & \text{se } s \neq \varnothing \\ x & \text{se } s = \varnothing \end{cases}$$

Exemplo 5.8. Em $(\omega, \leq_\bullet)$, dados $a, b \in \omega \smallsetminus \{0\}$, temos $\sup\{a, b\} = \mathrm{mmc}(a, b)$ e $\inf\{a, b\} = \mathrm{mdc}(a, b)$. Além disso, temos $\sup \omega = 0$ e $\inf \omega = 1$.

Definição 5.7. Dado um conjunto ordenado $(a, \leq)$, dizemos que a é um *reticulado* se para quaisquer $u, v \in a$ existem o supremo e o ínfimo de $\{u, v\}$.

Definição 5.8. Dado um conjunto ordenado $(a, \leq)$, dizemos que um subconjunto $s \subseteq a$ é uma *cadeia* se para todos $u, v \in s$ é verificado $u \leq v$ ou $v \leq u$. Se $a \subseteq a$ for uma cadeia, dizemos que a é *totalmente ordenado* e que $\leq$ é uma ordem *total*, caso contrário dizemos que a é *parcialmente ordenado* e que $\leq$ é uma ordem *parcial*. Se $\{x, y\} \subseteq a$ é uma cadeia, dizemos que x e y são *comparáveis*.

Exemplo 5.9. Se x tem ao menos dois elementos, então o conjunto $(\mathcal{P}(x), \subseteq_{\mathcal{P}(x)})$ é parcialmente ordenado, pois dados $u, v \in x$ distintos, os conjuntos $\{u\}$ e $\{v\}$ não são comparáveis.

Exemplo 5.10. O conjunto $(\omega, \leq_+)$ é totalmente ordenado, ao passo que $(\omega, \leq_\bullet)$ é parcialmente ordenado (2 e 3 não são comparáveis). Os conjuntos da forma $\{n^k : k \in \omega\}$ com $n \in \omega$ são cadeias em $(\omega, \leq_\bullet)$.

Definição 5.9. Dado um conjunto ordenado $(a, \leq)$, dizemos que a é *bem ordenado* se todo subconjunto $s \subseteq a$ não-vazio tem mínimo. Nessas condições, dizemos ainda que $\leq$ é uma *boa ordem*.

Não é difícil ver que toda boa ordem é uma ordem total. De fato, dados $x, y \in a$, o conjunto $\{x, y\}$ tem mínimo. Os teoremas 5.1 e 5.2 a seguir são equivalentes ao Axioma da Escolha, e as demonstrações podem ser encontradas em (HRBACEK; JECH, 1999, p. 142-143).

Teorema* 5.1 (Lema de Zorn)**.** Dado um conjunto ordenado $(a, \leq)$, se toda cadeia de a tiver um limitante superior, então a tem um elemento maximal.

Teorema* 5.2 (Axioma de Zermelo)**.** Dado um conjunto a, existe uma ordem $\leq$ em a tal que $(a, \leq)$ é bem ordenado.

Definição 5.10. Dado um conjunto ordenado $(a, \leq)$, dizemos que a é uma *floresta* se para todo $u \in a$, todo subconjunto $s \subseteq \{k \in a : k \leq u\}$ não-vazio tem mínimo. Se a é uma floresta tal que a tem mínimo, então dizemos que a é uma *árvore*. Se a é uma floresta, dizemos que uma cadeia $c \subseteq a$ é um *ramo* de a se, em $(\mathcal{P}(a), \subseteq_{\mathcal{P}(a)})$, c é um elemento maximal de $\{k \in \mathcal{P}(a) : k \text{ é uma cadeia}\}$.

Definição 5.11. Dados dois conjuntos ordenados $(a, \leq)$ e $(b, \preceq)$ e uma função $f : a \to b$, dizemos que f é *crescente* se $x \leq y$ implica $f(x) \preceq f(y)$ para todos $x, y \in a$. Ainda, dizemos que f é *estritamente crescente* se $x < y$ implica $f(x) \prec f(y)$ para todos $x, y \in a$. Analogamente, dizemos que f é *decrescente* se $x \leq y$ implica $f(y) \preceq f(x)$ para todos $x, y \in a$ e *estritamente decrescente* se $x < y$ implica $f(y) \prec f(x)$ para todos $x, y \in a$. Se f é crescente ou decrescente, dizemos que f é *monótona*, e se f é estritamente crescente ou estritamente decrescente, dizemos que f é *estritamente monótona*.

Definição 5.12. Dados dois conjuntos ordenados $(a, \leq)$ e $(b, \preceq)$, dizemos que a e b são *isomorfos*, ou que a e b possuem o *mesmo tipo de ordem*, se existir uma função bijetora $f : a \to b$ tal que para quaisquer $x, y \in a$, temos $x \leq y$ se e somente se $f(x) \preceq f(y)$. A função f é chamada de *isomorfismo*.

Definição 5.13. Dados dois conjuntos ordenados $(a, \leq)$ e $(b, \preceq)$ com $a \cap b = \varnothing$, definimos a *ordem união*, ou *ordem soma*, em $a \uplus b$ como:

$$x \leq_\cup y \text{ se e somente se } (x, y \in a \wedge x \leq y) \vee (x, y \in b \wedge x \preceq y) \vee (x \in a \wedge y \in b)$$

Definição 5.14. Dados dois conjuntos ordenados $(a, \leq)$ e $(b, \preceq)$, definimos a *ordem produto*, ou *ordem lexicográfica*, em $a \times b$ como:

$$(x, y) \leq_\times (w, z) \text{ se e somente se } (x < w \vee (x = w \wedge y \preceq z))$$

5.2 NÚMEROS ORDINAIS

Definição 5.15. Um conjunto a é *transitivo* se para todo $x \in a$ temos $x \subseteq a$. Equivalentemente, a é transitivo se $a \subseteq \mathcal{P}(a)$, ou ainda, a é transitivo se $\bigcup a \subseteq a$.

Definição 5.16. Um conjunto a é um *número ordinal*, ou simplesmente um *ordinal*, se a é transitivo e $(a, \underline{\in}_a)$ é bem ordenado. É usual denotar ordinais por letras gregas minúsculas. A classe de todos os ordinais é denotada por **Ord**.

Teorema 5.3. O conjunto vazio é um ordinal e sucessor de ordinais é um ordinal.

Demonstração. É imediato que o conjunto vazio é um ordinal (as duas condições são satisfeitas por vacuidade).
Dado um ordinal α, seja $x \in \mathcal{S}(\alpha)$. Se $x = \alpha$, claro que $x \subseteq \mathcal{S}(\alpha)$. Se $x \in \alpha$, então $x \subseteq \alpha \subseteq \mathcal{S}(\alpha)$. Logo, $\mathcal{S}(\alpha)$ é transitivo. Seja $y \subseteq \mathcal{S}(\alpha)$ não-vazio. Se $\alpha \notin y$, então $y \subseteq \alpha$, logo y tem mínimo. Se $y = \{\alpha\}$, então $\min y = \alpha$. Caso contrário, $y \setminus \{\alpha\} \neq \varnothing$, e como $y \setminus \{\alpha\} \subseteq \alpha$, existe $z = \min(y \setminus \{\alpha\})$. Como $y \setminus \{\alpha\} \subseteq \alpha$, segue que $z \in \alpha$, e portanto $z = \min y$. Logo, $\mathcal{S}(\alpha)$ é bem ordenado por $\underline{\in}$. Portanto $\mathcal{S}(\alpha)$ é um ordinal. □

Corolário 5.3.1. Os números naturais são ordinais.

Demonstração. Como $0 = \varnothing$, temos que 0 é um ordinal. Se $n \in \omega$ é um ordinal, então $\mathcal{S}(n)$ é um ordinal. Segue por indução finita que todos os números naturais são ordinais. □

Teorema 5.4. Os elementos de ordinais são ordinais.

Demonstração. Seja α um ordinal e tome $\beta \in \alpha$. Seja $x \in \beta$. Como $\beta \subseteq \alpha$, segue que $x \in \alpha$, logo $x \subseteq \alpha$. Seja $u \in x$. Como $x \subseteq \alpha$, temos $u \in \alpha$. Assim, como $u \in x \in \beta$ e $\underline{\in}$ é uma ordem em α, segue que $u \in \beta$, logo $x \subseteq \beta$, e portanto β é transitivo. Seja $y \subseteq \beta$ não-vazio. Como $\beta \subseteq \alpha$, segue que $y \subseteq \beta \subseteq \alpha$, e portanto y tem mínimo. Logo, β é bem ordenado por $\underline{\in}$. Portanto β é um ordinal. □

Teorema 5.5. Dados dois ordinais α e β, se $\alpha \subsetneq \beta$, então $\alpha \in \beta$.

Demonstração. Seja $x = \beta \setminus \alpha$. Como $x \neq \varnothing$ e $x \subseteq \beta$, seja $y = \min x$. Como $y \in \beta$, segue que $y \subseteq \beta$. Seja $z \in y$. Temos $z \in \beta$, e se $z \notin \alpha$, então $z \in x$, logo $y \underline{\in} z$, absurdo, assim $z \in \alpha$. Portanto, $y \subseteq \alpha$. Seja $w \in \alpha$. Temos $w \in \beta$, logo $w \underline{\in} y$ ou $y \underline{\in} w$. Se $y \underline{\in} w$, como $w \in \alpha$, temos $y \in \alpha$, mas $y \in x$, absurdo. Deste modo, segue que $w \in y$, e assim $\alpha \subseteq y$. Logo $\alpha = y$ e portanto $\alpha \in \beta$. □

Corolário 5.5.1. Dados dois ordinais α e β, temos que $\alpha \underline{\in} \beta$ se e somente se $\alpha \subseteq \beta$.

Demonstração. ($\Rightarrow$) É imediato da definição.
($\Leftarrow$) Decorre do teorema anterior. $\square$

Teorema 5.6. A intersecção de um conjunto de ordinais é um ordinal.

Demonstração. Considere $a \neq \varnothing$ um conjunto cujos elementos são ordinais. Seja $x \in \bigcap a$. Para todo $\alpha \in a$ temos $x \in \alpha$, logo $x \subseteq \alpha$ para todo $\alpha \in a$, e segue que $x \subseteq \bigcap a$. Assim, $\bigcap a$ é transitivo. Seja $y \subseteq \bigcap a$ não-vazio. Para todo $\alpha \in a$ temos $y \subseteq \alpha$, e portanto y tem mínimo. Logo, $\bigcap a$ é bem ordenado por $\underline{\in}$. Portanto $\bigcap a$ é um ordinal. $\square$

Teorema 5.7. Dados dois ordinais α e β, temos que exatamente uma das seguintes situações acontece: $\alpha \in \beta$; $\beta \in \alpha$; ou $\alpha = \beta$.

Demonstração. Seja $\gamma = \alpha \cap \beta$. Temos $\gamma \subseteq \alpha$ e $\gamma \subseteq \beta$. Se $\gamma = \alpha$, temos $\alpha \subseteq \beta$, logo $\alpha = \beta$ ou $\alpha \in \beta$. Se $\gamma = \beta$, temos $\alpha \supseteq \beta$, logo $\alpha = \beta$ ou $\beta \in \alpha$. Se $\gamma \subsetneq \alpha$ e $\gamma \subsetneq \beta$, obtemos $\gamma \in \alpha$ e $\gamma \in \beta$, logo $\gamma \in \alpha \cap \beta = \gamma$, absurdo. Portanto, uma das condições $\alpha \in \beta$, $\beta \in \alpha$ ou $\alpha = \beta$ deve ser satisfeita, e como duas quaisquer delas resulta em absurdo, segue que somente uma delas é satisfeita. $\square$

Teorema 5.8. A união de um conjunto de ordinais é um ordinal.

Demonstração. Considere $a \neq \varnothing$ um conjunto cujos elementos são ordinais. Seja $x \in \bigcup a$. Existe $\alpha \in a$ tal que $x \in \alpha$, logo $x \subseteq \alpha$, e segue que $x \subseteq \bigcup a$. Assim, $\bigcup a$ é transitivo. Seja $y \subseteq \bigcup a$ não-vazio. Seja $z = \{\min(k \cap y) : k \in \{\ell \in a : \ell \cap y \neq \varnothing\}\}$. Existe $v \in a$ tal que $v \cap y \neq \varnothing$, logo $z \neq \varnothing$. Tome um $\xi \in z$. Se $\xi \cap z = \varnothing$, então para todo $\alpha \in z$ temos $\alpha \notin \xi$, isto é, $\xi \underline{\in} \alpha$, e portanto $\xi = \min z$. Se $\xi \cap z \neq \varnothing$, então $\xi \cap z \subseteq \xi$ tem mínimo, seja $\eta = \min(\xi \cap z)$. Dado $\nu \in z$, se $\nu \in \eta$, como $\eta \in \xi$, teríamos $\nu \in \xi$, logo $\nu \in \xi \cap z$, absurdo, pois η é o mínimo de $\xi \cap z$, logo $\eta = \min z$. Deste modo, existe $\gamma = \min z$ ($\gamma = \xi$ ou $\gamma = \eta$). Dado $w \in y$, existe $\delta \in a$ tal que $w \in \delta \cap y$, logo $\gamma \underline{\in} \min(\delta \cap y) \underline{\in} w$, e além disso $\gamma \in y$, portanto $\gamma = \min y$. Assim, $\bigcup a$ é bem ordenado por $\underline{\in}$. Portanto $\bigcup a$ é um ordinal. $\square$

Corolário 5.8.1. O conjunto dos números naturais é um ordinal.

Demonstração. Como $\omega = \bigcup \omega$, segue do Corolário 5.3.1 que ω é um ordinal. $\square$

Corolário 5.8.2. A classe **Ord** é uma classe própria.

Demonstração. Suponha que **Ord** é um conjunto. Temos que $\alpha = \bigcup \mathbf{Ord}$ é um ordinal, logo $\mathcal{S}(\alpha) \in \mathbf{Ord}$, e assim $\mathcal{S}(\alpha) \subseteq \alpha$, o que implica $\alpha \in \alpha$, absurdo. Portanto **Ord** é uma classe própria. $\square$

Definição 5.17. Dado um ordinal α, se existir um ordinal β tal que $\alpha = \mathcal{S}(\beta)$, dizemos que α é um *ordinal sucessor*. Caso contrário, dizemos que α é um *ordinal limite*.

Exemplo 5.11. O conjunto dos números naturais é um ordinal limite. De fato, se existisse um ordinal α tal que $\mathcal{S}(\alpha) = \omega$, teríamos $\alpha \in \omega$, e assim $\mathcal{S}(\alpha) \in \omega$, implicando $\omega \in \omega$, absurdo.

Definição 5.18. Definimos a *ordem* entre ordinais como $\alpha \leq \beta$ se e somente se $\alpha \subseteq \beta$, e $\alpha < \beta$ se e somente se $\alpha \in \beta$.

Teorema 5.9. Se $(a, \leq)$ é bem ordenado, então existe um único ordinal α tal que a e α possuem o mesmo tipo de ordem.

A demonstração do Teorema 5.9 pode ser vista em (HRBACEK; JECH, 1999, p. 111-113).

5.3 INDUÇÃO E RECURSÃO TRANSFINITAS

Teorema 5.10 (Indução Transfinita)**.** Se uma propriedade $\varphi(x, p)$ (com parâmetro p) é tal que

(i) $\varphi(0, p)$ é verificada;

(ii) para cada ordinal α, temos que $\varphi(\alpha, p)$ implica $\varphi(\mathcal{S}(\alpha), p)$;

(iii) para cada ordinal limite $\kappa \neq 0$, temos que $\varphi(\alpha, p)$ para todo $\alpha < \kappa$ implica $\varphi(\kappa, p)$;

então $\varphi(x, p)$ é satisfeita por todos os ordinais.

Demonstração. Suponha que $\varphi(\beta, p)$ não é satisfeita para algum ordinal β. Seja $u = \{x \leq \beta : \neg\varphi(x, p)\}$. Como $\beta \in u$, temos que u é não-vazio e portanto tem mínimo. Seja $\gamma = \min u$. Por (i), temos que $\gamma \neq 0$. Como $\varphi(\delta, p)$ é satisfeita para todo ordinal $\delta < \gamma$, segue de (ii), se γ for um ordinal sucessor, ou de (iii), se γ for um ordinal limite, que $\varphi(\gamma, p)$ é satisfeita, absurdo. $\square$

Teorema 5.11 (Recursão Transfinita)**.** Dados um conjunto a e uma função$^\blacklozenge$ G com domínio $\mathcal{V}$, existe uma única função$^\blacklozenge$ F com domínio **Ord** tal que

(i) $F(0) = a$;

(ii) $F(\mathcal{S}(\alpha)) = G((F(\alpha), \alpha))$ para todo ordinal α;

(iii) $F(\kappa) = G((F \restriction \kappa, \kappa))$ para todo ordinal $\kappa \neq 0$ limite.

Demonstração. Temos que $F(0)$ está bem definido. Supondo que $F(\alpha)$ está bem definido para o ordinal α, seja $t = F(\alpha)$. Temos $F(\mathcal{S}(\alpha)) = G((F(\alpha), \alpha)) = G((t, \alpha))$, logo $F(\mathcal{S}(\alpha))$ está bem definido. Supondo que $F(\beta)$ está bem definido para todo ordinal $\beta < \kappa$, κ ordinal limite, seja $f = \{(\nu, F(\nu)) : \nu < \kappa\}$. Temos $F(\kappa) = G((F \restriction \kappa, \kappa)) = G((f, \kappa))$, logo $F(\kappa)$ está bem definido. Segue por indução transfinita que $F(\xi)$ está bem definido para todo ordinal ξ. $\square$

5.4 ARITMÉTICA ORDINAL

Definição 5.19. Definimos a *adição* de ordinais como segue via recursão transfinita, para cada ordinal γ:

$$\begin{cases} \gamma + 0 = \gamma \\ \gamma + \mathcal{S}(\alpha) = \mathcal{S}(\gamma + \alpha) & \text{para cada ordinal } \alpha \\ \gamma + \kappa = \bigcup\limits_{\beta < \kappa} (\gamma + \beta) & \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Definição 5.20. Definimos a *multiplicação* de ordinais como segue via recursão transfinita, para cada ordinal γ:

$$\begin{cases} \gamma \cdot 0 = 0 \\ \gamma \cdot \mathcal{S}(\alpha) = \gamma \cdot \alpha + \gamma & \text{para cada ordinal } \alpha \\ \gamma \cdot \kappa = \bigcup\limits_{\beta < \kappa} (\gamma \cdot \beta) & \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Definição 5.21. Definimos a *exponenciação* de ordinais como segue via recursão transfinita, para cada ordinal γ:

$$\begin{cases} \gamma^0 = 1 \\ \gamma^{\mathcal{S}(\alpha)} = \gamma^\alpha \cdot \gamma & \text{para cada ordinal } \alpha \\ \gamma^\kappa = \bigcup\limits_{\beta < \kappa} (\gamma^\beta) & \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Na ausência de parênteses, a multiplicação tem prioridade sobre a adição, a exponenciação tem prioridade sobre a adição e a multiplicação.

Teorema 5.12. As seguintes propriedades são válidas para quaisquer ordinais α, β e γ:

(i) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

(ii) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$;

(iii) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$;

(iv) $\alpha^{\beta + \gamma} = \alpha^\beta \cdot \alpha^\gamma$;

(v) $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$;

(vi) se $\alpha \leq \beta$, então existe um único ordinal δ tal que $\alpha + \delta = \beta$;

(vii) se $\alpha \neq 0$, então existem um único ordinal ξ e um único ordinal $\rho < \alpha$ tais que $\alpha \cdot \xi + \rho = \beta$.

Demonstração. Por indução transfinita (alguns passos já foram provados no Teorema 3.7). Seja $\kappa \neq 0$ um ordinal limite.
(i) $(\alpha+\beta)+\kappa = \bigcup_{\nu<\kappa}((\alpha+\beta)+\nu) = \bigcup_{\nu<\kappa}(\alpha+(\beta+\nu)) = \alpha+\bigcup_{\nu<\kappa}(\beta+\nu) = \alpha+(\beta+\kappa)$

(ii) $\alpha \cdot (\beta + \kappa) = \alpha \cdot \bigcup_{\nu < \kappa}(\beta + \nu) = \bigcup_{\nu < \kappa}(\alpha \cdot (\beta + \nu)) = \bigcup_{\nu < \kappa}(\alpha \cdot \beta + \alpha \cdot \nu) =$
$= \alpha \cdot \beta + \bigcup_{\nu < \kappa}(\alpha \cdot \nu) = \alpha \cdot \beta + \alpha \cdot \kappa$
(iii) $(\alpha \cdot \beta) \cdot \kappa = \bigcup_{\nu < \kappa}((\alpha \cdot \beta) \cdot \nu) = \bigcup_{\nu < \kappa}(\alpha \cdot (\beta \cdot \nu)) = \alpha \cdot \bigcup_{\nu < \kappa}(\beta \cdot \nu) = \alpha \cdot (\beta \cdot \kappa)$
(iv) $\alpha^{\beta + \kappa} = \alpha^{\bigcup_{\nu < \kappa}(\beta + \nu)} = \bigcup_{\nu < \kappa}(\alpha^{\beta + \nu}) = \bigcup_{\nu < \kappa}(\alpha^{\beta} \cdot \alpha^{\nu}) = \alpha^{\beta} \cdot \bigcup_{\nu < \kappa} \alpha^{\nu} = \alpha^{\beta} \cdot \alpha^{\kappa}$
(v) $(\alpha^{\beta})^{\kappa} = \bigcup_{\nu < \kappa}((\alpha^{\beta})^{\nu}) = \bigcup_{\nu < \kappa}(\alpha^{\beta \cdot \nu}) = \alpha^{\bigcup_{\nu < \kappa}(\beta \cdot \nu)} = \alpha^{\beta \cdot \kappa}$
(vi) e (vii) podem ser encontrados em (HRBACEK; JECH, 1999, p. 121, 124). $\square$

Note que os itens (vi) e (vii) do Teorema 5.12 nos permitem definir subtração e divisão de ordinais de maneira análoga aos números naturais.

Teorema 5.13. As seguintes propriedades **não** são válidas para quaisquer ordinais α, β e γ:

(i) $\alpha + \beta = \beta + \alpha$;

(ii) $\alpha \cdot \beta = \beta \cdot \alpha$;

(iii) $(\alpha + \beta) \cdot \gamma = (\alpha \cdot \gamma) + (\beta \cdot \gamma)$;

(iv) se $\alpha + \gamma = \beta + \gamma$, então $\alpha = \beta$;

(v) se $\alpha \cdot \gamma = \beta \cdot \gamma$ e $\gamma \neq 0$, então $\alpha = \beta$;

(vi) $(\alpha \cdot \beta)^{\gamma} = \alpha^{\gamma} \cdot \beta^{\gamma}$.

Demonstração. Contraexemplos:
(i) $1 + \omega = \bigcup_{n \in \omega}(1 + n) = \omega \neq \mathcal{S}(\omega) = \omega + 1$
(ii) $2 \cdot \omega = \bigcup_{n \in \omega}(2 \cdot n) = \omega \neq \omega + \omega = \omega \cdot 2$
(iii) $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega \neq \omega + \omega = 1 \cdot \omega + 1 \cdot \omega$
(iv) $0 + \omega = \omega = 1 + \omega$, mas $0 \neq 1$
(v) $1 \cdot \omega = \omega = 2 \cdot \omega$ e $\omega \neq 0$, mas $1 \neq 2$
(vi) $(\omega \cdot 2)^2 = (\omega \cdot 2) \cdot (\omega \cdot 2) = (\omega \cdot 2) \cdot (\omega + \omega) = (\omega \cdot 2) \cdot \omega + (\omega \cdot 2) \cdot \omega = \omega \cdot (2 \cdot \omega) + \omega \cdot (2 \cdot \omega) =$
$= \omega \cdot \omega + \omega \cdot \omega = \omega^2 + \omega^2 = \omega^2 \cdot 2 \neq \omega^2 \cdot 4 = \omega^2 \cdot 2^2$ $\square$

Teorema 5.14. Para quaisquer ordinais α e β, temos que $\alpha \cdot \beta = 0$ se e somente se $\alpha = 0$ ou $\beta = 0$.

Demonstração. ($\Rightarrow$) Sejam $\alpha \neq 0$ e $\beta \neq 0$.
Se α e β forem ordinais sucessores, então existem ordinais γ e δ tais que $\alpha = \mathcal{S}(\gamma)$ e $\beta = \mathcal{S}(\delta)$, logo $\alpha \cdot \beta = \mathcal{S}(\gamma) \cdot \mathcal{S}(\delta) = \mathcal{S}(\mathcal{S}(\gamma) \cdot \delta + \gamma) \neq \varnothing$.
Se $\alpha = \mathcal{S}(\gamma)$ mas β for um ordinal limite, então existe $\eta \in \beta$ com $\mathcal{S}(\eta) \in \beta$, logo $\alpha \cdot \beta = \bigcup_{\nu < \beta}(\alpha \cdot \nu) \supseteq \alpha \cdot \mathcal{S}(\eta) = \mathcal{S}(\gamma) \cdot \mathcal{S}(\eta) = \mathcal{S}(\mathcal{S}(\gamma) \cdot \eta + \gamma) \neq \varnothing$.
Analogamente, se $\beta = \mathcal{S}(\delta)$ mas α for um ordinal limite, então existe $\mu \in \alpha$ com $\mathcal{S}(\mu) \in \alpha$, logo $\alpha \cdot \beta = \alpha \cdot \mathcal{S}(\delta) = \alpha \cdot \delta + \alpha = \bigcup_{\nu < \alpha}(\alpha \cdot \delta + \nu) \supseteq \alpha \cdot \delta + \mathcal{S}(\mu) = \mathcal{S}(\alpha \cdot \delta + \mu) \neq \varnothing$.
Se ambos α e β forem ordinais limites, tome $\mathcal{S}(\mu) \in \alpha$ e $\mathcal{S}(\eta) \in \beta$. Temos $\alpha \cdot \beta = \bigcup_{\nu < \beta}(\alpha \cdot \nu) \supseteq \alpha \cdot \mathcal{S}(\eta) = \alpha \cdot \eta + \alpha = \bigcup_{\nu < \alpha}(\alpha \cdot \eta + \nu) \supseteq \alpha \cdot \eta + \mathcal{S}(\mu) = \mathcal{S}(\alpha \cdot \eta + \mu) \neq \varnothing$.
Portanto $\alpha \cdot \beta \neq 0$. O resultado segue da contrapositiva.
($\Leftarrow$) Se $\beta = 0$, é imediato da definição que $\alpha \cdot \beta = 0$. Se $\alpha = 0$, temos por indução transfinita: $0 \cdot 0 = 0$; $0 \cdot \mathcal{S}(\nu) = 0 \cdot \nu + 0 = 0 \cdot \nu = 0$; e $0 \cdot \kappa = \bigcup_{\nu < \kappa} 0 \cdot \nu = \bigcup_{\nu < \kappa} 0 = 0$. $\square$

Teorema 5.15. Dados dois conjuntos bem ordenados a e b disjuntos, se a possui o mesmo tipo de ordem do ordinal α e b possui o mesmo tipo de ordem do ordinal β, então $a \uplus b$ com a ordem soma possui o mesmo tipo de ordem do ordinal $\alpha + \beta$.

Demonstração. Sejam $f : a \to \alpha$ e $g : b \to \beta$ isomorfismos. A função $h : a \uplus b \to \alpha + \beta$ dada por $h(x) = f(x)$ se $x \in a$ e $h(x) = \alpha + g(x)$ se $x \in b$ é um isomorfismo. □

Teorema 5.16. Dados dois conjuntos bem ordenados a e b, se a possui o mesmo tipo de ordem do ordinal α e b possui o mesmo tipo de ordem do ordinal β, então $a \times b$ com a ordem produto possui o mesmo tipo de ordem do ordinal $\alpha \cdot \beta$.

Demonstração. Sejam $f : a \to \alpha$ e $g : b \to \beta$ isomorfismos. A função $h : a \times b \to \alpha \cdot \beta$ dada por $h((x, y)) = \alpha \cdot g(y) + f(x)$ é um isomorfismo. □

5.5 SEQUÊNCIAS

Definição 5.22. Dado um ordinal ϑ, uma *sequência* de *comprimento* ϑ é uma função f cujo domínio é ϑ, e escrevemos $f = \langle f(\xi) : \xi < \vartheta \rangle$. É usual denotar $f(\xi)$ por f_ξ.

Definição 5.23. Uma *sequência*$^\blacklozenge$ é uma função$^\blacklozenge$ F cujo domínio é **Ord**.

Teorema 5.17. Não existe uma sequência $f = \langle f(x) : x < \omega \rangle$ tal que $f(n) \ni f(\mathcal{S}(n))$ para todo $n \in \omega$.

Demonstração. Suponha que existe uma tal sequência f. Seja $a = \{f(k) : k \in \omega\}$. Dado $f(n) \in a$, temos $f(\mathcal{S}(n)) \in a \cap f(n)$, logo $a \cap f(n) \neq \varnothing$ para todo $n \in \omega$, isto é, a não é regular, absurdo. □

Corolário 5.17.1. Não existe uma sequência $f = \langle f(x) : x \leq n \rangle$ com $n \in \omega$ tal que $f(m) \in f(\mathcal{S}(m))$ para todo $m < n$ e $f(n) \in f(0)$.

Demonstração. É imediato. □

Definição 5.24. Dadas duas sequências f e g respectivamente de comprimentos α e β, definimos a *concatenação* de f e g como a sequência $f \frown g$ de comprimento $\alpha + \beta$ tal que $(f \frown g)(\xi) = f(\xi)$ para cada $\xi < \alpha$ e $(f \frown g)(\alpha + \xi) = g(\xi)$ para cada $\xi < \beta$.

Definição 5.25. Dados um ordinal limite ϑ e uma sequência f de comprimento ϑ cujo contradomínio é um ordinal, se f é crescente, definimos o *limite* de f como $\lim f = \sup\{f(\xi) : \xi \in \vartheta\} = \bigcup_{\xi < \vartheta} f(\xi)$.

Definição 5.26. Dado um ordinal limite κ, definimos a *cofinalidade* de κ como o menor ordinal limite ϑ tal que κ é o limite de uma sequência crescente de ordinais menores do que κ de comprimento ϑ, e denotamos ϑ por $\operatorname{cof} \kappa$.

Exemplo 5.12. Temos $\operatorname{cof}\omega = \omega$, pois toda sequência de comprimento menor do que ω é uma sequência finita.

Exemplo 5.13. Temos $\operatorname{cof}(\omega + \omega) = \operatorname{cof}(\omega \cdot \omega) = \operatorname{cof}\omega^\omega = \omega$, pois $\omega + \omega$, $\omega \cdot \omega$ e ω^ω são limites respectivamente das sequências $\langle \omega + n : n < \omega \rangle$, $\langle \omega \cdot n : n < \omega \rangle$ e $\langle \omega^n : n < \omega \rangle$.

Teorema 5.18. Dado um ordinal limite κ, temos $\operatorname{cof}\kappa \leq \kappa$.

Demonstração. Considere a sequência crescente $f = \langle \xi : \xi < \kappa \rangle$ de comprimento κ. Claro que $\kappa = \lim f$, e portanto $\operatorname{cof}\kappa \leq \kappa$. $\square$

Teorema 5.19. Dado um ordinal limite κ, temos $\operatorname{cof}\operatorname{cof}\kappa = \operatorname{cof}\kappa$.

Demonstração. Sejam f e g sequências crescentes respectivamente de comprimentos $\operatorname{cof}\operatorname{cof}\kappa$ e $\operatorname{cof}\kappa$ e tais que $\lim f = \operatorname{cof}\kappa$ e $\lim g = \kappa$. A sequência $g \circ f$ tem comprimento $\operatorname{cof}\operatorname{cof}\kappa$ e $\lim(g \circ f) = \bigcup_{\xi < \operatorname{cof}\operatorname{cof}\kappa} g(f(\xi)) = \bigcup_{\xi < \operatorname{cof}\kappa} g(\xi) = \kappa$, logo $\operatorname{cof}\kappa \leq \operatorname{cof}\operatorname{cof}\kappa$, e portanto $\operatorname{cof}\operatorname{cof}\kappa = \operatorname{cof}\kappa$. $\square$

6 NÚMEROS CARDINAIS

6.1 CARDINALIDADE

Definição 6.1. Dados dois conjuntos a e b, dizemos que a e b são *equipotentes*, ou que a e b têm a mesma *cardinalidade*, ou que a e b têm a mesma *potência*, se existir uma função bijetora de a em b, e escrevemos $|a| = |b|$. Caso contrário escrevemos $|a| \neq |b|$. Se existir uma função injetora de a em b, escrevemos $|a| \leq |b|$. Se $|a| \leq |b|$ e $|a| \neq |b|$, escrevemos $|a| < |b|$.

Note que o a Definição 6.1 não fornece um significado para o símbolo $|\ \ |$ isoladamente, mas apenas comparações entre cardinalidades. Somente daremos significado para $|\ \ |$ na Definição 6.9.

Teorema 6.1. Para quaisquer conjuntos a, b e c, são satisfeitas:

(i) $|a| = |a|$;

(ii) se $|a| = |b|$, então $|b| = |a|$;

(iii) se $|a| = |b|$ e $|b| = |c|$, então $|a| = |c|$.

Demonstração. (i) A função identidade $\mathrm{Id}_a : a \to a$ é bijetora.
(ii) Seja $f : a \to b$ bijetora. A função $f^{-1} : b \to a$ é bijetora.
(iii) Sejam $f : a \to b$ e $g : b \to c$ bijetoras. A função $g \circ f : a \to c$ é bijetora. □

Teorema 6.2. Para quaisquer conjuntos a, b e c, são satisfeitas:

(i) se $|a| \leq |b|$ e $|b| \leq |c|$, então $|a| \leq |c|$;

(ii) se $|a| \leq |b|$ e $|b| < |c|$, então $|a| < |c|$;

(iii) se $|a| < |b|$ e $|b| \leq |c|$, então $|a| < |c|$.

Demonstração. (i) Sejam $f : a \to b$ e $g : b \to c$ injetoras. A função $g \circ f : a \to c$ é injetora.
(ii) Segue de (i) que $|a| \leq |c|$. Se $|a| = |c|$, teríamos $|c| \leq |b|$, absurdo, logo $|a| < |c|$.
(iii) Análogo a (ii). □

Teorema 6.3. Para quaisquer conjuntos a e b, são satisfeitas:

(i) se $a \subseteq b$, então $|a| \leq |b|$;

(ii) se $|a| \leq |b|$, então existe $u \subseteq b$ tal que $|a| = |u|$.

Demonstração. (i) A função identidade de a em b é injetora.
(ii) Seja $f : a \to b$ injetora. A função $f : a \to \operatorname{Im} f$ é bijetora, logo basta tomar $u = \operatorname{Im} f$. $\square$

Teorema 6.4. Para quaisquer conjuntos a, b, c e d tais que $|a| = |c|$ e $|b| = |d|$, são satisfeitas:

(i) se $a \cap b = c \cap d = \varnothing$, então $|a \uplus b| = |c \uplus d|$;

(ii) $|a \times b| = |c \times d|$;

(iii) $|\mathcal{F}(a, b)| = |\mathcal{F}(c, d)|$.

Demonstração. Sejam $f : a \to c$ e $g : b \to d$ bijetoras.
(i) A função $u : a \uplus b \to c \uplus d$ dada por

$$u(x) = \begin{cases} f(x) & \text{se } x \in a \\ g(x) & \text{se } x \in b \end{cases}$$

é bijetora.
(ii) A função $v : a \times b \to c \times d$ dada por $v((x, y)) = (f(x), g(y))$ é bijetora.
(iii) A função $w : \mathcal{F}(a, b) \to \mathcal{F}(c, d)$ dada por $w(x) = g \circ x \circ f^{-1}$ é bijetora. $\square$

Teorema 6.5. Para qualquer conjunto a, vale $|\mathcal{P}(a)| = |\mathcal{F}(a, 2)|$.

Demonstração. A função $f : \mathcal{P}(a) \to \mathcal{F}(a, 2)$ dada por $f(x) = \chi_x$, em que χ_x é a função característica de x com domínio a, isto é,

$$\chi_x(y) = \begin{cases} 1 & \text{se } y \in x \\ 0 & \text{se } y \in a \smallsetminus x \end{cases}$$

é bijetora. $\square$

Teorema 6.6 (Cantor)**.** Para qualquer conjunto a, vale $|a| < |\mathcal{P}(a)|$.

Demonstração. A função $f : a \to \mathcal{P}(a)$ dada por $f(x) = \{x\}$ é injetora, logo $|a| \leq |\mathcal{P}(a)|$. Suponha que exista $g : a \to \mathcal{P}(a)$ bijetora. Seja $b = \{k \in a : k \notin g(k)\}$. Tome um $x \in a$. Se $x \in b$, segue que $x \notin g(x)$, logo $g(x) \neq b$. Se $x \notin b$, segue que $x \in g(x)$, logo $g(x) \neq b$. Desde modo, $b \notin \operatorname{Im} g$, absurdo. Portanto $|a| < |\mathcal{P}(a)|$. $\square$

Corolário 6.6.1. Dado um ordinal α, existe um ordinal β tal que $|\alpha| < |\beta|$.

Demonstração. Pelo Teorema de Cantor, temos $|\alpha| < |\mathcal{P}(\alpha)|$, e pelos teoremas 5.2 e 5.9, existe um ordinal β tal que $|\beta| = |\mathcal{P}(\alpha)|$, e portanto $|\alpha| < |\beta|$. $\square$

Teorema 6.7. Para quaisquer conjuntos a, b e c, se $a \supseteq b \supseteq c$ e $|a| = |c|$, então $|a| = |b|$.

Demonstração. Seja $u : a \to c$ bijetora. Considere as funções $f, g : \omega \to \mathcal{P}(a)$ definidas via recorrência finita como seguem:

$$\begin{cases} f(0) = a \\ f(\mathcal{S}(n)) = u[f(n)] \end{cases} \qquad\qquad \begin{cases} g(0) = b \\ g(\mathcal{S}(n)) = u[g(n)] \end{cases}$$

Considere ainda a função $h : \omega \to \mathcal{P}(a)$ dada por $h(n) = f(n) \smallsetminus g(n)$. Temos $f(0) \supseteq g(0) \supseteq f(1)$, e portanto $f(n) \supseteq g(n) \supseteq f(\mathcal{S}(n))$ para todo $n \in \omega$, o que implica $h(m) \cap h(n) = \varnothing$ para $m \neq n$. Seja $d = \dot\bigcup_{n \in \omega} h(n)$. Para cada $n \in \omega$, temos

$$u[h(n)] = u[f(n) \smallsetminus g(n)] = u[f(n)] \smallsetminus u[g(n)] = f(\mathcal{S}(n)) \smallsetminus g(\mathcal{S}(n)) = h(\mathcal{S}(n)),$$

logo $u[d] = d \smallsetminus h(0) = d \smallsetminus (a \smallsetminus b) \subseteq b$. Assim, a função $v : a \to b$ dada por

$$v(x) = \begin{cases} u(x) & \text{se } x \in d \\ x & \text{caso contrário} \end{cases}$$

é bijetora. □

Teorema 6.8 (Cantor-Bernstein-Schröder)**.** Para quaisquer conjuntos a e b, se $|a| \leq |b|$ e $|b| \leq |a|$, então $|a| = |b|$.

Demonstração. Sejam $f : a \to b$ e $g : b \to a$ injetoras. A função $g \circ f : a \to a$ é injetora. Assim, temos $|a| = |g[f[a]]|$ e $|b| = |g[b]|$. Além disso, temos $g[f[a]] \subseteq g[b] \subseteq a$, e portanto $|a| = |b|$. □

Teorema* 6.9. Para quaisquer conjuntos a e b, temos $|a| \leq |b|$ ou $|b| \leq |a|$.

Demonstração. Pelo Axioma de Zermelo, existem ordinais α e β tais que $|a| = |\alpha|$ e $|b| = |\beta|$, e como $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$, o resultado segue. □

6.2 CONJUNTOS FINITOS E INFINITOS

Definição 6.2. Dado um conjunto a, dizemos que a é *finito* se existir um $n \in \omega$ tal que $|a| = |n|$. Caso contrário dizemos que a é *infinito.*

Exemplo 6.1. Cada número natural é um conjunto finito, ao passo que o conjunto dos números naturais é um conjunto infinito.

Definição 6.3. Dado um conjunto a, considere a ordem $\subseteq_{\mathcal{P}(a)}$. Dizemos que a é *T-finito* se todo subconjunto $s \subseteq \mathcal{P}(a)$ não-vazio tiver um elemento maximal. Caso contrário dizemos que a é *T-infinito.* (T de Tarski)

Definição 6.4. Dado um conjunto a, dizemos que a é *D-finito* se para todo subconjunto próprio $s \subsetneq a$ temos $|s| < |a|$. Caso contrário dizemos que a é *D-infinito.* (D de Dedekind)

Exemplo 6.2. Como a função sucessor é uma bijeção de ω em $\omega \setminus \{0\}$, temos que ω é D-infinito.

Teorema★ 6.10. Para qualquer conjunto a, temos que as seguintes afirmações são equivalentes:

(i) a é infinito; (ii) a é T-infinito; (iii) a é D-infinito.

Definição 6.5. Dado um conjunto a, definimos o *conjunto das partes finitas* de a como $\mathcal{P}_{<\omega}(a) = \{k \in \mathcal{P}(a) : k \text{ é finito}\}$.

Definição 6.6. Dado um conjunto a, dizemos que a é *enumerável* se $|a| \leq |\omega|$.

Teorema 6.11. Dados dois conjuntos enumeráveis a e b, temos que $a \times b$ é enumerável.

Demonstração. Sejam $f : a \to \omega$ e $g : b \to \omega$ injetoras. A função $h : \omega \times \omega \to \omega$ dada por $h((x, y)) = 2^x \cdot (2 \cdot y + 1)$ é bijetora. Assim, a função $u : a \times b \to \omega$ dada por $u((x, y)) = h((f(x), g(y)))$ é injetora, e portanto $a \times b$ é enumerável. $\square$

Teorema 6.12. Dado um conjunto a, se a é enumerável e cada elemento de a é enumerável, então $\bigcup a$ é enumerável.

Demonstração. Sejam $f : a \to \omega$ injetora e, para cada $u \in a$, $f_u : u \to \omega$ injetora. Seja $g = f^{-1} \mathbin{\dot\cup} \{(k, \varnothing) : k \in \omega \setminus \operatorname{Im} f\}$. Temos que g é uma função de ω em $a \cup \{\varnothing\}$ com $a \subseteq \operatorname{Im} g$. Seja $h : \bigcup a \to \omega$ dada por $h(x) = \min\{k \in \omega : x \in g(k)\}$. A função $t : \bigcup a \to \omega \times \omega$ dada por $t(x) = (f(g(h(x))), f_{g(h(x))}(x))$ é injetora, e portanto $\bigcup a$ é enumerável. $\square$

Definição 6.7. Dada uma família não-vazia $a = \{a_k : k \in \lambda\}$, se λ é enumerável, então dizemos que $\bigcup_{k \in \lambda} a_k$ é uma *união enumerável* e que $\bigcup_{k \in \lambda} a_k$ é uma *intersecção enumerável*.

Exemplo 6.3. O conjunto $\mathcal{P}(\omega)$ não é enumerável (pelo Teorema de Cantor), mas o conjunto $\mathcal{P}_{<\omega}(\omega)$ é enumerável, já que é uma união enumerável de enumeráveis.

Exemplo 6.4. Os ordinais $\omega + \omega$, $\omega \cdot \omega$, ω^ω são enumeráveis. Se $\alpha_0 = \omega$ e $\alpha_{\mathcal{S}(n)} = \omega^{\alpha_n}$ para cada $n \in \omega$, o ordinal $\varepsilon = \bigcup_{k \in \omega} \alpha_k$ é enumerável, bem como $\varepsilon + \varepsilon$, $\varepsilon \cdot \varepsilon$, ε^ε. De fato, se α e β são ordinais enumeráveis, então qualquer ordinal obtido a partir de α e β por meio das operações definidas até o momento será enumerável. O primeiro ordinal não-enumerável é $\omega_1 = \{k \in \mathbf{Ord} : k \text{ é enumerável}\}$.

6.3 NÚMEROS CARDINAIS

Definição 6.8. Um ordinal κ é um *cardinal* se para todo $\alpha < \kappa$ temos $|\alpha| < |\kappa|$. A classe de todos os cardinais é denotada por **Card**.

Teorema 6.13. Os números naturais são cardinais, bem como o conjunto dos números naturais é um cardinal.

Demonstração. É imediato que o conjunto vazio é um cardinal (por vacuidade). Seja $n \in \omega$. Como n é finito, não existe bijeção entre n e um subconjunto próprio de n, em particular com os números naturais $m < n$, logo n é um cardinal. Como ω é infinito e todo $n < \omega$ é finito, segue que $|n| < |\omega|$, portanto ω é um cardinal. $\square$

Teorema 6.14. Dado um ordinal infinito α, se α é um cardinal então α é um ordinal limite.

Demonstração. Suponha que α é um ordinal sucessor. Seja β tal que $\mathcal{S}(\beta) = \alpha$. A função $f : \beta \to \alpha$ dada por

$$f(\xi) = \begin{cases} n & \text{se } \xi \in \omega \text{ e } \mathcal{S}(n) = \xi \\ \xi & \text{se } \xi \notin \omega \\ \beta & \text{se } \xi = 0 \end{cases}$$

é bijetora, logo $|\beta| = |\alpha|$, e como $\beta < \alpha$, segue que α não é um cardinal. O resultado segue da contrapositiva. $\square$

Teorema* 6.15. Para qualquer conjunto a, existe um único cardinal α tal que $|a| = |\alpha|$.

Demonstração. Pelos teoremas 5.2 e 5.9, existe um cardinal α tal que $|a| = |\alpha|$. Seja β um cardinal tal que $|a| = |\beta|$. Se $\alpha < \beta$, temos $|\alpha| < |\beta|$, absurdo. Se $\beta < \alpha$, temos $|\beta| < |\alpha|$, absurdo. Portanto, devemos ter $\alpha = \beta$. $\square$

Definição 6.9. Para cada conjunto a, representamos o cardinal equipotente a a por $|a|$, e dizemos que $|a|$ é a *cardinalidade* de a, ou que $|a|$ é a *potência* de a.

6.4 ARITMÉTICA CARDINAL

Definição 6.10. Definimos a *adição* de cardinais como segue: dados dois cardinais α e β, considere conjuntos disjuntos a e b tais que $|a| = \alpha$ e $|b| = \beta$. Com isso, definimos $\alpha + \beta$ como $|a \uplus b|$.

Definição 6.11. Definimos a *multiplicação* de cardinais como segue: dados dois cardinais α e β, considere conjuntos a e b tais que $|a| = \alpha$ e $|b| = \beta$. Com isso, definimos $\alpha \cdot \beta$ como $|a \times b|$.

Definição 6.12. Definimos a *exponenciação* de cardinais como segue: dados dois cardinais α e β, considere conjuntos a e b tais que $|a| = \alpha$ e $|b| = \beta$. Com isso, definimos α^β como $|\mathcal{F}(b, a)|$.

O Teorema 6.4 nos garante que as operações não dependem dos conjuntos a e b. Assim, elas estão bem definidas.

Na ausência de parênteses, a multiplicação tem prioridade sobre a adição, a exponenciação tem prioridade sobre a adição e a multiplicação. Note que as operações entre cardinais não coincidem com as operações entre ordinais (coincidem somente no caso finito), o contexto deixará claro a que operações nos referimos.

Teorema 6.16. As seguintes propriedades são válidas para quaisquer cardinais κ, λ e μ:

(i) $(\kappa+\lambda)+\mu=\kappa+(\lambda+\mu)$;

(ii) $(\kappa\cdot\lambda)\cdot\mu=\kappa\cdot(\lambda\cdot\mu)$;

(iii) $\kappa+\lambda=\lambda+\kappa$;

(iv) $\kappa\cdot\lambda=\lambda\cdot\kappa$;

(v) $\kappa\cdot(\lambda+\mu)=(\kappa\cdot\lambda)+(\kappa\cdot\mu)$;

(vi) $(\kappa+\lambda)\cdot\mu=(\kappa\cdot\mu)+(\lambda\cdot\mu)$;

(vii) $\kappa^{\lambda+\mu}=\kappa^{\lambda}\cdot\kappa^{\mu}$;

(viii) $(\kappa\cdot\lambda)^{\mu}=\kappa^{\mu}\cdot\lambda^{\mu}$;

(ix) $(\kappa^{\lambda})^{\mu}=\kappa^{\lambda\cdot\mu}$;

(x) $\kappa\cdot\lambda=0$ se e somente se $\kappa=0$ ou $\lambda=0$.

Demonstração. Considere conjuntos k, ℓ e m tais que $|k|=\kappa$, $|\ell|=\lambda$ e $|m|=\mu$.
(i) A união de conjuntos é associativa.
(ii) A função $f:(k\times\ell)\times m\to k\times(\ell\times m)$ dada por $f((x,y),z)=(x,(y,z))$ é bijetora.
(iii) A união de conjuntos é comutativa.
(iv) A função $f:k\times\ell\to\ell\times k$ dada por $f(x,y)=(y,x)$ é bijetora.
(v) e (vi) O produto cartesiano é distributivo em relação à união.
(vii) A função $f:\mathcal{F}(\ell\uplus m,k)\to\mathcal{F}(\ell,k)\times\mathcal{F}(m,k)$ dada por $f(g)=(g\restriction\ell,g\restriction m)$ é bijetora.
(viii) A função $f:\mathcal{F}(m,k\times\ell)\to\mathcal{F}(m,k)\times\mathcal{F}(m,\ell)$ dada por $f(g)=(\pi_1\circ g,\pi_2\circ g)$, em que π_1 e π_2 são respectivamente as projeções na primeira e na segunda coordenadas, é bijetora.
(ix) A função $f:\mathcal{F}(m,\mathcal{F}(\ell,k))\to\mathcal{F}(\ell\times m,k)$ dada por $f(g)(x,y)=g(y)(x)$ é bijetora.
(x) A propriedade análoga vale para o produto cartesiano (Teorema 1.10). □

6.5 ÁLEFS

O símbolo $\aleph$ é a primeira letra do alfabeto hebraico, chamada álef. Os álefs constituem a sequência♦ crescente dos cardinais infinitos, e essa seção dedica-se principalmente à sua apresentação.

Definição 6.13. Para cada conjunto x, seja $\mathcal{H}(x)$ o menor ordinal tal que $|x|<|\mathcal{H}(x)|$. O ordinal $\mathcal{H}(x)$ é chamado de *número de Hartogs* de x.

Teorema 6.17. Para qualquer conjunto x, temos que $\mathcal{H}(x)$ é o menor ordinal que não é equipotente a um subconjunto de x.

Demonstração. Claro que $\mathcal{H}(x)$ não é equipotente a um subconjunto de x. Seja α um ordinal que não é equipotente a um subconjunto de x. Como $|\alpha| \leq |x|$ contraria o Teorema 6.3, temos $|x| < |\alpha|$, e pela definição de número de Hartogs temos $\mathcal{H}(x) \leq \alpha$. □

Teorema 6.18. Para qualquer conjunto x, temos que $\mathcal{H}(x)$ é um cardinal.

Demonstração. Seja $\alpha < \mathcal{H}(x)$. Pela definição de número de Hartogs, segue que $|\alpha| < |\mathcal{H}(x)|$, logo $\mathcal{H}(x)$ é um cardinal. □

Definição 6.14. Dado um cardinal κ, definimos o *cardinal sucessor* de κ como $\kappa^+ = \mathcal{H}(\kappa)$. Um cardinal que não é sucessor é chamado de *cardinal limite*.

Definição 6.15. Definimos os *álefs* via recursão transfinita como segue:

$$\begin{cases} \aleph_0 = \omega \\ \aleph_{\mathcal{S}(\alpha)} = \mathcal{H}(\aleph_\alpha) & \text{para cada ordinal } \alpha \\ \aleph_\kappa = \bigcup\limits_{\beta < \kappa} \aleph_\beta & \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Teorema 6.19. Se κ é um cardinal infinito, então existe um ordinal α tal que $\kappa = \aleph_\alpha$.

Demonstração. Seja $\gamma = \{\beta : \aleph_\beta < \kappa\}$. Se $\gamma = \varnothing$, então $\kappa = \omega = \aleph_0$. Se γ é um ordinal limite diferente do vazio, então $\aleph_\gamma = \bigcup_{\beta < \gamma} \aleph_\beta \leq \kappa$, e como $\kappa \leq \aleph_\gamma$, segue que $\kappa = \aleph_\gamma$. Se γ é um ordinal sucessor, então existe $\delta \in \gamma$ tal que $\mathcal{S}(\delta) = \gamma$. Temos $\aleph_\delta < \kappa \leq \aleph_\gamma = \aleph_{\mathcal{S}(\delta)}$, e segue pela definição dos álefs que $\kappa = \aleph_\gamma$. □

Corolário 6.19.1. A classe **Card** é uma classe própria.

Demonstração. Suponha que **Card** é um conjunto. Como **Ord** é uma classe própria, a função♦ $F = \{(\kappa, \aleph_\kappa) : \kappa \in \mathbf{Ord}\}$ é uma classe própria. Como F é tal que $\alpha \neq \beta$ implica $F(\alpha) \neq F(\beta)$, a classe $F^{-1} = \{(\aleph_\kappa, \kappa) : \kappa \in \mathbf{Ord}\}$ também é uma função♦, e como o domínio de F^{-1} está contido em **Card**, segue que F^{-1} é uma função, absurdo. Portanto **Card** é uma classe própria. □

Os teoremas 6.20 e 6.21 tratam das operações de cardinais entre álefs. As demonstrações podem ser vistas em (HRBACEK; JECH, 1999, p. 134-136, 166-167).

Teorema 6.20. Dados dois álefs $\aleph_\alpha$ e $\aleph_\beta$, temos $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\max\{\alpha, \beta\}}$.

Definição 6.16. O cardinal $\mathfrak{c} = 2^{\aleph_0}$ é chamado de *potência do continuum*, ou simplesmente de *continuum*.

Hipótese do Continuum. Temos $\mathfrak{c} = \aleph_1$, isto é, não existe um conjunto x tal que $|\omega| < |x| < |\mathcal{P}(\omega)|$.

Hipótese Generalizada do Continuum. Temos $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ para todo ordinal α.

O Teorema de Cantor, juntamente com o Teorema 6.5, nos garante que $\aleph_0 < 2^{\aleph_0}$, isto é, $\aleph_1 \leq 2^{\aleph_0}$, e mais geral, $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$ para todo ordinal α. A Hipótese do Continuum, abreviada como CH (*Continuum Hypothesis*), é independente dos axiomas de ZFC (veremos o que significa "ser independente" no Capítulo 9). A Hipótese Generalizada do Continuum, abreviada como GCH (*Generalized Continuum Hypothesis*), também independente dos axiomas de ZFC e que, como o próprio nome diz, generaliza CH, pode ser enunciada, utilizando a definição a seguir, como $\aleph_\alpha = \beth_\alpha$ para todo ordinal α.

Definição 6.17. Definimos os *béts* via recursão transfinita do seguinte modo:

$$\begin{cases} \beth_0 = \omega \\ \beth_{\mathcal{S}(\alpha)} = |\mathcal{P}(\beth_\alpha)| & \text{para cada ordinal } \alpha \\ \beth_\kappa = \bigcup_{\beta<\kappa} \beth_\beta & \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Teorema 6.21. Assumindo GCH, dados dois álefs $\aleph_\alpha$ e $\aleph_\beta$, temos:

$$\aleph_\alpha^{\aleph_\beta} = \begin{cases} \aleph_\alpha & \text{se } \aleph_\beta < \operatorname{cof} \aleph_\alpha \\ \aleph_{\alpha+1} & \text{se } \operatorname{cof} \aleph_\alpha \leq \aleph_\beta \leq \aleph_\alpha \\ \aleph_{\beta+1} & \text{se } \aleph_\alpha \leq \aleph_\beta \end{cases}$$

.

6.6 CARDINAIS REGULARES E SINGULARES

Teorema 6.22. Para cada ordinal α, temos $\alpha \leq \aleph_\alpha$.

Demonstração. Considere a função $f : \alpha \to \aleph_\alpha$ dada por $f(\xi) = \aleph_\xi$. Claro que f é injetora e crescente, logo $f : \alpha \to \operatorname{Im} f$ é um isomorfismo, e portanto $\alpha \leq \aleph_\alpha$. $\square$

Teorema 6.23. Dado um ordinal limite $\alpha \neq 0$, se α não é um cardinal então $\operatorname{cof} \alpha < \alpha$.

Demonstração. Seja $\kappa = |\alpha|$. Existe uma função bijetora $f : \kappa \to \alpha$. Considere a sequência g de comprimento γ definida como $g(0) = f(0)$,

$$g(\mathcal{S}(\beta)) = \min\{f(k) \in \alpha : g(\beta) < f(k) \land \forall \delta \in \kappa\ (g(\beta) = f(\delta) \to \delta < k)\}$$

para cada $\beta < \gamma$, que existe pois α e κ são ordinais limites, e

$$g(\mu) = \min\{f(k) \in \alpha : \forall \nu \in \mu \ (g(\nu) < f(k) \wedge \forall \delta \in \kappa \ (g(\nu) = f(\delta) \rightarrow \delta < k))\}$$

se μ é um ordinal limite e o mínimo existe. Claro que γ é um ordinal limite com $\gamma \leq \kappa$ e g é crescente com $\lim g = \alpha$, logo $\operatorname{cof} \alpha \leq \gamma \leq \kappa < \alpha$. □

Definição 6.18. Dado um cardinal infinito κ, dizemos que κ é *regular* se $\operatorname{cof} \kappa = \kappa$, e *singular* se $\operatorname{cof} \kappa < \kappa$.

Exemplo 6.5. O cardinal $\aleph_0$ é regular, ao passo que o cardinal $\aleph_\omega$ é singular, pois é o limite da sequência $\langle \aleph_n : n < \omega \rangle$.

Exemplo 6.6. Os cardinais $\aleph_{\omega+\omega}$, $\aleph_{\omega\cdot\omega}$, $\aleph_{\omega^\omega}$ e $\aleph_{\omega_1}$ são singulares, pois são limites respectivamente das sequências $\langle \aleph_{\omega+n} : n < \omega \rangle$, $\langle \aleph_{\omega\cdot n} : n < \omega \rangle$, $\langle \aleph_{\omega^n} : n < \omega \rangle$ e $\langle \aleph_\nu : \nu < \omega_1 \rangle$.

Exemplo 6.7. Dado um cardinal $\aleph_\gamma$, o cardinal $\aleph_{\gamma+\omega}$ é singular, pois é limite da sequência $\langle \aleph_{\gamma+n} : n < \omega \rangle$.

Teorema 6.24. Dado um ordinal limite κ, temos que $\operatorname{cof} \kappa$ é um cardinal regular.

Demonstração. Segue do Teorema 5.19 que $\operatorname{cof} \operatorname{cof} \kappa = \operatorname{cof} \kappa$, portanto $\operatorname{cof} \kappa$ é regular. □

Teorema 6.25. Dado um cardinal infinito κ, temos que κ^+ é regular.

Demonstração. Seja f uma sequência crescente de ordinais de comprimento $\vartheta < \kappa^+$ tal que $f(\xi) < \kappa^+$ para todo $\xi < \vartheta$, isto é, $|\vartheta| < \kappa^+$ e $|f(\xi)| < \kappa^+$ para todo $\xi < \vartheta$, isto é, $|\vartheta| \leq \kappa$ e $|f(\xi)| \leq \kappa$ para todo $\xi < \vartheta$. Temos $\lim f = \bigcup_{\xi < \vartheta} f(\xi) \leq \kappa \cdot \kappa = \kappa < \kappa^+$. Portanto κ^+ é regular. □

Teorema 6.26. Dado um cardinal limite não-enumerável κ, temos que se κ é regular então $\aleph_\kappa = \kappa$.

Demonstração. Seja $\kappa = \aleph_\gamma$. Como $\gamma \neq 0$ é um ordinal limite, temos que κ é o limite da sequência crescente $\langle \aleph_\nu : \nu < \gamma \rangle$, logo $\aleph_\gamma = \kappa = \operatorname{cof} \kappa \leq \gamma$, e pelo Teorema 6.22 segue que $\aleph_\gamma = \gamma$. Portanto $\aleph_\kappa = \kappa$. □

Teorema 6.27. Existem cardinais singulares κ tais que $\aleph_\kappa = \kappa$.

Demonstração. Tome um cardinal $\aleph_\gamma$ e considere a sequência crescente de comprimento ω dada por $\alpha_0 = \aleph_\gamma$ e $\alpha_{\mathcal{S}(n)} = \aleph_{\alpha_n}$ para cada $n \in \omega$. Seja $\alpha = \lim \alpha_n$. Temos $\alpha = \lim \alpha_n = \lim \alpha_{\mathcal{S}(n)} = \lim \aleph_{\alpha_n} = \aleph_{\lim \alpha_n} = \aleph_\alpha$. Além disso, $\operatorname{cof} \alpha = \omega < \alpha$. □

Definição 6.19. Dado um cardinal κ, dizemos que κ é *fracamente inacessível* se κ é não-enumerável, limite e regular.

Definição 6.20. Dado um cardinal κ, dizemos que κ é um *cardinal limite forte* se para todo cardinal $\alpha < \kappa$ temos $2^\alpha < \kappa$.

Exemplo 6.8. O cardinal $\aleph_0$ é um cardinal limite forte.

Teorema 6.28. Dado um cardinal κ, se κ é um cardinal limite forte então κ é um cardinal limite.

Demonstração. Suponha que κ é um cardinal sucessor, isto é, existe um cardinal λ tal que $\kappa = \lambda^+$. Claro que $\lambda < \kappa$, mas $\lambda < 2^\lambda$ implica $\kappa = \lambda^+ \leq 2^\lambda$, logo κ não é um cardinal limite forte. O resultado segue da contrapositiva. $\square$

Definição 6.21. Dado um cardinal κ, dizemos que κ é *fortemente inacessível* se κ é não-enumerável, limite forte e regular.

A existência de um cardinal fortemente inacessível implica a existência de um cardinal fracamente inacessível. Entretanto, a existência de cardinais inacessíveis (fracamente e fortemente) é independente dos axiomas de ZFC (veremos o que significa "ser independente" no Capítulo 9).

7 FILTROS E ULTRAFILTROS

7.1 FILTROS

Definição 7.1. Dados um conjunto a e um subconjunto $f \subseteq \mathcal{P}(a)$, dizemos que f é um *filtro* de a se

- $\varnothing \notin f$ e $a \in f$;
- dados $u, v \in f$ temos $u \cap v \in f$;
- dado $w \in f$, se $s \subseteq a$ é tal que $w \subseteq s$ então $s \in f$.

Exemplo 7.1. Dado um conjunto não-vazio a, o conjunto $\{a\}$ é um filtro de a.

Definição 7.2. Dados um conjunto não-vazio a e um subconjunto não-vazio $s \subseteq a$, o conjunto $\{k \in \mathcal{P}(a) : s \subseteq k\}$ é um filtro de a, chamado de *filtro principal gerado* por s.

Definição 7.3. Dado um conjunto infinito a, o conjunto $f = \{k \in \mathcal{P}(a) : a \smallsetminus k \text{ é finito}\}$ é um filtro de a, chamado de *filtro de Fréchet* de a. Os elementos de f são chamados de subconjuntos *cofinitos* de a.

Teorema 7.1. Dado um conjunto a, temos que existe um filtro não-principal de a se e somente se a é infinito.

Demonstração. ($\Rightarrow$) Suponha que a é finito. Seja f um filtro de a. Como a é finito, segue que f é finito, logo $\bigcap f \in f$, mas dado $u \in f$ temos $\bigcap f \subseteq u$, isto é, f é principal gerado por $\bigcap f$. O resultado segue da contrapositiva.
($\Leftarrow$) Seja g o filtro de Fréchet de a. Dados $s \subseteq a$ não-vazio e $v \in s$, temos $a \smallsetminus \{v\} \in g$, e como $s \nsubseteq a \smallsetminus \{v\}$, segue que g é não-principal. □

Note que o Teorema 7.1 fornece uma outra maneira de caracterizar conjuntos infinitos.

Definição 7.4. Dado um conjunto não-vazio c, dizemos que c satisfaz a *propriedade da intersecção finita* se para todo subconjunto finito não-vazio $s \subseteq c$ temos $\bigcap s \neq \varnothing$.

Teorema 7.2. Dados um conjunto a e um subconjunto não-vazio $g \subseteq \mathcal{P}(a)$, se g satisfaz a propriedade da intersecção finita, então existe um filtro f de a tal que $g \subseteq f$.

Demonstração. Seja $f = \{k \in \mathcal{P}(a) : \exists w \in \mathcal{P}(g)\ (w \text{ é finito} \wedge w \neq \varnothing \wedge \bigcap w \subseteq k)\}$. Claro que $a \in f$, $\varnothing \notin f$, e se $z \in f$ com $z \subseteq s \subseteq a$ então $s \in f$. Sejam $x, y \in f$. Existem $u, v \subseteq g$

finitos e não-vazios tais que $\bigcap u \subseteq x$ e $\bigcap v \subseteq y$, segue que $\bigcap(u \cup v) = \bigcap u \cap \bigcap v \subseteq x \cap y$, logo $x \cap y \in f$ e portanto f é um filtro de a. Dado $t \in g$, claro que $\bigcap\{t\} \subseteq t$, logo $t \in f$ e portanto $g \subseteq f$. □

Definição 7.5. Dados um conjunto a e um subconjunto não-vazio $g \subseteq \mathcal{P}(a)$ tal que g satisfaz a propriedade da intersecção finita, definimos o *filtro gerado* por g como $f = \bigcap\{k \in \mathcal{P}(\mathcal{P}(a)) : k \text{ é um filtro de } a \wedge g \subseteq k\}$. Esse filtro coincide com o filtro construído na demonstração do Teorema 7.2.

Teorema 7.3. Dado um conjunto a, se p é um conjunto não-vazio cujos elementos são filtros de a, então $\bigcap p$ é um filtro de a.

Demonstração. Claro que $\varnothing \notin \bigcap p$. Como $a \in f$ para todo $f \in p$, segue que $a \in \bigcap p$. Dados $u, v \in \bigcap p$, temos que $u, v \in f$ para todo $f \in p$, logo $u \cap v \in f$ para todo $f \in p$, e segue que $u \cap v \in \bigcap p$. Dados $w \in \bigcap p$ e $s \subseteq a$ tal que $w \subseteq s$, temos $w \in f$ para todo $f \in p$, logo $s \in f$ para todo $f \in p$, e segue que $s \in \bigcap p$. Portanto $\bigcap p$ é um filtro de a. □

Teorema 7.4. Dado um conjunto a, se p é uma cadeia (segundo a ordem da inclusão) não-vazia cujos elementos são filtros de a, então $\bigcup p$ é um filtro de a.

Demonstração. Claro que $\varnothing \notin \bigcup p$ e $a \in \bigcup p$. Dados $u, v \in \bigcup p$, existem $f, g \in p$ tais que $u \in f$ e $v \in g$. Como $f \subseteq g$ ou $f \supseteq g$, isto é, $f \cup g = f$ ou $f \cup g = g$, temos $f \cup g \in p$ e $u, v \in f \cup g$, logo $u \cap v \in f \cup g$, e segue que $u \cap v \in \bigcup p$. Dados $w \in \bigcup p$ e $s \subseteq a$ tal que $w \subseteq s$, existe $h \in p$ tal que $w \in h$, logo $s \in h$ e segue que $s \in \bigcup p$. Portanto $\bigcup p$ é um filtro de a. □

Definição 7.6. Dados um conjunto a e um filtro f de a, dizemos que f é um *ultrafiltro* de a, ou que f é um *filtro maximal* de a, se para qualquer filtro g de a tal que $f \subseteq g$ temos $f = g$.

Exemplo 7.2. Dados um conjunto não-vazio a e um elemento $x \in a$, o filtro principal gerado por $\{x\}$ é um ultrafiltro de a.

Teorema 7.5. Dados um conjunto a e um filtro f de a, temos que f é um ultrafiltro de a se e somente se para todo $s \subseteq a$ temos $s \in f$ ou $a \setminus s \in f$.

Demonstração. ($\Rightarrow$) Suponha que existe um subconjunto $s \subseteq a$ tal que $s \notin f$ e $a \setminus s \notin f$. Claro que $s \neq \varnothing$. Seja $g = f \cup \{s\}$. Dado $u \subseteq f$ finito não-vazio, temos $\bigcap u \in f$, logo $\bigcap u \neq \varnothing$. Dado $v \in f$, se $v \cap s = \varnothing$ então $v \subseteq a \setminus s$ e teríamos $a \setminus s \in f$, absurdo, logo $v \cap s \neq \varnothing$. Assim, $\bigcap(u \cup \{s\}) = \bigcap u \cap s \neq \varnothing$, portanto g satisfaz a propriedade da intersecção finita, e existe um filtro h de a tal que $g \subseteq h$, o que implica $f \subsetneq h$, logo f não é um ultrafiltro. O resultado segue da contrapositiva.
($\Leftarrow$) Seja t um filtro de a tal que $f \subseteq t$. Se $t \setminus f \neq \varnothing$, então existe $w \in t \setminus f$, e como $w \notin f$ temos $a \setminus w \in f$, logo $a \setminus w \in t$, o que implica $\varnothing = w \cap (a \setminus w) \in t$, absurdo, logo $t \setminus f = \varnothing$, isto é, $f = t$, e portanto f é um ultrafiltro. □

Teorema 7.6. Dados um conjunto a, dois subconjuntos $b, c \subseteq a$ e um ultrafiltro f de a, se $b \cup c \in f$ então $b \in f$ ou $c \in f$.

Demonstração. Se $b \notin f$, então $a \setminus b \in f$, logo $(a \setminus b) \cap (b \cup c) \in f$, e como $(a \setminus b) \cap (b \cup c) = c \setminus b \subseteq c$, segue que $c \in f$. □

Teorema★ 7.7 (Tarski)**.** Dados um conjunto a e um filtro f de a, existe um ultrafiltro g de a tal que $f \subseteq g$.

Demonstração. Considere o conjunto $p = \{k \in \mathcal{P}(\mathcal{P}(a)) : k \text{ é um filtro de } a \wedge f \subseteq k\}$ e a ordem da inclusão em p. Pelo Teorema 7.4, toda cadeia em p tem um limitante superior, logo, pelo Lema de Zorn, segue que p tem um elemento maximal g. □

7.2 IDEAIS

Definição 7.7. Dados um conjunto a e um subconjunto $i \subseteq \mathcal{P}(a)$, dizemos que i é um *ideal* de a se

- $\varnothing \in i$ e $a \notin i$;
- dados $u, v \in i$ temos $u \cup v \in i$;
- dado $w \in i$, se $s \subseteq w$ então $s \in i$.

Teorema 7.8. Dados um conjunto a e um subconjunto $b \subseteq \mathcal{P}(a)$, temos que b é um filtro de a se e somente se $\{a \setminus k : k \in b\}$ é um ideal de a. Analogamente, temos que b é um ideal de a se e somente se $\{a \setminus k : k \in b\}$ é um filtro de a. Em outras palavras, as noções de filtro e de ideal são *duais*.

Demonstração. É imediato. □

Definição 7.8. Dado um conjunto não-vazio r, se para quaisquer $u, v \in r$ temos $u \cap v \in r$ e $u \triangle v \in r$, então dizemos que r é um *anel de conjuntos*.

Exemplo 7.3. Dado um conjunto a, os conjuntos $\mathcal{P}(a)$ e $\mathcal{P}_{<\omega}(a)$ são anéis de conjuntos.

Teorema 7.9. Dados um conjunto a e um subconjunto $b \subsetneq \mathcal{P}(a)$, temos que b é um ideal de a se e somente se b é um anel de conjuntos tal que para todo $u \in b$ e $v \subseteq a$ vale $u \cap v \in b$.

Demonstração. ($\Rightarrow$) Dados $x, y \in b$, temos $x \cup y \in b$, e como $x \cap y \subseteq x \cup y$ e $x \triangle y \subseteq x \cup y$, segue que $x \cap y, x \triangle y \in b$, portanto b é um anel de conjuntos. Além disso, dado $s \subseteq a$, como $x \cap s \subseteq x$, temos que $x \cap s \in b$.
($\Leftarrow$) Dados $w, z \in b$, temos $\varnothing = w \triangle w \in b$ e $w \cup z = (w \cap z) \triangle (w \triangle z) \in b$. Se $t \subseteq w$, como $t \subseteq a$, temos $t = w \cap t \in b$. Além disso, como $b \subsetneq \mathcal{P}(a)$, temos $a \notin b$, portanto b é um ideal de a. □

7.3 CONJUNTOS FECHADOS E ILIMITADOS

Definição 7.9. Dados um cardinal infinito κ e um subconjunto $a \subseteq \kappa$, dizemos que a é *limitado* se $\bigcup a < \kappa$, e *ilimitado* se $\bigcup a = \kappa$. Note que essa definição coincide com a Definição 5.5.

Teorema 7.10. Dados um cardinal regular κ e um subconjunto $a \subseteq \kappa$, temos que se a é ilimitado então $|a| = \kappa$.

Demonstração. Como $a \subseteq \kappa$, então a é bem ordenado. Sejam α o ordinal que tem o mesmo tipo de ordem de a e $f : \alpha \to a$ um isomorfismo. A sequência $\langle f(\xi) : \xi < \alpha \rangle$ é tal que $\lim f = \bigcup_{\xi < \alpha} f(\xi) = \bigcup a = \kappa$, logo $\kappa = \operatorname{cof} \kappa \leq \alpha$, mas $|\alpha| \leq \kappa$, portanto $\alpha = \kappa$ e segue que $|a| = \kappa$. □

Definição 7.10. Dados um cardinal não-enumerável κ e um subconjunto $a \subseteq \kappa$, dizemos que a é *fechado* se para todo ordinal limite $\gamma < \kappa$ tal que $\bigcup(a \cap \gamma) = \gamma$ temos $\gamma \in a$.

Teorema 7.11. Dados um cardinal regular não-enumerável κ e um subconjunto $a \subseteq \kappa$, temos que a é fechado se e somente se toda sequência crescente $\langle f(\xi) : \xi < \vartheta \rangle$ de comprimento $\vartheta < \kappa$ de elementos de a satisfaz $\lim f \in a$.

Demonstração. ($\Rightarrow$) Temos

$$\bigcup(a \cap \lim f) = \bigcup(a \cap \bigcup_{\xi < \vartheta} f(\xi)) = \bigcup \bigcup_{\xi < \vartheta} (a \cap f(\xi)) = \bigcup_{\xi < \vartheta} \bigcup(a \cap f(\xi)).$$

Para cada $\xi < \vartheta$, como $f(\xi) \in a \cap f(\mathcal{S}(\xi))$, temos $f(\xi) \subseteq \bigcup(a \cap f(\mathcal{S}(\xi)))$, e como para cada $\eta \in a \cap f(\xi)$ temos $\eta \in f(\xi)$ e assim $\eta \subseteq f(\xi)$, segue que $f(\xi) \supseteq \bigcup(a \cap f(\mathcal{S}(\xi)))$. Portanto $\bigcup(a \cap \lim f) = \bigcup_{\xi < \vartheta} \bigcup(a \cap f(\xi)) = \bigcup_{\xi < \vartheta} f(\xi) = \lim f$, logo $\lim f \in a$.
($\Leftarrow$) Seja $\beta < \kappa$ um ordinal limite tal que $\bigcup(a \cap \beta) = \beta$. Seja δ o ordinal que tem o mesmo tipo de ordem que $a \cap \beta$ e $g : \delta \to a \cap \beta$ um isomorfismo. Como $|\delta| \leq \beta < \kappa$, segue que $\delta < \kappa$, e assim $\beta = \bigcup(a \cap \beta) = \bigcup_{\xi < \delta} g(\xi) = \lim g \in a$. □

Teorema 7.12. Dados um cardinal regular não-enumerável κ e dois subconjuntos $a, b \subseteq \kappa$ fechados e ilimitados, temos que $a \cap b$ é fechado e ilimitado.

Demonstração. Seja $\gamma < \kappa$ um ordinal limite tal que $\bigcup((a \cap b) \cap \gamma) = \gamma$. Temos $\gamma = \bigcup((a \cap b) \cap \gamma) \subseteq \bigcup(a \cap \gamma) \subseteq \gamma$, logo $\bigcup(a \cap \gamma) = \gamma$ e $\gamma \in a$, e de forma análoga obtemos $\gamma \in b$, portanto $\gamma \in a \cap b$, e concluímos que $a \cap b$ é fechado. Dado $\eta < \kappa$ qualquer, como a e b são ilimitados, existem $\mu \in a$ e $\nu \in b$ tais que $\eta < \mu$ e $\eta < \nu$. Assim, supondo que $\bigcup(a \cap b) = \lambda < \kappa$, existe uma sequência crescente $\langle f(n) : n < \omega \rangle$ em κ tal que $\lambda < f(0)$, $f(n) \in a$ para n par e $f(n) \in b$ para n ímpar, logo $\bigcup_{k < \omega} f(k) = \bigcup_{k < \omega} f(2k) \in a$ e $\bigcup_{k < \omega} f(k) = \bigcup_{k < \omega} f(2k+1) \in b$, logo $\bigcup_{k < \omega} f(k) \in a \cap b$ e $\lambda \in \bigcup(a \cap b) = \lambda$, absurdo, portanto $\bigcup(a \cap b) = \kappa$, isto é, $a \cap b$ é ilimitado. □

Corolário 7.12.1. Dado um cardinal regular não-enumerável κ, o conjunto $\{k \in \mathcal{P}(\kappa) : k$ é fechado e ilimitado$\}$ satisfaz a propriedade da intersecção finita.

Demonstração. Seja $a \subseteq \{k \in \mathcal{P}(\kappa) : k$ é fechado e ilimitado$\}$ finito não-vazio. Existe $n \in \omega$ tal que existe $f : n \to a$ bijetora. Temos que $f(0)$ é fechado e ilimitado. Dado $m < n$, supondo que $\bigcap_{k \leq m} f(k)$ é fechado e limitado, segue que $\bigcap_{k \leq \mathcal{S}(m)} f(k) = f(\mathcal{S}(m)) \cap \bigcap_{k \leq m} f(k)$ é fechado e ilimitado, e portanto $\bigcap a = \bigcap_{k \leq n} f(k)$ é fechado e ilimitado, logo $\bigcap a \neq \varnothing$. $\square$

Definição 7.11. Dado um cardinal regular não-enumerável κ, o filtro gerado por $\{k \in \mathcal{P}(\kappa) : k$ é fechado e ilimitado$\}$ é chamado de *filtro fechado e ilimitado* de κ.

8 HIERARQUIA CUMULATIVA

Os resultados principais desse capítulo são decorrentes do Axioma da Regularidade, que nos permite classificar os conjuntos segundo níveis de uma hierarquia.

8.1 HIERARQUIA CUMULATIVA

Teorema 8.1. Dado um conjunto a, existe um conjunto transitivo t tal que $a \subseteq t$.

Demonstração. Considere a seguinte sequência de conjuntos definida via recursão transfinita:

$$\begin{cases} t_0 = a \\ t_{\mathcal{S}(n)} = \bigcup t_n \quad \text{para cada } n \in \omega \end{cases}$$

Claro que $a \subseteq \bigcup_{k \in \omega} t_k$, e $\bigcup \bigcup_{k \in \omega} t_k = \bigcup_{k \in \omega} \bigcup t_k = \bigcup_{k \in \omega} t_{\mathcal{S}(k)} \subseteq \bigcup_{k \in \omega} t_k$, logo $\bigcup_{k \in \omega} t_k$ é transitivo. $\square$

Definição 8.1. Dado um conjunto a, considerando a sequência $\langle t_n : n < \omega \rangle$ dada por $t_0 = a$ e $t_{\mathcal{S}(n)} = \bigcup t_n$ para cada $n \in \omega$, o conjunto $\mathcal{T}(a) = \bigcup_{k < \omega} t_k$ é chamado de *fecho transitivo* de a. O conjunto $\mathcal{T}(a)$ é o menor (segundo a ordem da inclusão) conjunto transitivo que contém a.

Definição 8.2. Definimos a seguinte sequência♦ de conjuntos via recursão transfinita:

$$\begin{cases} \mathcal{V}_0 = \varnothing \\ \mathcal{V}_{\mathcal{S}(\alpha)} = \mathcal{P}(\mathcal{V}_\alpha) \quad \text{para cada ordinal } \alpha \\ \mathcal{V}_\kappa = \bigcup_{\beta < \kappa} \mathcal{V}_\beta \quad \text{se } \kappa \neq 0 \text{ é um ordinal limite} \end{cases}$$

Essa sequência♦ é chamada de *hierarquia cumulativa* dos conjuntos, e cada $\mathcal{V}_\alpha$ é chamado de *nível* da hierarquia.

Teorema 8.2. Para cada ordinal α, o conjunto $\mathcal{V}_\alpha$ é transitivo.

Demonstração. Por indução transfinita. Claro que $\mathcal{V}_0 = \varnothing$ é transitivo. Supondo que $\mathcal{V}_\mu$ é transitivo, então dado $u \in \mathcal{V}_{\mathcal{S}(\mu)}$, temos $u \in \mathcal{P}(\mathcal{V}_\mu)$, isto é, $u \subseteq \mathcal{V}_\mu$, de forma que dado $v \in u$ temos $v \in \mathcal{V}_\mu$, logo $v \subseteq \mathcal{V}_\mu$, e segue que $v \in \mathcal{P}(\mathcal{V}_\mu) = \mathcal{V}_{\mathcal{S}(\mu)}$, e portanto $\mathcal{V}_{\mathcal{S}(\mu)}$ é transitivo. Supondo que $\mathcal{V}_\beta$ é transitivo para todo $\beta < \kappa$, com κ ordinal limite, então dado $u \in \mathcal{V}_\kappa$, existe $\gamma < \kappa$ tal que $u \in \mathcal{V}_\gamma$, logo $u \subseteq \mathcal{V}_\gamma$ e segue que $u \subseteq \mathcal{V}_\kappa$, e portanto $\mathcal{V}_\kappa$ é transitivo. Assim, $\mathcal{V}_\alpha$ é transitivo para todo ordinal α. $\square$

Teorema 8.3. Dado um conjunto a, existe um ordinal α tal que $a \in \mathcal{V}_\alpha$.

Demonstração. Suponha que existe um conjunto s tal que $s \notin \mathcal{V}_\alpha$ para todo ordinal α, isto é, $s \notin \bigcup_{\gamma \in \mathbf{Ord}} \mathcal{V}_\gamma$. Seja $t = \{k \in \mathcal{T}(\{s\}) : k \notin \bigcup_{\gamma \in \mathbf{Ord}} \mathcal{V}_\gamma\}$, que é não-vazio pois $s \in t$. Seja u um $\in$-minimal elemento de t. Se $u = \varnothing$, então $u \in \{\varnothing\} = \mathcal{V}_1$, absurdo, logo $u \neq \varnothing$. Para cada $v \in u$ temos $v \notin t$, isto é, $v \notin \mathcal{T}(\{s\})$ ou $v \in \mathcal{V}_\beta$ para algum ordinal β. Como $\mathcal{T}(\{s\})$ é transitivo e $u \in \mathcal{T}(\{s\})$, segue que $v \in \mathcal{T}(\{s\})$, logo $v \in \mathcal{V}_\beta$ para algum ordinal β. Sejam $p = \{\min\{\xi : k \in \mathcal{V}_\xi\} : k \in u\}$ e $\eta = \bigcup p$. Temos $v \in \mathcal{V}_\eta$ para todo $v \in u$, isto é, $u \subseteq \mathcal{V}_\eta$, logo $u \in \mathcal{V}_{\mathcal{S}(\eta)}$, absurdo, pois $u \notin \bigcup_{\gamma \in \mathbf{Ord}} \mathcal{V}_\gamma$. Portanto não existe um tal conjunto s. □

Corolário 8.3.1. Temos $\mathcal{V} = \bigcup_{\gamma \in \mathbf{Ord}} \mathcal{V}_\gamma$, a classe universal. A classe $\mathcal{V}$ também é chamada de *Universo de Von Neumann*.

Demonstração. É imediato. □

Definição 8.3. Dado um conjunto a, definimos o *ranque* de a como o menor ordinal α tal que $a \in \mathcal{V}_{\mathcal{S}(\alpha)}$, e denotamos por $\alpha = \operatorname{rank} a$.

Teorema 8.4. Dados dois conjuntos a e b, se $a \in b$ então $\operatorname{rank} a < \operatorname{rank} b$.

Demonstração. Sejam $\alpha = \operatorname{rank} a$ e $\beta = \operatorname{rank} b$. Como $b \in \mathcal{V}_{\mathcal{S}(\beta)} = \mathcal{P}(\mathcal{V}_\beta)$, segue que $b \subseteq \mathcal{V}_\beta$, logo $a \in \mathcal{V}_\beta$. Se β é um ordinal sucessor, considere o ordinal γ tal que $\mathcal{S}(\gamma) = \beta$, como $a \in \mathcal{V}_{\mathcal{S}(\gamma)}$, temos $\alpha \leq \gamma < \mathcal{S}(\gamma) = \beta$. Se β é um ordinal limite, então $a \in \bigcup_{\delta < \beta} \mathcal{V}_\delta = \bigcup_{\delta < \beta} \mathcal{V}_{\mathcal{S}(\delta)}$, logo existe $\eta < \beta$ tal que $a \in \mathcal{V}_{\mathcal{S}(\eta)}$, e portanto $\alpha \leq \eta < \beta$. □

Teorema 8.5. Dado um ordinal α, temos $\operatorname{rank} \alpha = \alpha$.

Demonstração. Por indução transfinita. Como $\varnothing \in \{\varnothing\} = \mathcal{V}_1 = \mathcal{V}_{\mathcal{S}(0)}$, temos $\operatorname{rank} 0 = 0$. Supondo que para um ordinal μ temos $\operatorname{rank} \mu = \mu$, então $\mu \in \mathcal{V}_{\mathcal{S}(\mu)}$, e como $\mu \subseteq \mathcal{V}_{\mathcal{S}(\mu)}$, segue que $\mathcal{S}(\mu) \subseteq \mathcal{V}_{\mathcal{S}(\mu)}$, e assim $\mathcal{S}(\mu) \in \mathcal{V}_{\mathcal{S}(\mathcal{S}(\mu))}$, logo $\mu = \operatorname{rank} \mu < \operatorname{rank} \mathcal{S}(\mu) \leq \mathcal{S}(\mu)$, e portanto $\operatorname{rank} \mathcal{S}(\mu) = \mathcal{S}(\mu)$. Supondo que $\operatorname{rank} \beta = \beta$ para todo $\beta < \kappa$, com κ ordinal limite, então $\beta \in \mathcal{V}_{\mathcal{S}(\beta)}$ para todo $\beta < \kappa$, logo $\kappa \subseteq \bigcup_{\beta < \kappa} \mathcal{V}_{\mathcal{S}(\beta)} = \mathcal{V}_\kappa$, e segue que $\kappa \in \mathcal{V}_{\mathcal{S}(\kappa)}$, logo $\operatorname{rank} \kappa \leq \kappa$, mas se $\operatorname{rank} \kappa < \kappa$ então $\operatorname{rank} \kappa = \operatorname{rank} \operatorname{rank} \kappa < \operatorname{rank} \kappa$, absurdo, portanto $\operatorname{rank} \kappa = \kappa$. Assim, $\operatorname{rank} \alpha = \alpha$ para todo ordinal α. □

8.2 $\in$-INDUÇÃO E $\in$-RECURSÃO

Teorema 8.6 ($\in$-Indução)**.** Se uma propriedade $\varphi(x, p)$ (com parâmetro p) é tal que

- para cada conjunto t, temos que $\varphi(u, p)$ para todo $u \in t$ implica $\varphi(t, p)$;

então $\varphi(x, p)$ é satisfeita por todos os conjuntos.

Demonstração. Por indução transfinita. Para cada ordinal α, considere a fórmula $\psi(\alpha, p)$ dada por "$\forall x \ (\operatorname{rank} x < \alpha \rightarrow \varphi(x, p))$".
Temos que $\psi(0, p)$ é verificada por vacuidade. Supondo que $\psi(\mu, p)$ é verificada pelo ordinal μ, seja v um conjunto tal que $\operatorname{rank} v = \mu$. Para todo elemento $y \in v$, como $\operatorname{rank} y < \mu$, temos que $\varphi(y, p)$ é verificada, logo, pela condição do enunciado, temos que $\varphi(v, p)$ é verificada, e como v é um conjunto qualquer com $\operatorname{rank} v = \mu$, temos que $\psi(\mathcal{S}(\mu), p)$ é verificada. Supondo que $\psi(\beta, p)$ é verificada para todo ordinal $\beta < \kappa$, com κ um ordinal limite, seja w um conjunto tal que $\operatorname{rank} w = \gamma < \kappa$. Para todo elemento $z \in w$, como $\operatorname{rank} z < \gamma < \kappa$, temos que $\psi(\gamma, p)$ é verificada, e assim $\varphi(z, p)$ também é verificada, logo, pela condição do enunciado, temos que $\varphi(w, p)$ é verificada, e como w é um conjunto qualquer com $\operatorname{rank} w < \kappa$, temos que $\psi(\kappa, p)$ é verificada.
Portanto $\psi(\alpha, p)$ é verificada para todo ordinal α, e portanto $\varphi(x, p)$ é verificada para todo conjunto x. □

Teorema 8.7 ($\in$-Recursão)**.** Dados um conjunto a e uma função$^\blacklozenge$ G com domínio $\mathcal{V}$, existe uma única função$^\blacklozenge$ F com domínio $\mathcal{V}$ tal que $F(x) = G(F \restriction x)$ para todo conjunto x.

Demonstração. Dado um conjunto x, suponha que para cada $u \in x$ o conjunto $F(u)$ está bem definido. Seja $f = \{(k, F(k)) : k \in x\}$. Temos $F(x) = G(F \restriction x) = G(f)$, logo $F(x)$ está bem definido. Segue por $\in$-indução que $F(a)$ está bem definido para todo conjunto a. □

9 MODELOS

No presente capítulo trabalhamos com conceitos apresentados nos capítulos anteriores, porém extrapolados num certo aspecto. Usamos a palavra "coleção" num sentido intuitivo similar à noção de conjunto, porém cujos elementos não precisam ser necessariamente conjuntos.

Neste capítulo nos referimos sempre a teorias axiomáticas em linguagens de primeira ordem baseadas em Lógica Clássica, e assumimos que este não é o primeiro contato do leitor com essa lógica.

9.1 LINGUAGEM E LÓGICA CLÁSSICA

Uma *linguagem* $\mathcal{L}$ consiste de uma coleção de *símbolos de predicados* P_i, *símbolos de funções* F_j e *símbolos de constantes* C_k, sendo que cada símbolo de predicado e de função tem uma aridade finita, isto é, um número finito de argumentos. As fórmulas na linguagem $\mathcal{L}$ são sequências finitas de símbolos de $\mathcal{L}$ e símbolos lógicos (variáveis, conectivos, quantificadores, parênteses, igualdade) que satisfazem determinadas regras de formação.

A Lógica Clássica se baseia nos princípios da Não Contradição e do Terceiro Excluído, apresentados a seguir.

Princípio da Não Contradição. Para toda sentença φ na linguagem $\mathcal{L}$, não podem ambas as sentenças φ e $\neg\varphi$ serem verdadeiras.

Princípio do Terceiro Excluído. Para toda sentença φ na linguagem $\mathcal{L}$, ao menos uma das sentenças φ ou $\neg\varphi$ é verdadeira.

Uma *regra de inferência* é uma maneira de concluir determinadas fórmulas a partir de outras. Essencialmente é um modo de traduzir a linguagem natural para a linguagem $\mathcal{L}$. Nesse contexto, a linguagem natural funciona como uma *metalinguagem*, isto é, uma linguagem que se refere às fórmulas de $\mathcal{L}$ como objetos. A seguir apresentamos alguns exemplos de regras de inferência.

Modus Ponens (ou Eliminação da Implicação)**.** Dadas duas fórmulas φ e ψ numa linguagem $\mathcal{L}$, se temos φ e $\varphi \to \psi$, então concluímos ψ.

Introdução da Implicação. Dadas duas fórmulas φ e ψ numa linguagem $\mathcal{L}$, se a partir de φ obtemos ψ, então concluímos $\varphi \to \psi$.

As regras de inferência Modus Ponens e Introdução da Implicação estão por trás das demonstrações diretas.

Modus Tollens. Dadas duas fórmulas φ e ψ numa linguagem $\mathcal{L}$, se temos $\neg\,\psi$ e $\varphi \,\rightarrow\, \psi$, então concluímos $\neg\,\varphi$.

Introdução da Negação. Dada uma fórmula φ numa linguagem $\mathcal{L}$, se a partir de φ obtemos uma contradição, então concluímos $\neg\,\varphi$.

Dupla Negação. Dada uma fórmula φ numa linguagem $\mathcal{L}$, se temos $\neg\,(\neg\,\varphi)$, então concluímos φ.

As regras de inferência Modus Tollens e Dupla Negação estão por trás das demonstrações pela contrapositiva, e juntamente com a Introdução da Negação das demonstrações por absurdo.

Eliminação da Disjunção. Dadas três fórmulas φ, ψ e χ numa linguagem $\mathcal{L}$, se temos $\varphi \,\vee\, \psi$, a partir de φ obtemos χ e a partir de ψ obtemos χ, então concluímos χ.

A regra de inferência Eliminação da Disjunção está por trás das demonstrações por separação em casos.

Introdução da Conjunção. Dadas duas fórmulas φ e ψ numa linguagem $\mathcal{L}$, se temos φ e ψ, então concluímos $\varphi \,\wedge\, \psi$.

A regra de inferência Introdução da Conjunção está por trás das demonstrações por partes.

Generalização. Dada uma fórmula $\varphi(x,p)$ numa linguagem $\mathcal{L}$ com variável livre x, se obtemos $\varphi(u,p)$ para um u genérico, então concluímos $\forall x\ \varphi(x,p)$.

A regra de inferência Generalização aparece, por exemplo, quando provamos que um conjunto a está contido num conjunto b. Tomamos um $u \in a$ qualquer e mostramos que $u \in b$, isto é, que $u \in a \,\rightarrow\, u \in b$. Como o u é qualquer, a Generalização nos fornece $\forall x\ (x \in a \,\rightarrow\, x \in b)$, isto é, $a \subseteq b$.

Há outras regras de inferência que podem ser consideradas, tais como, dadas duas fórmulas φ e ψ numa linguagem $\mathcal{L}$: de ambos φ ou ψ concluímos $\varphi \vee \psi$ (Introdução da Disjunção); de $\varphi \wedge \psi$ concluímos ambos φ e ψ (Eliminação da Conjunção); dentre outras. De fato, podemos assumir somente as regras de inferência Modus Ponens e Generalização que as demais decorrem dessas e de axiomas lógicos.

9.2 SINTAXE

Definição 9.1. Dadas uma coleção de fórmulas Γ e uma fórmula φ numa linguagem $\mathcal{L}$, dizemos que φ é uma *consequência sintática* de Γ, ou que Γ *deduz* φ, ou que φ é *dedutível* de Γ, e escrevemos $\Gamma \vdash \varphi$, se existe uma sequência finita de fórmulas $\langle \varphi_i : i \leq n \rangle$ na linguagem $\mathcal{L}$, $n \in \omega$, tal que φ_n é φ e cada φ_i pertence a Γ ou pode ser obtido a partir de $\langle \varphi_j : j < i \rangle$ por meio de alguma regra de inferência. A sequência de fórmulas $\langle \varphi_i : i \leq n \rangle$ é chamada de *dedução formal* de φ, ou simplesmente de *dedução* de φ. Caso contrário, escrevemos $\Gamma \nvdash \varphi$. Se Γ for vazio, ao invés de $\Gamma \vdash \varphi$ escrevemos simplesmente $\vdash \varphi$.

Uma *teoria axiomática* Θ consiste de uma linguagem $\mathcal{L}$ e de uma coleção de fórmulas Γ na linguagem $\mathcal{L}$ (os axiomas). É comum representarmos a teoria pela sua coleção de axiomas. Não consideramos os axiomas lógicos como axiomas da teoria, sendo admitidos como fatos primitivos.

Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, se $\Theta \vdash \varphi$ dizemos que φ é um *teorema* de Θ. Note que todas as demonstrações dos teoremas da teoria podem ser reduzidas a deduções formais. Os teoremas que não tratam de objetos da teoria, mas de fórmulas, deduções, etc., são chamados de *metateoremas*. É extremamente comum, como o leitor já deve ter percebido, escrevermos teoremas na linguagem natural, no nosso caso a Língua Portuguesa.

Exemplo 9.1. Em qualquer teoria axiomática, os axiomas são, trivialmente, teoremas cujas deduções têm comprimento 1. A afirmação "Em qualquer teoria axiomática, os axiomas são teoremas." é um metateorema, e segue de que se φ pertence a Γ, então $\Gamma \vdash \varphi$.

Exemplo 9.2. Em ZFC, os corolários 5.8.2 e 6.19.1 são metateoremas, uma vez que **Ord** e **Card** não são objetos de ZFC. O que poderíamos dizer dentro de ZFC é "Não existe o conjunto de todos os ordinais." e "Não existe o conjunto de todos os cardinais.".

Teorema 9.1. Dadas uma coleção de fórmulas Γ e uma fórmula φ numa linguagem $\mathcal{L}$, temos que $\Gamma \vdash \psi \to \varphi$ se e somente se $\Gamma \cup \{\psi\} \vdash \varphi$.

Demonstração. ($\Rightarrow$) É imediato de Modus Ponens.
($\Leftarrow$) Segue da Introdução da Implicação. $\square$

Teorema 9.2. Dadas uma coleção de fórmulas Γ e uma fórmula φ numa linguagem $\mathcal{L}$, temos que se $\Gamma \vdash \varphi$ então existe Γ_0 finito contido em Γ tal que $\Gamma_0 \vdash \varphi$.

Demonstração. Note que se $\Gamma \vdash \varphi$, mesmo se Γ for infinito, somente um número finito de fórmulas de Γ aparecem na dedução formal de φ, de forma que existe Γ_0 finito contido em Γ tal que $\Gamma_0 \vdash \varphi$. $\square$

Definição 9.2. Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, representamos a teoria formada por Θ acrescida do axioma φ por $\Theta + \varphi$.

Exemplo 9.3. ZFC é a teoria ZF + AC.

Definição 9.3. Dizemos que uma teoria axiomática Θ é *consistente* se não existe uma fórmula φ na linguagem de Θ tal que $\Theta \vdash \varphi$ e $\Theta \vdash \neg\varphi$, e escrevemos $\mathrm{Con}(\Theta)$.

Definição 9.4. Dizemos que uma teoria axiomática Θ é *completa* se para toda fórmula φ na linguagem de Θ temos $\Theta \vdash \varphi$ ou $\Theta \vdash \neg\varphi$.

Teorema 9.3. Dada uma teoria axiomática Θ, temos que Θ é consistente se e somente se existe uma fórmula φ na linguagem de Θ tal que $\Theta \nvdash \varphi$.

Demonstração. ($\Rightarrow$) Dada uma fórmula φ, como Θ é consistente, temos $\Theta \nvdash \varphi$ ou $\Theta \nvdash \neg\varphi$. ($\Leftarrow$) Suponha que Θ não é consistente e seja ψ uma fórmula tal que $\Theta \vdash \psi$ e $\Theta \vdash \neg\psi$. Temos $\Theta \vdash \psi \wedge \neg\psi$, e como $\psi \wedge \neg\psi$ se trata de uma contradição, para toda fórmula ϕ temos que $\Theta \vdash (\psi \wedge \neg\psi) \rightarrow \phi$, e portanto $\Theta \vdash \phi$. O resultado segue da contrapositiva. $\square$

Definição 9.5. Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, dizemos que φ pode ser *provada* em Θ, ou que φ é *provável* em Θ, se $\Theta \vdash \varphi$, e dizemos que φ pode ser *refutada* em Θ, ou que φ é *refutável* em Θ, se $\Theta \vdash \neg\varphi$.

Definição 9.6. Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, dizemos que φ é *consistente* com Θ se $\Theta \nvdash \neg\varphi$, isto é, se φ não pode ser refutada em Θ.

Teorema 9.4. Dadas uma teoria axiomática Θ e uma fórmula φ cosistente com Θ, temos que $\mathrm{Con}(\Theta)$ implica $\mathrm{Con}(\Theta + \varphi)$.

Demonstração. De fato, se ψ é uma fórmula tal que $\Theta + \varphi \vdash \psi$ e $\Theta + \varphi \vdash \neg\psi$, então $\Theta \vdash \varphi \rightarrow \psi$ e $\Theta \vdash \varphi \rightarrow \neg\psi$, gerando um absurdo e portanto $\Theta \vdash \neg\varphi$, isto é, φ não é consistente com Θ. O resultado segue da contrapositiva. $\square$

Definição 9.7. Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, dizemos que φ é *independente* de Θ, ou que φ é *indecidível* em Θ, se $\Theta \nvdash \varphi$ e $\Theta \nvdash \neg\varphi$, isto é, se φ não pode ser provada nem refutada em Θ, isto é, se ambas φ e $\neg\varphi$ são consistentes com Θ.

9.3 SEMÂNTICA

Definição 9.8. Um *modelo* numa linguagem $\mathcal{L}$ é uma estrutura $\mathfrak{A} = (\mathcal{A}, \mathcal{I})$ em que $\mathcal{A}$ é chamado de *universo de discurso* e $\mathcal{I}$ é a *interpretação* dos símbolos de $\mathcal{L}$, isto é, para cada símbolo de predicado P_i em $\mathcal{L}$ de aridade m associa uma relação m-ária $P_i^{\mathfrak{A}}$ em $\mathcal{A}^m$, para cada símbolo de função F_j em $\mathcal{L}$ de aridade n associa uma função n-ária $F_j^{\mathfrak{A}}$ de $\mathcal{A}^n$ em $\mathcal{A}$ e para cada símbolo de constante C_k em $\mathcal{L}$ associa um elemento $C_k^{\mathfrak{A}}$ de $\mathcal{A}$. Dada uma fórmula φ na linguagem $\mathcal{L}$, denotamos por $\varphi^{\mathfrak{A}}$ a fórmula φ *interpretada* por $\mathfrak{A}$, isto é, quando os símbolos de $\mathcal{L}$ que aparecem em φ são substituídos por suas respectivas interpretações em $\mathfrak{A}$ e os quantificadores são restritos a $\mathcal{A}$.

Definição 9.9. Dadas uma teoria axiomática Θ, uma fórmula φ e um modelo $\mathfrak{A} = (\mathcal{A}, \mathcal{I})$ na linguagem de Θ, dizemos que $\mathfrak{A}$ *satisfaz* φ, ou que φ é *satisfatível* em $\mathfrak{A}$, e escrevemos $\mathfrak{A} \vDash \varphi$, se $\varphi^{\mathfrak{A}}$ é verificada em $\mathfrak{A}$, caso contrário escrevemos $\mathfrak{A} \nvDash \varphi$. Se $\mathfrak{A}$ satisfaz todos os axiomas de Θ, então dizemos que $\mathfrak{A}$ é um *modelo* de Θ e escrevemos $\mathfrak{A} \vDash \Theta$, caso contrário escrevemos $\mathfrak{A} \nvDash \Theta$. Além disso, dizemos que φ é uma *consequência semântica* de Θ, ou que Θ *satisfaz* φ, ou que φ é *satisfatível* em Θ, e escrevemos $\Theta \vDash \varphi$, se para todo modelo $\mathfrak{M} \vDash \Theta$ temos $\mathfrak{M} \vDash \varphi$, caso contrário escrevemos $\Theta \nvDash \varphi$.

Exemplo 9.4. Considere a Aritmética de Peano PA apresentada na Seção 3.4, cuja linguagem é $\mathcal{L} = \{s, \theta\}$ em que s é um símbolo de função unária, θ é um símbolo de constante e cujos axiomas são:

(i) $\neg\exists x\ (s(x) = \theta)$;

(ii) $\forall x\ \forall y\ (s(x) = s(y)\ \rightarrow\ x = y)$;

(iii) $\forall p\ ((\varphi(\theta, p)\ \wedge\ \forall x\ (\varphi(x, p)\ \rightarrow\ \varphi(s(x), p)))\ \rightarrow\ \forall x\ \varphi(x, p))$.

A teoria PA possui um modelo $\mathfrak{N}$ em ZFC em que o universo de discurso é $\mathcal{A} = \omega$ e os símbolos de $\mathcal{L}$ são interpretados como $s^{\mathfrak{N}} = \{(k, \mathcal{S}(k)) : k \in \omega\}$ e $\theta^{\mathfrak{N}} = \varnothing$. Note que PA, da maneira como foi formulada, possui infinitos axiomas, uma vez que (iii) é um esquema de axiomas.

Exemplo 9.5. Considere a teoria P cuja linguagem é $\mathcal{L} = \{\leq\}$ em que $\leq$ é um símbolo de predicato binário e cujos axiomas são:

(i) $\forall x\ (x \leq x)$;

(ii) $\forall x\ \forall y\ ((x \leq y\ \wedge\ y \leq x)\ \rightarrow\ x = y)$;

(iii) $\forall x\ \forall y\ \forall z\ ((x \leq y\ \wedge\ y \leq z)\ \rightarrow\ x \leq z)$.

Essa teoria é chamada de *ordem*. Dois possíveis modelos $\mathfrak{O}_0$ e $\mathfrak{O}_1$ de P dentro de ZFC são, considerando como universo de discurso de ambos $\mathcal{A} = \omega$, interpretar o símbolo de $\mathcal{L}$ como:

- $\leq^{\mathfrak{O}_0} = \{(k, \ell) \in \omega \times \omega : k \leq_+ \ell\}$;
- $\leq^{\mathfrak{O}_1} = \{(k, \ell) \in \omega \times \omega : k \leq_\bullet \ell\}$.

Considere a fórmula φ "$\forall x\ \forall y\ (x \leq y\ \vee\ y \leq x)$". Temos $\mathfrak{O}_0 \vDash \varphi$, mas $\mathfrak{O}_1 \vDash \neg\varphi$.

Exemplo 9.6. Considere a teoria R cuja linguagem é $\mathcal{L} = \{+, \cdot, \overline{0}\}$ em que $+$ e $\cdot$ são símbolos de funções binárias, $\overline{0}$ é um símbolo de constante e cujos axiomas são:

(i) $\forall x\ \forall y\ \forall z\ ((x+y)+z = x+(y+z))$;

(ii) $\forall x\ \forall y\ (x+y = y+x)$;

(iii) $\forall x\ (x+\overline{0} = x)$;

(iv) $\forall x\ \exists u\ (x+u = \overline{0})$;

(v) $\forall x\ \forall y\ \forall z\ ((x\cdot y)\cdot z = x\cdot(y\cdot z))$;

(vi) $\forall x\ \forall y\ \forall z\ (x\cdot(y+z) = (x\cdot y)+(x\cdot z))$;

(vii) $\forall x\ \forall y\ \forall z\ ((x+y)\cdot z = (x\cdot z)+(y\cdot z))$.

Essa teoria é chamada de *anel*. Dois possíveis modelos $\mathfrak{R}_0$ e $\mathfrak{R}_1$ de R dentro de ZFC são, tomando um conjunto infinito a, considerar como universos de discursos de $\mathfrak{R}_0$ e de $\mathfrak{R}_1$ respectivamente $\mathcal{A}_0 = \mathcal{P}(a)$ e $\mathcal{A}_1 = \mathcal{P}_{<\omega}(a)$, e interpretar os símbolos de $\mathcal{L}$ como:

- $+^{\mathfrak{R}_i} = \{((k,\ell), k \triangle \ell) : (k,\ell) \in \mathcal{A}_i \times \mathcal{A}_i\}$ para $i \in 2$;
- $\cdot^{\mathfrak{R}_i} = \{((k,\ell), k \cap \ell) : (k,\ell) \in \mathcal{A}_i \times \mathcal{A}_i\}$ para $i \in 2$;
- $\overline{0}^{\mathfrak{R}_i} = \varnothing$ para $i \in 2$.

Considere a fórmula φ "$\exists u\ \forall x\ (u\cdot x = x)$". Temos $\mathfrak{R}_0 \vDash \varphi$ (basta tomar $u = a$), mas $\mathfrak{R}_1 \vDash \neg\varphi$.

Exemplo 9.7. Considere o modelo $\mathfrak{V}$ na linguagem $\mathcal{L} = \{\in\}$ cujo universo de discurso é o Universo de Von Neumann $\mathcal{V}$ e a interpretação da pertinência é dada pela relação♦ $\in^{\mathfrak{V}} = \{(x,y) : x \in y\}$. Obtemos assim um modelo $\mathfrak{V} \vDash$ ZFC. Observe no entanto que esse modelo não está em ZFC, uma vez que $\mathcal{V}$ e $\in^{\mathfrak{V}}$ são classes próprias.

Teorema 9.5. Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, se existe um modelo $\mathfrak{M}$ de Θ tal que $\mathfrak{M} \vDash \Theta + \varphi$, então $\Theta \nvdash \neg\varphi$.

Note que o Teorema 9.5 fornece uma estratégia para verificar quando que uma fórmula φ é consistente com uma teoria Θ.

Exemplo 9.8. Considere uma ordem P e a fórmula φ "$\forall x\ \forall y\ (x \leq y \vee y \leq x)$". Como existem modelos $\mathfrak{A}$ e $\mathfrak{B}$ tais que $\mathfrak{A} \vDash \mathrm{P} + \varphi$ e $\mathfrak{B} \vDash \mathrm{P} + \neg\varphi$, segue que $\mathrm{P} \nvdash \varphi$ e $\mathrm{P} \nvdash \neg\varphi$, isto é, φ é indecidível em P.

Exemplo 9.9. Considere um anel R e a fórmula φ "$\exists u\ \forall x\ (u\cdot x = x)$". Como existem modelos $\mathfrak{A}$ e $\mathfrak{B}$ tais que $\mathfrak{A} \vDash \mathrm{R} + \varphi$ e $\mathfrak{B} \vDash \mathrm{R} + \neg\varphi$, segue que $\mathrm{R} \nvdash \varphi$ e $\mathrm{R} \nvdash \neg\varphi$, isto é, φ é indecidível em R.

9.4 TEOREMAS DE GÖDEL

Teorema 9.6 (Teorema da Completude de Gödel)**.** Dada uma teoria Θ, se Θ é consistente, então existe um modelo $\mathfrak{M}$ de Θ.

Dadas uma teoria axiomática Θ e uma fórmula φ na linguagem de Θ, decorre do Teorema Da Completude de Gödel que se $\Theta \vDash \varphi$ então $\Theta \vdash \varphi$. De fato, como $\Theta \vDash \varphi$, então para todo modelo $\mathfrak{M}$, se $\mathfrak{M} \vDash \Theta$ então $\mathfrak{M} \vDash \varphi$, logo $\mathfrak{M} \nvDash \neg\varphi$, isto é, $\mathfrak{M} \nvDash \Theta + \neg\varphi$, e portanto $\Theta + \neg\varphi$ não tem modelo. Pelo Teorema da Completude de Gödel, segue que $\Theta + \neg\varphi$ não é consistente, logo $\Theta + \neg\varphi \vdash \varphi$, e segue que $\Theta \vdash \neg\varphi \to \varphi$. Como $(\neg\varphi \to \varphi) \to \varphi$ é uma tautologia, segue que $\Theta \vdash (\neg\varphi \to \varphi) \to \varphi$, e por Modus Ponens temos $\Theta \vdash \varphi$.

Definição 9.10. Dada uma teoria Θ, dizemos que Θ é *forte o suficiente para abranger a Aritmética de Peano* se existe um modelo $\mathfrak{M}$ em Θ tal que $\mathfrak{M} \vDash \mathrm{PA}$.

Exemplo 9.10. Conforme mostrado no Exemplo 9.4, ZFC é forte o suficiente para abranger a Aritmética de Peano.

Teorema 9.7 (Primeiro Teorema da Incompletude de Gödel)**.** Se Θ é uma teoria consistente forte o suficiente para abranger a Aritmética de Peano, então Θ não é completa.

Teorema 9.8 (Segundo Teorema da Incompletude de Gödel)**.** Se Θ é uma teoria consistente forte o suficiente para abranger a Aritmética de Peano, então Θ não demonstra a própria consistência. Equivalentemente, se uma teoria Θ forte o suficiente para abranger a Aritmética de Peano demonstra a própria consistência, então Θ é inconsistente.

Decorre do Primeiro Teorema da Incompletude de Gödel que se ZFC é consistente, então é esperado que existam afirmações indecidíveis dentro de ZFC, como por exemplo CH. Além disso, independente de quantos axiomas forem acrescentados a ZFC mantendo sua consistência, ainda haverá afirmações indecidíveis dentro da teoria. Ainda, decorre do Segundo Teorema da Incompletude de Gödel que se ZFC é consistente, então ZFC não prova a própria consistência, implicando na inexistência de modelos de ZFC dentro de ZFC.

CONSIDERAÇÕES FINAIS

O objetivo inicial do Projeto de TCC era chegar em Forcing e usá-lo para provar as independências da Hipótese do Continuum de ZFC e do Axioma da Escolha de ZF, aprofundando os estudos num futuro mestrado. Não chegamos ao Forcing, mas ainda há o plano de estudá-lo no mestrado, dentre outras coisas de Teoria dos Conjuntos e Fundamentos da Matemática, bem como de outras áreas de interesse, tais como Topologia e Análise.

REFERÊNCIAS

CONIGLIO, M. E. Um curso de teoria de modelos. *Notas de aula. Disponível em <http://www.researchgate.net/profile/Marcelo_Coniglio/publication/266481339_Um_curso_de_Teoria_de_Modelos/links/55245cc20cf2b123c5173b59.pdf>*, 1999.

HALBEISEN, L. J. *Combinatorial Set Theory: With a Gentle Introduction to Forcing*. [S.l.]: Springer, 2012. (Springer Monographs in Mathematics).

HRBACEK, K.; JECH, T. *Introduction to Set Theory*. 3nd ed., rev. and expanded. ed. [S.l.]: Marcel Dekker, 1999. (Monographs and Textbooks in Pure and Applied Mathematics).

JECH, T. *Set Theory*. 3nd millennium ed., rev. and expanded. ed. [S.l.]: Springer, 2002. (Springer Monographs in Mathematics).

KUNEN, K. *Set Theory, An Introduction to Independence Proofs*. [S.l.]: Elsevier, 1980. (Studies in Logic and the Foundations of Mathematics).

ÍNDICE REMISSIVO