Teoria Axiomática de Conjuntos: Uma Introdução

Marcelo Esteban Coniglio
GTAL, Departmento de Filosofia
Universidade Estadual de Campinas
P.O. Box 6133, 13081-970
Campinas, SP, Brazil
E-mail: coniglio@cle.unicamp.br

Abstract

O presente texto corresponde às notas de aula do curso *HF005-Teoria de Conjuntos*, do Programa de Pós-Graduação em Filosofia da UNICAMP, que ministrei no segundo semestre de 1997. Trata-se principalmente de uma adaptação do livro *Axiomatic Set Theory*, de P. Suppes (Dover, 1972). Alguns tópicos (principalmente, teoria de ordinais e de cardinais) foram adaptados do livro *Set Theory: an Introduction to Large Cardinals*, de F.R. Drake (North Holland, 1974).

Contents

Introdução

A Teoria de Conjuntos (TC) ocupa um lugar privilegiado dentre as disciplinas da Matemática moderna: todas as entidades estudadas na matemática (com algumas exceções) podem ser consideradas conjuntos. Portanto, as questões acerca da natureza da matemática são basicamente questões acerca de conjuntos.

A TC foi iniciada a partir das pesquisas de Georg Cantor em 1870 sobre a teoria das séries infinitas em Análise; a partir destes trabalhos, Cantor foi levado a considerar conjuntos infinitos ou classes de caráter arbitrário. Mas o que são os conjuntos? A nossa idéia intuitiva os define como coleções de objetos. Segundo Cantor, "um conjunto é uma coleção, considerada como um todo, de objetos distintos e definidos da nossa intuição ou pensamento. Os objetos são chamados de elementos do conjunto". Os paradoxos surgidos logo no início do estudo da teoria mostraram que a concepção "ingênua" de Cantor não podia formar uma base satisfatória para a TC, e muito menos para a Matemática. Isto levou a uma reformulação dos princípios básicos da teoria. Os paradoxos apareceram principalmente pelo uso indiscriminado das noções de conjunto, número cardinal e ordinal, etc. Um paradoxo consiste na derivação no sistema lógico de φ e $\neg\varphi$ para alguma afirmação φ, ou então a derivação de uma afirmação da forma $\varphi \leftrightarrow \neg\varphi$. O primeiro paradoxo foi descoberto pelo próprio Cantor em 1895 e não foi publicado imediatamente, mas foi redescoberto por Burali-Forti em 1897, que também não conseguiu fornecer uma solução. O paradoxo surgiu com relação à teoria dos ordinais, num estágio relativamente avançado da teoria, e não foi levado muito a sério. A aparição em 1902 do célebre paradoxo de Russell fez mudar as coisas, pois ele surge no primeiro estágio da teoria: dado que, pelo axioma de compreensão, podemos definir os conjuntos $\{x : \varphi(x)\}$, onde $\varphi(x)$ é uma fórmula denotando uma propriedade, então é lícito formular o conjunto $A = \{x : x \notin x\}$ (considerando $\varphi(x) \equiv_{def} x \notin x$). Logo, podemos nos perguntar se é o caso que $A \in A$ ou não é o caso que $A \in A$, obtendo: $A \in A$ sse $A \notin A$!! Este fato causou uma verdadeira revolução no méio acadêmico ligado à fundamentação da matemática, obrigando Dedekind a suspender a publicação do seu ensáio sobre a natureza dos números. Enquanto isso, Frege acabara de publicar sua obra prima, fruto de décadas de esforços, admitindo por fim que um dos pilares do seu edifício tinha sido sacudido por Russell.

Os paradoxos tem uma origem antiga: o exemplo clássico é o *Paradoxo do Mentiroso* (Epimênides), que pode ser formulado simplesmente como: "Esta frase é falsa". É claro que supor a verdade ou a falsidade da frase leva a uma contradição. O paradoxo de Grelling-Nelson (1908) diz o seguinte: defina como *heterológicos* os adjetivos tais que eles mesmos não satisfazem a propriedade que eles denotam. Por exemplo, "inglês", "azul" ou "frio" são heterológicos, enquanto que "polissilábico" ou "português" não o são; em símbolos, dado um adjetivo "S", temos que "S" é heterológico sse "S" não é (não satisfaz) S. Logo, "heterológico" é heterológico sse "heterológico" não é heterológico. O paradoxo de Richard (1905) diz o seguinte: considere os números reais entre 0 e 1 que podem ser definidos por um número finito (não limitado) de palavras em português: por exemplo, "ponto cinco", "o maior número tal que elevado ao quadrado e multiplicado por três é igual a dois". Os números definidos desta maneira podem ser enumerados (só temos uma quantidade enumerável de frases de tamanho finito). Considere o seguinte número: "o número real entre 0 e 1 cuja n-ésima casa decimal é três se a n-ésima casa decimal do n-ésimo número é cinco, e é cinco em caso contrário". Logo, esta frase define um número diferente de todos os números da lista, uma contradição (este paradoxo é baseado no método diagonal de Cantor para provar que o conjunto dos números reais não é enumerável). Ramsey distingue dois tipos de paradoxos: os *semânticos* e os *lógicos*. Todos os paradoxos mencionados acima (com exceção do paradoxo de Russell) são semânticos; dentre os paradoxos lógicos podemos mencionar o paradoxo de Russell, o de Cantor e o de Burali-Forti. O paradoxo de Cantor (1899) diz: considere U o conjunto de todos os conjuntos. Logo, o conjunto $\mathcal{P}(U)$ das partes de U tem cardinal estritamente maior do que o cardinal de U, o que contradiz a hipótese de que U seja o maior conjunto. O paradoxo de Burali-Forti (1897) diz: o conjunto bem ordenado W de todos os ordinais tem um ordinal maior que todo elemento de W, portanto maior que todo ordinal.

1 Teoria Cumulativa de Tipos

Todos os paradoxos vistos têm a mesma origem: a auto-referência. No caso dos paradoxos em TC, podemos solucionar o problema considerando que os conjuntos são formados em etapas ou estágios; assim, um conjunto só pode ser criado a partir de conjuntos que já foram definidos ou criados anteriormente. Isto dá origem à *teoria simples de tipos*:

Nível 0: alguns *indivíduos* (urelemente), sem propriedades específicas.
Nível 1: todas as coleções formadas por indivíduos.
Nível 2: todas as coleções formadas por elementos no nível 1, etc.

Assim, se os indivíduos são os números naturais, então 3 é um conjunto no nível 0, $\{1, 2\}$ está no nível 1, e $\{\{2\}, \{4, 6\}\}$ está no nível 2. As questões são: (a) qual é o problema em considerar $\{1, \{1\}\}$ como conjunto? (b) o conjunto vazio $\emptyset$, assumindo que seja um indivíduo, seria diferente nas diferentes etapas em que pudesse aparecer? Com relação à (a), é óbvio que o modelo é restritivo demais, logo consideramos a *teoria cumulativa de tipos*:

Nível 0: alguns indivíduos.
Nível 1: todas as coleções formadas por indivíduos.
Nível 2: todas as coleções formadas por elementos no nível 0 ou 1.
Em cada nível, considerar as coleções cujos elementos estão em níveis anteriores.

Logo, $\{1, \{1\}\}$ aparece no nível 2, no nosso exemplo. Com relação à (b), temos que assumir que uma vez que um conjunto aparece num nível, toda aparição posterior *é a mesma*. As questões seguintes são: quantos indivíduos deveriam ser tomados? os níveis têm final? Com relação à primeira questão, parece claro que $\emptyset$ deveria ser considerado o único indivíduo; isto equivale a não tomar indivíduos (logo, $\emptyset$ será o único conjunto do nível 1). Com relação à segunda questão, a resposta é "não". Se existisse um máximo nível α, é claro que poderiamos criar um nível adicional $\alpha+1$ com os conjuntos que temos definidos, uma contradição.

2 Axiomas Básicos da Teoria de Conjuntos

A primeira axiomatização de TC foi dada por Zermelo em 1908, e modificada por Fraenkel em 1922, dando origem ao sistema Zermelo-Fraenkel (ZF). Existem muitos outros sistemas, como o de von Neumann-Gödel-Bernays (NGB) e o de Kelley-Morse (KM). Estes últimos usam classes juntamente com conjuntos. Uma *classe* pode ser pensada como uma coleção "enorme", de maneira que os conjuntos viriam ser classes "pequenas". Por exemplo,

$$\mathcal{V} = \{x \ : \ x = x\}$$

é a coleção de todos os conjuntos, chamada de *classe universal*. $\mathcal{V}$ é uma *classe própria*, isto é, ela não é um conjunto, portanto não aparece em nenhum nível da hierarquia cumulativa. Se todos os membros de uma classe aparecem antes de um dado nível, então a classe é um conjunto nesse nível. Neste curso estudaremos apenas ZF.

A formulações ZF de TC é realizada numa linguagem de primeira ordem, utilizando constantes para os (eventuais) indivíduos, duas relações binárias ($=$, $\in$), os conectivos $\vee$, $\wedge$, $\neg$, $\rightarrow$, $\leftrightarrow$, e os quantificadores $\forall$ (*para todo*) e $\exists$ (*existe*), junto com um repertório enumerável de variáveis. As variáveis são denotadas: a, b, $\ldots$, x, y, z (com ou sem índices). Como é usual, as fórmulas $\neg(x = y)$ e $\neg(x \in y)$ serão denotadas por $(x \neq y)$ e $(x \notin y)$, respectivamente.

Começamos enunciando o primeiro axioma de ZF:

Axioma de Extensionalidade:

[A1] $(\forall z)(z \in x \leftrightarrow z \in y) \rightarrow (x = y)$

Aqui é evidenciada a intenção de que, quando uma coleção aparecer em diferentes níveis, ela seja considerada como sendo a mesma; por outro lado, é estabelecido que o que interessa com relação aos conjuntos são os seus elementos, mais do que *o que eles são*. Observe que a implicação recíproca $(x = y) \rightarrow (\forall z)(z \in x \leftrightarrow z \in y)$ é logicamente válida.

Axioma de Compreensão ou Separação:

[A2] $(\exists y)(\forall x)(x \in y \leftrightarrow (x \in a \wedge \varphi(x)))$

Isto significa que estamos "separando" alguns elementos de a, exatamente aqueles que satisfazem a propriedade φ. Aqui, $\varphi(x)$ é uma fórmula onde x aparece livre, podendo aparecer outras variáveis livres em φ (os *parâmetros* do conjunto criado), mas **a variável y não aparece livre em φ.** O axioma de compreeensão tenta tomar, em cada estágio, todos os conjuntos já criados, para formar os conjuntos do nível seguinte. O axioma é limitado, pois só tomamos os conjuntos formados pelas fórmulas φ. Observe que [A2] é um *axioma-esquema*, isto é, cada fórmula φ determina um axioma. A condição sobre y não ocorrer livre em φ está relacionada com a auto-referência, e é fundamental para evitar o paradoxo de Russell; caso contrário, podemos considerar $(\exists a)(\forall x)(x \in a \leftrightarrow x = b)$ (esta fórmula é demonstrável em ZF, como veremos depois de incorporar outros axiomas) e $\varphi(x, y) \equiv_{def} x \notin y$ em [A2]; logo, teremos: $x \in y \leftrightarrow (x \in a \wedge x \notin y)$, e então $x \in a \rightarrow (x \in y \leftrightarrow x \notin y)$ para todo x. Portanto, tomando a como acima, teremos: $x = b \rightarrow (x \in y \leftrightarrow x \notin y)$ para todo x, donde, tomando b no lugar de x, obtemos $b \in y \leftrightarrow b \notin y$, contradição. Como provaremos na Proposição 11.1, o axioma [A2] será dedutível dos outros axiomas de ZF (especificamente, [A2] é um caso particular do axioma [A7], a ser introduzido na Seção 11). Porém, na primeira parte deste texto faremos um uso pesado do axioma [A2] sem precisar usar por enquanto o axioma mais forte [A7].

A partir de agora adotaremos a seguinte notação: $\{x : \varphi\}$ é um (meta)termo s em que toda ocorrência de x é limitada (φ é uma fórmula). Logo,

$s = t$ denota $(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge z = t)$;
$t = s$ denota $(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge t = z)$;
$s \in t$ denota $(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge z \in t)$;
$t \in s$ denota $(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge t \in z)$

onde z não ocorre em φ nem em t.

Assim, por exemplo, se $s \equiv_{def} \{x : \varphi(x)\}$ e $t \equiv_{def} \{x : \phi(x)\}$ então $s \in t$ denota a fórmula $(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge z \in t)$. Por sua vez, $z \in t$ denota a fórmula $(\exists u)((\forall x)(x \in u \leftrightarrow \phi) \wedge z \in u)$, portanto $s \in t$ denota a fórmula

$$(\exists z)((\forall x)(x \in z \leftrightarrow \varphi) \wedge (\exists u)((\forall x)(x \in u \leftrightarrow \phi) \wedge z \in u)).$$

Se $(\exists y)(\forall x)(x \in y \leftrightarrow \varphi(x))$ é demonstrado a partir dos axiomas, dizemos que $\{x : \varphi(x)\}$ é *legitimado*. Logo, o axioma de separação diz que o (meta)termo

$$\{x : x \in a \wedge \varphi(x)\}$$

é legitimado. Note que este (meta)termo depende de a (e das variáveis diferentes de x que ocorrem livres em $\varphi(x)$).

Observação 2.1 Se $s_i \equiv_{def} \{x : \varphi_i(x)\}$ é legitimado ($i = 1, \ldots, n$), então $(\forall x_1) \cdots (\forall x_n)\phi(x_1, \ldots, x_n)$ implica $\phi(s_1, \ldots, s_n)$, onde $\phi(s_1, \ldots, s_n)$ é a expressão obtida de ϕ substituindo x_i por s_i (eliminando *a posteriori* os s_i aplicando as regras de redução definidas acima). Portanto, se $s \equiv_{def} \{x : \varphi(x)\}$ é legitimado, então de $x \in y \leftrightarrow \phi(x)$ deduzimos $s \in y \leftrightarrow (\exists z)((\forall x)(x \in z \leftrightarrow \varphi(x)) \wedge \phi(z))$ e $s \in y \leftrightarrow \phi(s)$ (lembrando que devemos eliminar s para obter fórmulas a partir dessas expresões). ■

Proposição 2.2 *Suponha que* $s \equiv_{def} \{x \ : \ \varphi(x)\}$ *é legitimado; logo, são demonstráveis:*

$x \in s \leftrightarrow \varphi(x)$, $(s = y) \leftrightarrow (\forall x)(x \in s \leftrightarrow x \in y)$ *e*
$(s = y) \leftrightarrow (\forall x)(x \in y \leftrightarrow \varphi(x))$.

Demonstração: Sejam $\alpha \equiv_{def} (\exists y)(\forall x)(x \in y \leftrightarrow \varphi(x))$ e $\beta \equiv_{def} (\exists y)((\forall z)(z \in y \leftrightarrow \varphi(z)) \wedge x \in y)$, isto é, β é $x \in \{x \ : \ \varphi(x)\}$; logo, $\alpha \wedge \beta$ implica β implica $\varphi(x)$. Por outro lado, $\varphi(x) \wedge (x \in y \leftrightarrow \varphi(x))$ implica $x \in y$, e então $\varphi(x) \wedge \alpha$ implica β. Para provar a segunda equivalência, considere $\phi(z, y) \equiv_{def} (z = y) \leftrightarrow (\forall x)(x \in z \leftrightarrow x \in y)$. Por [A1] vale $(\forall z)\phi(z, y)$ e então, pela Observação 2.1 obtemos $\phi(s, y)$, i.e., $(s = y) \leftrightarrow (\forall x)(x \in s \leftrightarrow x \in y)$. A última afirmação é uma conseqüência das duas primeiras. ■

Desta maneira, se $s \equiv_{def} \{x \ : \ \varphi(x)\}$ e $t \equiv_{def} \{x \ : \ \phi(x)\}$ são legitimados, então, para provar $(s = t)$, basta provar $\varphi(x) \leftrightarrow \phi(x)$.

Axioma do Conjunto Vazio:

[VZ] $(\exists y)(\forall x)(x \notin y)$

Este axioma é redundante, pois pode ser deduzido de [A2]: considere $\varphi(x) \equiv_{def} (x \neq x)$; como $(x \in y \leftrightarrow (x \in a \wedge x \neq x)) \sim (x \notin y \leftrightarrow (x \notin a \vee x = x)) \sim (x \notin y \leftrightarrow (x = x)) \sim x \notin y$, então o axioma [VZ] se segue por [A2]. Assim, o termo $\{x \ : \ x \neq x\}$, que será denotado $\emptyset$, é legitimado em ZF. Note que $(s = \emptyset)$ sse $(\forall x)\neg\varphi(x)$, se $s \equiv_{def} \{x \ : \ \varphi(x)\}$.

Corolário 2.3 $[A1], [A2] \vdash x \notin \emptyset$.

Demonstração: Pela Proposição 2.2,

$$\vdash (\exists y)(\forall x)(x \in y \leftrightarrow x \neq x) \rightarrow (x \in \emptyset \leftrightarrow x \neq x)$$

(note que o antecedente desta implicação expressa que $\emptyset \equiv_{def} \{x \ : \ x \neq x\}$ é legitimado). Logo, $[VZ] \vdash (x \in \emptyset \leftrightarrow x \neq x)$, donde $[A1], [A2] \vdash x \notin \emptyset$. ■

Axioma do Par:

[PR] $(\exists y)(\forall x)(x \in y \leftrightarrow ((x = a) \vee (x = b)))$

Este axioma afirma que existe o conjunto com a e b como únicos membros, legitimando o termo $\{x \ : \ (x = a) \vee (x = b)\}$, que será denotado $\{a, b\}$ (note que o nome do termo depende de a e b). Em função da hierarquia cumulativa, o par $\{a, b\}$ pode ser formado em qualquer estágio depois que a e b foram formados; logo, não tem último estágio. O conjunto $\{a, a\}$ será denotado $\{a\}$, sendo que contém a como único elemento. Este axioma é redundante, como provaremos depois na Proposição 11.2. O axioma [PR] permitirá formar, junto com o axioma [RF] da reunião finita a ser introduzido a seguir, os conjuntos finitos da forma $\{a_1, \ldots, a_n\}$.

Corolário 2.4 *(a)* $[A1], [A2], [PR] \vdash x \in \{a, b\} \leftrightarrow (x = a) \vee (x = b)$.
(b) $[A1], [A2], [PR] \vdash x \in \{a\} \leftrightarrow x = a$.

Adotemos a notação $x \subseteq y$ e $x \subset y$ para indicar as fórmulas

$$(\forall z)(z \in x \to z \in y) \;\text{ e }\; (x \subseteq y) \wedge (x \neq y),$$

respectivamente. É claro que $s \subseteq t \leftrightarrow (\forall x)(\varphi(x) \to \phi(x))$ se $s \equiv_{def} \{x \;:\; \varphi(x)\}$ e $t \equiv_{def} \{x \;:\; \phi(x)\}$ são legitimados.

Axioma da Reunião Finita:

[RF] $(\exists y)(\forall x)(x \in y \leftrightarrow (x \in a \vee x \in b))$

Aqui estabelecemos que $a \cup b \equiv_{def} \{x \;:\; (x \in a) \vee (x \in b)\}$ é legitimado. Este axioma será redundante na presença dos outros axiomas, como provaremos na Proposição 3.2. Por outro lado, $a \cap b \equiv_{def} \{x \;:\; (x \in a) \wedge (x \in b)\}$ é legitimado, por [A2]. Logo, podemos provar o seguinte:

Proposição 2.5 $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$*, e* $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$.

Demonstração: $x \in (a \cup b) \cap c$ sse $x \in (a \cup b) \wedge x \in c$ sse $(x \in a \vee x \in b) \wedge x \in c$ sse $(x \in a \wedge x \in c) \vee (x \in b \wedge x \in c)$ see $(x \in a \cap c) \vee (x \in b \cap c)$ sse $x \in (a \cap c) \cup (b \cap c)$. A outra afirmação é provada analogamente. ■

Por [A2], $a - b \equiv_{def} \{x \;:\; (x \in a) \wedge (x \notin b)\}$ é legitimado.

Proposição 2.6 $a - (a \cap b) = a - b$.

Demonstração: $x \in a - (a \cap b)$ sse $x \in a \wedge x \notin (a \cap b)$ sse $x \in a \wedge \neg(x \in a \wedge x \in b)$ see $x \in a \wedge (x \notin a \vee x \notin b)$ sse $(x \in a \wedge x \notin a) \vee (x \in a \wedge x \notin b)$ see $x \in a \wedge x \notin b$ see $x \in a - b$. ■

Exercícios 2.7 *Provar na TC obtida até agora o seguinte:*
(1) $x \subseteq x$*;* $(x \subseteq y \wedge y \subseteq x) \to (x = y)$*;* $(x \subseteq y \wedge y \subseteq z) \to (x \subseteq z)$.
(2) $\emptyset \subseteq x$*;* $(x \subseteq \emptyset) \to (x = \emptyset)$.
(3) $\neg(x \subset x)$*;* $(x \subset y) \to \neg(y \subset x)$.
(4) $a \cap b$ *e* $a - b$ *são legitimados.*
(5) $a \cap b = b \cap a$*;* $(a \cap b) \cap c = a \cap (b \cap c)$*;* $a \cap \emptyset = \emptyset$*;* $a \cap b \subseteq a$*;* $(a \subseteq b) \leftrightarrow (a \cap b = a)$.
(6) $(a \subseteq b) \leftrightarrow (a \cup b = b)$*;* $a \cup \emptyset = a$*;* $a \subseteq a \cup b$.
(7) $a \cap (a - b) = a - b$*;* $(a - b) \cup b = a \cup b$*;* $(a \cup b) - b = a - b$*;* $a - (b \cup c) = (a - b) \cap (a - c)$*;* $a - (b \cap c) = (a - b) \cup (a - c)$*;* $(a \subseteq b) \to (a - b = \emptyset)$.
(8) Obter o paradoxo de Russell a partir de $(\exists y)(\forall x)(x \in y)$.
(9) Opinar sobre a verdade ou falsidade das seguintes afirmações:
- *(9.1) O termo* $\{x \;:\; x = x\}$ *não pode ser legitimado.*
- *(9.2)* $\varphi(x) \to x \in \{x \;:\; \varphi(x)\}$.
- *(9.3)* $\{x \;:\; x \in y\} = y$.
- *(9.4)* $(\forall x)(\varphi(x) \to \phi(x)) \to (\{x \;:\; \varphi(x)\} \subseteq \{x \;:\; \phi(x)\})$.
- *(9.5)* $(\forall x)(\varphi(x) \leftrightarrow \neg\phi(x)) \to (\{x \;:\; \varphi(x)\} = \{x \;:\; \phi(x)\})$.

(10) Sejam $s \equiv_{def} \{x \; : \; \varphi(x)\}$ e $t \equiv_{def} \{x \; : \; \phi(x)\}$ legitimados. Então
$s \in t \leftrightarrow (\exists w)((\forall x)(x \in w \leftrightarrow \varphi(x)) \wedge \phi(w))$.
(11) $x \in a \leftrightarrow \{x\} \subseteq a$.

Observação 2.8 A partir das expressões obtidas na Proposição 2.2 e no Exercício 2.7 (10), vemos que podemos iterar os termos $\{x \; : \; \varphi\}$, uma vez que eles são legitimados. Assim, se os (meta)termos

$$s_i \equiv_{def} \{x \; : \; \phi_i(x)\} \; (i = 1, \ldots, n) \quad \text{e} \quad \{x \; : \; \varphi(x, x_1, \ldots, x_n, z_1, \ldots, z_k)\}$$

são legitimados então, usando a Proposição 2.2, $\{x \; : \; \overline{\varphi}(x, z_1, \ldots, z_k)\}$ é legitimado, onde $\overline{\varphi}$ é obtida de φ substituindo x_i por s_i e , *a posteriori*, $(w \in s_i)$, $(s_i \in w)$, $(s_i = w)$, $(s_i \in s_j)$ e $(s_i = s_j)$ pela expressão correspondente (w é uma variável que ocorre livre ou limitada em φ). Por exemplo, os termos $a \cup b \equiv_{def} \{x \; : \; x \in a \vee x \in b\}$ e $s \equiv_{def} \{a\} \equiv \{x \; : \; x = a\}$ são legitimados, logo $\{a\} \cup b$ é legitimado, obtido como $\{x \; : \; x \in s \vee x \in b\} \equiv \{x \; : \; x = a \vee x \in b\}$. Se, por outro lado, queremos formar $\{s_1\} \cup s_2$, onde $s_i \equiv_{def} \{x \; : \; \phi_i(x)\}$ são legitimados $(i = 1, 2)$ então teremos $t_1 \equiv_{def} \{s_1\} \equiv \{x \; : \; x = s_1\} \equiv \{x \; : (\forall y)(y \in x \leftrightarrow \phi_1(x)\}$, logo $t_1 \cup s_2 \equiv_{def} \{x \; : \; x \in t_1 \vee x \in s_2\} \equiv \{x \; : \; (\forall y)(y \in x \leftrightarrow \phi_1(x)) \vee \phi_2(x)\}$. É nesse sentido que devemos entender, por exemplo, o (meta)termo $(a \cup b) \cap c \equiv_{def} \{x \; : \; x \in (a \cup b) \wedge x \in c\} \equiv \{x \; : \; (x \in a \vee x \in b) \wedge x \in c\}$ na Proposição 2.5. ■

3 Axiomas Adicionais

Nesta seção definiremos três axiomas adicionais da TC dada por ZF.

Axioma das Partes:

[A3] $(\exists y)(\forall x)(x \in y \leftrightarrow (\forall z)(z \in x \rightarrow z \in a))$

Este axioma garante en ZF que o conjunto $\{x \; : \; x \subseteq a\}$ pode ser formado, uma vez que a foi formado. A notação utilizada para este (meta)termo será $\mathcal{P}(a)$. Como todo subconjunto de a será formado ao menos no nível de a, então $\mathcal{P}(a)$ aparecerá só no nível seguinte. Logo, este axioma é verdadeiro na teoria cumulativa de tipos, assumindo que não existe um máximo nível.

Proposição 3.1 *(1) $a \in \mathcal{P}(a)$; $\emptyset \in \mathcal{P}(a)$ na TC introduzida até agora.*
(2) Se $s \equiv_{def} \{x \; : \; \phi(x)\}$ e $t \equiv_{def} \{x \; : \; \varphi(x)\}$ são legitimados em ZF, então $s \in \mathcal{P}(t)$ sse $s \subseteq t$ sse $(\forall x)(\phi(x) \rightarrow \varphi(x))$; em particular, $s \in \mathcal{P}(s)$ e $\emptyset \in \mathcal{P}(s)$.
(3) $ZF \vdash \mathcal{P}(\emptyset) = \{\emptyset\}$.
(4) $ZF \vdash \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
(5) $ZF \vdash a \subseteq b \leftrightarrow \mathcal{P}(a) \subseteq \mathcal{P}(b)$.
(6) $ZF \vdash \mathcal{P}(a) \cup \mathcal{P}(b) \subseteq \mathcal{P}(a \cup b)$.
(7) $ZF \vdash \mathcal{P}(a \cap b) = \mathcal{P}(a) \cap \mathcal{P}(b)$.
(8) $ZF \vdash \mathcal{P}(a - b) \subseteq (\mathcal{P}(a) - \mathcal{P}(b)) \cup \{\emptyset\}$.

Demonstração: (1) $a \in \mathcal{P}(a)$ sse $a \subseteq a$. Pelo Exercício 2.7 (10),

$$\emptyset \in \mathcal{P}(a) \sim (\exists w)((\forall x)(x \in w \leftrightarrow x \neq x) \wedge (\forall x)(x \in w \rightarrow x \in a)).$$

Logo, $\emptyset \in \mathcal{P}(a) \sim (\exists w)((\forall x)(x \notin w) \wedge (\forall x)(x \in w \rightarrow x \in a)$. Mas $(\forall x)(x \notin w)$ implica $(\forall x)(x \in w \rightarrow x \in a)$; portanto, pelo axioma do conjunto vazio obtemos $\emptyset \in \mathcal{P}(a)$.
(2) Basta considerar $\psi(x, y) \equiv_{def} (x \in \mathcal{P}(y) \leftrightarrow x \subseteq y)$ e usar a Observação 2.1.
(3) $\mathcal{P}(\emptyset) = \{x \ : \ (\forall y)(y \in x \rightarrow y \neq y)\} = \{x \ : \ x = \emptyset\} = \{\emptyset\}$ $(= \{y \ : \ (\forall z)(z \notin y)\})$.
(4) Por (3) temos que $(y \in \mathcal{P}(\emptyset)) \leftrightarrow (\forall z)(z \notin y)$. Assim,

$$\begin{aligned} \mathcal{P}(\mathcal{P}(\emptyset)) &= \{x \ : \ (\forall y)(y \in x \rightarrow (\forall z)(z \notin y))\} \\ &\equiv_{def} \{x \ : \ \phi(x)\}. \end{aligned}$$

Por outro lado,

$$\begin{aligned} \{\emptyset, \{\emptyset\}\} &= \{x \ : \ x = \emptyset \vee x = \{\emptyset\}\} \\ &= \{x \ : \ (\forall y)(y \notin x) \vee (\forall y)(y \in x \leftrightarrow (\forall z)(z \notin y))\} \\ &\equiv_{def} \{x \ : \ \varphi(x)\}. \end{aligned}$$

Devemos provar então a equivalência de $\phi(x)$ e $\varphi(x)$, as fórmulas que definem os meta-termos $\mathcal{P}(\mathcal{P}(\emptyset))$ e $\{\emptyset, \{\emptyset\}\}$, respectivamente. Partindo de $\varphi(x)$, se assumimos $\alpha(x) \equiv_{def} (\exists y)(y \in x)$ então obtemos $\phi(x)$, pois $\varphi(x) \sim (\alpha(x) \rightarrow \phi(x))$. Assumindo $\neg\alpha(x)$ então também obtemos $\phi(x)$, porque nesse caso $x = \emptyset$, e $\emptyset \in \mathcal{P}(s)$ para todo s legitimado, por (2). Assim,

$$\varphi(x), \ (x = \emptyset) \vee (x \neq \emptyset) \ \text{ implica } \psi,$$

portanto $\varphi(x)$ implica $\phi(x)$, pelo *Princípio do Terceiro Excluído*. Analogamente (analisando os casos em que $x = \emptyset$ ou $x \neq \emptyset$) provamos que $\phi(x)$ implica $\varphi(x)$.
(5) Suponha que $a \subseteq b$, e seja $x \in \mathcal{P}(a)$. Se $y \in x$ então $y \in a$, logo $y \in b$. Assim $y \in x$ implica $y \in b$, donde $x \in \mathcal{P}(b)$, isto é, $\mathcal{P}(a) \subseteq \mathcal{P}(b)$. Reciprocamente, suponha que $\mathcal{P}(a) \subseteq \mathcal{P}(b)$. Como $a \in \mathcal{P}(a)$, então $a \in \mathcal{P}(b)$, donde $a \subseteq b$.
(6), (7) e (8): São deixados como exercício. ■

Axioma da Reunião:

[A4] $(\exists y)(\forall x)(x \in y \leftrightarrow (\exists z)((x \in z) \wedge (z \in a))$

Este axioma legitima em ZF o meta-termo

$$\bigcup a \equiv_{def} \{x \ : \ (\exists z)((x \in z) \wedge (z \in a))\},$$

definindo a reunião da coleção de conjuntos a; os elementos de $\bigcup a$ são exatamente os elementos dos elementos de a. Como os elementos dos elementos de a ocorrem em níveis anteriores ao de a, então $\bigcup a$ ocorre no nível de a (e possivelmente no nível anterior). Isto é válido na estrutura cumulativa de tipos.

Observe que, pelo axioma do par, existe $\{a, b\}$; logo, pelo axioma da reunião, existe $\bigcup\{a, b\}$. É fácil provar que este conjunto é exatamente $a \cup b$. Vemos assim que o axioma da reunião finita resulta agora redundante.

Proposição 3.2 *(1)* [A1], [PR], [A4] $\vdash \bigcup\{a, b\} = a \cup b$. *Portanto, o axioma* [RF] *é deduzido dos outros axiomas introduzidos até agora.*
(2) Se $s \equiv_{def} \{x \ : \ \phi(x)\}$ *e* $t \equiv_{def} \{x \ : \ \varphi(x)\}$ *são legitimados então*

$$\bigcup\{s, t\} = s \cup t = \{x \ : \ \phi(x) \vee \varphi(x)\}.$$

Demonstração: (1) Por definição,

$$\begin{aligned}\bigcup\{a, b\} \quad &= \{x \ : \ (\exists z)(z \in \{a, b\} \wedge x \in z)\} \\ &= \{x \ : \ (\exists z)((z = a \vee z = b) \wedge x \in z)\} \\ &= \{x \ : \ (\exists z)((z = a \wedge x \in z) \vee (z = b \wedge x \in z))\} \\ &= \{x \ : \ x \in a \vee x \in b\} \\ &= a \cup b.\end{aligned}$$

(2) Considere $\psi(a, b) \equiv_{def} (\forall x)(x \in \bigcup\{a, b\} \leftrightarrow x \in a \cup b)$ (lembrando que devemos eliminar os meta-termos para obter uma fórmula). Por (1) temos $(\forall a)(\forall b)\psi(a, b)$ e então, pela Observação 2.1, deduzimos $\psi(s, t)$, pois s e t são legitimados. ∎

Observe que, por [A2], sempre podemos definir a interseção de uma familia não vazia de conjuntos:

Proposição 3.3 [A2]*,* $(\exists x)(x \in a) \vdash (\exists w)(\forall x)(x \in w \leftrightarrow (\forall y)(y \in a \to x \in y))$. *Em outras palavras, se* $a \neq \emptyset$*, então* $\bigcap a \equiv_{def} \{x \ : \ (\forall y)(y \in a \to x \in y)\}$ *é legitimado.*

Demonstração: Por [A2] temos que existe $s = \{x \ : \ x \in b \wedge (\forall y)(y \in a \to x \in y)\}$. Mas $b \in a$ e $(\forall y)(y \in a \to x \in y)$ implicam que $x \in b$, logo $s = \{x \ : \ (\forall y)(y \in a \to x \in y)\}$. ∎

Provaremos algumas propriedades básicas da interseção e a reunião arbitrária de conjuntos. Antes disso, precissamos ampliar a nossa notação permitindo (meta)termos da forma $\{t \ : \ \varphi\}$, onde t é um (meta)termo da forma $\{x \ : \ \phi\}$. Definimos $\{t \ : \ \varphi\}$ como sendo $\{x \ : \ (\exists u_1) \cdots (\exists u_n)((x = t) \wedge \varphi)\}$ onde u_1, $\ldots$, u_n são algumas das variáveis livres comuns a t e φ (no contexto ficará claro quais variáveis serão livres, funcionando como parâmetros). Por exemplo, podemos formar o termo $s \equiv_{def} \{a \cap c \ : \ c \in b\}$, com variáveis livres a e b, a partir do termo $t \equiv_{def} a \cap c$ (com variáveis livres a e c). Logo, s denota o termo $\{x \ : \ (\exists c)((x = a \cap c) \wedge c \in b)\}$; aqui, c e b são as variáveis livres de $\varphi(c, b) \equiv_{def} c \in b$. É imediato que se t é legitimado, então φ implica $t \in \{t \ : \ \varphi\}$.

Proposição 3.4 *Na TC introduzida até agora temos o seguinte:*
(1) $\bigcup \emptyset = \emptyset$.
(2) $\bigcup\{a\} = a$.
(3) Se $s \equiv_{def} \{x \ : \ \phi(x)\}$ *é legitimado, então* $\bigcup\{s\} = s$*; em particular,* $\bigcup\{\emptyset\} = \emptyset$.

(4) $\bigcup(a\cup b) = (\bigcup a)\cup(\bigcup b)$.
(5) $\bigcap\{a,b\} = a\cap b$.
(6) Se $s \equiv_{def} \{x \ : \ \phi(x)\}$ *e* $t \equiv_{def} \{x \ : \ \varphi(x)\}$ *são legitimados, então* $\bigcap\{s,t\} = s\cap t$.
(7) Se $a\neq\emptyset$ *e* $b\neq\emptyset$*, então existe* $\bigcap(a\cup b)$*, e* $\bigcap(a\cup b) = (\bigcap a)\cap(\bigcap b)$.
(8) Se $a\neq\emptyset$*, então* $\bigcap a\subseteq\bigcup a$.
(9) $a\cap(\bigcup b) = \bigcup\{a\cap c \ : \ c\in b\}$.
(10) Se $b\neq\emptyset$*, então existe* $\bigcap\{a\cup c \ : \ c\in b\}$*, e* $a\cup(\bigcap b) = \bigcap\{a\cup c \ : \ c\in b\}$.

Demonstração: (1) $x\in\bigcup\emptyset$ sse $(\exists z)(x\in z\wedge z\in\emptyset)$ see $(\exists z)(x\in z\wedge z\neq z)$ sse $(\exists z)(z\neq z)$. Logo, $x\notin\bigcup\emptyset$ para todo x.
(2) $x\in\bigcup\{a\}$ sse $(\exists z)(x\in z\wedge z\in\{a\})$ sse $(\exists z)(x\in z\wedge z=a)$ sse $x\in a$.
(3) É conseqüência de (2), considerando $\psi(a)\equiv_{def}(\forall x)(x\in\bigcup\{a\}\leftrightarrow x\in a)$, a Observação 2.1, e o fato de s ser legitimado.
(4) $x\in\bigcup(a\cup b)$ sse $(\exists z)(x\in z\wedge z\in a\cup b)$ sse $(\exists z)(x\in z\wedge(z\in a\vee z\in b))$ sse $(\exists z)((x\in z\wedge z\in a)\vee(x\in z\wedge z\in b))$ sse $(\exists z)(x\in z\wedge z\in a)\vee(\exists z)(x\in z\wedge z\in b)$ sse $x\in(\bigcup a)\cup(\bigcup b)$ (lembre que $(\exists z)(\phi(z)\vee\varphi(z))\sim(\exists z)\phi(z)\vee(\exists z)\varphi(z)$).
(5) $x\in\bigcap\{a,b\}$ sse $(\forall y)(y\in\{a,b\}\to x\in y)$ sse $(\forall y)((y=a\vee y=b)\to x\in y)$ sse $(\forall y)((y=a\to x\in y)\wedge(y=b\to x\in y))$ sse $(\forall y)(y=a\to x\in y)\wedge(\forall y)(y=b\to x\in y)$ sse $x\in a\wedge x\in b$ sse $x\in a\cap b$ (lembre que $(\forall y)(\phi(y)\wedge\varphi(y))\sim(\forall y)\phi(y)\wedge(\forall y)\varphi(y)$).
(6) Considere $\psi(a,b)\equiv_{def}(\forall x)(x\in\bigcap\{a,b\}\leftrightarrow x\in x\in a\cap b)$. Por (5), vale $(\forall a)(\forall b)\psi(a,b)$, donde deduzimos $\psi(s,t)$ para s e t legitimados, pela Observação 2.1.
(7) A prova é similar à do item (5).
(8) É imediato.
(9) $x\in\bigcup\{a\cap c \ : \ c\in b\}$ sse $(\exists z)(x\in z\wedge(\exists c)(z=(a\cap c)\wedge c\in b)$ sse $(\exists c)(x\in(a\cap c)\wedge c\in b)$ sse $(\exists c)((x\in a\wedge(x\in c\wedge c\in b))$ sse $x\in a\wedge(\exists c)(x\in c\wedge c\in b)$ sse $x\in a\cap(\bigcup b)$ (lembre que $(\exists c)(\varphi\wedge\phi(c))\sim\varphi\wedge(\exists c)\phi(c)$ se c não ocorre livre em φ).
(10) $x\in a\cup(\bigcap b)$ sse $x\in a\vee(\forall c)(c\in b\to x\in c)$. Por outro lado, $x\in\bigcap\{a\cup c \ : \ c\in b\}$ sse $(\forall y)(y\in\{a\cup c \ : \ c\in b\}\to x\in y)$.
Seja $x\in a\cup(\bigcap b)$ e $y\in\{a\cup c \ : \ c\in b\}$; logo, existe $c'\in b$ tal que $y=a\cup c'$. Se $x\in a$, então $x\in(a\cup c')=y$. Se $(\forall c)(c\in b\to x\in c)$, então, tomando c' no lugar de c, obtemos $x\in c'$ e então $x\in y$. Em todo caso, provamos que $x\in a\cup(\bigcap b)$ implica $y\in\{a\cup c \ : \ c\in b\}\to x\in y$, donde $x\in a\cup(\bigcap b)$ implica $x\in\bigcap\{a\cup c \ : \ c\in b\}$. Reciprocamente, seja $x\in\bigcap\{a\cup c \ : \ c\in b\}$, e $c\in b$. Como $a\cup c\in\{a\cup c \ : \ c\in b\}$, então $x\in a\cup c$, donde $x\in a\vee x\in c$. Desta maneira, $x\in\bigcap\{a\cup c \ : \ c\in b\}$ implica $c\in b\to(x\in a\vee x\in c)$ e então $x\in a\vee(c\in b\to x\in c)$. Portanto, $x\in\bigcap\{a\cup c \ : \ c\in b\}$ implica $(\forall c)(x\in a\vee(c\in b\to x\in c))$ que implica $x\in a\vee(\forall c)(c\in b\to x\in c)$ (lembre que $(\forall c)(\alpha\vee\beta(c))\sim\alpha\vee(\forall c)\beta(c)$, se c não ocorre livre em α). ■

Finalmente formularemos o axioma da regularidade. Este axioma, devido a Zermelo (1930) (existe uma versão prévia de von Neumann em 1925) é fundamental para evitar situações da forma $x \in x$ ou, em geral,

$$x_1 \in x_2 \in \cdots \in x_n \in x_1.$$

Além disso, este axioma evita "descensos infinitos" da forma

$$\cdots \in x_n \in x_{n-1} \in \cdots \in x_2 \in x_1$$

(isto significa que a relação $x \in y$ é *bem fundada*, como estudaremos depois).

Axioma da Regularidade:

[A5] $(\exists y)(y \in x) \to (\exists y)(y \in x \wedge (\forall z)\neg(z \in x \wedge z \in y))$

Este é o único axioma expressando a idéia que os conjuntos ocorrem en níveis ou tipos, e é precisso utilizar a teoria cumulativa de tipos para entendé-lo. Com efeito, consideremos um conjunto x não vazio. Comecemos a analizar os níveis de baixo para cima, até encontrar o primeiro nível em que foram formados elementos de x. Por exemplo, se $x = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$, então o primeiro nível em que aparecem elementos de x é o nível 2, assumindo que não temos indivíduos. Assim se $y \in x$ está no nível mínimo, então os elementos de y (se existirem) devem necessariamente ter sido criados em níveis anteriores, logo não podem pertencer a x, isto é: $y \cap x = \emptyset$ (o que se confirma no nosso exemplo). Os axiomas de extensionalidade e regularidade são os únicos que exigem conjuntos satisfazendo certas propriedades; os outros axiomas estabelecem a existência de suficientes conjuntos em alguma direção.

Definição 3.5 *S é o sistema axiomático da TC que consiste dos axiomas* [A1]-[A5] *mais* [PR].

Proposição 3.6 *(1) $S \vdash a \notin a$.*
(2) $S \vdash \neg(a \in b \wedge b \in a)$.

Demonstração: (1) $a \in a$ implica $a \in \{a\} \cap a$. Por [A5] existe $x \in \{a\}$ tal que $\{a\} \cap x = \emptyset$. Mas $x \in \{a\}$ sse $x = a$ e então $\{a\} \cap a = \emptyset$, o que contradiz $a \in \{a\} \cap a$.
(2) Se $a \in b \wedge b \in a$, então $a \in \{a, b\} \cap b$ e $b \in \{a, b\} \cap a$. Por [A5] existe $x \in \{a, b\}$ tal que $\{a, b\} \cap x = \emptyset$. Mas $x \in \{a, b\}$ sse $x = a$ ou $x = b$. Os dois casos levam a uma contradição. ■

A partir de agora, desenvolveremos um estudo da TC obtida através do sistema S. O sistema completo ZF da TC será introduzido na Seção 11. Porém, é importante observar que uma parte interessante da TC "finita" pode ser desenvolvida utilizando apenas o sub-sistema S de ZF, como veremos nas próximas seções.

4 Produtos Cartesianos

Estamos em condições de começar a desenvolver as primeiras aplicações do fragmento S de ZF introducido até agora. Antes de estudar a teoria de relações e funções na próxima seção, é necessário definir o conceito de *par ordenado*, a partir do qual são introduzidos os produtos cartesianos de conjuntos.

Definição 4.1 (Kuratowski) *(i)* $\langle a, b\rangle \equiv_{def} \{\{a\}, \{a, b\}\}$.
(ii) $\langle a_1, \ldots, a_{n+1}\rangle \equiv_{def} \langle\langle a_1, \ldots, a_n\rangle, a_{n+1}\rangle$ *para* $n \geq 2$.

É claro que o axioma [PR] assegura a existência de $\langle a, b\rangle$ para todo a e b. Observe que a definição de $\langle a, b, c\rangle$ como sendo $\{\{a\}, \{a, b\}, \{a, b, c\}\}$ não funciona (porqué?).

Proposição 4.2 $\mathrm{S} \vdash \langle a, b\rangle = \langle c, d\rangle \leftrightarrow (a = c) \wedge (b = d)$.

Demonstração: $x \in \langle a, b\rangle$ sse $x = \{a\}$ ou $x = \{a, b\}$, e $x \in \langle c, d\rangle$ sse $x = \{c\}$ ou $x = \{c, d\}$. Suponha que $\langle a, b\rangle = \langle c, d\rangle$; a prova de que $a = c$ e $b = d$ será feita por análise de casos.
Caso 1: $a = b$. Logo, $\langle a, b\rangle = \{\{a\}\} = \{\{c\}, \{c, d\}\}$ e então, pelo Corolário 2.4, $\{c\} = \{a\} = \{c, d\}$ donde, usando novamente o Corolário 2.4, obtemos que $c = a = d$.
Caso 2: $a \neq b$. Dado que $\{a\} \in \langle c, d\rangle$, então $\{a\} = \{c\}$ ou $\{a\} = \{c, d\}$ (usando o Corolário 2.4).
Caso 2.a: $\{a\} = \{c\}$. Logo $a = c$, e então $\langle c, d\rangle = \{\{a\}, \{a, d\}\}$. Como $\{a, b\} \in \langle c, d\rangle$ e $\{a, b\} \neq \{a\}$ (pelo Corolário 2.4 e a hipótese $a \neq b$), então $\{a, b\} = \{a, d\}$. Daqui obtemos, de $a \neq b$, que $b = d$.
Caso 2.b: $\{a\} = \{c, d\}$. Logo $c = a = d$ e então $\langle c, d\rangle = \{\{a\}\}$. Mas $\{a, b\} \in \langle c, d\rangle$, donde $\{a, b\} = \{a\}$, e então $a = b$, o que contradiz a hipótese $a \neq b$. Daqui inferimos que vale o caso 2.a.
Claramente, $a = c$, $b = d$ implica $\langle a, b\rangle = \langle c, d\rangle$, pelas regras da igualdade. ■

Uma vez que possuimos a definição de par ordenado, podemos criar o conjunto de todos os pares ordenados $\langle x, y\rangle$, onde $x \in a$ e $y \in b$, fixados a e b.

Definição 4.3 *O produto cartesiano de* a *e* b *é dado por* $a \times b \equiv_{def} \{\langle x, y\rangle : x \in a \wedge y \in b\}$.

Provaremos agora que o termo $a \times b$ é legitimado.

Proposição 4.4 $a \times b = \{x : x \in \mathcal{P}(\mathcal{P}(a \cup b)) \wedge (\exists y)(\exists z)(x = \langle y, z\rangle \wedge (y \in a) \wedge (z \in b))\}$. *Portanto,* $a \times b$ *é legitimado por* [A2] *(dado que os termos envolvidos na definição são legitimados pelos outros axiomas de S).*

Demonstração: Temos que $\{x : x \in \mathcal{P}(\mathcal{P}(a \cup b)) \wedge (\exists y)(\exists z)(x = \langle y, z\rangle \wedge (y \in a) \wedge (z \in b))\}$ é legitimado por [A2]. Provaremos em S que

$$(\exists y)(\exists z)(x = \langle y, z\rangle \wedge (y \in a) \wedge (z \in b)) \rightarrow$$
$$\rightarrow x \in \mathcal{P}(\mathcal{P}(a \cup b)) \wedge (\exists y)(\exists z)(x = \langle y, z\rangle \wedge (y \in a) \wedge (z \in b))$$

e então (dado que a implicação recíproca é sempre verdadeira) teremos provado o resultado. Seja então $x = \langle y, z\rangle$ tal que $y \in a$, $z \in b$. Portanto, $\{y\} \subseteq a \cup b$ e $\{y, z\} \subseteq a \cup b$, donde $\{y\} \in \mathcal{P}(a \cup b)$ e $\{y, z\} \in \mathcal{P}(a \cup b)$. Desta maneira, $x = \{\{y\}, \{y, z\}\} \subseteq \mathcal{P}(a \cup b)$ e então $x \in \mathcal{P}(\mathcal{P}(a \cup b))$. ■

Proposição 4.5 $S \vdash a \times b = \emptyset \leftrightarrow a = \emptyset \vee b = \emptyset$.

Demonstração: Suponha que $a \times b = \emptyset$. Assuma que $\neg(a = \emptyset \vee b = \emptyset)$, isto é, $a \neq \emptyset$ e $b \neq \emptyset$. Logo, $(\exists y)(y \in a)$ e $(\exists z)(z \in b)$. Daqui $\langle y, z\rangle \in a \times b$, uma contradição. Portanto, inferimos que $a = \emptyset \vee b = \emptyset$. Reciprocamente, suponha que $a = \emptyset \vee b = \emptyset$; logo, $\neg(\exists y)(y \in a) \vee \neg(\exists z)(z \in b)$ e então $\neg(\exists y)(\exists z)((y \in a) \wedge (z \in b) \wedge x = \langle y, z\rangle)$ para todo x. Portanto, $x \notin a \times b$ para todo x, donde $a \times b = \emptyset$. ■

Proposição 4.6 $S \vdash a \times b = b \times a \leftrightarrow (a = \emptyset \vee b = \emptyset \vee a = b)$.

Demonstração: Suponha que $a \times b = b \times a$; assumindo $a \neq \emptyset$, $b \neq \emptyset$ e $a \neq b$ provaremos uma contradição. Com efeito, de $a \neq b$ inferimos que existe $x \in a$, $x \notin b$ ou existe $x \in b$, $x \notin a$, por [A1]. Assumamos $x \in a$, $x \notin b$ (o raciocínio para a outra possibilidade é simétrico). Seja $y \in b$ (assumimos $b \neq \emptyset$). Portanto, $\langle x, y\rangle \in a \times b = b \times a$, e então $(x \in b) \wedge (y \in a)$, donde $x \in b$, uma contradição. Reciprocamente, suponha que $(a = \emptyset \vee b = \emptyset \vee a = b)$. Temos que $(a = \emptyset \vee b = \emptyset)$ implica $a \times b = \emptyset = b \times a$, pela Proposição 4.5. Por outro lado, $a = b$ implica $a \times b = b \times a$, pelas regras da igualdade. ■

Proposição 4.7 *(i)* $S \vdash (a \neq \emptyset \wedge a \times b \subseteq a \times c) \rightarrow (b \subseteq c)$.
(ii) $S \vdash (b \subseteq c) \rightarrow (a \times b \subseteq a \times c)$.

Demonstração: (i) O caso $b = \emptyset$ é trivial. Assuma então $b \neq \emptyset$ e seja $y \in b$. Fixe $x \in a$ (assumimos $a \neq \emptyset$); logo $\langle x, y\rangle \in a \times b$, e $a \times b \subseteq a \times c$, donde $\langle x, y\rangle \in a \times c$. Daqui $(x \in a) \wedge (y \in c)$, e então $y \in c$; isto é, $b \subseteq c$.
(ii) O caso $a \times b = \emptyset$ é trivial. Seja $z \in a \times b$; logo, $z = \langle x, y\rangle$ para $x \in a$ e $y \in b$. Mas $b \subseteq c$, donde $y \in c$ e então $z = \langle x, y\rangle \in a \times c$. Portanto $a \times b \subseteq a \times c$. ■

Proposição 4.8 *(i)* $S \vdash a \times (b \cap c) = (a \times b) \cap (a \times c)$.
(ii) $S \vdash a \times (b \cup c) = (a \times b) \cup (a \times c)$.
(iii) $S \vdash a \times (b - c) = (a \times b) - (a \times c)$.

Demonstração: (i) $\langle x, y\rangle \in a \times (b \cap c)$ sse $(x \in a) \wedge (y \in (b \cap c))$ sse $(x \in a) \wedge ((y \in b) \wedge (y \in c))$ sse $((x \in a) \wedge (y \in b)) \wedge ((x \in a) \wedge (y \in c))$ sse $(\langle x, y\rangle \in a \times b) \wedge (\langle x, y\rangle \in a \times c)$ sse $\langle x, y\rangle \in (a \times b) \cap (a \times c)$.
(ii), (iii): São deixados como exercício. ■

Proposição 4.9 $S \vdash (a \subseteq a \times a) \rightarrow a = \emptyset$.

Demonstração: Se $z \in a$ então, de $a \subseteq a \times a$, inferimos

$$z = \{\{x\}, \{x, y\}\} \in a \times a \text{ para algum } x, y \in a. \qquad (*)$$

Suponha então $a \neq \emptyset$. Pelo axioma de regularidade aplicado a $a \cup (\bigcup a) \neq \emptyset$, existe $c \in a \cup (\bigcup a)$ tal que $c \cap (a \cup (\bigcup a)) = \emptyset$. Observe que os elementos de $a \cup (\bigcup a)$ são conjuntos não vazios, por $(*)$. Daqui, $c \neq \emptyset$. Se $c \in a$, então $c \subseteq \bigcup a$ (isto é uma conseqüência imediata da definição de $\bigcup a$, e é deixado como exercício). Daqui $\emptyset \neq c = c \cap (\bigcup a)$, o que contradiz $c \cap (a \cup (\bigcup a)) = \emptyset$. Portanto $c \in \bigcup a$ donde, por $(*)$, teremos que $c = \{x\}$ ou $c = \{x, y\}$ para $x, y \in a$. Nos dois casos $c \cap a \neq \emptyset$, uma contradição. ■

5 Relações em S

Nesta seção trataremos a teoria elementar de relações em S, utilizando os resultados sobre produtos cartesianos provados na seção anterior.

Definição 5.1 *Introduzimos as notações seguintes:*
$rel(r)$ *para* $(\forall x)(x \in r \to (\exists y)(\exists z)(x = \langle y, z\rangle))$
"r é uma relação (um conjunto de pares ordenados)";
$u\ r\ v$ *para* $\langle u, v\rangle \in r$
"u está em relação r com v";
$dom(r)$ *para* $\{x\ :\ (\exists y)(x\ r\ y)\}$
(o domínio de r);
$im(r)$ *para* $\{y\ :\ (\exists x)(x\ r\ y)\}$
(a imagem de r);
$r|z$ *para* $\{u\ :\ u \in r \wedge (\exists x)(\exists y)(u = \langle x, y\rangle \wedge x \in z)\}$
(r com domínio restrito a z);
r^{-1} *para* $\{u\ :\ (\exists x)(\exists y)(u = \langle x, y\rangle \wedge y\ r\ x)\}$
(a relação inversa de r);
$r``z$ *para* $\{y\ :\ (\exists x)(x \in z \wedge x\ r\ y)\}$*, isto é,* $im(r|z)$
(a imagem de z por r);
$r(z)$ *para* $\{y\ :\ (\exists u)((\forall w)(z\ r\ w \leftrightarrow w = u) \wedge y \in u)\}$
(o único valor de r em z, se existir, ou $\emptyset$ em caso contrário).

Proposição 5.2 *(a)* $(rel(r) \wedge (s \subseteq r)) \to rel(s)$*; em particular,* $rel(\emptyset)$*.*
(b) $(rel(r) \wedge rel(s)) \to rel(r \cup s) \wedge rel(r \cap s) \wedge rel(r - s)$*.*

Demonstração: (a) $z \in s$ implica $z \in r$ implica $z = \langle x, y\rangle$ para algum x e y; logo, $rel(s)$.
(b) $z \in r \cup s$ implica $z \in r$ ou $z \in s$; nos dois casos, $z = \langle x, y\rangle$ para algum x, y. Os outros casos são similares. ■

Proposição 5.3 *Os meta-termos da Definição 5.1 são legitimados.*

Demonstração: $dom(r)$: Por [A2], existe $\{x\ :\ x \in \bigcup\bigcup r \wedge (\exists y)(x\ r\ y)\}$. Provaremos que a condição $x \in \bigcup\bigcup r$ pode ser eliminada. Com efeito, suponha que $(\exists y)(x\ r\ y)$. Logo $\langle x, y\rangle \in r$, isto é, $\{\{x\}, \{x, y\}\} \in r$. Daqui $\{x\} \in \bigcup r$ e então $x \in \bigcup\bigcup r$.
$im(r)$: A prova é análoga à anterior.
$r|z$: É legitimado por [A2].
r^{-1}: Por [A2] existe $\{u\ :\ u \in im(r) \times dom(r) \wedge (\exists x)(\exists y)(u = \langle x, y\rangle \wedge y\ r\ x)\}$. Provaremos que a condição $u \in im(r) \times dom(r)$ é implicada pela outra condição. Seja então u satisfazendo: $(\exists x)(\exists y)(u = \langle x, y\rangle \wedge y\ r\ x)$. Logo, $u = \langle x, y\rangle$ tal que $y\ r\ x$, donde $y \in dom(r)$ e $x \in im(r)$, e então $u = \langle x, y\rangle \in im(r) \times dom(r)$.
$r``z$: Temos que $r``z = im(r|z)$, sendo portanto legitimado.
$r(z)$: Por [A2], existe $\{y\ :\ y \in \bigcup im(r) \wedge (\exists u)((\forall w)(z\ r\ w \leftrightarrow w = u) \wedge y \in u)\}$. Como antes, veremos que a condição de separação $y \in \bigcup im(r)$ é redundante. Com efeito, suponha que y satisfaz $(\exists u)((\forall w)(z\ r\ w \leftrightarrow w = u) \wedge y \in u)$, e seja

u satisfazendo $(\forall w)(z\ r\ w \leftrightarrow w = u) \wedge y \in u$. Tomando $w = u$ obtemos que z $r\ u$, donde $u \in im(r)$. Mas $y \in u$, portanto $y \in \bigcup im(r)$. ■

Proposição 5.4 *(a)* $dom(r \cup s) = dom(r) \cup dom(s)$.
(b) $dom(r \cap s) \subseteq dom(r) \cap dom(s)$.
(c) $dom(r) - dom(s) \subseteq dom(r - s)$.
(d) $im(r \cup s) = im(r) \cup im(s)$.
(e) $im(r \cap s) \subseteq im(r) \cap im(s)$.
(f) $im(r) - im(s) \subseteq im(r - s)$.

Demonstração: (a) Temos que $x \in dom(r \cup s)$ sse $(\exists y)(x\ (r \cup s)\ y)$ sse $(\exists y)((x\ r\ y) \vee (x\ s\ y))$ sse $(\exists y)(x\ r\ y) \vee (\exists y)(x\ s\ y)$ sse $x \in dom(r) \vee x \in dom(s)$ sse $x \in dom(r) \cup dom(s)$.
(b)-(f): As provas são análogas, e são deixadas como exercício. ■

Com relação a r^{-1} temos as seguintes propriedades:

Proposição 5.5 *(a)* $(r^{-1})^{-1} \subseteq r$; $rel(r) \to r \subseteq (r^{-1})^{-1}$.
(b) $(r \cup s)^{-1} = r^{-1} \cup s^{-1}$.
(c) $(r \cap s)^{-1} = r^{-1} \cap s^{-1}$.
(d) $(r - s)^{-1} = r^{-1} - s^{-1}$.

Demonstração: (a) $z \in (r^{-1})^{-1}$ implica que $z = \langle x, y\rangle$ tal que $x\ (r^{-1})^{-1}\ y$. Mas $x\ (r^{-1})^{-1}\ y$ implica $y\ r^{-1}\ x$ implica $x\ r\ y$, isto é, $z = \langle x, y\rangle \in r$. Reciprocamente, se $rel(r)$, seja $z \in r$; então $z = \langle x, y\rangle$ tal que $x\ r\ y$, e a prova é como acima, revertendo as implicações.
(b) $\langle x, y\rangle \in (r \cup s)^{-1}$ sse $\langle y, x\rangle \in r \cup s$ sse $(\langle y, x\rangle \in r) \vee (\langle y, x\rangle \in s)$ sse $\langle x, y\rangle \in r^{-1} \vee \langle x, y\rangle \in s^{-1}$ see $\langle x, y\rangle \in r^{-1} \cup s^{-1}$.
(c) Análoga à prova anterior.
(d) $\langle x, y\rangle \in (r - s)^{-1}$ sse $\langle y, x\rangle \in r - s$ sse $(\langle y, x\rangle \in r) \wedge (\langle y, x\rangle \notin s)$ sse $\langle x, y\rangle \in r^{-1} \wedge \langle x, y\rangle \notin s^{-1}$ see $\langle x, y\rangle \in r^{-1} - s^{-1}$. ■

Definição 5.6 *A composição de r e s é definida como*

$$r \circ s \equiv_{def} \{\langle x, y\rangle \ : \ (\exists z)((x\ r\ z) \wedge (z\ s\ y))\}.$$

Proposição 5.7 *$r \circ s$ é legitimado em S.*

Demonstração: Provaremos que

$$r \circ s = \{u \ : \ u \in dom(r) \times im(s) \wedge (\exists x)(\exists y)(\exists z)((u = \langle x, y\rangle) \wedge (x\ r\ z) \wedge (z\ s\ y))\},$$

donde o resultado segue por [A2]. Assim, suponha que $u = \langle x, y\rangle$ tal que $x\ r\ z$, $z\ s\ y$ para algum z. Logo $x \in dom(r)$ e $y \in im(s)$, donde $u = \langle x, y\rangle \in dom(r) \times im(s)$. ■

A composição satisfaz as seguintes propriedades:

Proposição 5.8 *(a)* $r \circ (s \cup t) = (r \circ s) \cup (r \circ t)$.
(b) $r \circ (s \cap t) \subseteq (r \circ s) \cap (r \circ t)$.
(c) $(r \circ s) - (r \circ t) \subseteq r \circ (s - t)$.
(d) $(r \circ s)^{-1} = s^{-1} \circ r^{-1}$.
(e) $r \circ (s \circ t) = (r \circ s) \circ t$

Demonstração: (a) Temos que

$$\begin{array}{l} x\ (r \circ (s \cup t))\ y \\ \text{see } (\exists z)((x\ r\ z) \wedge (z\ (s \cup t)\ y)) \\ \text{see } (\exists z)((x\ r\ z) \wedge ((z\ s\ y) \vee (z\ t\ y))) \\ \text{see } (\exists z)(((x\ r\ z) \wedge (z\ s\ y)) \vee ((x\ r\ z) \wedge (z\ t\ y))) \\ \text{see } (\exists z)((x\ r\ z) \wedge (z\ s\ y)) \vee (\exists z)((x\ r\ z) \wedge (z\ t\ y)) \\ \text{see } (x\ (r \circ s)\ y) \vee (x\ (r \circ t)\ y) \\ \text{see } x\ ((r \circ s) \cup (r \circ t))\ y. \end{array}$$

(b) Temos que

$$\begin{array}{l} x\ (r \circ (s \cap t))\ y \\ \text{implica } (\exists z)((x\ r\ z) \wedge (z\ (s \cap t)\ y)) \\ \text{implica } (\exists z)((x\ r\ z) \wedge ((z\ s\ y) \wedge (z\ t\ y))) \\ \text{implica } (\exists z)(((x\ r\ z) \wedge (z\ s\ y)) \wedge ((x\ r\ z) \wedge (z\ t\ y))) \\ \text{implica } (\exists z)((x\ r\ z) \wedge (z\ s\ y)) \wedge (\exists z)((x\ r\ z) \wedge (z\ t\ y)) \\ \text{implica } (x\ (r \circ s)\ y) \wedge (x\ (r \circ t)\ y) \\ \text{implica } x\ ((r \circ s) \cap (r \circ t))\ y, \end{array}$$

lembrando que $(\exists z)(\phi \wedge \psi) \rightarrow ((\exists z)\phi \wedge (\exists z)\psi)$. A recíproca desta propriedade lógica não é verdadeira em geral, donde não vale em geral a igualdade em (b).
(c) A prova é análoga à anterior.
(d) $x\ (r \circ s)^{-1}\ y$ sse $y\ (r \circ s)\ x$ sse $(\exists z)((y\ r\ z) \wedge (z\ s\ x))$ sse $(\exists z)((z\ r^{-1}\ y) \wedge (x\ s^{-1}\ z))$ sse $x\ (s^{-1} \circ r^{-1})\ y$.
(e) É deixada como exercício. ■

A restrição satisfaz as seguintes propriedades:

Proposição 5.9 *(a)* $r|z = r \cap (z \times im(r))$.
(b) $r|(a \cap b) = (r|a) \cap (r|b)$.
(c) $r|(a \cup b) = (r|a) \cup (r|b)$.
(d) $r|(a - b) = (r|a) - (r|b)$.
(e) $(r \circ s)|a = (r|a) \circ s$.

Demonstração: Exercício. ■

Finalmente, a imagem $r``z$ satisfaz as seguintes propriedades:

Proposição 5.10 *(a)* $r``(a \cup b) = r``a \cup r``b$.
(b) $r``(a \cap b) \subseteq r``a \cap r``b$.

(c) $r``a - r``b \subseteq r``(a - b)$.
(d) $(a \subseteq b) \to (r``a \subseteq r``b)$.
(e) $(r``a = \emptyset) \leftrightarrow (dom(r) \cap a = \emptyset)$.

Demonstração: (a) Temos que
$y \in r``(a \cup b)$
sse $(\exists x)((x\ r\ y) \wedge (x \in a \cup b))$
sse $(\exists x)((x\ r\ y) \wedge (x \in a)) \vee (\exists x)((x\ r\ y) \wedge (x \in b))$
sse $(y \in r``a) \vee (y \in r``b)$
sse $y \in (r``a \cup r``b)$.
(b) A prova é análoga, usando agora $(\exists x)(\phi \wedge \psi) \to ((\exists x)\phi \wedge (\exists x)\psi)$.
(c) Análoga à anterior.
(d) $y \in r``a$ implica $(\exists x)((x\ r\ y) \wedge (x \in a))$ implica $(\exists x)((x\ r\ y) \wedge (x \in b))$ implica $y \in r``b$.
(e) $y \in r``a$ implica $(\exists x)((x\ r\ y) \wedge (x \in a))$. Portanto, se $(x\ r\ y) \wedge (x \in a)$, então $x \in dom(r) \cap a$. Isto é, $r``a \neq \emptyset$ implica $dom(r) \cap a \neq \emptyset$. Reciprocamente, se $x \in dom(r) \cap a$, então $x\ r\ y$ para algum y, e $x \in a$, donde $(\exists x)((x\ r\ y) \wedge (x \in a))$. Portanto $y \in r``a$, isto é: $dom(r) \cap a \neq \emptyset$ implica $r``a \neq \emptyset$. ■

Exemplo 5.11 Assumindo os números naturais como indivíduos, sejam

$$r = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,3\rangle\}, \qquad s = \{\langle 2,1\rangle, \langle 3,5\rangle\}.$$

Portanto,

$$\begin{array}{ll} dom(r) = \{1,2\}, & im(r) = \{1,2,3\}, \\ r``(\{1\}) = \{2,3\}, & r``(\{3\}) = \emptyset, \\ s^{-1} = \{\langle 1,2\rangle, \langle 5,3\rangle\}, & r \circ s = \{\langle 1,1\rangle, \langle 1,5\rangle, \langle 2,5\rangle\}, \\ s \circ r = \{\langle 2,2\rangle, \langle 2,3\rangle\}, & r|\{2\} = \{\langle 2,1\rangle, \langle 2,3\rangle\}, \\ im(r|\{2\}) = \{1,3\} = r``\{2\}, & (r^{-1})``\{3\} = \{1,2\}. \end{array}$$ ■

6 Relações de Ordem

Um tipo muito importante de relações é a classe das relações de ordem. Elas ocorrem em quase todas as áreas da matemática, sendo que o seu estudo constitui, em si, uma área relevante dentro da Matemática.

Definição 6.1 *Introduzimos as notações seguintes:*
$ref(r,a)$ *para* $(\forall x)(x \in a \to (x\ r\ x))$
(r é reflexiva em a);
$irr(r,a)$ *para* $(\forall x)(x \in a \to \neg(x\ r\ x))$
(r é irreflexiva em a);
$sim(r,a)$ *para* $(\forall x)(\forall y)(((x \in a) \wedge (y \in a) \wedge (x\ r\ y)) \to (y\ r\ x))$
(r é simétrica em a);
$asim(r,a)$ *para* $(\forall x)(\forall y)(((x \in a) \wedge (y \in a) \wedge (x\ r\ y)) \to \neg(y\ r\ x))$
(r é asimétrica em a);

$anti(r,a)$ para $(\forall x)(\forall y)(((x \in a) \wedge (y \in a) \wedge (x\ r\ y) \wedge (y\ r\ x)) \rightarrow (x = y))$;
(r é antisimétrica em a);
$tran(r,a)$ para
$(\forall x)(\forall y)(\forall z)(((x \in a) \wedge (y \in a) \wedge (z \in a) \wedge (x\ r\ y) \wedge (y\ r\ z)) \rightarrow (x\ r\ z))$
(r é transitiva em a);
$con(r,a)$ para $(\forall x)(\forall y)(((x \in a) \wedge (y \in a) \wedge (x \neq y)) \rightarrow ((x\ r\ y) \vee (y\ r\ x)))$
(r é conectada em a);
$fcon(r,a)$ para $(\forall x)(\forall y)(((x \in a) \wedge (y \in a)) \rightarrow ((x\ r\ y) \vee (y\ r\ x)))$
(r é fortemente conectada em a).

As definições usuais (r é reflexiva, r é simétrica, etc.) são obtidas considerando $a = dom(r) \cup im(r) \equiv_{def} F(r)$; assim, $ref(r)$ denota $ref(r, F(r))$, $sim(r)$ denota $sim(r, F(r))$, etc. Será muito útil definir a relação identidade sobre um conjunto a, dada pelo termo $I(a) = \{\langle x, x \rangle\ :\ x \in a\}$.

Proposição 6.2 *O termo $I(a)$ é legitimado em S.*

Demonstração: O termo $s \equiv_{def} \{z\ :\ z \in \mathcal{PP}(a) \wedge (\exists x)(z = \langle x, x \rangle \wedge (x \in a))\}$ é legitimado por [A2]. Basta então provar que $(\exists x)(z = \langle x, x \rangle \wedge (x \in a))$ implica $z \in \mathcal{PP}(a)$. Com efeito, $z = \langle x, x \rangle$ implica $z = \{\{x\}\}$. Por outro lado, $x \in a$ implica $\{x\} \in \mathcal{P}(a)$, portanto $z \subseteq \mathcal{P}(a)$, isto é, $z \in \mathcal{PP}(a)$. Logo $I(a) = s$, sendo portanto legitimado. ■

Proposição 6.3 *Seja r uma relação. As seguintes propriedades são demonstráveis em S:*
(a) $asim(r) \rightarrow irr(r)$.
(b) $asim(r) \rightarrow anti(r)$.
(c) $(sim(r) \wedge tran(r)) \rightarrow ref(r)$.

Demonstração: (a) Seja $x \in F(r)$; como r é asimétrica, então $(x\ r\ x)$ implica $\neg(x\ r\ x)$, donde obtemos $\neg(x\ r\ x)$.
(b) Sejam $x, y \in F(r)$ tais que $(x\ r\ y) \wedge (y\ r\ x)$. Logo, obtemos $\neg(y\ r\ x)$, pois r é asimétrica, donde deduzimos uma contradição. Portanto $(x, y \in F(r)) \wedge asim(r)$ implica $\neg((x\ r\ y) \wedge (y\ r\ x))$, e a posteriori $\neg((x\ r\ y) \wedge (y\ r\ x)) \vee (x = y)$, isto é, $((x\ r\ y) \wedge (y\ r\ x)) \rightarrow (x = y)$.
(c) Suponha que $x \in F(r)$. Se $x \in dom(r)$, então $x\ r\ y$ para algum $y \in F(r)$. Como $sim(r)$, então $y\ r\ x$, donde $(x\ r\ y) \wedge (y\ r\ x)$. Portanto $x\ r\ x$, pois $tran(r)$. Por outro lado, se $x \in im(r)$, então $y\ r\ x$ para algum $y \in F(r)$, e a prova é análoga. ■

Podemos definir cinco tipos de ordens:

Definição 6.4 *Sejam r uma relação e a um conjunto. Definimos o seguinte:*
(a) $qo(r,a)$ denota $ref(r,a) \wedge tran(r,a)$ (r é uma quase ordem em a).
(b) $op(r,a)$ denota $ref(r,a) \wedge anti(r,a) \wedge tran(r,a)$ (r é uma ordem parcial em a).
(c) $os(r,a)$ denota $anti(r,a) \wedge tran(r,a) \wedge fcon(r,a)$ (r é uma ordem simples em a).

(d) $ope(r, a)$ denota $asim(r, a) \wedge tran(r, a)$ (r é uma ordem parcial estrita em a).
(e) $ose(r, a)$ denota $asim(r, a) \wedge tran(r, a) \wedge con(r, a)$ (r é uma ordem simples estrita em a).
(f) $qo(r)$ denota $qo(r, F(r))$, etc.

Se r satisfaz alguma das definições de ordem introduzidas na Definição 6.4, então escreveremos $x \leq y$ ou ainda $x < y$ (se r é irreflexiva) no lugar de $x\ r\ y$, quando não existir risco de confusão.

Exemplos 6.5 (1) Dado um conjunto b, então $a = \mathcal{P}(b)$ é parcialmente ordenado pela relação $x \leq y$ sse $x \subseteq y \subseteq b$. Com efeito, $\leq$ é parcial, pois nem todo par de subconjuntos x, y de b deve ser necessariamente comparável pela relação de inclusão.
(2) O conjunto $\mathbb{N}$ dos números naturais é ordenado pela relação: $n \leq m$ sse $n|m$ (n *divide a* m). Com efeito, $n \leq n$ para todo n, pois $n = 1.n$, donde $n|n$. Por outro lado, $n|m$ e $m|n$ significa: existem k, h em $\mathbb{N}$ tais que $m = kn$, $n = hm$, portanto $m = k(hm) = (kh)m$. Se $m = 0$, então $n = h.0 = 0 = m$. Se $m \neq 0$, então de $m = (kh)m$ inferimos $1 = kh$, e então $k = 1 = h$, donde $n = m$. Finalmente, se $n \leq m$ e $m \leq r$, então $m = kn$ e $r = hm$ para certos $k, h \in \mathbb{N}$. Portanto $r = hm = h(kn) = (hk)n$ para $hk \in \mathbb{N}$ donde $n|r$, isto é, $n \leq r$. Observe que $1|n$ para todo n, pois $n = n.1$; logo $1 \leq n$ para todo n, isto é, 1 é o mínimo elemento de $\mathbb{N}$ com a ordem *divide a*. Por outro lado, $0 = 0.n$ para todo n, e então $n|0$ para todo n, isto é, $n \leq 0$ para todo n. Daqui 0 é o máximo elemento de $\mathbb{N}$ com a ordem *divide a*. Observe que a ordem não é conectada: $2 \not\leq 3$ e $3 \not\leq 2$, pois 2 e 3 são co-primos. Os números primos positivos são os elementos *minimais*, isto é, se $n \leq p$ e p é primo, então $n = 1$ (o mínimo elemento com relação a $\leq$) ou $n = p$. Reciprocamente, se p é minimal, então p deve ser necessariamente primo. ∎

Proposição 6.6 *Em S temos o seguinte:*
(a) $op(r) \rightarrow qo(r)$.
(b) $os(r) \rightarrow op(r)$.
(c) $os(r) \rightarrow os(r^{-1})$.
(d) $qo(r) \wedge qo(s) \rightarrow qo(r \cap s)$.

Demonstração: (a) Imediato das definições.
(b) Só falta provar a reflexividade da r. Mas $x \in F(r)$ implica $((x\ r\ x) \vee (x\ r\ x))$, isto é, $x\ r\ x$, pois $fcon(r)$.
(c) É claro que $tran(r) \rightarrow tran(r^{-1})$. Com efeito, $((x\ r^{-1}\ y) \wedge (y\ r^{-1}\ z))$ implica $((y\ r\ x) \wedge (z\ r\ y))$ implica $z\ r\ x$ (pois $tran(r)$) implica $x\ r^{-1}\ z$. Da mesma maneira provamos que $anti(r) \rightarrow anti(r^{-1})$ e $fcon(r) \rightarrow fcon(r^{-1})$.
(d) Seja $x \in F(r \cap s)$, logo $x \in F(r) \cap F(s)$, donde $((x\ r\ x) \wedge (x\ s\ x))$, pois $ref(r) \wedge ref(s)$. Portanto $x\ (r \cap s)\ x$, isto é, $ref(r \cap s)$. Suponha agora que $((x\ (r \cap s)\ y) \wedge (y\ (r \cap s)\ z))$. Daqui obtemos $((x\ r\ y) \wedge (y\ r\ z))$, donde $x\ r\ z$, pois $tran(r)$. Analogamente $x\ s\ z$, e então $x\ (r \cap s)\ z$; isto é, $tran(r \cap s)$. ∎

Observe que a reunião de duas quase-ordens não resulta necessariamente numa quase-ordem. Por exemplo

$$r = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 1,2\rangle\}, \quad s = \{\langle 2,2\rangle, \langle 3,3\rangle, \langle 2,3\rangle\}$$

são duas quase-ordens, mas a união, embora reflexiva, não é transitiva. A situação muda se $F(r) \cap F(s) = \emptyset$.

Proposição 6.7 $S \vdash (qo(r) \wedge qo(s) \wedge (F(r) \cap F(s) = \emptyset)) \to qo(r \cup s)$.

Demonstração: É claro que $r \cup s$ é reflexiva. Suponha que $((x\ (r \cup s)\ y) \wedge (y\ (r \cup s)\ z))$. Como $F(r) \cap F(s) = \emptyset$, então só vale uma das seguintes afirmações:

$$((x\ r\ y) \wedge (y\ r\ z)), \quad ((x\ s\ y) \wedge (y\ s\ z)).$$

Nos dois casos, obtemos $x\ (r \cup s)\ z$, pois $tran(r) \wedge tran(s)$. ■

Proposição 6.8 $S \vdash ((r \subseteq s) \wedge (s \subseteq (a \times a)) \wedge ose(r,a) \wedge ose(s,a)) \to (r = s)$.

Demonstração: Suponha que $x\ s\ y$ mas $\neg(x\ r\ y)$. Como $asim(s)$, então $x \neq y$, donde $y\ r\ x$, pois $con(r,a)$. Portanto $y\ s\ x$, pois $r \subseteq s$, o que contradiz $asim(s)$. ■

O significado da proposição precedente é o seguinte: uma ordem simples estrita em a ordena *todos* os elementos de a numa ordem estrita, isto é: $x \not< x$ para todo $x \in a$. Portanto, se r, s são duas ordens estritas simples em a tal que s estende r, então elas devem necessariamente coincidir, pois r já ordenou todos os elementos de a.

Introduziremos agora a importante noção de boa ordem. Uma boa ordem em a é uma ordem simples estrita r tal que todo subconjunto não vazio de a tem um elemento mínimo segundo r. De fato, a conectividade de r implicará a transitividade e asimetria de r. Antes da definição, analizaremos alguns exemplos.

Exemplos 6.9 (a) O conjunto $\mathbb{N}$ dos números naturais é bem ordenado pela relação $<$ usual (*menor que*). De fato, $\emptyset \neq A \subseteq \mathbb{N}$ possui um elemento mínimo.
(b) $\mathbb{N}$ não é bem ordenado pela ordem simples estrita $>$ (*maior que*). Com efeito, $\emptyset \neq A \subseteq \mathbb{N}$ tem elemento mínimo com relação a $>$ significa que existe $n \in A$ tal que $n > m$ para todo $m \in A$. Em particular, o próprio $\mathbb{N}$ deveria ter um primeiro elemento relativo a $>$, isto é, deveria existir $n \in \mathbb{N}$ tal que $n > m$ para todo $m \in \mathbb{N}$; mas isto não é verdade ($n \not> n+1$).
(c) Considere $A = \{(n-1)/n \ : \ n \in \mathbb{N} \wedge n \neq 0\} \cup \{1\}$ ordenado pela relação $<$ usual (em $\mathbb{Q}$, o conjunto dos números racionais). Logo, A é bem ordenado. Com efeito,

$$(n-1)/n < (m-1)/m \quad \text{sse} \quad m(n-1) < n(m-1) \quad \text{sse}$$

$$mn - m < nm - n \quad \text{sse} \quad -m < -n \quad \text{sse} \quad n < m.$$

Portanto, $\emptyset \neq B \subseteq A$ tem primeiro elemento $(n-1)/n$, onde n é o mínimo m tal que $(m-1)/m \in B$. Se $B = \{1\}$, então claramente 1 é o primeiro elemento de B.
(d) Seja A como no item (c). Logo, $>$ (a ordem *maior que* de $\mathbb{Q}$) não é uma boa ordem em A, pois $B = A - \{1\}$ não tem primeiro elemento. Com efeito, se $x = (n-1)/n$ fosse mínimo, então $(n-1)/n > n/(n+1)$ donde $n > n+1$, uma contradição. ■

Definição 6.10 *Definimos o seguinte:*
(a) $min(x,r,a)$ *denota* $x \in a \wedge (\forall y)(y \in a \to \neg(y\ r\ x))$ *(*x *é um elemento* r*-minimal de* a*).*
(b) $pe(x,r,a)$ *denota* $x \in a \wedge (\forall y)((y \in a \wedge x \neq y) \to x\ r\ y)$ *(*x *é um* r*-primeiro elemento de* a*).*
(c) $bo(r,a)$ *denota* $con(r,a) \wedge (\forall b)((b \subseteq a \wedge b \neq \emptyset) \to (\exists x)min(x,r,b))$ *(*r *é uma boa ordem em* a*).*

Observação 6.11 Um elemento minimal não tem antecessores, enquanto que um primeiro elemento precede todo outro elemento diferente dele mesmo. Se r é asimétrica, então todo primeiro elemento é minimal. Com efeito, seja $x \in a$ primeiro elemento de r. Se $y \in a$, então $\neg(y\ r\ x)$ se $y = x$, pois r é irreflexiva. Se $y \neq x$, então $x\ r\ y$, pois x é primeiro elemento. Logo $\neg(y\ r\ x)$, pois r é asimétrica, e então x é minimal. Observe que $r = \{\langle 1,1\rangle\}$ em $a = \{1\}$ tem trivialmente 1 como primeiro elemento, mas 1 não é minimal, pois $1\ r\ 1$; vemos que a hipótese de asimetria é fundamental. A recíproca não vale em geral: 1 é minimal em $r = \{\langle 1,2\rangle\}$ sobre $a = \{1,2,3\}$, mas 1 não é primeiro elemento, pois $\neg(1\ r\ 3)$. Se r é conectada e asimétrica, as duas noções coincidem. Com efeito, se x é minimal e $y \neq x$, então $\neg(y\ r\ x)$, pois x é minimal. Mas r é conectada, portanto $x\ r\ y$. Daqui x é primeiro elemento. ■

Proposição 6.12 $S \vdash bo(r,a) \to (asim(r,a) \wedge tran(r,a))$.

Demonstração: Sejam $x, y \in a$ tais que $x\ r\ y$, $y\ r\ x$. Logo, $\{x,y\}$ não tem elemento minimal. Com efeito, y não é minimal, pois $x\ r\ y$. Analogamente, $y\ r\ x$ implica que x não é minimal; isto contraria o fato de r ser uma boa ordem. Portanto, r deve ser asimétrica. Sejam agora $x, y, z \in a$ tais que $x\ r\ y$, $y\ r\ z$, $\neg(x\ r\ z)$. Como r é asimétrica, então $x \neq z$. Logo, $z\ r\ x$, pois r é conectada. Mas então $\{x,y,z\}$ não tem elemento minimal: $x\ r\ y$ implica que y não é minimal; $y\ r\ z$ implica que z não é minimal. Finalmente, $z\ r\ x$ implica que x não pode ser minimal. Daqui, inferimos que r é transitiva. ■

Proposição 6.13
(a) $\vdash bo(r,a) \leftrightarrow (asim(r,a) \wedge con(r,a) \wedge (\forall b)(b \neq \emptyset \wedge b \subseteq a \to (\exists x)pe(x,r,b)))$.
(b) $\vdash bo(r,a) \wedge a \neq \emptyset \to (\exists! x)pe(x,r,a)$. *Aqui, a notação* $(\exists! x)\varphi(x)$ *indica:*
$(\exists x)(\varphi(x) \wedge (\forall y)(\varphi(y) \to (y = x)))$ *("existe um único* x *tal que* $\varphi(x)$*").*
(c) $\vdash bo(r,a) \wedge b \subseteq a \to bo(r,b)$.

Demonstração: (a) Assuma $bo(r,a)$; pela Proposição 6.12, obtemos $asim(r,a)$. Claro que $con(r,a)$, pela definição de boa ordem. Se $\emptyset \neq b \subseteq a$, então existe $x \in b$ tal que $min(x,r,b)$. Pela Observação 6.11, $pe(x,r,b)$. Reciprocamente, suponha que $(\forall b)(b \neq \emptyset \wedge b \subseteq a \rightarrow (\exists x)pe(x,r,b))$, $asim(r,a)$ e $con(r,a)$. Logo, $con(r,a)$. Dado $\emptyset \neq b \subseteq a$, seja $x \in b$ tal que $pe(x,r,b)$. Pela Observação 6.11 obtemos $min(x,r,b)$, pois $asim(r,a)$.
(b) Se $\emptyset \neq a$, então, de $a \subseteq a$, obtemos $(\exists x)pe(x,r,a)$, pelo item (a). Sejam $x, y \in a$ tais que $pe(x,r,a)$, $pe(y,r,a)$. Se $x \neq y$, então $x\ r\ y$, $y\ r\ x$. Mas $asim(r,a)$, pela Proposição 6.12. Logo $x = y$.
(c) Suponha que $bo(r,a)$ e $b \subseteq a$. É claro que $con(r,b)$. Se $\emptyset \neq c \subseteq b$, então $\emptyset \neq c \subseteq a$, donde $min(x,r,c)$ para algum $x \in c$. Portanto $bo(r,b)$. ■

Definição 6.14 *$si(y,x,r)$ denota $(x\ r\ y) \wedge (\forall z)((x\ r\ z) \rightarrow (z = y \vee (y\ r\ z)))$ ("y é um r-sucessor imediato de x").*
$ue(x,r,a)$ denota $(x \in a) \wedge (\forall y)(((y \in a) \wedge y \neq x) \rightarrow y\ r\ x)$ ("x é um r-último elemento de a").

Proposição 6.15 *$S \vdash pe(x,r,a) \leftrightarrow ue(x,r^{-1},a)$.*

Demonstração: Imediata. ■

Proposição 6.16
$$S \vdash (bo(r,a) \wedge (F(r) \subseteq a) \wedge (x \in a) \wedge \neg ue(x,r,a)) \rightarrow (\exists! y)si(y,x,r).$$

Demonstração: Por [A2] podemos formar $b = \{y : y \in F(r) \wedge (x\ r\ y)\}$. Dado que $F(r) \subseteq a$, então obtemos que $b = \{y : x\ r\ y\} \subseteq a$. Pela Proposição 6.13(c), temos que $bo(r,b)$. Como x não é um último r-elemento de a, então $b \neq \emptyset$. Portanto, existe um único r-primeiro elemento y de b, pela Proposição 6.13(b). Temos que $x\ r\ y$, pois $y \in b$. Por outro lado, se $(x\ r\ z)$ e $z \neq y$, então $y\ r\ z$, pela definição de b e a definição de primeiro elemento. Portanto, y é um r-sucessor imediato de x. Por outro lado, z é um r-sucessor imediato de x sse z é um primeiro elemento de b. Portanto, y é único. ■

7 Relações de Equivalência

As relações de equivalência são utilizadas com frequência na Matemática. São relações reflexivas, simétricas e transitivas. Dois exemplos básicos são a relação de identidade e a relação de paralelismo entre retas. Como veremos depois, uma relação de equivalência num conjunto *a classifica* os seus elementos de acordo com algum critério. Esta é uma ferramenta muito útil nas construções matemáticas, pois permite simplificar os domínios, analizando as classes dos objetos no lugar dos próprios objetos. Os objetos pertencentes a uma mesma classe são considerados idênticos.

Definição 7.1 *$equiv(r)$ denota $rel(r) \wedge ref(r) \wedge sim(r) \wedge tran(r)$ ("r é uma relação de equivalência").*
$equiv(r,a)$ denota $a = F(r) \wedge equiv(r)$ ("r é uma relação de equivalência em a").

Proposição 7.2 *(a)* $S \vdash equiv(r) \to (r \circ r^{-1} = r)$.
(b) $S \vdash qo(r) \to equiv(r^{-1} \cap r)$.

Demonstração: (a) Se $x\ (r \circ r^{-1})\ y$ então existe z tal que $x\ r\ z$, $z\ r^{-1}\ y$. Daqui obtemos $y\ r\ z$ e então $z\ r\ y$, pois $sim(r)$, donde $x\ r\ y$, pois $tran(r)$. Isto é, $r \circ r^{-1} \subseteq r$. Por outro lado, $x\ r\ y$ implica $(x\ r\ y) \wedge (y\ r^{-1}\ y)$, donde $x\ (r \circ r^{-1})\ y$. Portanto $r = r \circ r^{-1}$.
(b) É imediato que $r^{-1} \cap r = \{\langle x, y\rangle\ :\ (x\ r\ y) \wedge (y\ r\ x)\}$. Daqui o resultado é trivial. ■

Definição 7.3 $r[x] = \{y\ :\ x\ r\ y\}$.

Dado que $r[x] = \{y\ :\ y \in F(r) \wedge (x\ r\ y)\}$, então $r[x]$ é legitimado. É imediato que $r[x] = r``\{x\}$. A notação usual em Matemáticas para $r[x]$ é simplesmente $[x]$, isto é, r é subentendida.

Proposição 7.4 $S \vdash (x, y \in F(r) \wedge equiv(r)) \to (r[x] = r[y] \leftrightarrow (x\ r\ y))$.

Demonstração: Assuma $r[x] = r[y]$, isto é, $(x\ r\ z) \leftrightarrow (y\ r\ z)$. Como $y\ r\ y$, então $x\ r\ y$. Suponha agora $x\ r\ y$, e seja z tal que $x\ r\ z$. De $sim(r)$ obtemos $y\ r\ x$, e então inferimos: $(y\ r\ x)$, $(x\ r\ z)$ implica $y\ r\ z$, pois $tran(r)$. De $x\ r\ y$ provamos analogamente $(y\ r\ z) \to (x\ r\ z)$. Isto é, $r[x] = r[y]$. ■

Proposição 7.5 $S \vdash equiv(r) \to (r[x] = r[y] \vee (r[x] \cap r[y] = \emptyset))$.

Demonstração: Suponha que $r[x] \neq r[y]$; se $x \notin F(r)$ ou $y \notin F(r)$ então claramente $r[x] \cap r[y] = \emptyset$. Se $x, y \in F(r)$, então seja $z \in r[x] \cap r[y]$. Logo $(x\ r\ z)$ e $(y\ r\ z)$, donde obtemos $x\ r\ y$ e posteriormente, pela Proposição 7.4, $r[x] = r[y]$, uma contradição . Portanto, $r[x] \cap r[y] = \emptyset$. ■

Veremos a continuação a estreita relação entre partições e relações de equivalência.

Definição 7.6 $par(\Pi, a)$ *denota*

$$\begin{aligned}&(\bigcup \Pi = a) \wedge (\forall b)(\forall c)(((b \in \Pi) \wedge (c \in \Pi) \wedge b \neq c) \to b \cap c = \emptyset) \wedge \\ &\qquad \wedge (\forall x)(x \in \Pi \to (\exists y)(y \in x))\end{aligned}$$

("Π é uma partição de a").

Por exemplo, se $a = \{1, 2, 3, 4, 5\}$, então $\Pi = \{\{1, 4\}, \{2\}, \{3, 5\}\}$ é uma partição de a, enquanto que

$$\Pi_1 = \{\{1\}, \{2, 3, 4\}\}, \qquad \Pi_2 = \{\{1, 2\}, \{2, 3\}, \{4\}, \{5\}\}$$

não são partições de a (porqué?). Observe que $\emptyset$ é a única partição possível do conjunto $\emptyset$.

Proposição 7.7 $S \vdash a \neq \emptyset \to par(\{a\}, a)$.

Demonstração: Temos que $\bigcup\{a\} = a$. Dado que não existem $b, c \in \{a\}$ com $b \neq c$, então a segunda condição de $par(\Pi, a)$ é trivialmente satisfeita. Finalmente, seja $x \in \{a\}$; é claro que $x = a$. Dado que $a \neq \emptyset$, então existe $y \in a$, e a terceira condição de $par(\Pi, a)$ é satisfeita por $\Pi = \{a\}$. ■

Um conceito importante entre partições é a relação *mais fina que*. Intuitivamente, uma partição Π_1 é mais fina que Π_2 se todo elemento de Π_1 está contido em algum elemento de Π_2, e dai a denominação *mais fina* resulta óbvia. Por exemplo, considere as seguintes partições de $a = \{1, 2, 3, 4, 5\}$:

$$\Pi_1 = \{\{1\}, \{2, 3\}, \{4, 5\}\}, \qquad \Pi_2 = \{\{1\}, \{2, 3\}, \{4\}, \{5\}\},$$

$$\Pi_3 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}, \qquad \Pi_4 = \{\{1, 2, 3\}, \{4\}, \{5\}\}.$$

É imediato que Π_2 é mais fina que Π_1 e Π_4, enquanto que Π_3 é mais fina do que as outras partições. Por outro lado, Π_1 e Π_4 não são comparáveis pela relação "mais fina que".

Definição 7.8 $mf(\Pi_1, \Pi_2)$ *denota* $\Pi_1 \neq \Pi_2 \wedge (\forall x)(x \in \Pi_1 \to (\exists y)((y \in \Pi_2) \wedge (x \subseteq y)))$ *("a partição* Π_1 *é mais fina do que a partição* Π_2*").*

Proposição 7.9 *Todo conjunto tem uma partição mais fina do que todas as outras partições do conjunto.*

Demonstração: Seja $\Pi = \{y \ : \ y \in \mathcal{P}(a) \wedge (\exists x)((x \in a) \wedge y = \{x\})\}$. Temos que Π é legitimado por [A2], e podemos escrever $\Pi = \{\{x\} \ : \ x \in a\}$. Provaremos $par(\Pi, a)$. Primeiro de tudo, temos $\bigcup\Pi = a$. Com efeito, seja $x \in \bigcup\Pi$; logo, existe $y \in \Pi$ tal que $x \in y$. Mas $y = \{z\}$ com $z \in a$, pela definição de Π. Daqui, $x \in y$, $y = \{z\}$ implica $x = z$ e logo $x \in a$. Isto é, $\bigcup\Pi \subseteq a$. Por outro lado, seja $x \in a$; logo $y = \{x\} \in \Pi$ tal que $x \in y$, donde $x \in \bigcup\Pi$, isto é, $a = \bigcup\Pi$. Sejam $b, c \in \Pi$ com $b \neq c$. Logo $b = \{x\}$, $c = \{y\}$ tal que $x, y \in a$. Portanto, $b \neq c$ implica $x \neq y$, e então $b \cap c = \emptyset$. Finalmente, $b \in \Pi$ implica que $b = \{x\}$ para algum $x \in a$; daqui $x \in b$ e logo $(\exists z)(z \in b)$. Isto prova que $par(\Pi, a)$. Suponha agora que $par(\Pi_1, a)$ e $\Pi_1 \neq \Pi$. Seja $y \in \Pi$; logo $y = \{x\}$ com $x \in a$. Como $\bigcup\Pi_1 = a$, então existe $z \in \Pi_1$ tal que $x \in z$, donde $y = \{x\} \subseteq z$, isto é, $mf(\Pi, \Pi_1)$. ■

Vemos então que Π_3 no exemplo acima é de fato a partição mais fina sobre a.

Provaremos a continuação que toda relação de equivalência sobre um conjunto a origina uma partição sobre a.

Definição 7.10 $\Pi(r) = \{b \ : \ (\exists x)(x \in F(r) \ \wedge \ b = r[x])\}$.

É imediato que $\Pi(r) = \{b \ : \ (b \in \mathcal{P}(F(r))) \wedge (\exists x)(x \in F(r) \ \wedge \ b = r[x])\}$, portanto $\Pi(r)$ é legitimado por [A2]. O resultado procurado é o seguinte:

Proposição 7.11 $S \vdash equiv(r, a) \to par(\Pi(r), a)$.

Demonstração: Temos que $equiv(r, a)$ implica $equiv(r) \wedge (a = F(r))$. Podemos escrever $\Pi(r) = \{r[x] \ : \ x \in a\}$. Seja $y \in \bigcup \Pi(r)$; logo existe $x \in a$ tal que $y \in r[x]$, donde $x \ r \ y$, isto é, $y \in a$. Daqui $\bigcup \Pi(r) \subseteq a$. Por outro lado, seja $x \in a$. Logo $(x \in r[x]) \wedge (r[x] \in \Pi(r))$, donde $x \in \bigcup \Pi(r)$. Isto é, $\bigcup \Pi(r) = a$. Sejam $r[x], r[y] \in \Pi(r)$. Se $r[x] \neq r[y]$ então $r[x] \cap r[y] = \emptyset$, pela Proposição 7.5. Finalmente, dado $r[x] \in \Pi(r)$, temos que $x \in r[x]$, isto é, $(\exists y)(y \in r[x])$, provando assim que $par(\Pi(r), a)$. ■

Podemos relacionar a inclusão de relações de equivalência com a relação "mais fina que" das partições associadas.

Proposição 7.12 $S \vdash (equiv(r, a) \wedge equiv(s, a)) \rightarrow (r \subset s \leftrightarrow mf(\Pi(r), \Pi(s))$.

Demonstração: Assuma $equiv(r, a) \wedge equiv(s, a)$. Suponha $r \subset s$; como $r \neq s$, existem $x, y \in a$ tais que $x \ s \ y$ mas $\neg(x \ r \ y)$. Desta maneira, $y \in s[x] - r[x]$ e então $r[x] \neq s[x]$. Seja $z \in r[x]$; portanto $x \ r \ z$, donde $x \ s \ z$, pois $r \subset s$. Daqui $z \in s[x]$, e então $r[x] \subset s[x]$. Assim $r[x] \neq s[w]$ para todo $w \in a$, pois $par(\Pi(s), a)$. Daqui $r[x] \in \Pi(r) - \Pi(s)$ e então $\Pi(r) \neq \Pi(s)$. Seja $y \in \Pi(r)$; logo $y = r[x]$ para algum $x \in a$, e então $r[x] \subseteq s[x]$, com $s[x] \in \Pi(s)$, pois $r \subset s$. Isto é, $mf(\Pi(r), \Pi(s))$. Reciprocamente, suponha $mf(\Pi(r), \Pi(s))$. Logo $\Pi(r) \neq \Pi(s)$. Se $x \ r \ y$ então $y \in r[x]$; mas $r[x] \subseteq s[z]$ para algum z, donde $y \in s[z]$, isto é, $y \ s \ z$. Mas $x \in r[x] \subseteq s[z]$, portanto $x \in s[z]$, donde $x \ s \ z$. De $y \ s \ z$ obtemos $z \ s \ y$ e então $x \ s \ y$; logo $r \subseteq s$. Finalmente, suponha que $r = s$. Logo, $r[x] = s[x]$ para todo $x \in a$, donde $\Pi(r) = \Pi(s)$, contradição. Portanto $r \subset s$. ■

Provaremos agora que uma partição origina uma relação de equivalência.

Definição 7.13 $r(\Pi) = \{\langle x, y \rangle \ : \ (\exists b)((b \in \Pi) \wedge x, y \in b)\}$.

É imediato que $r(\Pi)$ é legitimado, pois

$$r(\Pi) = \{z \ : \ z \in (\bigcup \Pi) \times (\bigcup \Pi) \wedge (\exists x)(\exists y)(z = \langle x, y \rangle \wedge (\exists b)((b \in \Pi) \wedge x, y \in b))\}.$$

Proposição 7.14 $S \vdash par(\Pi, a) \rightarrow equiv(r(\Pi), a)$.

Demonstração: É imediato que $par(\Pi, a)$ implica $F(r(\Pi)) = a$. Se $x \in a$, então existe $b \in \Pi$ tal que $x \in b$; daqui $x \ r(\Pi) \ x$, isto é, $ref(r(\Pi), a)$. A prova da simetria de $r(\Pi)$ é imediata. Sejam $x, y \in a$ tais que $x \ r(\Pi) \ y$, $y \ r(\Pi) \ z$; então $x, y \in b$ e $y, z \in c$ para $b, c \in \Pi$. Logo $y \in b \cap c$, donde $b = c$. Daqui $x, z \in c$, $c \in \Pi$, e então $x \ r(\Pi) \ z$. Isto é, $tran(r(\Pi), a)$, portanto $equiv(r(\Pi), a)$. ■

Vamos agora relacionar partições com relações de equivalência. Provaremos que, partindo de uma relação de equivalência r, então a partição $\Pi(r)$ é tal que a relação de equivalência gerada, $r(\Pi(r))$, coincide com r. Analogamente, a relação $r(\Pi)$ gerada por uma partição Π é tal que $\Pi(r(\Pi)) = \Pi$.

Proposição 7.15 $S \vdash (par(\Pi, a) \wedge equiv(r, a)) \rightarrow (\Pi = \Pi(r) \leftrightarrow r(\Pi) = r)$.

Demonstração: Assuma $par(\Pi, a) \wedge equiv(r, a)$. Suponha $\Pi = \Pi(r)$. De $equiv(r, a)$ obtemos $x\ r\ y$ sse $(\exists z)(x, y \in r[z])$. Mas $b \in \Pi$ sse $(\exists z)(b = r[z])$, por hipótese. Logo

$$x\ r\ y \ \text{ sse } \ (\exists b)(x, y \in b \wedge b \in \Pi) \ \text{ sse } \ x\ r(\Pi)\ y,$$

isto é, $r = r(\Pi)$. Reciprocamente, suponha $r = r(\Pi)$. Se $b \in \Pi$, então existe $x \in a$ tal que $x \in b$. Portanto $y \in b$ sse $x\ r(\Pi)\ y$ sse $x\ r\ y$ sse $y \in r[x]$. Daqui $b = r[x] \in \Pi(r)$. Por outro lado, seja $r[x] \in \Pi(r)$. Como $x \in a$, então existe $b \in \Pi$ tal que $x \in b$. Portanto $b = r[x]$, como acabamos de provar. Logo $r[x] \in \Pi$. Isto é, $\Pi = \Pi(r)$. ■

Finalmente provaremos que a relação "mais fina que" é de fato uma ordem parcial estrita. Considere $PAR(a) = \{\Pi \ : \ par(\Pi, a)\}$. Temos que $PAR(a)$ é legitimado, pois

$$PAR(a) = \{\Pi \ : \ \Pi \in \mathcal{PP}(a) \wedge par(\Pi, a)\}$$

Considere agora

$$<_a = \{u \ : \ u \in PAR(a) \times PAR(a) \wedge (\exists \Pi_1)(\exists \Pi_2)(u = \langle \Pi_1, \Pi_2 \rangle \wedge mf(\Pi_1, \Pi_2)\}$$

Temos que $<_a$ é legitimado por [A2], e $\Pi_1 <_a \Pi_2$ sse $mf(\Pi_1, \Pi_2)$ para toda $\Pi_1, \Pi_2 \in PAR(a)$.

Proposição 7.16 *(a)* $S \vdash (\Pi_1 <_a \Pi_2) \leftrightarrow (r(\Pi_1) \subset r(\Pi_2))$.
(b) $S \vdash ope(<_a, PAR(a))$.

Demonstração: (a) Sejam $\Pi_1, \Pi_2 \in PAR(a)$. Logo,

$\Pi_1 <_a \Pi_2$ sse $mf(\Pi_1, \Pi_2)$ sse

$mf(\Pi(r(\Pi_1)), \Pi(r(\Pi_2))) \wedge equiv(r(\Pi_1), a) \wedge equiv(r(\Pi_2), a)$
(por 7.14, 7.11, 7.15) sse

$r(\Pi_1) \subset r(\Pi_2)$ (por 7.12).

(b) Sejam $\Pi_1, \Pi_2 \in PAR(a)$ tais que $\Pi_1 <_a \Pi_2$; por (a) temos que $r(\Pi_1) \subset r(\Pi_2)$. Se $\Pi_2 <_a \Pi_1$ então $r(\Pi_2) \subset r(\Pi_1)$, uma contradição. Logo, $<_a$ é asimétrica. Se $\Pi_1 <_a \Pi_2$, $\Pi_2 <_a \Pi_3$, então $r(\Pi_1) \subset r(\Pi_2)$ e $r(\Pi_2) \subset r(\Pi_3)$, donde $r(\Pi_1) \subset r(\Pi_3)$. Portanto $\Pi_1 <_a \Pi_3$, por (a). Isto é, $<_a$ é uma ordem parcial estrita em $PAR(a)$. ■

Exemplo 7.17 Fixemos $k \in \mathbb{Z}$, onde $\mathbb{Z}$ denota o conjunto dos números inteiros. Definimos em $\mathbb{Z}$ a relação seguinte:

$$n\, R_k\, m \ \text{ sse } \ k|(n - m) \ \text{ sse existe } z \in \mathbb{Z} \text{ tal que } \ n - m = z.k\ .$$

Observe que $n\ R_k\ m$ sse n e m tém o mesmo resto na divisão por k. Com efeito, assumamos que $n\ R_k\ m$; logo, $n - m = z.k$. Por outro lado, $n = z_1.k + r_1$, $m = z_2.k + r_2$, onde $0 \leq r_1, r_2 < k$. Se $r_1 \geq r_2$, então

$$n - m = (z_1.k + r_1) - (z_2.k + r_2) = (z_1 - z_2).k + (r_1 - r_2) = z.k$$

onde $0 \leq r_1 - r_2 < k$. Pela unicidade do algoritmo da divisão, temos que $r_1 - r_2 = 0$, donde $r_1 = r_2$. Analogamente, se $r_1 \leq r_2$, então

$$m - n = (z_2.k + r_2) - (z_1.k + r_1) = (z_2 - z_1).k + (r_2 - r_1) = (-z).k$$

onde $0 \leq r_2 - r_1 < k$. Pela unicidade do algoritmo da divisão, temos que $r_2 - r_1 = 0$, donde $r_1 = r_2$. Reciprocamente, se n e m têm o mesmo resto na divisão por k, então $n = z_1.k + r_1$, $m = z_2.k + r_1$, portanto $n - m = (z_1 - z_2).k$, donde $k|(n - m)$, isto é, $n\ R_k\ m$. Provaremos a seguir que R_k é uma relação de equivalência (observe que $F(R_k) = \mathbb{Z}$).

Se $n \in \mathbb{Z}$, então $n - n = 0 = 0.k$, donde $n\ R_k\ n$, isto é, R_k é reflexiva. Se $n\ R_k\ m$, então $n - m = z.k$, donde $m - n = (-z).k$, com $-z \in \mathbb{Z}$; isto é, $m\ R_k\ n$. Finalmente, assumamos que $n\ R_k\ m$, $m\ R_k\ w$. Logo, $n - m = z_1.k$, $m - w = z_2.k$, donde $n - w = (n - m) + (m - w) = z_1.k + z_2.k = (z_1 + z_2).k$, com $z_1 + z_2 \in \mathbb{Z}$. Daqui $n\ R_k\ w$, e R_k é uma relação de equivalência. O conjunto $\Pi(R_k)$ é usualmente denotado por $\mathbb{Z}_k$. Observe que $R_k = R_{-k}$ para todo $k \in \mathbb{Z}$. Para ilustrar estas definições, considere $k = 6$; logo, os únicos restos possíveis da divisão de n por 6 são: 0, 1,..., 5. Daqui inferimos que as únicas classes de equivalência possíveis para R_6 são $\overline{n} \equiv_{def} R_6[n]$, com $0 \leq n \leq 5$, portanto $\mathbb{Z}_6 = \{\overline{0}, \ldots, \overline{5}\}$, sendo que, para $0 \leq n \leq 5$, $\overline{n}$ é o conjunto dos números inteiros m tais que o resto da divisão de m por 6 é n. Analogamente, $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, onde agora $\overline{n} = \{m\ :$ o resto da divisão de m por 3 é $n\}$ $(n = 0, 1, 2)$. Observe que, se $6|(n - m)$, então $3|(n - m)$, pois $3|6$; daqui, R_6 é mais fina do que R_3. Dado que $3 = 1.3 + 0$, $4 = 1.3 + 1$, $5 = 1.3 + 2$, então $R_6[3] \subseteq R_3[0]$, $R_6[4] \subseteq R_3[1]$ e $R_6[5] \subseteq R_3[2]$, donde

$$R_3[0] = R_6[0] \cup R_6[3],\ \ R_3[1] = R_6[1] \cup R_6[4],\ \ R_3[2] = R_6[2] \cup R_6[5].$$

Em geral, R_m é mais fina do que R_n sse $n|m$. Temos portanto que R_0 produz a partição mais fina de $\mathbb{Z}$, pois $m|0$ para todo m. Para verificar isto diretamente, observe que $n\ R_0\ m$ sse $n - m = z.0 = 0$ sse $n = m$, donde $R_0[n] = \{n\}$ para todo $n \in \mathbb{Z}$. Por outro lado, R_1 produz a partição menos fina $\{\mathbb{Z}\}$. Com efeito, $1|n$ para todo n, donde R_n é mais fina do que R_1. É claro que $n\ R_1$ m sse $1|(n - m)$, condição que resulta verdadeira para todo $n, m \in \mathbb{Z}$, e então $R_1[0] = \mathbb{Z}$. ■

8 Funções

O importante conceito de função, cuja definição foi discutida até finais do século 19, pode ser introduzido elegantemente na linguagem da TC. Informalmente, uma função é uma relação em que cada elemento do domínio tem associado um único elemento na imagem; isto não proibe, é claro, que dois elementos diferentes do domínio possam ter associados o mesmo elemento na imagem.

Definição 8.1 *$fun(f)$ denota $rel(f) \wedge (\forall x)(\forall y)(\forall z)(((x\ f\ y) \wedge (x\ f\ z)) \rightarrow y = z)$ ("f é uma função").*

É claro que $fun(f)$ equivale a: $rel(f) \wedge (\forall x)(x \in dom(f) \rightarrow (\exists! y)(x\ f\ y))$. Usaremos a notação $f(x)$ para indicar o único y tal que $x\ f\ y$. Por exemplo, se $f = \{\langle 1,2\rangle, \langle 2,2\rangle, \langle 3,5\rangle\}$, então $f(1) = 2$, $f(2) = 2$, $f(3) = 5$. A notação $f(x)$ (introduzida na Definição 5.1) é legitimada pela Proposição 5.3. A composição $f \bullet g$ de duas funções f, g é definida de maneira que $(f \bullet g)(x) = f(g(x))$. Isto significa que $f \bullet g$ é a composição (como relações) $g \circ f$ introduzida na Definição 5.6.

Lema 8.2 *(a) $S \vdash fun(f) \rightarrow (\forall x)(\forall y)((x\ f\ y) \rightarrow y = f(x))$.*
(b) $S \vdash (fun(f) \wedge x \in dom(f)) \rightarrow (x\ f\ f(x))$.

Demonstração: (a) Assuma $fun(f)$. Se $x\ f\ y$, provaremos:

$$z \in y \leftrightarrow (\exists u)((\forall w)((x\, f\, w) \leftrightarrow w = u) \wedge z \in u)$$

(lembrando que a formula à direita do primeiro " $\leftrightarrow$ " significa "$z \in f(x)$"). Daqui, teremos, por [A1], que $y = f(x)$. Com efeito, temos o seguinte:
$fun(f)$, $x\ f\ y$, $x\ f\ w$ implica $w = y$; $x\ f\ y$, $w = y$ implica $x\ f\ w$, portanto $fun(f)$, $x\ f\ y$ implica $(\forall w)(x\ f\ w \leftrightarrow w = y)$, donde $fun(f)$, $x\ f\ y$, $z \in y$ implica $(\forall w)(x\ f\ w \leftrightarrow w = y) \wedge z \in y$. Daqui obtemos $(\exists u)((\forall w)((x\ f\ w) \leftrightarrow w = u) \wedge z \in u)$, isto é: $fun(f)$, $x\ f\ y$ implica $z \in y \rightarrow z \in f(x)$.
Por outro lado, $x\ f\ y$, $(\forall w)((x\ f\ w) \leftrightarrow w = u)$ implica $(x\ f\ y) \wedge (x\ f\ u)$, donde, usando $fun(f)$, obtemos $y = u$. Daqui, provamos: $fun(f)$, $x\ f\ y$, $z \in f(x)$ implica $z \in y$, isto é: $fun(f)$, $x\ f\ y$ implica $z \in f(x) \rightarrow z \in y$, portanto $fun(f)$, $x\ f\ y$ implica $y = f(x)$.
(b) Assuma $fun(f) \wedge x \in dom(f)$. Provaremos que $x\ f\ f(x)$. Com efeito, $fun(f)$, $x\ f\ u$ implica $u = f(x)$, por (a). Logo, $fun(f)$, $x\ f\ u$ implica $x\ f\ f(x)$. Portanto $fun(f)$, $(\exists u)(x\ f\ u)$ implica $x\ f\ f(x)$. Mas $x \in dom(f)$ implica $(\exists u)(x\ f\ u)$, portanto: $fun(f)$, $x \in dom(f)$ implica $x\ f\ f(x)$. ■

Proposição 8.3 *(a) $S \vdash (fun(f) \wedge fun(g)) \rightarrow ((x\ (g \circ f)\ y) \rightarrow y = f(g(x)))$.*
(b) $S \vdash (fun(f) \wedge fun(g) \wedge x \in dom(g) \wedge g(x) \in dom(f)) \rightarrow (x\ (g \circ f)\ f(g(x)))$.

Demonstração: (a) Se $x\ (g \circ f)\ y$, então $x\ g\ z$, $z\ f\ y$ para algum z. Pelo Lema 8.2(a) obtemos $z = g(x)$ e $y = f(z)$, donde $y = f(g(x))$, pelas regras da igualdade.
(b) Pelo Lema 8.2(b), temos que $g(x)\ f\ f(g(x))$, pois $g(x) \in dom(f)$. Como $x \in dom(g)$, então $x\ g\ g(x)$, novamente por 8.2(b). Daqui obtemos: $x\ g\ g(x)$, $g(x)\ f\ f(g(x))$, e então $x\ (g \circ f)\ f(g(x))$, pela Definição 5.6. ■

Vemos assim que $f \bullet g \equiv_{def} g \circ f$ satisfaz a propriedade desejada $x\ (f \bullet g)\ y$ sse $y = f(g(x))$ (sob certas condições razoáveis estabelecidas na Proposição 8.3(b)). Uma propriedade fundamental é que a composição de funções é uma função.

Proposição 8.4 *(a) $S \vdash (fun(f) \wedge fun(g)) \rightarrow (fun(f \cap g) \wedge fun(f \bullet g))$.*
(b) $S \vdash (fun(f) \wedge fun(g) \wedge x \in dom(f \bullet g)) \rightarrow (f \bullet g)(x) = f(g(x))$.

Demonstração: (a) Sejam x, y, z tais que , $x\ (f \cap g)\ y$, $x\ (f \cap g)\ z$. Daqui obtemos $x\ f\ y$, $x\ g\ y$, $x\ f\ z$, $x\ g\ z$. Como $fun(f)$, $fun(g)$, então $y = z$, donde $fun(f \cap g)$. Por outro lado, suponha que $x\ (f \bullet g)\ y$, $x\ (f \bullet g)\ z$. Pela Proposição 8.3(a) obtemos $y = f(g(x))$, $z = f(g(x))$, donde $y = z$ e então $fun(f \bullet g)$.
(b) Assuma $fun(f)$, $fun(g)$, $x \in dom(f \bullet g)$. Pelo item (a) obtemos $fun(f \bullet g)$, $x \in dom(f \bullet g)$, donde $x\ (f \bullet g)\ ((f \bullet g)(x))$, pelo Lema 8.2(b). Pela Proposição 8.3(a) obtemos $(f \bullet g)(x) = f(g(x))$. ■

Daqui em diante, quando não houver risco de confusão, escreveremos $f \circ g$ no lugar de $f \bullet g$, se f e g são funções. Algumas das propriedades provadas na Proposição 5.10 podem ser fortalecidas, no caso em que f é função.

Proposição 8.5 *(a)* $S \vdash (f \bullet g)|z = f \bullet (g|z)$.
(b) $S \vdash fun(f) \to (f^{-1}``(a \cap b) = f^{-1}``(a) \cap f^{-1}``(b)) \land (f^{-1}``(a - b) = f^{-1}``(a) - f^{-1}``(b))$.

Demonstração: (a) É uma reformulação da Proposição 5.9(e).
(b) Assuma $fun(f)$. Pela Proposição 5.10(b),(c), basta provar

$$f^{-1}``(a) \cap f^{-1}``(b) \subseteq f^{-1}``(a \cap b),$$

e $f^{-1}``(a - b) \subseteq f^{-1}``(a) - f^{-1}``(b)$.
Se $x \in f^{-1}``(a) \cap f^{-1}``(b)$, então existem $y \in a$, $w \in b$ tais que $x\ f\ y$, $x\ f\ w$. Como $fun(a)$, então $y = w$, portanto $y \in a \cap b$ tal que $x\ f\ y$, donde $x \in f^{-1}``(a \cap b)$.
Seja agora $x \in f^{-1}``(a - b)$. Logo, existe $y \in a - b$ tal que $x\ f\ y$, e então $x \in f^{-1}``(a)$. Se $x \in f^{-1}``(b)$, então existe $z \in b$ tal que $x\ f\ z$. Como $fun(f)$, obtemos $y = z$ donde $y \in b$, uma contradição. Portanto $x \in f^{-1}``(a) - f^{-1}``(b)$. ■

Definição 8.6 *$inj(f)$ denota $fun(f) \land fun(f^{-1})$ (“f é injetora”).*

Proposição 8.7 *(a)* $S \vdash (inj(f) \land x, y \in dom(f)) \to (f(x) = f(y) \leftrightarrow x = y)$.
(b) $S \vdash (inj(f) \land x \in dom(f) \land y \in im(f)) \to (f^{-1}(y) = x \leftrightarrow y = f(x))$.
(c) $S \vdash (inj(f) \land x \in dom(f)) \to f^{-1}(f(x)) = x$.
(d) $S \vdash (inj(f) \land y \in im(f)) \to f(f^{-1}(y)) = y$.
(e) $S \vdash (inj(f) \land inj(g)) \to inj(f \cap g)$.
(f) $S \vdash (inj(f) \land inj(g) \land dom(f) \cap dom(g) = \emptyset \land im(f) \cap im(g) = \emptyset)$
$\to inj(f \cup g)$.

Demonstração: (a) Assuma $inj(f) \land x \in dom(f) \land y \in dom(f)$. Se $f(x) = f(y)$, então obtemos que $f(x)\ f^{-1}\ x$, $f(x)\ f^{-1}\ y$. Mas $fun(f^{-1})$, portanto $x = y$. Reciprocamente, $x = y$ implica $f(x) = f(y)$, pelas regras da igualdade.
(b) Assuma $inj(f) \land x \in dom(f) \land y \in im(f)$. Como $fun(f^{-1}) \land y \in dom(f^{-1})$, então $x = f^{-1}(y)$ implica $y\ f^{-1}\ x$, pelo Lema 8.2(b). Daqui, $x\ f\ y$ e então, pelo Lema 8.2(a), obtemos $y = f(x)$; isto é, $x = f^{-1}(y) \to y = f(x)$. Simetricamente provamos $y = f(x) \to x = f^{-1}(y)$.

(c) Assuma $inj(f) \wedge x \in dom(f)$. Logo $f(x) \in im(f)$ e $f(x) = f(x)$. Pelo item (b) obtemos $x = f^{-1}(f(x))$.
(d) Análogo ao item (c).
(e) Imediato a partir da Proposição 8.4 (a).
(f) $x\ (f \cup g)\ y$, $x\ (f \cup g)\ z$ implica que $(x\ f\ y) \wedge (x\ f\ z)$ ou $(x\ g\ y) \wedge (x\ g\ z)$, mas não ambas simultaneamente. Daqui $y = z$, e $fun(f \cup g)$. Da mesma maneira (lembrando que $(f \cup g)^{-1} = f^{-1} \cup g^{-1}$), $x\ (f \cup g)^{-1}\ y$, $x\ (f \cup g)^{-1}\ z$ implica $(x\ f^{-1}\ y) \wedge (x\ f^{-1}\ z)$ ou $(x\ g^{-1}\ y) \wedge (x\ g^{-1}\ z)$, mas não ambas simultaneamente. Daqui $y = z$, e $fun((f \cup g)^{-1})$. Portanto $inj(f \cup g)$. ■

Definição 8.8 *(a) $fun(f, a, b)$ denota $fun(f) \wedge (dom(f) = a) \wedge (im(f) \subseteq b)$ ("f é uma função de a em b").*
(b) $sobre(f, a, b)$ denota $fun(f) \wedge (dom(f) = a) \wedge (im(f) = b)$ ("f é uma função sobrejetora de a em b").
(c) $inj(f, a, b)$ denota $inj(f) \wedge (dom(f) = a) \wedge (im(f) \subseteq b)$ ("f é uma função injetora de a em b").
(d) $bij(f, a, b)$ denota $inj(f, a, b) \wedge sobre(f, a, b)$ ("f é uma função bijetora de a em b").
(e) $a^b = \{f\ :\ fun(f, b, a)\}$ ("a^b é o conjunto de todas as funções de b em a").

Observação 8.9 *Podemos a partir de agora utilizar a notação usual $f : a \longrightarrow b$ para denotar $fun(f, a, b)$. De fato, utilizaremos as duas notações indistintamente.* ■

Proposição 8.10 *(a) $S \vdash (fun(f, a, b) \wedge fun(g, b, c)) \rightarrow fun(g \circ f, a, c)$.*
(b) $S \vdash inj(f, a, b) \rightarrow (bij(f, a, im(f)) \wedge bij(f^{-1}, im(f), a))$.
(c) $S \vdash bij(f, a, b) \rightarrow bij(f^{-1}, b, a)$.
(d) $S \vdash (bij(f, a, b) \wedge bij(g, b, c)) \rightarrow bij(g \circ f, a, c)$.
(e) $S \vdash bij(f, a, b) \rightarrow ((f \circ f^{-1} = I(b)) \wedge (f^{-1} \circ f = I(a)))$.
(f) $S \vdash fun(f, a, b) \rightarrow ((I(b) \circ f = f) \wedge (f \circ I(a) = f))$.

Demonstração: (a) Notar que $g \circ f$ é utilizado para denotar $g \bullet f$, isto é, $f \circ g$ (como relações). Assuma então $f : a \longrightarrow b$, $g : b \longrightarrow c$. Daqui obtemos:

$$fun(f),\ dom(f) = a,\ im(f) \subseteq b,\ fun(g),\ dom(g) = b,\ im(g) \subseteq c.$$

Pela Proposição 8.4(a) obtemos $fun(g \circ f)$. Por definição de composição, $dom(g \circ f) \subseteq dom(f)$, $im(g \circ f) \subseteq im(g)$; isto é, $dom(g \circ f) \subseteq a$, $im(g \circ f) \subseteq c$. Seja $x \in a$; pela Proposição 8.3(b) temos que $x\ (g \circ f)\ (g(f(x))$, pois $a = dom(f)$ e $b = dom(g)$, donde $x \in dom(f) \wedge f(x) \in dom(g)$. Daqui $x \in dom(g \circ f)$, isto é, $dom(g \circ f) = a$. Portanto $fun(g \circ f, a, c)$.
(b) Observe que $dom(f^{-1}) = im(f)$, $im(f^{-1}) = dom(f)$. Assuma $inj(f, a, b)$. Logo, temos o seguinte:

$$fun(f),\ fun(f^{-1}),\ dom(f^{-1}) = im(f),\ im(f^{-1}) = a.$$

Daqui obtemos imediatamente $inj(f^{-1}, im(f), a)$, $sobre(f^{-1}, im(f), a)$, isto é, $bij(f^{-1}, im(f), a)$. A fórmula $bij(f, a, im(f))$ é obtida trivialmente.

(c) Por (b) inferimos $bij(f,a,b) \to bij(f^{-1},b,a)$, pois $im(f) = b$.
(d) Assuma $bij(f,a,b)$, $bij(g,b,c)$. Daqui obtemos:

$$fun(f,a,b),\ fun(f^{-1},b,a),\ fun(g,b,c),\ fun(g^{-1},c,b).$$

Por (a) e pela Proposição 5.8(d) obtemos $fun(g \circ f, a, c)$, $fun((g \circ f)^{-1}, c, a)$. Daqui $dom(g \circ f) = a$, $im(g \circ f) = c$, $fun(g \circ f)$, $fun((g \circ f)^{-1})$, e então $bij(g \circ f, a, c)$.
(e) Por (a) temos $fun(f \circ f^{-1}, b, b)$, $fun(f^{-1} \circ f, a, a)$. Seja $x \in b$; $x\ f \circ f^{-1}\ y$ implica $x\ f^{-1}\ z$, $z\ f\ y$ para algum $z \in a$. Daqui $z\ f\ x$, $z\ f\ y$ e então $y = x$, isto é: $(f \circ f^{-1})(x) = x$ para todo $x \in b$, donde $f \circ f^{-1} = I(b)$. Seja agora $x \in a$; $x\ f^{-1} \circ f\ y$ implica $x\ f\ z$, $z\ f^{-1}\ y$ para algum $z \in b$. Daqui $z\ f^{-1}\ x$, $z\ f^{-1}\ y$, donde $x = y$, isto é: $(f^{-1} \circ f)(x) = x$ para todo $x \in a$. Portanto $f^{-1} \circ f = I(a)$.
(f) Por (a), $fun(I(b) \circ f, a, b) \wedge fun(f \circ I(a), a, b)$. Seja $x \in a$; logo $(I(b) \circ f)(x) = I(b)(f(x)) = f(x)$, donde $I(b) \circ f = f$. Por outro lado, $(f \circ I(a))(x) = f(I(a)(x)) = f(x)$, donde $f \circ I(a) = f$. ■

Proposição 8.11 *(a) O termo a^b é legitimado em S.*
(b) $a^{\emptyset} = \{\emptyset\}$.
(c) $a \neq \emptyset \to \emptyset^a = \emptyset$.
(d) $a^b = \emptyset \leftrightarrow a = \emptyset \wedge b \neq \emptyset$.
(e) $a^{\{x\}} = \{\{\langle x, y\rangle\} \ :\ y \in a\}$.
(f) $a \subseteq b \to a^c \subseteq b^c$.

Demonstração: (a) Claramente $a^b = \{f \ :\ f \in \mathcal{P}(b \times a) \wedge fun(f,b,a)\}$, legitimado portanto por [A2].
(b) $a^{\emptyset} \subseteq \mathcal{P}(\emptyset \times a) = \mathcal{P}(\emptyset) = \{\emptyset\}$. Por outro lado $fun(\emptyset, \emptyset, a)$ é satisfeita trivialmente, e então $a^{\emptyset} = \{\emptyset\}$.
(c) Seja $a \neq \emptyset$, e suponha que $fun(f, a, \emptyset)$. Seja $x \in a$; logo, $x \in dom(f)$, portanto $f(x) \in \emptyset$, uma contradição.
(d) Assuma $f \in a^b$. Se $b \neq \emptyset$, seja $x \in b$; portanto $f(x) \in a$, donde $a \neq \emptyset$, provando assim: $a^b \neq \emptyset \to (b \neq \emptyset \to a \neq \emptyset)$. Mas $b \neq \emptyset \to a \neq \emptyset$ equivale a $\neg(a = \emptyset \wedge b \neq \emptyset)$. Reciprocamente, suponha $\neg(a = \emptyset \wedge b \neq \emptyset)$, isto é, $a \neq \emptyset \vee b = \emptyset$. Se $a \neq \emptyset$, seja $y \in a$. Logo, é imediato que $f = \{\langle x, y\rangle \ :\ x \in b\}$ é legitimado, e $fun(f, b, a)$. Daqui $a^b \neq \emptyset$. Por outro lado, $b = \emptyset$ implica que $a^b = \{\emptyset\} \neq \emptyset$, por (b). Portanto $\neg(a = \emptyset \wedge b \neq \emptyset) \to a^b \neq \emptyset$.
(e) Seja $b = \{\{\langle x, y\rangle\} \ :\ y \in a\}$; é claro que b é legitimado, e $b \subseteq a^{\{x\}}$. Seja $f \in a^{\{x\}}$; como $dom(f) = \{x\}$, então $f(x) \in a$ tal que $f = \{\langle x, f(x)\rangle\}$; daqui $f \in b$.
(f) Imediato das definições. ■

9 Equipolência

A noção de *equipolência* foi apontada por Cantor como um conceito fundamental, pois permite generalizar a noção de número natural para *cardinais*. Essencialmente, dois conjuntos são *equipolentes* se existe uma bijeção entre eles, o que equivale a afirmar que possuem o mesmo cardinal.

Definição 9.1 *$a \approx b$ denota $(\exists f)bij(f, a, b)$ ("a e b são equipolentes").*

Exemplo 9.2 Sejam $a = \{1, 2, 3\}$, $b = \{3, 4, 5\}$. Então

$$f = \{\langle 1, 3\rangle, \langle 2, 4\rangle, \langle 3, 5\rangle\}, \; g = \{\langle 1, 5\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle\}$$

são duas bijeções entre a e b, cada uma delas garantindo $a \approx b$. ∎

A intuição por trás de $a \approx b$ é que "a e b têm o mesmo número de elementos", o que pode ser percebido nos exemplos em que a e b são finitos (todas estas são noções por enquanto intuitivas, mas serão formalizadas em ZF). É também claramente intuitivo que um conjunto finito não pode ser equipolente com um subconjunto próprio. No caso de a ser infinito, esta propriedade deixa de ser verdadeira: o conjunto $\mathbb{P}$ dos números naturais pares é um subconjunto próprio do conjunto $\mathbb{N}$ dos números naturais, embora $f(n) = 2.n$ seja uma bijeção entre $\mathbb{N}$ e $\mathbb{P}$. Vemos assim que *a parte é menor do que a totalidade* não tem mais validade no caso infinito.

Proposição 9.3 *(a) $S \vdash a \approx a$.*
(b) $S \vdash (a \approx b) \to (b \approx a)$.
(c) $S \vdash ((a \approx b) \wedge (b \approx c)) \to (a \approx c)$.

Demonstração: (a) Pode ser provado facilmente que a relação $I(a)$ introduzida previamente à Proposição 6.2 é uma bijeção entre a e a.
(b), (c) São conseqüências imediatas da Proposição 8.10(c),(d), respectivamente. ∎

Os seguintes resultados serão úteis para a definição da artimética cardinal.

Proposição 9.4 *As seguintes fórmulas são teoremas de S:*
(a) $((a \approx b) \wedge (c \approx d) \wedge (a \cap c = \emptyset) \wedge (b \cap d = \emptyset)) \to (a \cup c \approx b \cup d)$.
(b) $((a \approx b) \wedge (c \approx d)) \to (a \times c \approx b \times d)$.
(c) $a \times b \approx b \times a$.
(d) $a \times (b \times c) \approx (a \times b) \times c$.
(e) $(a \times \{x\} \approx a) \wedge (\{x\} \times a \approx a)$.
(f) $(\exists c)(\exists d)((a \approx c) \wedge (b \approx d) \wedge (c \cap d = \emptyset))$.

Demonstração: (a) Sejam f, g tais que $bij(f, a, b)$, $bij(g, c, d)$. Por hipótese temos que $dom(f) \cap dom(g) = \emptyset$, $im(f) \cap im(g) = \emptyset$, portanto $inj(f \cup g)$, pela Proposição 8.7(f). É imediato provar $bij(f \cup g, a \cup c, b \cup d)$.
(b) Sejam f, g tais que $bij(f, a, b)$, $bij(g, c, d)$. É imediato que $h \subseteq (a \times c) \times (b \times d)$ dado por

$$h = \{\langle\langle x, y\rangle, \langle f(x), g(y)\rangle\rangle \; : \; (x \in a) \wedge (y \in c)\}$$

é legitimado, estabelecendo uma bijeção $h(\langle x, y\rangle) = \langle f(x), g(y)\rangle$ entre $a \times c$ e $b \times d$.
(c) É imediato que $f(\langle x, y\rangle) = \langle y, x\rangle$ é uma bijeção entre $a \times b$ e $b \times a$.
(d) $f(\langle x, \langle y, z\rangle\rangle) = \langle\langle x, y\rangle, z\rangle$ é uma bijeção entre $a \times (b \times c)$ e $(a \times b) \times c$.

(e) $f_1(\langle y,x\rangle) = y$, $f_2(\langle x,y\rangle) = y$ são bijeções.
(f) Sejam $c = a \times \{\emptyset\}$, $d = b \times \{\{\emptyset\}\}$. Logo $a \approx c$, $b \approx d$, pelo item (e), e $c \cap d = \emptyset$. ■

Os seguintes resultados serão utilizados para a exponenciação cardinal.

Proposição 9.5 *Em S as seguintes fórmulas são teoremas:*
(a) $((a \approx b) \wedge (c \approx d)) \to (a^c \approx b^d)$.
(b) $(b \cap c = \emptyset) \to (a^{b\cup c} \approx a^b \times a^c)$.
(c) $(a \times b)^c \approx a^c \times b^c$.
(d) $(a^b)^c \approx a^{b\times c}$.

Demonstração: (a) Se $a^c = \emptyset$ então $a = \emptyset$ e $c \neq \emptyset$, donde $b = \emptyset$ e $d \neq \emptyset$. Logo $b^d = \emptyset$ e então $a^c \approx b^d$. Suponha agora que $a^c \neq \emptyset$. Sejam f, g tais que $bij(f,a,b)$, $bij(g,c,d)$. Dada $h \in a^c$, então $f \circ h \in b^c$, pela Proposição 8.10(a). A partir dai, obtemos da mesma maneira $f \circ h \circ g^{-1} \in b^d$. Definimos então uma função $f'(h) = f \circ h \circ g^{-1}$ tal que $f' : a^c \longrightarrow b^d$. Dado $h' \in b^d$, então $h = f^{-1} \circ h' \circ g$ é o único elemento de a^c tal que $h' = f \circ h \circ g^{-1} = f'(h)$, pela Proposição 8.10(e),(f). Portanto f' é uma bijeção com inversa $f'^{-1}(h') = f^{-1} \circ h' \circ g$.
(b) $a^{b\cup c} = \emptyset$ implica $a = \emptyset$, $b \cup c \neq \emptyset$ implica $a = \emptyset$ e: $b \neq \emptyset$ ou $c \neq \emptyset$ implica $a^b = \emptyset$ ou $a^c = \emptyset$ implica $a^b \times a^c = \emptyset$. Logo $a^{b\cup c} \approx a^b \times a^c$. Suponha agora que $a^{b\cup c} \neq \emptyset$. Dado $f \in a^{b\cup c}$, então $\langle f|b, f|c\rangle \in a^b \times a^c$. Defina

$$h = \{\langle f, \langle f|b, f|c\rangle\rangle \ : \ f \in a^{b\cup c}\},$$

legitimado por [A2]. É claro que $h : a^{b\cup c} \longrightarrow a^b \times a^c$ é uma função. Por outro lado, se $\langle f_1, f_2\rangle \in a^b \times a^c$, então $f_1 \cup f_2 \in a^{b\cup c}$ tal que $h(f_1 \cup h_2) = \langle f_1, f_2\rangle$. Se $h(f) = \langle f_1, f_2\rangle$, então $f = f_1 \cup f_2$, donde $h^{-1} : a^b \times a^c \longrightarrow a^{b\cup c}$ é uma função. Daqui infere-se que $bij(h, a^{b\cup c}, a^b \times a^c)$.
(c) Se $(a \times b)^c = \emptyset$ então $a \times b = \emptyset$ e $c \neq \emptyset$, donde $a = \emptyset$ ou $b = \emptyset$, e $c \neq \emptyset$. Daqui $a^c = \emptyset$ ou $b^c = \emptyset$ donde $a^c \times b^c = \emptyset$, e então $(a \times b)^c \approx a^c \times b^c$. Suponha agora que $(a \times b)^c \neq \emptyset$. Dada $f \in (a \times b)^c$, considere

$$f_a = \{\langle x, y\rangle \ : \ (\exists z)(\langle x, \langle y, z\rangle\rangle \in f)\}, \qquad f_b = \{\langle x, z\rangle \ : \ (\exists y)(\langle x, \langle y, z\rangle\rangle \in f)\}.$$

Isto é, se $\pi_1 \in a^{a\times b}$ e $\pi_2 \in b^{a\times b}$ são dadas por $\pi_1(\langle x,y\rangle) = x$ e $\pi_2(\langle x,y\rangle) = y$ (as *projeções canônicas*), então $f_a = \pi_1 \circ f$ e $f_b = \pi_2 \circ f$. É claro que $f_a \in a^c$, $f_b \in b^c$, $h = \{\langle f, \langle f_a, f_b\rangle\rangle \ : \ f \in (a \times b)^c\}$ é legitimado, e $h : (a \times b)^c \longrightarrow a^c \times b^c$ é uma função. Dada $\langle f_1, f_2\rangle \in a^c \times b^c$, então $f = \{\langle x, \langle f_1(x), f_2(x)\rangle\rangle \ : \ x \in c\}$ é legitimado, $f \in (a \times b)^c$, e $h(f) = \langle f_1, f_2\rangle$. E claro que $h(f') = h(f)$ implica $f = f'$, portanto $fun(h^{-1}, a^c \times b^c, (a \times b)^c)$ e assim $bij(h, (a \times b)^c, a^c \times b^c)$.
(d) $a^{b\times c} = \emptyset$ implica $a = \emptyset$, $b \times c \neq \emptyset$ implica $a = \emptyset$, $b \neq \emptyset$, $c \neq \emptyset$ implica $a^b = \emptyset$, $c \neq \emptyset$ implica $(a^b)^c = \emptyset$. Logo $(a^b)^c \approx a^{b\times c}$. Suponha agora que $a^{b\times c} \neq \emptyset$. Seja $f \in a^{b\times c}$. Para cada $y \in c$, seja

$$f_y = \{\langle x, z\rangle \ : \ \langle\langle x, y\rangle, z\rangle \in f\}.$$

É claro que f_y é legitimado, $f_y \in a^b$, e $f_y(x) = f(\langle x, y\rangle)$. Além disso, $h_f = \{\langle y, f_y\rangle \ : \ y \in c\} \in (a^b)^c$, onde $h_f(y) = f_y$. Portanto $h = \{\langle f, h_f\rangle \ : \ f \in a^{b\times c}\}$

é legitimado, e $h : a^{b\times c}\longrightarrow(a^b)^c$ é uma função, onde $h(f) = h_f$. Dada $f' \in (a^b)^c$, então $f(\langle x, y\rangle) = f'(y)(x)$ é uma função, $f \in a^{b\times c}$, e $h(f) = f'$. Além disso, $h(f_1) = h(f_2)$ implica $f_1 = f_2$, portanto $fun(h^{-1}, (a^b)^c, a^{b\times c})$ e assim $bij(h, a^{b\times c}, (a^b)^c)$. ■

Observação 9.6 Neste ponto da nossa exposição sobre a Teoria Axiomática de Conjuntos assumiremos que o leitor já assimilou o fato de que os enunciados dos teoremas, assim como as respectivas demonstrações, são realizados no marco formal de ZF (ou de certos fragmentos, tais como S). Para simplificar a exposição, a partir daqui os enunciados e demonstrações dos teoremas de ZF serão feitos numa linguagem coloquial, omitindo os detalhes mais formais. ■

Antecipando a definição de $2 = \{\emptyset, \{\emptyset\}\}$, provamos o seguinte resultado útil, introduzindo a idéia que os subconjuntos de um conjunto a são as funções características sobre a.

Proposição 9.7 *Temos que* $\mathcal{P}(a) \approx 2^a$.

Demonstração: Seja $b \subseteq a$. Definimos a função $g_b : a\longrightarrow 2$ pela regra: $g_b(x) = \{\emptyset\}$ se $x \in b$, e $g_b(x) = \emptyset$ se $x \notin b$. Logo, $h(b) = g_b$ define uma função $h : \mathcal{P}(a)\longrightarrow 2^a$. Por outro lado, $h(b) = h(c)$ implica $g_b = g_c$, isto é, $g_b(x) = g_b(x)$ para todo $x \in a$. Portanto: $g_b(x) = \{\emptyset\}$ sse $g_c(x) = \{\emptyset\}$, donde $x \in b$ sse $x \in c$. Por [A1] obtemos $b = c$, e então h é injetora. Por outro lado, se $g \in 2^a$, considere $b = \{x \ : \ x \in a \wedge g(x) = \{\emptyset\}\}$. Logo b é legitimado por [A2], e claramente $h(b) = g$. Daqui h é sobrejetora, e então h é uma bijeção entre $\mathcal{P}(a)$ e 2^a. Assim $\mathcal{P}(a) \approx 2^a$. ■

Vamos definir a continuação o conceito de *ser menor ou igual* em termos de *tamanho* (obviamente estes conceitos são ainda difusos).

Definição 9.8 $a \preceq b$ *denota* $(\exists c)(c \subseteq b \wedge a \approx c)$.

Proposição 9.9 *(a)* $a \approx b$ *implica* $a \preceq b$.
(b) $a \subseteq b$ *implica* $a \preceq b$.
(c) $a \preceq a \cup b$.
(d) $a \preceq b$ *e* $b \preceq c$ *implica* $a \preceq c$.

Demonstração: (a) Temos que $a \approx c$ com $c = b \subseteq b$. Logo $a \preceq b$.
(b) A função $I(a)$ produz: $a \approx c$ com $c = a \subseteq b$. Logo $a \preceq b$.
(c) É uma conseqüência direta de (b).
(d) Suponha que $a \approx a_1$ (via f) com $a_1 \subseteq b$, e $b \approx b_1$ (via g) com $b_1 \subseteq c$. Logo $g \circ f$ é uma bijeção de a em $g``a_1 \subseteq c$. Daqui $a \preceq c$. ■

O seguinte resultado, cuja demonstração é mais complicada, foi conjecturado por Cantor e provado independientemente por Schröder e Bernstein em 1890. A seguinte prova é devida a Fraenkel e Whitaker.

Teorema 9.10 (Cantor-Schröder-Bernstein)
Se $a \preceq b$ *e* $b \preceq a$*, então* $a \approx b$*.*

Demonstração: Seja f uma bijeção de a em $b_1 \subseteq b$, e g uma bijeção de b em $a_1 \subseteq a$. Observe que o resultado ($a \approx b$) estará provado se encontramos um conjunto $d \subseteq a$ tal que $g|(b - f``d)$ é uma bijeção de $b - f``d$ em $a - d$. Com efeito, nesse caso teriamos que $h = (f|d) \cup (g^{-1}|(a - d))$ é uma bijeção entre a e b, como pode ser facilmente conferido usando a Proposição 8.7(f). O nosso objetivo é portanto achar um conjunto d com a propriedade mencionada acima. Para isso considere o conjunto

$$u = \{c \ : \ c \subseteq a \wedge g``(b - f``(c)) \subseteq a - c\}.$$

Dado que $c \subseteq a$ sse $c \in \mathcal{P}(a)$, então u é legitimado por [A2].
Fatos: (1) Dados $x, y \subseteq z$, então: $x \subseteq z - y$ sse $y \subseteq z - x$, e $x = z - y$ sse $y = z - x$.
(2) Sejam z, y conjuntos. Se $x \subseteq y$ para todo $x \in z$, então $\bigcup z \subseteq y$.
(3) Se $c_1 \subseteq c_2 \subseteq a$, então $a - g``(b - f``c_1) \subseteq a - g``(b - f``c_2)$.
(4) $\bigcup u \subseteq a - g``(b - f``\bigcup u)$ (onde u é deinido como acima).
Com efeito:
(1) Suponha que $x \subseteq z - y$. Seja $w \in y$; logo, $w \in z$, pois $y \subseteq z$. Se $w \in x$, então $w \in z - y$, isto é, $w \notin y$, uma contradição. Portanto $w \notin x$, donde $w \in z - x$ e então $y \subseteq z - x$. Simetricamente, $y \subseteq z - x$ implica $x \subseteq z - y$. Para a segunda parte, suponha que $x = z - y$; logo $x \subseteq z - y$ e então, pela primeira parte, $y \subseteq z - x$. Seja $w \in z - x$; se $w \notin y$, então $w \in z - y = x$. Mas $w \notin x$, por hipótese. Esta contradição mostra que $w \in y$, isto é: $z - x = y$. A prova de que $y = z - x$ implica $x = z - y$ é simétrica.
(2) Assuma que $x \subseteq y$ para todo $x \in z$, e seja $w \in \bigcup z$. Logo $w \in x$ para algum $x \in z$, pela definição de $\bigcup z$. Mas $x \subseteq y$, por hipótese; logo $w \in y$. Daqui $\bigcup z \subseteq y$.
(3) Se $c_1 \subseteq c_2 \subseteq a$, então $f``c_1 \subseteq f``c_2 \subseteq b$ donde $b - f``(c_2) \subseteq b - f``(c_1)$. Portanto

$$g``(b - f``(c_2)) \subseteq g``(b - f``(c_1)) \subseteq a$$

e então $a - g``(b - f``c_1) \subseteq a - g``(b - f``c_2)$.
(4) Seja $c \in u$; logo $g``(b - f``(c)) \subseteq a - c$ e então, por (1),

$$c \subseteq a - g``(b - f``(c)). \qquad (*)$$

Por outro lado $\bigcup u \subseteq a$, por (2). Além disso, $c \subseteq \bigcup u$: com efeito, se $x \in c$ então $(x \in c) \wedge (c \in u)$ portanto $x \in \bigcup u$. De $c \subseteq \bigcup u \subseteq a$ infere-se que $a - g``(b - f``(c)) \subseteq a - g``(b - f``\bigcup u)$, por (3). Portanto $c \subseteq a - g``(b - f``\bigcup u)$ para todo $c \in u$, por $(*)$, donde $\bigcup u \subseteq a - g``(b - f``\bigcup u)$, por (2). Isto conclui a prova dos **Fatos**.
Considere $w = a - g``(b - f``\bigcup u)$. Por (4) temos que $\bigcup u \subseteq w \subseteq a$, logo

$$w = a - g``(b - f``\bigcup u) \subseteq a - g``(b - f``w),$$

por (3). Por (1) obtemos $g``(b - f``w) \subseteq a - w$, isto é, $w \in u$. Daqui $w \subseteq \bigcup u$, donde $w = \bigcup u$. Isto é,

$$a - g``(b - f``\bigcup u) = \bigcup u.$$

Pela segunda parte de (1) obtemos $g``(b - f``\bigcup u) = a - \bigcup u$. Vemos assim que $d = \bigcup u$ satisfaz a propriedade requerida. ■

Proposição 9.11 *Se $a \preceq b$ e $c \preceq d$, então:*
(i) Se $b \cap d = \emptyset$ então $a \cup c \preceq b \cup d$;
(ii) $a \times c \preceq b \times d$;
(iii) $a^c \preceq b^d$ se não é o caso que: $a = b = c = \emptyset$ e $d \neq \emptyset$.

Demonstração: Sejam f_1 e f_2 bijeções de a em $b_1 \subseteq b$ e de c em $d_1 \subseteq d$, respectivamente.
(i) Temos que $a \cup c = (a - c) \cup c$, com $(a - c) \cap c = \emptyset$. Como $b \cap d = \emptyset$, então $f_1``(a - c) \cap d_1 = \emptyset$. Portanto $h = (f_1|(a - c)) \cup f_2$ é uma bijeção entre $a \cup c$ e $f_1``(a - c) \cup d_1 \subseteq b \cup d$.
(ii) Pela Proposição 9.4(b), $a \times c \approx b_1 \times d_1 \subseteq b \times d$.
(iii) $a \approx b_1$ e $c \approx d_1$ implicam que $a^c \approx b_1^{d_1} \subseteq b^{d_1}$, pela Proposição 9.5(a). A prova estará terminada se encontrarmos uma injeção de b^{d_1} em b^d. O único caso em que isto não é possível é quando $b^d = \emptyset$ e $b^{d_1} \neq \emptyset$, e é por isso que a hipótese adicional (*não é o caso que $a = b = c = \emptyset$ e $d \neq \emptyset$*) foi colocada. Com efeito, se $b^d = \emptyset$, então $d \neq \emptyset$ e $b = \emptyset$, pela Proposição 8.11(d). Nesse caso $a = \emptyset$. Agora, se $d_1 = \emptyset$ (o que equivale a ter $b^{d_1} \neq \emptyset$), então $c = \emptyset$, donde $a = b = c = \emptyset$ e $d \neq \emptyset$, contrariando a nossa hipótese. Logo $d_1 \neq \emptyset$ e então $b^{d_1} = \emptyset$, pela Proposição 8.11(d). Ou seja: $b^d = \emptyset$ implica $b^{d_1} = \emptyset$, e então $a^c = \emptyset$, donde $a^c \preceq b^d$. Suponha finalmente que $b^d \neq \emptyset$. Os casos $b^{d_1} = \emptyset$ ou $d = \emptyset$ implicam trivialmente que $a^c \preceq b^d$. Suponha então que $b^{d_1} \neq \emptyset$ e $d \neq \emptyset$. Dado que $b^d \neq \emptyset$ e $d \neq \emptyset$, então $b \neq \emptyset$. Fixemos $x_0 \in b$. Para $f \in b^{d_1}$ e $x \in d$, defina

$$h(f)(x) = \begin{cases} f(x) & \text{se } x \in d_1 \\ x_0 & \text{se } x \in d - d_1 \end{cases}.$$

Ou seja: $h(f) = f \cup \{\langle x, x_0\rangle : x \in d - d_1\}$. Claramente $h(f) \in b^d$ e então $h : b^{d_1} \longrightarrow b^d$ é uma função. Observe que $f \cap \{\langle x, x_0\rangle : x \in d - d_1\} = \emptyset$ (pois $\langle x, y\rangle \in f$ implica $x \in d_1$ implica $\langle x, y\rangle \notin \{\langle x, x_0\rangle : x \in d - d_1\}$). Daqui $h(f) = h(g)$ implica $f = g$, isto é, h é injetora. Seja g é uma bijeção entre a^c e $b_1^{d_1}$ (lembre que $a^c \approx b_1^{d_1}$). Daqui $h \circ g$ é uma bijeção de a^c em $h``(b_1^{d_1}) \subseteq b^d$, isto é, $a^c \preceq b^d$. ■

Definição 9.12 *$a \prec b$ denota $a \preceq b \wedge \neg(b \preceq a)$.*

Proposição 9.13 *(i) Não é o caso que $a \prec a$.*
(ii) Se $a \prec b$ então não é o caso que $b \prec a$.
(iii) Se $a \prec b$ e $b \prec c$ então $a \prec c$.

Demonstração: (i) Pela Definição 9.12, $a \prec a$ sse $a \preceq a$ e não é o caso que $a \preceq a$, uma contradição. Logo não é o caso que $a \prec a$.
(ii) Assuma $a \prec b$; isto implica que $a \preceq b$ e não $b \preceq a$. Por outro lado, $b \prec a$ equivale a $b \preceq a$ e não $a \preceq b$. Portanto não podemos ter $b \prec a$, pois $a \preceq b$, por hipótese.
(iii) Assuma $a \prec b$ e $b \prec c$. Logo $a \preceq b$ e $b \preceq c$, donde $a \preceq c$. Se $c \preceq a$, então $c \preceq b$, contrariando $b \prec c$. Portanto não podemos ter $c \preceq a$, donde $a \prec c$. ■

Estabeleceremos algumas relações entre $\preceq$ e $\prec$.

Proposição 9.14 *(i) Se $a \preceq b$ então não $b \prec a$.*
(ii) Se $a \preceq b$ e $b \prec c$ então $a \prec c$.
(iii) Se $a \prec b$ e $b \preceq c$, então $a \prec c$.
(iv) $a \preceq b$ sse $a \approx b$ ou $a \prec b$.

Demonstração: (i) Pela Definição 9.12, $b \prec a$ implica que não $a \preceq b$. Portanto $a \preceq b$ implica $b \not\prec a$.
(ii) Assuma $a \preceq b$ e $b \prec c$. Daqui $a \preceq b$ e $b \preceq c$, donde $a \preceq c$. Se $c \preceq a$ então $c \preceq b$, contrariando $b \prec c$. Portanto não é o caso que $c \preceq a$, donde $a \prec c$.
(iii) Assuma $a \prec b$ e $b \preceq c$. Como antes, obtemos $a \preceq c$. Se $c \preceq a$ então $b \preceq a$, pois $b \preceq c$; mas isto contraria $a \prec b$. Portanto $c \not\preceq a$, donde $a \prec c$.
(iv) Assuma que $a \preceq b$. Se $a \not\prec b$ então, pela Definição 9.12, inferimos que $b \preceq a$ ou $a \not\preceq b$. Daqui obtemos que $b \preceq a$ e então, pelo Teorema 9.10, $a \approx b$. provamos desta maneira que $a \preceq b$ implica $a \approx b$ ou $a \prec b$. Reciprocamente, suponha que $a \approx b$. Logo $a \preceq b$. Se $a \prec b$, então $a \preceq b$, pela Definição 9.12. Isto prova que $a \approx b$ ou $a \prec b$ implica $a \preceq b$. ■

Observe que o item (iv) da proposição acima justifica a denominação intuitiva de *menor ou igual* para a relação $\preceq$.

Teorema 9.15 (Cantor) $a \prec \mathcal{P}(a)$.

Demonstração: A função $f(x) = \{x\}$ de a em $\mathcal{P}(a)$ é injetora, portanto $a \preceq \mathcal{P}(a)$. Suponha que $a \approx \mathcal{P}(a)$ via uma função $g : a \longrightarrow \mathcal{P}(a)$. Considere

$$b = \{y \ : \ (y \in a) \wedge (y \notin g(y))\}.$$

É claro que b é legitimado por [A2], e $b \in \mathcal{P}(a)$. Como g é sobrejetora, deve existir algum $x \in a$ tal que $g(x) = b$. Portanto:

$$x \in g(x) \ \text{ sse } \ x \notin g(x).$$

Daqui inferimos que não pode existir uma tal g, isto é, $a \not\approx \mathcal{P}(a)$. Por outro lado, observe que Teorema 9.10 pode ser refraseado como: $a \preceq b$ implica ($a \not\approx b$ implica $b \not\preceq a$). Logo, de $a \preceq \mathcal{P}(a)$ e $a \not\approx \mathcal{P}(a)$ inferimos, pelo Teorema 9.10, que $\mathcal{P}(a) \not\preceq a$. Pela Definição 9.12, $a \prec \mathcal{P}(a)$. ■

10 Conjuntos Finitos

Estudaremos nesta seção os conjuntos finitos. A definição intuitiva de conjunto finito é a seguinte: um conjunto a é finito se a tem n elementos, para algum número natural n. Esta idéia é correta, mas utiliza o conceito de números inteiros. Dedekind propôs em 1888 uma definição não numérica extremamente elegante: um conjunto a é finito se a não é equipolente com nenhum subconjunto próprio. Em outras palavras, os conjuntos finitos são exatamente aqueles em que *a parte é menor do que o todo*. É evidente que esta definição pode ser facilmente introduzida em ZF. O problema que envolve esta definição é que, para provar que todo conjunto finito (no sentido de Dedekind) é finito (no sentido usual), devemos usar o Axioma da Escolha [AE]. Este axioma, a ser introduzido posteriormente, é o mais questionado dos axiomas da TC, existindo inclusive TCs que rejeitam este princípio (de fato, na literatura são diferenciados os sistemas ZF e ZFC, sendo que ZFC consiste de ZF com o acréscimo do Axioma da Escolha). Tarski propôs em 1924 a seguinte definição de finitude a qual, embora seja menos intuitiva, tem a vantagem que não requer [AE] para provar a equivalência com a definição usual de finitude.

Definição 10.1 *(i)* $min(x, u)$ *denota* $x \in u \land (\forall y)(y \in u \to \neg(y \subset x))$
("x é um elemento minimal de u").
(ii) $max(x, u)$ *denota* $x \in u \land (\forall y)(y \in u \to \neg(x \subset y))$
("x é um elemento maximal de u").

Por exemplo, se $b = \{1, 2, 3, 4\}$ e $u \subseteq \mathcal{P}(b)$, $u = \{\{1, 2, 4\}, \{2\}, \{2, 4\}, \{1, 3\}\}$, então $\{1, 2, 4\}$ e $\{1, 3\}$ são os elementos maximais de u, enquanto que $\{2\}$ e $\{1, 3\}$ são os elementos minimais de u. Por outro lado, seja $b = \mathbb{N}$ e

$$\mathbb{N}_n = \mathbb{N} - \{1, \ldots, n-1\} = \{n, n+1, n+2, \ldots\}\ (n \in \mathbb{N});\ u = \{\mathbb{N}_n\ :\ n \in \mathbb{N}\} \subseteq \mathcal{P}(b).$$

Dado que $\mathbb{N}_n \subset \mathbb{N}_m$ se $n > m$, então u não tem elementos minimais. Esta é a situação que caracteriza os conjuntos b infinitos, segundo a descoberta de Tarski.

Definição 10.2 (Tarski) $fin(b)$ *denota a fórmula*
$(\forall u)((u \subseteq \mathcal{P}(b) \land (u \neq \emptyset)) \to (\exists z)min(z, u))$
("b é finito se toda família não vazia de subconjuntos de b possui um elemento minimal").

As primeiras propriedades simples da finitude são as seguintes:

Proposição 10.3 *(i)* $\emptyset$ *é finito.*
(ii) $\{x\}$ *é finito.*
(iii) Se b *é finito e* $c \subseteq b$*, então* c *é finito.*
(iv) Se c *é finito então* $c \cap b$ *e* $c - b$ *são finitos.*

Demonstração: (i) Observe que $\mathcal{P}(\emptyset) = \{\emptyset\}$, portanto $u = \{\emptyset\}$ é a única família não vazia de subconjuntos de $\emptyset$. É claro que $\emptyset$ é um elemento minimal de u, portanto $fin(\emptyset)$.

(ii) Temos que $\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}$. Logo, as únicas famílias não vazias de subconjuntos de $\{x\}$ são $u_1 = \{\emptyset\}$, $u_2 = \{\{x\}\}$, e $u_3 = \{\emptyset, \{x\}\}$. É imediato que todo conjunto da forma $\{z\}$ tem um elemento minimal (o próprio z), portanto u_1 e u_2 possuem elemento minimal. Finalmente, $\emptyset$ é o elemento minimal de u_3. Isto prova $fin(\{x\})$.
(iii) Assuma que b é finito, e seja $c \subseteq b$. Seja $u \subseteq \mathcal{P}(c)$, $u \neq \emptyset$. Logo $u \subseteq \mathcal{P}(b)$, $u \neq \emptyset$. Dado que $fin(b)$, então u possui um elemento minimal z. Daqui $fin(c)$.
(iv) Suponha que c é finito. Para todo b temos que $c - b \subseteq c$ e $c \cap b \subseteq c$. Pelo item (iii) obtemos que $fin(c - b)$ e $fin(c \cap b)$. ■

A seguinte propriedade exige uma demonstração um pouco mais complicada.

Proposição 10.4 *Se c e b são finitos, então $c \cup b$ é finito.*

Demonstração: Assuma $fin(c)$ e $fin(b)$. Seja $u \subseteq \mathcal{P}(c \cup b)$, $u \neq \emptyset$. Provaremos que u tem um elemento minimal. Considere

$$w = \{a \ : \ a \subseteq c \wedge (\exists d)((d \subseteq b) \wedge a \cup d \in u)\}.$$

Temos que $w \neq \emptyset$. Com efeito, seja $z \in u$. Dado que $z = (z \cap c) \cup (z - c)$, então $a = z \cap c$ e $d = z - c$ satisfazem: $a \subseteq c$; $d \subseteq b$ (pois $z \subseteq c \cup b$); $a \cup d \in u$. Logo a é um elemento de w. Daqui $w \subseteq \mathcal{P}(c)$, $w \neq \emptyset$. Como c é finito, deve existir $a^* \in w$ minimal. Logo

(1) $\quad a^* \in w, \quad a^* \subseteq c.$

Considere agora

$$w_1 = \{d \ : \ d \subseteq b \wedge (a^* \cup d \in u)\}.$$

Por (1) temos que $a^* \cup d \in u$ para algum $d \subseteq b$, logo $d \in w_1$. Portanto $w_1 \subseteq \mathcal{P}(b)$, $w_1 \neq \emptyset$. Como b é finito existe um elemento minimal $d^* \in w_1$, donde

(2) $\quad d^* \in w_1, \quad d^* \subseteq b, \quad a^* \cup d^* \in u.$

Provaremos que $a^* \cup d^*$ é um elemento minimal de u. Suponha que $s \in u$ tal que $s \subseteq a^* \cup d^*$. Daqui $s \cap a^* \subseteq a^* \subseteq c$ e $s \cap d^* \subseteq d^* \subseteq b$. Dado que $s \subseteq a^* \cup d^*$, então

(3) $\quad s = s \cap (a^* \cup d^*) = (s \cap a^*) \cup (s \cap d^*).$

Como $s \in u$ obtemos que $s \cap a^* \in w$, e $s \cap a^* \subseteq a^*$. Dado que a^* é minimal, inferimos $s \cap a^* = a^*$. Por (3) obtemos que $a^* \cup (s \cap d^*) \in u$, donde $s \cap d^* \in w_1$. Logo $s \cap d^* = d^*$, pois d^* é minimal. Usando (3) vemos que $s = a^* \cup d^*$. Portanto $a^* \cup d^*$ é um elemento minimal de u. Isto prova que $c \cup b$ é finito. ■

Corolário 10.5 *Se b é finito, então $b \cup \{x\}$ é finito.*

Podemos definir um princípio de indução para conjuntos finitos. Antes disso, provaremos que existe uma caracterização da finitude em termos de conjuntos maximais.

Proposição 10.6 *(a) Toda família não vazia de subconjuntos de um conjunto finito possui um elemento maximal.*
(b) Se toda família não vazia de subconjuntos de um conjunto b possui um elemento maximal, então b é finito.

Demonstração: (a) Dado a finito, seja $u \subseteq \mathcal{P}(a)$, $u \neq \emptyset$. Considere $v = \{a - x \ : \ x \in u\}$. Claro que v é legitimado por [A2], $v \subseteq \mathcal{P}(a)$, e $v \neq \emptyset$ (pois $u \neq \emptyset$). Como a é finito, existe $a - x \in v$ minimal, onde $x \in u$. Provaremos que x é maximal em u. Para isto, observe que

(1) para todo $w, y \subseteq a$ temos que: $y \subset w$ sse $a - w \subset a - y$.

A prova é simples, e é deixada como exercício. Suponha então que x não é maximal em u. Logo, deve existir $y \in u$ tal que $x \subset y$. Por (1) obtemos $a - y \subset a - x$, onde $a - y \in v$. Isto contradiz a minimalidade de $a - x$ em v, portanto x é maximal.
(b) A prova é análoga à do item anterior. Assim, considere $u \subseteq \mathcal{P}(b)$, $u \neq \emptyset$. Logo

$$v = \{b - x \ : \ x \in u\}$$

é uma família não vazia de subconjuntos de b. Por hipótese, existe um elemento maximal $b - x$ em v, com $x \in u$. Utilizando (1) vemos que x é minimal em u, portanto b é finito. ■

Teorema 10.7 *Seja $\varphi(b)$ uma fórmula em que b ocorre livre e nem c nem x ocorrem livres (outras variáveis podem ocorrer livres em φ). Suponha o seguinte:*
(i) c é finito;
(ii) $\varphi(\emptyset)$;
(iii) $(\forall x)(\forall b)(((x \in c) \wedge (b \subseteq c) \wedge \varphi(b)) \to \varphi(b \cup \{x\}))$.
Então $\varphi(c)$.

Demonstração: Considere $u = \{b \ : \ b \subseteq c \wedge \varphi(b)\}$. Logo $u \subseteq \mathcal{P}(c)$ e $u \neq \emptyset$ pois $\emptyset \in u$, pela hipótese (ii). Dado que c é finito, por (i), então existe $b \in u$ maximal, pela Proposição 10.6(a). Provaremos que $b = c$, e logo $\varphi(c)$ como queriamos. Por redução ao absurdo, suponha que $b \neq c$. Como $b \subseteq c$, deve existir $x \in c - b$. Por (iii), temos que $\varphi(b \cup \{x\})$ e então $b \cup \{x\} \in u$, sendo que $b \subset b \cup \{x\}$. Isto contradiz a maximalidade de b em u. Daqui $b = c$ e $\varphi(c)$. ■

Em particular, obtemos a seguinte formulação conjuntista do princípio de indução para conjuntos finitos:

Teorema 10.8 *Suponha o seguinte:*
(i) c é finito;
(ii) $\emptyset \in w$;
(iii) $(\forall x)(\forall b)(((x \in c) \wedge (b \subseteq c) \wedge b \in w) \to b \cup \{x\} \in w)$.
Então $c \in w$.

Demonstração: Basta considerar no Teorema 10.7 a fórmula $\varphi(b)$ como sendo "$b \in w$". ■

Observe que o Teorema 10.7 é uma conseqüência do Teorema 10.8 considerando $w = \{b \ : \ (b \in \mathcal{P}(c)) \wedge \varphi(b)\}$ (legitimado por [A2]). Daqui, os Teoremas 10.7 e 10.8 são equivalentes. De fato, as propriedades (ii) e (iii) do Teorema 10.8 caracterizam os conjuntos finitos, como provaremos a seguir.

Proposição 10.9 *c é finito sse c pertence a todo w satisfazendo as condições (ii) e (iii) do Teorema 10.8.*

Demonstração: Se c é finito, então a conclusão vale pelo Teorema 10.8. Reciprocamente, assuma que $c \in w$ para todo w satisfazendo as condições (ii) e (iii) do Teorema 10.8. Seja w o conjunto de todos os subconjuntos finitos de c (w é legitimado por [A2]; confira!). Pela Proposição 10.3(i) temos que $\emptyset \in w$. Se $b \in w$ e $x \in c$ então $b \cup \{x\} \in w$ pelo Corolário 10.5. Portanto w satisfaz as condições (ii) e (iii) do Teorema 10.8, donde $c \in w$. Isto é, c é finito. ■

Proposição 10.10 *Se c é finito e f é uma função com domínio c e imagem b, então b é finito.*

Demonstração: Seja $w = \{a \ : \ (a \subseteq c) \wedge fin(f``a)\}$. Provaremos pelo Teorema 10.8 que $c \in w$, donde $im(f) = f``c$ resultará ser finito. Observe que $\emptyset \subseteq c$ e $f``\emptyset = \emptyset$ (finito); então $\emptyset \in w$. Seja $x \in c$ e $a \in w$; logo $a \cup \{x\} \subseteq c$. Como $f$ é função, então $f``\{x\} = \{f(x)\}$, logo $f``\{x\}$ é finito, pela Proposição 10.3(ii). Daqui $f``(a \cup \{x\}) = f``a \cup f``\{x\}$ é finito, pela Proposição 10.4, e então $a \cup \{x\} \in w$. Pelo Teorema 10.8 temos que $c \in w$, portanto $im(f)$ é finito. ■

Proposição 10.11 *Se c é finito, então $\mathcal{P}(c)$ é finito.*

Demonstração: Considere $w = \{b \ : \ b \subseteq c \wedge fin(\mathcal{P}(b))\}$. Temos que $\emptyset \in w$. Suponha $b \in w$ e $x \in c$. Se $x \in b$ então $b \cup \{x\} \in w$. Se $x \notin b$, então $b \cup \{x\} \subseteq c$. Defina

$$f = \{\langle a, a \cup \{x\}\rangle \ : \ a \in \mathcal{P}(b)\}.$$

Temos que f é legitimado por [A2], e f é função com domínio $\mathcal{P}(b)$ (finito). Pela Proposição 10.10 temos que a imagem de f é finita. Seja $z = \mathcal{P}(b \cup \{x\}) - \mathcal{P}(b)$. Provaremos que $im(f) = z$. Com efeito, dado $a \in \mathcal{P}(b)$, temos que $a \cup \{x\} \in z$, pois $x \notin b$. Logo $im(f) \subseteq z$. Por outro lado, se $d \in z$, então $x \in d$, $d - \{x\} \in \mathcal{P}(b)$ e $d = (d - \{x\}) \cup \{x\}$. Daqui $f(d - \{x\}) = d$, portanto $d \in im(f)$. Provamos então que $z = im(f)$ é finito. Mas $\mathcal{P}(b \cup \{x\}) = z \cup \mathcal{P}(b)$, portanto $\mathcal{P}(b \cup \{x\})$ é finito, pela Proposição 10.4. Desta maneira $b \cup \{x\} \in w$, donde $c \in w$, isto é, $\mathcal{P}(c)$ é finito. ■

Proposição 10.12 *Se c é finito e todo $x \in c$ é finito, então $\bigcup c$ é finito*

Demonstração: Considere $w = \{b \ : \ b \subseteq c \wedge fin(\bigcup b)\}$ (legitimado por [A2]). Claramente $\emptyset \in w$. Seja $b \in w$ e $x \in c$. Logo x é finito, por hipótese, e $\bigcup b$ é finito, pela hipótese de indução ($b \in w$). É fácil provar que

$$\bigcup(b \cup \{x\}) = (\bigcup b) \cup x$$

(exercício). Portanto $\bigcup(b \cup \{x\})$ é finito, pela Proposição 10.4, e então $b \cup \{x\} \in w$ (claramente $b \cup \{x\} \subseteq c$). Pelo Teorema 10.8 obtemos $c \in w$, isto é, $\bigcup c$ é finito. ■

Proposição 10.13 *Se $\mathcal{P}(c)$ é finito, então c é finito.*

Demonstração: Seja $b = \{\{x\} \ : \ x \in c\}$ (legitimado por [A2]). Como $\mathcal{P}(c)$ é finito e $b \subseteq \mathcal{P}(c)$, então a Proposição 10.3(iii) assegura que b é finito. Como todo elemento de b é da forma $\{x\}$ (portanto finito) então a Proposição 10.12 nos garante que $\bigcup b$ é finito. Mas é fácil provar que $\bigcup b = c$. Com efeito: se $y \in \bigcup b$, então existe $x \in c$ tal que $y \in \{x\}$, isto é, $y = x$ donde $y \in c$. Reciprocamente, se $x \in c$ então $x \in \{x\}$ onde $\{x\} \in b$, portanto $x \in \bigcup b$. Logo, c é finito. ■

Proposição 10.14 *(i) Se c é finito e $c \approx b$ então b é finito.*
(ii) Se c é finito e $b \preceq c$ então b é finito.

Demonstração: (i) Seja f uma bijeção de c em b. Como c é finito então $im(f)$ é finito, pela Proposição 10.10. Mas $im(f) = b$.
(ii) Se $b \preceq c$, então $b \approx a$ onde $a \subseteq c$. Se c é finito, então a é finito. Logo $a \approx b$ e a é finito, donde b é finito, pelo item (i). ■

A *Lei de Tricotomia* estabelece: para todo par de conjuntos c,b, temos que vale uma e só uma das seguinte possibilidades: $c \prec b$, $b \prec c$, ou $c \approx b$. Pode ser provado que a Tricotomia equivale ao Axioma da Escolha. Porém, se um dos conjuntos é finito, não precisamos de [AE] para provar esta propriedade.

Proposição 10.15 *Se c é finito então $c \prec b$, $b \prec c$, ou $c \approx b$.*

Demonstração: Faremos indução sobre os subconjuntos de c. Dado b, considere

$$w = \{a \ : \ a \subseteq c \wedge ((a \prec b) \vee (b \prec a) \vee (a \approx b))\}.$$

Claramente $\emptyset \in w$ pois, se $b = \emptyset$, então $\emptyset \approx b$ e, se $b \neq \emptyset$, então $\emptyset \prec b$. Seja $a \in w$ e $x \in c$; queremos provar que $a \cup \{x\} \in w$. O caso em que $x \in a$ é óbvio. Assumamos que $x \notin a$. Como $a \in w$, então temos três casos:
Caso 1: $a \prec b$. Logo, existe $y \in b - im(f)$, onde f é uma função injetora de a em b. Portanto, $g = f \cup \{\langle x, y\rangle\}$ é uma função injetora de $a \cup \{x\}$ em b, donde $a \cup \{x\} \preceq b$. Daqui inferimos $a \cup \{x\} \prec b$ ou $a \cup \{x\} \approx b$, pela Proposição 9.14(iv). Nos dois casos, $a \cup \{x\} \in w$.
Caso 2: $b \prec a$. Como $a \preceq a \cup \{x\}$, então $b \prec a \cup \{x\}$, pela Proposição 9.14(iii). Portanto $a \cup \{x\} \in w$.
Caso 3: $b \approx a$. Como $a \subseteq a \cup \{x\}$, então $a \approx a \cup \{x\}$ ou $a \prec a \cup \{x\}$. No primeiro caso $b \approx a \cup \{x\}$; no segundo caso $b \prec a \cup \{x\}$. Nos dois casos $a \cup \{x\} \in w$.
Em virtude do Teorema 10.8, $c \in w$, isto é, $c \prec b$, $b \prec c$, ou $c \approx b$. ■

Corolário 10.16 *Se c é finito e b não é finito, então $c \prec b$.*

Demonstração: Temos que $c \prec b$, $b \prec c$ ou $c \approx b$. Os dois últimos casos implicam a existência de uma bijeção f de $a \subseteq c$ em b. Mas a é finito, portanto $b = im(f)$ é finito, o que contradiz a hipótese. Logo, só pode ser $c \prec b$. ■

Provaremos agora que um conjunto finito (no sentido Tarski) é um conjunto finito (no sentido Dedekind). Como mencionamos anteriormente, toda prova conhecida da afirmação recíproca precisa do [AE].

Definição 10.17 *$Dedfin(c)$ denota $\neg(\exists b)(b \subset c \wedge c \approx b)$*
("c é Dedekind-finito se não é equipolente com nenhum subconjunto próprio").

Teorema 10.18 *Se c é finito, então c é Dedekind-finito.*

Demonstração: Seja c finito, e suponha que c não é Dedekind-finito. Logo, existe $b \subset c$ tal que $c \approx b$ (via uma bijeção f de c em b). Considere

$$u = \{a \ : \ a \subseteq c \wedge f``a \subset a\}.$$

Como $c \subseteq c$ e $f``c = b \subset c$, então $c \in u$, logo $u \neq \emptyset$. Como $c$ é finito e $u \subseteq \mathcal{P}(c)$ é não vazio, existe um elemento minimal $d$ em $u$. Dado que $f``d \subset d$ e d é minimal, então

(1) $\quad f``d \notin u.$

Por outro lado $f``d \subset d$ implica que existe $x \in (d - f``d)$. Note que $f``(f``d) \subseteq f``d$. Se $f(x) \in f``(f``d)$, então $f(x) = f(y)$ com $y \in f``d$. Mas f é injetora, portanto $f(x) = f(y)$ implica $x = y$, isto é, $x \in f``d$, uma contradição. Logo $f(x) \in f``d - f``(f``d)$, donde $f``(f``d) \subset f``d$. Daqui (e do fato de ter $f``d \subset d \subseteq c$) inferimos $f``d \in u$, em contradição com (1). Portanto a suposição inicial é falsa e então c é Dedekind-finito. ■

Proposição 10.19 *Sejam c e b finitos.*
(i) $c \times b$ é finito.
(ii) c^b é finito.

Demonstração: (i) Sejam c e b finitos. Se $c = \emptyset$ ou $b = \emptyset$ então $c \times b = \emptyset$ é finito. Se c e b são não vazios, então

$$c \times b = \bigcup a, \qquad a = \{c \times \{y\} \ : \ y \in b\}.$$

Dado que $c \approx c \times \{y\}$, então todo elemento de a é finito. Claramente $a \approx b$, donde a é finito. Pela Proposição 10.12 o conjunto $\bigcup a$ é finito, isto é, $c \times b$ é finito.
(ii) Temos que $c^b \subseteq \mathcal{P}(b \times c)$. Como $b \times c$ é finito, pelo item (i), então $\mathcal{P}(b \times c)$ é finito, donde c^b é finito. ■

11 Axiomas Finais de ZF. O Axioma da Escolha

Para definir a noção de ordinal precisaremos de acrescentar axiomas adicionais ao sistema S. A seguir completaremos a definição do sistema ZF, estudando as conseqüências da incorporação dos mesmos. O primeiro axioma a ser incorporado ao nosso sistema atual é o *Axioma da Infinidade*, que assegura a existência de un conjunto infinito.

Axioma da Infinidade:

[A6] $(\exists w)((\emptyset \in w) \wedge (\forall x)(x \in w \to x \cup \{x\} \in w))$

Por definição temos que $\emptyset \in w$, portanto

$\{\emptyset\} = \emptyset \cup \{\emptyset\} \in w$;
$\{\emptyset, \{\emptyset\}\} = \{\emptyset\} \cup \{\{\emptyset\}\} \in w$;
$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} \in w$; etc.

Dado que $\{x\}$ e logo $x \cup \{x\}$ só aparece num nível posterior ao nível em que foi criado x, então [A6] exige a existência de uma seqüência crescente infinita de níveis na estrutura cumulativa de tipos, sendo que w aparece só depois de todos esses níveis. Este axioma é a primeira tentativa de afirmar que os níveis não têm fim. Portanto, esta afirmação pode ser aceita por alguns matemáticos e rejeitada por outros. É fundamental perceber que este axioma separa claramente a Aritmética (que pode ser realizada sem assumir a existência de seqüências infinitas) de outras disciplinas da Matemática avanzada, tais como Análise, que fazem um uso essencial do Axioma da Infinidade.

A seguir introduziremos um axioma importantíssimo, o *Axioma de Substituição.* Não só obteremos o Axioma de Separação como um corolário, senão que poderemos assegurar a existência de ordinais e cardinais transfinitos.

Axioma de Substituição: Seja $\psi(x, y)$ uma fórmula com x e y livres, mas onde b não ocorre livre (outras variáveis podem ocorrer livres em ψ). Seja z uma variável nova, e FUN_ψ a fórmula $(\forall x)(\forall y)(\forall z)(\psi(x, y) \wedge \psi(x, z) \to (y = z))$.

[A7] $FUN_\psi \to (\exists b)(\forall y)(y \in b \leftrightarrow (\exists x)(x \in a \wedge \psi(x, y)))$

A hipótese FUN_ψ indica que ψ define uma função parcial, isto é: para cada x, existe no máximo um y tal que $\psi(x, y)$. Assumindo FUN_ψ, então [A7] assegura que o termo s dado por

$$s = \{y \ : \ (\exists x)((x \in a) \wedge \psi(x, y))\}$$

é legitimado; ele representa a imagem de a sob a função parcial definida por $\psi(x, y)$; se o termo r dado por

$$r = \{\langle x, y \rangle \ : \ \psi(x, y)\}$$

é legitimado, então s é $r``(a) = im(r|a)$. Dado que r não é necessariamente legitimado, devemos esperar que [A7] acrescente novos conjuntos. Observe que [A7] é um esquema de axioma, definindo um axioma particular para cada fórmula ψ. Ele afirma que, dado a, podemos *substituir* os seus elementos por outros conjuntos, desde que coloquemos no máximo um conjunto para cada elemento de a.

Em termos da teoria cumulativa de tipos, isto afirma que os níveis não têm fim. De fato, é a afirmação mais forte em ZF nessa direção. Assim, [A7] afirma que toda coleção de níveis colocados em correspondência com os elementos de um conjunto pode ser considerada como completada, portanto existem níveis superiores. Mais precisamente, seja $f(x)$ o nível em que aparece y tal que $\psi(x, y)$ (se não existir y então $f(x)$ pode ser tomado como o primeiro nível). Logo, a coleção de níveis $f(x)$ está em correspondência com os elementos de a, portanto existe um nível em que todos os y tais que $\psi(x, y)$ para algum $x \in a$ já foram criados. Nesse nível pode ser criado $b = \{y\ :\ (\exists x)((x \in a) \wedge \psi(x, y))\}$.

Observe que [A7] fornece um axioma para cada fórmula ψ apropriada; isto limita o poder de [A7], da mesma maneira que acontece con [A2]. Por outro lado, [A2] é um caso particular de [A7]:

Proposição 11.1 *Seja $\phi(x)$ uma fórmula em que x ocorre livre mas b não ocorre livre. Logo,*

$$[\text{A7}]\ \vdash (\exists b)(\forall x)(x \in b \leftrightarrow ((x \in a) \wedge \phi(x))).$$

Em outras palavras, [A2] *é implicado por* [A7].

Demonstração: Seja y uma variável nova (isto é, y não ocorre em $\phi(x)$ e $y \neq b$). Considere $\psi(x, y)$ dada por

$$\psi(x, y) \equiv_{def} \phi(x) \wedge (x = y).$$

Pelas regras da igualdade, provamos a fórmula

$$(*) \qquad (\exists x)((x \in a) \wedge \psi(x, y)) \leftrightarrow (y \in a) \wedge \phi(y).$$

Por outro lado, é fácil provar que $\psi(x, y)$ e $\psi(x, z)$ implica $y = z$. Logo FUN_ψ donde, por [A7], inferimos que $(\exists b)(\forall y)(y \in b \leftrightarrow (\exists x)((x \in a) \wedge \psi(x, y))$. Por $(*)$ obtemos

$$(\exists b)(\forall y)(y \in b \leftrightarrow ((y \in a) \wedge \phi(y))),$$

isto é, [A2]. ■

Provaremos agora que o axioma [PR] pode ser deduzido dos axiomas [A3] e [A7], conforme anunciado na Seção 2.

Proposição 11.2 [A3], [A7] $\vdash$ [PR].

Demonstração: Primeiro obtemos o seguinte:

Fato 1: [A7] $\vdash (\exists c)(\forall u)(u \notin c)$.
Com efeito, basta tomar $\psi_c(x,y) \equiv_{def} (x \neq x) \wedge (x = y)$ em [A7], e a uma variável qualquer (exercício).
Fato 2: [A3], [A7] $\vdash (\exists d)(\forall x)(x \in d \leftrightarrow (\forall w)(w \in x \rightarrow (\forall u)(u \notin w))$.
Com efeito, basta tomar c como no **Fato 1** e depois aplicar [A3] no conjunto c, obtendo o conjunto d com as propriedades requeridas (exercício).
Fato 3: Dados a e b considere a fórmula

$$\begin{aligned}\psi_{a,b}(x,y) \equiv_{def} & ((\forall w)(w \notin x) \wedge y = a) \\ & \vee ((\exists w)(w \in x) \wedge (\forall w)(w \in x \rightarrow (\forall u)(u \notin w)) \wedge y = b).\end{aligned}$$

Então $FUN_{\psi_{a,b}}$ (exercício).
Fato 4: Usando apenas lógica clássica temos que

$$(\exists x)((\forall w)(w \in x \rightarrow (\forall u)(u \notin w)) \wedge \psi_{a,b}(x,y)) \leftrightarrow (y = a \vee y = b)$$

(exercício).

Logo, pelo **Fato 3** e por [A7] temos que

$$(\exists z)(\forall y)(y \in z \leftrightarrow (\exists x)(x \in d \wedge \psi_{a,b}(x,y))).$$

Finalmente, tomando d como no **Fato 2** obtemos, pelo **Fato 4**, que

$$(\exists z)(\forall y)(y \in z \leftrightarrow (y = a \vee y = b)).$$

■

Definição 11.3 *O sistema ZF da Teoria de Conjuntos consiste do axioma* [A1] *junto com os axiomas* [A3]-[A7]. [1]

Uma vez que introduzimos a totalidade dos axiomas de TC, discutiremos o *Axioma da Escolha* ([AE]), que originou uma das principais discussões dentro da Teoria de Conjuntos. O sistema obtido de ZF acrescentando [AE] é usualmente denotado por ZFC. Uma possível formulação de [AE] é a seguinte:

Axioma da Escolha:

$$\begin{aligned}\text{[AE]}\ & ((\forall x)(x \in z \rightarrow x \neq \emptyset) \wedge (\forall x)(\forall y)(((x, y \in z) \wedge (x \neq y)) \\ & \rightarrow x \cap y = \emptyset)) \rightarrow (\exists u)(\forall x)(\exists v)(x \in z \rightarrow u \cap x = \{v\})\end{aligned}$$

Isto é: dado um conjunto z cujos elementos são não vazios e dois a dois disjuntos, então existe um *conjunto de escolhas* u, que tem exatamente um membro em comum com cada elemento de z. Observe que, embora u "escolha" um elemento de cada membro de z, o axioma nada diz respeito à existência de um procedimento efetivo para realizar esta escolha.

[1] Dado que, pela Proposição 11.1 o axioma [A2] é derivável em ZF, continuaremos a utilizá-lo no resto do texto, embora não seja parte da axiomática de ZF.

O caráter altamente não construtivo deste axioma foi alvo de críticas por parte das escolas matemáticas construtivistas. Porém, a quantidade de aplicações fundamentais de [AE] dentro de TC como na Matemática em geral fazem de [AE] um axioma praticamente imprescindível. Em TC é necessário [AE], por exemplo, para obter a Lei de Tricotomia para conjuntos. Existe uma série de importantes resultados matemáticos relacionados com o Axioma de Escolha, por exemplo: o Teorema de Hahn-Banach, o Teorema de Ideais Primos para Álgebras de Boole, a existência de bases em espaços vetoriais, e o Teorema de Tychonoff (o produto de espaços topológicos compactos é compacto). Estes dois últimos resultados são de fato equivalentes a [AE], assim como os seguintes Princípios:

Princípio da Boa Ordem: Todo conjunto admite uma boa ordem.

Lema de Zorn: Seja A um conjunto ordenado tal que todo subconjunto totalmente ordenado (ou *cadeia*) B tem um limitante superior. Então, A tem um elemento maximal.

A não-construtividade embutida em [AE] pode ser entendida através do seguinte exemplo intuitivo, devido a Bertrand Russell:

Exemplo 11.4 Considere uma coleção z de pares de sapatos idênticos. Nesse caso, é possível *escolher* sem problemas um único elemento (sapato) de cada par de sapatos de z, por exemplo através do algoritmo "pegue apenas os sapatos que correspondam ao pé direito". Por outro lado, se agora consideramos uma coleção z' de pares de meias idênticas (não existindo nenhuma diferença entre a meia do pé direito e a do pé esquerdo), não existe um método imaginável que permita *escolher* apenas uma meia de cada par de z'. Porém, o Axioma da Escolha garante que é possível fazer isto! ■

12 Introdução aos Ordinais

Embora os axiomas de ZF não mencionam explicitamente a existência dos níveis da teoria cumulativa de tipos, eles são fortes o suficiente como para permitir a sua definição. Os ordinais permitirão indexar os níveis (além de ter muitas outras aplicações).

Definição 12.1 (von Neumann) $transi(x)$ *denota*
$(\forall y)(\forall z)((y \in z) \wedge (z \in x) \rightarrow (y \in x))$
("x é transitivo");
$conec(x)$ *denota* $(\forall y)(\forall z)(y, z \in x \rightarrow ((y \in z) \vee (z \in y) \vee (y = z)))$
("x é conectado com relação a ∈");
$ord(x)$ *denota* $transi(x) \wedge conec(x)$
("x é um ordinal");
$x < y$ *denota* $ord(x) \wedge ord(y) \wedge x \in y$
("x é um ordinal menor que y");
$x \leq y$ *denota* $ord(x) \wedge ord(y) \wedge (x < y \vee x = y)$.

Teorema 12.2 *Utilizando os axiomas* [A1], [A2], [A4], [A5], [PR] *provamos o seguinte:*

(i) Se x é ordinal e $y \in x$, então y é ordinal.
(ii) $\emptyset$ é ordinal.
(iii) Se x é ordinal, então $x \cup \{x\}$ é ordinal.

Demonstração: (i) Fixe um ordinal x, e $y \in x$. Sejam $u, v \in y$. Como x é transitivo e $y \in x$, então $u, v \in x$. Como x é conectado com relação a $\in$, então $u \in v$ ou $v \in u$ ou $u = v$. Daqui y é conectado. Para provar que y é transitivo devemos utilizar o axioma da regularidade. Sejam então $u \in z$, $z \in y$. Como $y \in x$ e x é transitivo, obtemos que $u \in x$. Logo, de $conec(x)$ deduzimos: $y \in u$ ou $y = u$ ou $u \in y$. Queremos eliminar as duas primeiras possibilidades.
Caso 1: $y \in u$. Temos então: $u \in z$, $z \in y$, $y \in u$. Considere $a = \{u, y, z\}$ Logo:

$$y \in u \cap a, \quad z \in y \cap a, \quad u \in z \cap a.$$

Logo, $a \neq \emptyset$ não tem nenhum elemento disjunto com a, contrariando o axioma da regularidade. Portanto, não podemos ter $y \in u$.
Caso 2: $y = u$. Temos então: $u \in z$, $z \in y$, $y = u$; isto é, $y \in z$, $z \in y$. Mas, na Proposição 3.6(2) provamos que [A5] implica: $\neg(a \in b \wedge b \in a)$. Portanto não podemos ter $y = u$.
Assim $u \in y$, donde $transi(y)$. Daqui y é ordinal.
(ii) Todas as hipóteses são falsas, logo $\emptyset$ é trivialmente um ordinal.
(iii) Seja $y = x \cup \{x\}$. Observe que

$$(*) \quad z \in y \text{ sse } z \in x \text{ ou } z = x.$$

Para provar que y é transitivo sejam $u \in z$ e $z \in y$; queremos obter $u \in y$. Por $(*)$ temos dois casos a partir da hipótese $z \in y$:
Caso 1: $z \in x$. Logo $u \in z$, $z \in x$ implica $u \in x$, pois $transi(x)$. Daqui $u \in y$, por $(*)$.
Caso 2: $z = x$. Logo $u \in z$, $z = x$ implica $u \in x$. Portanto $u \in y$, por $(*)$.
Provamos assim $transi(y)$. Para provar que y é conectado considere $u \in y$, $z \in y$; queremos obter $z \in u$ ou $u \in z$ ou $z = u$. Por $(*)$ inferimos a partir de $u, z \in y$:
Caso 1: $u \in x$.
Caso 1.1: $z \in x$. Daqui $u \in x$, $z \in x$ implica $z \in u$ ou $u \in z$ ou $z = u$, pois $conec(x)$.
Caso 1.2: $z = x$. Logo $u \in x$, $x = z$ implica $u \in z$, donde $z \in u$ ou $u \in z$ ou $z = u$.
Caso 2: $u = x$.
Caso 2.1: $z \in x$. Daqui $z \in x$, $x = u$ implica $z \in u$, logo $z \in u$ ou $u \in z$ ou $z = u$.
Caso 2.2: $z = x$. Logo $u = x$, $x = z$ implica $u = z$, portanto $z \in u$ ou $u \in z$ ou $z = u$.
Provamos então que y é conectado, sendo portanto um ordinal. ■

Definição 12.3 *Introduzimos a notação seguinte:*
0 *denota $\emptyset$;*

$\mathbf{1}$ *denota* $\{\emptyset\}$*;*
$\mathbf{2}$ *denota* $\{\emptyset, \{\emptyset\}\}$*;*
$\mathbf{3}$ *denota* $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$*;*
em geral, $\mathbf{n}$ *denota* $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, ..., \mathbf{n-1}\}$*;*
$x + 1$ *denota* $x \cup \{x\}$ *(o sucessor de* x*).*

Podemos provar agora a *lei de tricotomia para ordinais* (não confundir com a lei de tricotomia enunciada anteriormente!). Esta propriedade é de fundamental importância.

Teorema 12.4 *Se* x *e* y *são ordinais, então:* $x \in y$ *ou* $y \in x$ *ou* $x = y$*.*

Demonstração: Provaremos primeiro o seguinte
Fato: Se x e y são ordinais e $x \subset y$, então $x \in y$.
Com efeito: Seja $z = y - x$. Logo $z \neq \emptyset$, portanto existe $u \in z$ tal que $u \cap z = \emptyset$, pelo axioma da regularidade. Logo $u \in y$, $u \notin x$. Como $u \cap z = \emptyset$, então $v \in u$ implica $v \notin z$, isto é, $v \notin y$ ou $v \in x$ ou, equivalentemente, $(v \in y \to v \in x)$. Ou seja: $v \in u$ implica $(v \in y \to v \in x)$. Como y é transitivo e $u \in y$, então $v \in u$ implica $v \in y$. Como também temos $(v \in y \to v \in x)$, então deduzimos $v \in x$. Ou seja: $v \in u$ implica $v \in x$, donde $u \subseteq x$. Por outro lado, seja $w \in x$; como $x \subseteq y$, então $w \in y$. Dado que $u \in y$ e y é conectado, então $u = w$ ou $u \in w$ ou $w \in u$. Se $u = w$, então de $w \in x$ inferimos $u \in x$, contradição $(u \in y - x)$. Se $u \in w$ então: $u \in w$, $w \in x$ implica $u \in x$ (pois x é transitivo), contradição. Portanto só podemos ter $w \in u$. Assim: $w \in x$ implica $w \in u$, donde $x \subseteq u$. Desta maneira $u = x$. Como $u \in y$, então $x \in y$, provando o **Fato**.
Sejam então x e y ordinais. É muito simples provar que $z = x \cap y$ é também um ordinal (exercício). Se $z \neq x$ e $z \neq y$, então $z \subset x$ e $z \subset y$, donde $z \in x$ e $z \in y$, pelo **Fato**. Daqui $z \in x \cap y$, isto é, $z \in z$, contradição. Logo $z = x$ ou $z = y$. Se $z = x$, então $x \subseteq y$. Se $x = y$, vale a tricotomia. Se $x \subset y$, então $x \in y$, pelo **Fato**, donde vale a tricotomia. O caso $z = y$ é similar. ∎

Corolário 12.5 ("Paradoxo" de Burali-Forti) *O termo* $\{x : ord(x)\}$ *não é legitimado.*

Demonstração: Suponha que definimos $On = \{x : ord(x)\}$. Provaremos que On é um ordinal, portanto $On \in On$, uma contradição. Com efeito, pelo Teorema 12.2(i) obtemos que On é transitivo. Pelo Teorema 12.4 inferimos que On é conectado. Daqui $ord(On)$. ∎

Desde o ponto de vista da teoria cumulativa de tipos, esperamos ter só um ordinal em cada nível (isto será provado depois). Logo, On não poderia ser jamais completado.

Definição 12.6 *Usaremos as letras gregas* α*,* β*,* γ*, etc., eventualmente com subíndices (mas não* ϕ*,* ψ*, as quais são reservadas para denotar fórmulas), como variáveis para indicar ordinais. Além disso,*
$(\forall\alpha)\phi(\alpha)$ *denotará* $(\forall\alpha)(ord(\alpha) \to \phi(\alpha))$*;*
$(\exists\alpha)\phi(\alpha)$ *denotará* $(\exists\alpha)(ord(\alpha) \wedge \phi(\alpha))$*, e*

$\{\alpha : \phi(\alpha)\}$ *denotará* $\{\alpha : ord(\alpha) \wedge \phi(\alpha)\}$.
A definição da quantificação $(\forall\alpha)$ *e* $(\exists\alpha)$ *é correta, pois existem ordinais.*

Definição 12.7 $suc(x)$ *denota* $ord(x) \wedge ((\exists y)(x = y + 1) \vee (x = \mathbf{0}))$
("x é zero ou um ordinal sucessor");
$lim(x)$ *denota* $ord(x) \wedge \neg suc(x)$
("x é um ordinal limite");
$int(x)$ *denota* $suc(x) \wedge (\forall y)(y < x \to suc(y))$
("x é um enteiro não negativo").

Se x é um ordinal sucessor da forma $x = y + 1$, então $y \in x$, pela definição de $y + 1$. Pelo Teorema 12.2(i), temos que y é também um ordinal. Portanto $y + 1$ é um ordinal sse y é um ordinal. Não existe razão para considerar $\mathbf{0}$ como sucessor ou limite, mas ele é incluido no conjunto dos sucessores. Observe que vale a seguinte propriedade:

$$\text{[LIM]} \qquad lim(x) \leftrightarrow ord(x) \wedge (x \neq \mathbf{0}) \wedge (\forall y)(y \in x \to y + 1 \in x).$$

Com efeito, $lim(x)$ implica $ord(x)$ e $\neg ord(x) \vee (\neg(\exists y)(x = y+1) \wedge x \neq \mathbf{0})$. Logo $ord(x)$, $x \neq \mathbf{0}$ e $(\forall y)(x \neq y + 1)$. Seja $y \in x$; como $ord(y)$, então $ord(y + 1)$ donde, por tricotomia, $y + 1 < x$ ou $y + 1 = x$ ou $x < y + 1$. Não podemos ter $x = y+1$. Por outro lado, $x < y+1$ implica: $x = y$ (portanto $x \in x$, contradição) ou $x \in y$ (portanto $x \in y$ e $y \in x$, contradição). Logo $y+1 < x$, isto é, $y+1 \in x$. Reciprocamente, suponha $ord(x)$, $x \neq \mathbf{0}$, $(\forall y)(y \in x \to y+1 \in x)$. Se $x = y+1$, então $y \in x$, donde $y + 1 \in x$, isto é, $x \in x$, contradição. Logo $x \neq y + 1$ para todo y donde x é ordinal limite.
Provaremos que um princípio fraco de indução matemática para os inteiros é válido no sistema S (lembre da Definição 3.5).

Teorema 12.8 (Indução Matemática) *Para cada fórmula* ψ *da linguagem de ZF, temos que:*

$$S \vdash (\psi(\mathbf{0}) \wedge (\forall\alpha)(\psi(\alpha) \to \psi(\alpha + 1))) \to (\forall\alpha)(int(\alpha) \to \psi(\alpha)).$$

Demonstração: Suponhamos que a conclusão do princípio de indução é falsa; provaremos que a hipótese é falsa. Assim, assumamos que existe um ordinal β tal que $int(\beta) \wedge \neg\psi(\beta)$. Observe que, dados ordinais γ e β, então $\gamma \leq \beta$ sse $\gamma = \beta$ ou $\gamma \in \beta$ sse $\gamma \in \beta + 1$. Portanto, por [A2] podemos criar o conjunto

$$y = \{\gamma : \gamma \leq \beta \wedge \neg\psi(\gamma)\} = \{\gamma : (\gamma \in \beta + 1) \wedge \neg\psi(\gamma)\}.$$

Por outro lado $y \neq \emptyset$, pois $\beta \in y$. Pelo axioma da regularidade existe $\gamma_0 \in y$ tal que $\gamma_0 \cap y = \emptyset$. Dado que $\gamma_0 \leq \beta$ e $int(\beta)$, então $suc(\gamma_0)$. Com efeito: $\gamma_0 = \beta$ implica $int(\gamma_0)$, logo $suc(\gamma_0)$. Por outro lado, $\gamma_0 < \beta$ implica $suc(\gamma_0)$, pela definição de $int(\beta)$. Dado que $suc(\gamma_0)$, então
Caso 1: $\gamma_0 = \mathbf{0}$. Daqui $\neg\psi(\mathbf{0})$, pois $\gamma_0 \in y$.
Caso 2: $\gamma_0 = \gamma_1 + 1$ para algum γ_1 (que resulta ser um ordinal, pela observação após a Definição 12.7). Como $\gamma_1 \in \gamma_0$ e $\gamma_0 \cap y = \emptyset$, então $\gamma_1 \notin y$. Daqui $\psi(\gamma_1)$, pois $\gamma_1 \leq \beta$. Isto é: $\psi(\gamma_1) \wedge \neg\psi(\gamma_1 + 1)$.

Vemos que cualquer dos casos acima contraria a hipótese do princípio de indução. ■

O princípio de indução 12.8 é mais fraco do que a indução utilizada freqüentemente em matemáticas, pois 12.8 é restrito às propriedades dos inteiros que podem ser expressadas mediante fórmulas da linguagem. O conjunto das fórmulas é enumerável, enquanto que o conjunto das propriedades dos inteiros positivos é o conjunto $\mathcal{P}(\mathbb{N})$, que não é enumerável.

Queremos provar que a coleção dos inteiros é um conjunto. Isto será provado a partir do axioma do infinito (de fato, o seguinte teorema é equivalente a [A6]).

Teorema 12.9 *Seja Z o sistema composto dos axiomas* [A1]-[A6] *mais* [PR], *isto é, Z é obtido de ZF substituindo o axioma de substituição* [A7] *pelos axiomas* [A2] *e* [PR]. *Logo*

$$Z \vdash (\exists y)(\forall z)(z \in y \leftrightarrow int(z)).$$

Demonstração: Pelo axioma [A6] existe um conjunto w tal que $\mathbf{0} \in w$ e se $x \in w$ então $x+1 \in w$. Considere a fórmula $\psi(x)$ dada por $x \in w$. Por indução matemática obtemos:

$$(\forall x)(int(x) \rightarrow x \in w).$$

Portanto inferimos que $int(x)$ sse $(x \in w) \wedge int(x)$ para todo x. Por otro lado, de [A2] deduzimos

$$(\exists y)(\forall x)(x \in y \leftrightarrow ((x \in w) \wedge int(x))).$$

Isto significa que existe $y = \{x \ : \ (x \in w) \wedge int(x)\} = \{x \ : \ int(x)\}$. ■

Definição 12.10 *ω denota $\{z \ : \ int(z)\}$*
(o conjunto dos inteiros não negativos).

Teorema 12.11 *(i) $Z \vdash ord(\omega)$.*
(ii) $Z \vdash lim(\omega)$.

Demonstração: (i) Considere $y \in x$ e $x \in \omega$. Logo $y \in x$ e $int(x)$; daqui y é um ordinal (pois $y \in x$ e x é um ordinal), e $y < x$. Logo $suc(y)$. Se $z \in y$, então $z \in x$, logo $suc(z)$. Daqui $int(y)$, isto é, $y \in \omega$. Isto prova que ω é transitivo. Sejam agora $x, y \in \omega$. Logo $ord(x)$ e $ord(y)$. Pela lei de tricotomia para ordinais obtemos $x \in y$ ou $y \in x$ ou $x = y$. Isto prova que ω é conectado para $\in$.
(ii) Observe que $\omega \neq \mathbf{0}$, pois $\mathbf{0} \in \omega$. Além disso ω é um ordinal, por (i). Claramente

$$(\forall y)(int(y) \rightarrow int(y+1)),$$

isto é, $(\forall y)(y \in \omega \rightarrow (y+1 \in \omega))$. Pela propriedade [LIM] obtemos que ω é um ordinal limite. ■

13 Indução e Recursão Transfinita

Introduziremos a seguir a importante noção de *fecho transitivo* de um conjunto, que será utilizada para provar que a relação de pertinência $\in$ é *bem fundada.* O fato de $\in$ ser bem fundada permitirá a introdução de definições e demonstrações por *recursão transfinita* em ZF, uma poderosa ferramenta na teoria de conjuntos.

Definição 13.1 *$FT(x)$ denota $\{y\ :\ (\forall z)(x \in z \wedge transi(z) \rightarrow y \in z)\}$ ("$FT(x)$ é o fecho transitivo de x").*

Por definição, $FT(x)$ é o menor conjunto transitivo z tal que $x \in z$, isto é, $FT(x)$ é a interseção de todos os conjuntos transitivos z tais que $x \in z$. Ele é formado intuitivamente da maneira seguinte: dado x, procuramos nos níveis anteriores os elementos y de x, e recomeçamos o processo, isto é, procuramos os elementos z de y, e depois os elementos w de z etc., obtendo o "histórico" de x através destas componentes. É claro que precisamos provar a existência de $FT(x)$ para todo x. Ela é garantida pelos axiomas da infinidade e da substituição. Enunciamos este resultado, omitindo a demonstração.

Teorema 13.2 *Em* ZF *o termo $FT(x)$ é legitimado, isto é:*

$$Z \vdash (\forall x)(\exists w)(\forall y)(y \in w \leftrightarrow (\forall z)(x \in z \wedge transi(z) \rightarrow y \in z)).$$

Podemos agora definir a classe de fórmulas a partir das quais podemos fazer indução, isto é, as fórmulas $\psi(x, y)$ que expressam relações bem fundadas.

Definição 13.3 *Seja $\phi(x, y)$ uma fórmula onde x e y ocorrem livres. $BF(\phi)$ denota*

$$(\forall x)((x \neq \emptyset \rightarrow (\exists v)(v \in x \wedge (\forall z)(z \in x \rightarrow \neg\phi(z, v))))\wedge$$
$$\wedge(\exists u)(x \subseteq u \wedge (\forall w, y)(y \in u \wedge \phi(w, y) \rightarrow w \in u)))$$

("a relação $\phi(x, y)$ é bem fundada").

A primeira parte da fórmula anterior afirma que todo conjunto não vazio deve ter um elemento ϕ-minimal; intuitivamente, não temos ϕ-ciclos nem ϕ-cadeias descendentes infinitas, isto é: não podemos ter $\phi(x, x_1)$, $\phi(x_1, x_2), ..., \phi(x_n, x)$ nem

$$\phi(x_1, x),\ \phi(x_2, x_1),\ \phi(x_3, x_2),\ \ldots,\ \phi(x_n, x_{n-1}),\ \ldots\ .$$

A segunda parte afirma que todo conjunto pode ser estendido a um conjunto u que é ϕ-fechado, isto é: todo conjunto ϕ-relacionado com um membro de u deve pertencer a u.

Proposição 13.4 *Em* ZF *provamos que as relações $x < y$ e $x \in y$ são bem fundadas.*

Demonstração: Nas duas relações, a primeira parte é uma conseqüência direta do axioma da regularidade. A segunda parte segue do Teorema 13.2, tomando u como sendo $FT(x)$. Com efeito: seja $y \in x$; se $x \in z$ e z é transitivo, então $y \in z$. Logo $y \in FT(x)$, donde $x \subseteq FT(x)$. Se $y \in FT(x)$ e $w \in y$, considere z

transitivo tal que $x \in z$. Logo $y \in z$, donde $w \in z$, pois z é transitivo. Daqui $w \in FT(x)$, portanto $FT(x)$ satisfaz as condições requeridas. ■

Podemos agora legitimar a noção de prova por ϕ-indução transfinita, assumindo que ϕ é bem fundada. Assim, para provar que $(\forall y)\psi(y)$ basta assumir a verdade de $\psi(z)$ para todos os ϕ-antecessores z de y. A hipótese de indução é $(\forall z)(\phi(z, y) \to \psi(z))$.

Teorema 13.5 (Indução Transfinita) *Em* S *provamos o seguinte:*

$$[BF(\phi) \wedge (\forall y)((\forall z)(\phi(z, y) \to \psi(z)) \to \psi(y))] \to (\forall y)\psi(y).$$

Demonstração: Suponha que $(\forall y)\psi(y)$ é falsa e $BF(\phi)$ é verdadeira. Encontraremos v_0 tal que

$$(1) \quad (\forall z)(\phi(z, v_0) \to \psi(z)) \wedge \neg\psi(v_0),$$

contrariando a hipótese do teorema. Seja então v tal que $\neg\psi(v)$; ele existe, pela suposição $\neg(\forall y)\psi(y)$. Como $BF(\phi)$, podemos estender $\{v\}$ a um conjunto ϕ-fechado u, isto é:

$$(2) \quad (v \in u) \wedge (z \in u \wedge \phi(w, z) \to w \in u).$$

Considere $u' = \{z \ : \ (z \in u) \wedge \neg\psi(z)\}$, legitimado por [A2]. Como $v \in u$, então $v \in u'$, portanto $u' \neq \emptyset$. Pela primeira parte de $BF(\phi)$ existe um elemento v_0 de u' que é ϕ-minimal. Logo, fixe z tal que $\phi(z, v_0)$; isto implica $z \notin u'$, pois v_0 é ϕ-minimal em u', portanto $z \notin u$ ou $\psi(z)$. Dado que $v_0 \in u$ (pois $v_0 \in u'$) e $\phi(z, v_0)$, então $z \in u$, por (2). Daqui $\psi(z)$, provando desta maneira: $\phi(z, v_0) \to \psi(z)$ para todo z. Como $v_0 \in u'$, então $\neg\psi(v_0)$. Desta maneira provamos (1) como queriamos. ■

As provas por indução transfinita são importantes, mas são mais úteis quando combinadas com a *definição por recursão transfinita*. Suponha que queremos definir a soma de ordinais de maneira a ter

$$(*) \quad \begin{array}{l} \alpha + \mathbf{0} = \alpha; \\ \alpha + (\beta + 1) = (\alpha + \beta) + 1; \\ \alpha + \lambda = \bigcup_{\delta < \lambda}(\alpha + \delta) \text{ se } \lambda \text{ é um ordinal limite.} \end{array}$$

Embora $+1$ e $\bigcup$ sejam operações conhecidas, vemos que a segunda e a terceira cláusula de $(*)$ utilizam $+$ nos dois lados da definição. Usualmente este tipo de definição circular seria rejeitada. Porém, devemos observar que os ordinais do lado direito utilizam $+$ em ordinais menores aos do lado esquerdo (o membro a ser definido). Podemos pensar que, fixado α, definimos sucessivamente $\alpha + \beta$ para ordinais β cada vez maiores, utilizando os valores $\alpha + \gamma$ com $\gamma < \beta$. O Teorema da Definição por Recursão Transfinita estabelece que, partindo de uma relação $\phi(x, y)$ bem fundada, então podem ser realizadas este tipo de definições que utilizam os ϕ-antecessores, e a definição é única. Ou seja, podemos definir novas operações por indução sobre uma relação bem fundada. Observe que a definição $(*)$, embora consista de varias cláusulas, elas podem ser juntadas numa só cláusula mediante disjunção de conjunções. Assim uma definição pode ser pensada como sendo introduzida por uma fórmula. Isto coincide com a idéia de definição de funções por recursão: se $h(\overrightarrow{x})$ e $g(x, y; \overrightarrow{x})$ são funções recursivas de números naturais, então podemos definir por recursão sobre x a função $f(x; \overrightarrow{x})$ (onde $\overrightarrow{x}$ consiste de parâmetros) da maneira seguinte:

$$f(0; \overrightarrow{x}) = h(\overrightarrow{x});$$
$$f(x+1; \overrightarrow{x}) = g(f(x; \overrightarrow{x}), x; \overrightarrow{x}).$$

Desta maneira f é definida a partir de g, que utiliza o valor anterior de f. Definiremos um análogo (mais geral) para TC, onde agora g utilizará todos os valores anteriores de f.

Definição 13.6 *Seja $G(x_1, ..., x_n, y)$ uma fórmula com ao menos x_1,..., x_n, y livres. Definimos*

$$G'\langle x_1, ..., x_n\rangle = \{z \ : \ (\exists y)((\forall w)(G(x_1, ..., x_n, w) \leftrightarrow y = w) \wedge (z \in y))\}.$$

Isto é, $G'\langle x_1, ..., x_n\rangle$ é o único y tal que $G(x_1, ..., x_n, y)$ (se existir), ou $\emptyset$ em caso contrário. Logo $G'\langle x_1, ..., x_n\rangle$ é sempre um conjunto.

Definição 13.7 *Seja $F(x_1, ..., x_n, y)$ uma fórmula com ao menos x_1, ..., x_n, y livres, e $\phi(u, v)$ com u, v livres. Definimos*

$$ANT(F, x_1, ..., x_n, \phi(u, v)) = \{\langle\langle z, x_2, x_3, ..., x_n\rangle, F'\langle z, x_2, ..., x_n\rangle\rangle \ : \ \phi(z, x_1)\}.$$

O termo $ANT(F, x_1, ..., x_n, \phi(u, v))$ define o conjunto dos valores de F prévios a x_1 (a variável de recursão).

Lema 13.8 *Se $\phi(u, v)$ é bem fundada, então $ANT(F, x_1, ..., x_n, \phi(u, v))$ é legitimado em* ZF*.*

Estabeleceremos a seguir o teorema de recursão transfinita. A partir de agora $G(x, x_1, ..., x_n, y)$ é uma fórmula definindo uma operação que é iterada na variável x_1, com x_2,..., x_n como parâmetros para definir uma operação $y = F'\langle x_1, ..., x_n\rangle$. Em $ANT(F, x_1, ..., x_n, \phi(u, v))$ estão disponíveis os valores anteriores de F, e permanecem no primeiro lugar de G na iteração, da mesma maneira que é feito na definição da função recursiva

$$f(x+1; \overrightarrow{x}) = g(f(x; \overrightarrow{x}), x; \overrightarrow{x}).$$

Teorema 13.9 (Recursão Transfinita) *Sejam $G(x, x_1, ..., x_n, y)$ e $\phi(u, v)$ fórmulas. Então existe uma fórmula $F(x_1, ..., x_n, y)$ tal que*

$$\begin{aligned} BF(\phi(u, v)) \rightarrow (\forall x_1)[(\exists! y)F(x_1, ..., x_n, y) \wedge (\forall y)(F(x_1, ..., x_n, y) \leftrightarrow \\ \leftrightarrow y = G'\langle ANT(F, x_1, ..., x_n, \phi(u, v)), x_1, x_2, ..., x_n\rangle)] \end{aligned}$$

é demonstrável em ZF*.*

Veremos a seguir dois exemplos de aplicação do princípio de definição por recursão transfinita: a função de posto e a hierarquia cumulativa de von Neumann.

Definição 13.10 $\rho(x) = \bigcup\{\rho(y)+1 \ : \ y \in x\}$
("$\rho(x)$ é o posto de x").

Proposição 13.11 *Em* ZF *provamos o seguinte:*
(i) $\rho(x)$ é definido para todo conjunto x.
(ii) $\rho(x)$ é um ordinal para todo conjunto x.
(iii) Se α é um ordinal, então $\rho(\alpha) = \alpha$.
(iv) se $x \in y$, então $\rho(x) < \rho(y)$.

Demonstração: (i) Usaremos o principio de recursão transfinita. Para isto, considere $\phi(u,v)$ como sendo $u \in v$; logo, a relação ϕ (isto é, a relação $\in$) é bem fundada, pela Proposição 13.4. Seja $G(X, x_1, y)$ a fórmula

$$G(X, x_1, y) \equiv_{def} (x_1 = x_1) \wedge (y = \bigcup\{w+1 \ : \ w \in im(X)\}).$$

Logo, a operação $F(x,y)$ definida no Teorema 13.9 satisfaz:

$$F'\langle x\rangle = G'\langle ANT(F,x,\in), x\rangle = \bigcup\{w+1 \ : \ w \in im(ANT(F,x,\in))\}.$$

Por outro lado:

$$ANT(F,x,\in) = \{\langle z, F'\langle z\rangle\rangle \ : \ z \in x\}$$

donde $im(ANT(F,x,\in)) = \{F'\langle z\rangle \ : \ z \in x\}$. Daqui

$$F'\langle x\rangle = \bigcup\{F'\langle z\rangle + 1 \ : \ z \in x\}.$$

Isto significa que a operação F é a função posto.
(ii) Considere a fórmula $\psi(x)$ dada por $ord(\rho(x))$. Provaremos por indução transfinita sobre a relação $\in$ que $\psi(x)$ é verdadeira para todo x. Assim fixemos y, e suponhamos que

$$(\forall z)(z \in y \rightarrow ord(\rho(z))$$

(a hipótese de indução) é verdadeira. Queremos provar que $\rho(y)$ é um ordinal. Se $z \in y$, então $ord(\rho(z))$, logo $ord(\rho(z)+1)$. Além disso, $\rho(y) = \bigcup\{\rho(z)+1 \ : \ z \in y\}$, logo $x \in \rho(y)$ sse existe $z \in y$ tal que $x \in \rho(z)+1$. Sejam então $x \in \rho(y)$ e $w \in x$; logo $w \in x$ e $x \in \rho(z)+1$ para algum $z \in y$, e $\rho(z)+1$ é um ordinal (portanto é transitivo). Daqui $w \in \rho(z)+1$ e então $w \in \rho(y)$. Logo, $\rho(y)$ é transitivo. Se $u, v \in \rho(y)$, então $u \in \rho(z)+1$ e $v \in \rho(z')+1$ para $z, z' \in y$. Dado que $\rho(z)+1$ e $\rho(z')+1$ são ordinais, então u e v são ordinais, portanto $u \in v$ ou $v \in u$ ou $u = v$, pela lei de tricotomia para ordinais. Daqui $\rho(y)$ é conectado, sendo portanto um ordinal.
(iii) Considere $\psi(x)$ a fórmula $(ord(x) \rightarrow x = \rho(x))$. Provaremos por indução transfinita sobre a relação bem fundada $<$ que $\psi(x)$ vale para todo x. Assumamos então, fixado y, a hipótese de indução $(\forall z)(z < y \rightarrow \psi(z))$, isto é,

$$(\forall z)[(ord(z) \wedge ord(y) \wedge z \in y) \rightarrow (ord(z) \rightarrow z = \rho(z))]$$

ou, equivalentemente,

$$(*) \quad (\forall z)[(ord(y) \wedge ord(z) \wedge z \in y) \to z = \rho(z)].$$

Queremos provar que $(ord(y) \to y = \rho(y))$. Suponha então que y é um ordinal. Logo, se $z \in y$ então z é um ordinal, e vale a hipótese de $(*)$ para z, portanto $z = \rho(z)$. Daqui

$$\rho(y) = \bigcup\{\rho(z) + 1 \ : \ z \in y\} = \bigcup\{z + 1 \ : \ z \in y\}.$$

Seja $x \in \rho(y)$; logo $x \in z + 1$ para algum $z \in y$. Temos dois casos:
(a) $x \in z$. Logo $x \in z$, $z \in y$ implica $x \in y$ (pois y é um ordinal portanto é transitivo).
(b) $x = z$. Logo $x = z$, $z \in y$ implica $x \in y$.
Vemos que em todos os casos $x \in \rho(y)$ implica $x \in y$, donde $\rho(y) \subseteq y$. Suponha agora que $x \in y$; logo $x \in x + 1$ tal que $x \in y$, donde $x \in \rho(y)$. Isto é, $y \subseteq \rho(y)$, portanto $y = \rho(y)$ como queriamos provar.
(iv) Seja $x \in y$. Como $\rho(x) \in \rho(x) + 1$ e $x \in y$, então $\rho(x) \in \bigcup\{\rho(z) + 1 \ : \ z \in y\} = \rho(y)$. Dado que $\rho(x)$ e $\rho(y)$ são ordinais, pelo item (ii), então inferimos que $\rho(x) < \rho(y)$. ■

Definição 13.12 *A Hierarchia Cumulativa de von Neumann é definida da maneira seguinte:*

$$\mathcal{V}_\alpha = \bigcup_{\beta<\alpha} \mathcal{P}(\mathcal{V}_\beta) = \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \alpha\}.$$

Exemplo 13.13 *Aplicando a definição acima temos que*

$$\begin{aligned}
\mathcal{V}_{\mathbf{0}} &= \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \mathbf{0}\} = \bigcup\emptyset = \emptyset; \\
\mathcal{V}_{\mathbf{1}} &= \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \mathbf{1}\} = \bigcup\{\mathcal{P}(\mathcal{V}_{\mathbf{0}})\} = \bigcup\{\mathcal{P}(\emptyset)\} = \bigcup\{\{\emptyset\}\} = \{\emptyset\}; \\
\mathcal{V}_{\mathbf{2}} &= \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \mathbf{2}\} = \bigcup\{\mathcal{P}(\mathcal{V}_{\mathbf{0}}), \mathcal{P}(\mathcal{V}_{\mathbf{1}})\} = \bigcup\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&= \{\emptyset, \{\emptyset\}\}; \\
\mathcal{V}_{\mathbf{3}} &= \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \mathbf{3}\} = \bigcup\{\mathcal{P}(\mathcal{V}_{\mathbf{0}}), \mathcal{P}(\mathcal{V}_{\mathbf{1}}), \mathcal{P}(\mathcal{V}_{\mathbf{2}})\} \\
&= \bigcup\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.
\end{aligned}$$

■

Teorema 13.14 *Em* ZF *provamos o seguinte:*
(i) $\mathcal{V}_\alpha$ *é definido para todos os ordinais* α.
(ii) Seja α *um ordinal. Logo* $\mathcal{V}_\alpha$ *é transitivo, e* $\mathcal{V}_{\alpha+1} = \mathcal{P}(\mathcal{V}_\alpha)$.
(iii) Seja λ *um ordinal limite. Logo* $\mathcal{V}_\lambda = \bigcup_{\beta<\lambda} \mathcal{V}_\beta$.
(iv) Seja α *um ordinal. Então* $x \in \mathcal{V}_\alpha$ *sse* $\rho(x) < \alpha$.
(v) $(\forall x)(\exists \alpha)(x \in \mathcal{V}_\alpha)$ *(aqui,* α *denota um ordinal).*

Demonstração: (i) Aplicaremos o principio de recursão transfinita 13.9. Considere a fórmula

$$G(X, x_1, y) \equiv_{def} (x_1 = x_1) \wedge (y = \bigcup\{\mathcal{P}(w) \ : \ w \in im(X)\}).$$

A operação $F(x, y)$ definida por recursão transfinita sobre $\in$ a partir de G satisfaz o seguinte:

$$F'\langle x\rangle = \bigcup\{\mathcal{P}(w) \ : \ w \in im(ANT(F, x, \in))\}.$$

Mas $im(ANT(F, x, \in)) = \{F'\langle y\rangle \ : \ y \in x\}$, logo

$$F'\langle x\rangle = \bigcup\{\mathcal{P}(F'\langle y\rangle) \ : \ y \in x\}.$$

Se α é um ordinal, então $\beta < \alpha$ sse $\beta \in \alpha$, logo $F'\langle\alpha\rangle$ representa $\mathcal{V}_\alpha$ sobre os ordinais α, isto é, $\mathcal{V}_\alpha$ está legitimado para todo ordinal α.
(ii) Faremos indução transfinita sobre a relação $<$ e a seguinte fórmula:

$$\psi(x) \equiv_{def} ord(x) \rightarrow (transi(\mathcal{V}_x) \wedge \mathcal{V}_{x+1} \subseteq \mathcal{P}(\mathcal{V}_x)).$$

Fixado um ordinal y, assuma que a hipótese de indução é verdadeira, isto é, $(\forall z)(z < y \rightarrow \psi(z))$ ou, equivalentemente,

$$(*) \quad (\forall z)(z \in y \rightarrow (transi(\mathcal{V}_z) \wedge \mathcal{V}_{z+1} \subseteq \mathcal{P}(\mathcal{V}_z)))$$

(pois, se y é ordinal, então $z < y$ sse $z \in y$). Queremos provar que $\mathcal{V}_y$ é transitivo e $\mathcal{V}_{y+1} \subseteq \mathcal{P}(\mathcal{V}_y)$. Pela definição de $\mathcal{V}_y$ temos que

$$(**) \quad x \in \mathcal{V}_y \text{ sse } x \in \mathcal{P}(\mathcal{V}_z) \text{ para algum } z \in y \text{ sse } x \subseteq \mathcal{V}_z \text{ para algum } z \in y.$$

Fato 1: Seja u transitivo e $w \in u$. Logo $w \subseteq u$.
Com efeito, se $z \in w$, então: $z \in w$, $w \in u$, $transi(u)$ implica $z \in u$, isto é: $z \in w$ implica $z \in u$. Daqui $w \subseteq u$, provando o **Fato 1**.
Seja então $x \in \mathcal{V}_y$ e $w \in x$. Por $(**)$ temos que $x \subseteq \mathcal{V}_z$ para algum $z \in y$. Dado que $w \in x$, então $w \in \mathcal{V}_z$. Por $(*)$ temos que $\mathcal{V}_z$ é transitivo, e $w \in \mathcal{V}_z$, logo $w \subseteq \mathcal{V}_z$, pelo **Fato 1**. Portanto $w \in \mathcal{V}_y$, por $(**)$. Isto significa que $\mathcal{V}_y$ é transitivo se y é um ordinal. Falta provar que $\mathcal{V}_{y+1} \subseteq \mathcal{P}(\mathcal{V}_y)$. Por $(*)$ temos que $\mathcal{V}_{z+1} \subseteq \mathcal{P}(\mathcal{V}_z)$ para todo $z \in y$, logo $\mathcal{V}_{z+1} = \mathcal{P}(\mathcal{V}_z)$ para todo $z \in y$ (a inclusão $\mathcal{P}(\mathcal{V}_z) \subseteq \mathcal{V}_{z+1}$ é imediata da Definição 13.12). Logo

$$\begin{aligned}\mathcal{V}_{y+1} &= \bigcup\{\mathcal{P}(\mathcal{V}_z) \ : \ z \in y+1\} = \bigcup(\{\mathcal{P}(\mathcal{V}_z) \ : \ z \in y\} \cup \{\mathcal{P}(\mathcal{V}_y)\}) \\ &= \bigcup(\{\mathcal{V}_{z+1} \ : \ z \in y\} \cup \{\mathcal{P}(\mathcal{V}_y)\}).\end{aligned}$$

Seja $x \in \mathcal{V}_{y+1}$; logo $x \in u$ tal que $u \in \{\mathcal{V}_{z+1} \ : \ z \in y\} \cup \{\mathcal{P}(\mathcal{V}_y)\}$, pela definição de $\bigcup$. Temos dois casos:
(a) $u = \mathcal{P}(\mathcal{V}_y)$. Logo, $x \in \mathcal{P}(\mathcal{V}_y)$.
(b) $u = \mathcal{V}_{z+1}$ para algum $z \in y$. Provaremos primeiro o seguinte
Fato 2: Se α e β são ordinais, então $\alpha < \beta + 1$ implica $\mathcal{V}_\alpha \subseteq \mathcal{V}_\beta$.
Com efeito, se $\alpha < \beta$, então: $\gamma \in \alpha$ implica $\gamma \in \beta$. Logo, se $w \in \mathcal{V}_\alpha$, então $w \in \mathcal{P}(\mathcal{V}_\gamma)$ para algum $\gamma \in \alpha$, pela Definição 13.12. Daqui $w \in \mathcal{P}(\mathcal{V}_\gamma)$ onde $\gamma \in \beta$, portanto $w \in \mathcal{V}_\beta$, isto é, $\mathcal{V}_\alpha \subseteq \mathcal{V}_\beta$. O caso $\alpha = \beta$ é óbvio. Isto prova o **Fato 2**.

Continuando com o caso (b), temos que $x \in u = \mathcal{V}_{z+1}$, onde $z \in y$. Logo existe $w \in z+1$ tal que $x \in \mathcal{P}(\mathcal{V}_w)$, pela Definição 13.12. Mas $w \in z+1$, $z \in y$ implica $w \in y$, pois y é ordinal. Daqui $w < y+1$ e então $\mathcal{V}_w \subseteq V_y$, pelo **Fato 2**. Dado que $x \in \mathcal{P}(\mathcal{V}_w)$, então $x \subseteq \mathcal{V}_w$, donde $x \subseteq \mathcal{V}_y$, isto é, $x \in \mathcal{P}(\mathcal{V}_y)$.
Vemos que os dois casos (a) e (b) nos levam à conclusão de que $x \in \mathcal{P}(\mathcal{V}_y)$. Portanto $\mathcal{V}_{y+1} \subseteq \mathcal{P}(\mathcal{V}_y)$. Desta maneira provamos $\psi(y)$ a partir da hipótese de indução. Logo, $\psi(x)$ vale para todo x, isto é: $\mathcal{V}_\alpha$ é transitivo e $\mathcal{V}_{\alpha+1} = \mathcal{P}(\mathcal{V}_\alpha)$, se α é um ordinal.
(iii) Seja λ um ordinal limite. Por (ii) temos que

$$\mathcal{V}_\lambda = \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \lambda\} = \bigcup\{\mathcal{V}_{\beta+1} \ : \ \beta < \lambda\}.$$

Se $\beta < \lambda$ então $\beta + 1 < \lambda$, por [LIM], donde $\mathcal{V}_\beta \subseteq \mathcal{V}_\lambda$ e $\mathcal{V}_{\beta+1} \subseteq \mathcal{V}_\lambda$, pelo **Fato 2**. Portanto $\mathcal{V}_\beta \in \mathcal{P}(\mathcal{V}_\lambda)$ e $\mathcal{V}_{\beta+1} \in \mathcal{P}(\mathcal{V}_\lambda)$. Isto significa que existem os conjuntos

$$a = \{\mathcal{V}_\beta \ : \ \beta < \lambda\} = \{x \ : \ x \in \mathcal{P}(\mathcal{V}_\lambda) \wedge (\exists\beta)(\beta < \lambda \wedge x = \mathcal{V}_\beta)\},$$

$$b = \{\mathcal{V}_{\beta+1} \ : \ \beta < \lambda\} = \{x \ : \ x \in \mathcal{P}(\mathcal{V}_\lambda) \wedge (\exists\beta)(\beta < \lambda \wedge x = \mathcal{V}_{\beta+1})\}.$$

Dado que $\beta < \lambda$ implica $\mathcal{V}_\beta \subseteq \mathcal{V}_\lambda$, então $\bigcup a \subseteq \mathcal{V}_\lambda$, pela definição de $\bigcup$. Por outro lado, como $\beta < \lambda$ implica $\beta + 1 < \lambda$ então $b \subseteq a$, donde $\mathcal{V}_\lambda = \bigcup b \subseteq \bigcup a$, isto é, $\mathcal{V}_\lambda = \bigcup a$ como queriamos.
(iv) Considere $\psi(x) \equiv_{def} (\forall\alpha)(x \in \mathcal{V}_\alpha \leftrightarrow \rho(x) < \alpha)$ (aqui, α é uma variável de ordinais). Provaremos por indução sobre $\in$ que $\psi(x)$ vale para todo x. Seja y, e suponhamos que

(HI) $\qquad (\forall z)(z \in y \to \psi(z))$.

Queremos provar que vale $\psi(y)$. Fixemos então um ordinal α.
Parte 1: $(y \in \mathcal{V}_\alpha \to \rho(y) < \alpha)$.
Assumamos que $y \in \mathcal{V}_\alpha$. Se $z \in y$, então $z \in \mathcal{V}_\alpha$, pois $\mathcal{V}_\alpha$ é transitivo por (ii). Por (HI) temos que $\rho(z) < \alpha$, portanto $\rho(z) + 1 \leq \alpha$. Suponha que existe $z \in y$ tal que $\alpha = \rho(z) + 1$. Logo, por (ii)

$$y \in \mathcal{V}_\alpha = \mathcal{V}_{\rho(z)+1} = \mathcal{P}(\mathcal{V}_{\rho(z)}).$$

Daqui $y \subseteq \mathcal{V}_{\rho(z)}$; mas $z \in y$, logo $z \in \mathcal{V}_{\rho(z)}$, e $\rho(z)$ é um ordinal. Por (HI) obtemos que $\rho(z) < \rho(z)$, uma contradição. Logo $\rho(z) + 1 < \alpha$ para todo $z \in y$. Portanto

$$\rho(y) = \bigcup\{\rho(z) + 1 \ : \ z \in y\} \subseteq \alpha$$

donde $\rho(y) \leq \alpha$. Suponha que $\alpha = \rho(y)$. Dado que $y \in \mathcal{V}_\alpha$, então existe $\beta \in \alpha$ tal que $y \in \mathcal{P}(\mathcal{V}_\beta)$, pela Definição 13.12. Dado que $\beta \in \alpha = \rho(y)$, então existe $z \in y$ tal que $\beta \in \rho(z)+1$. Mas $y \in \mathcal{P}(\mathcal{V}_\beta)$, então $y \subseteq \mathcal{V}_\beta$, e $z \in y$, donde $z \in \mathcal{V}_\beta$. Por (HI) temos que $\rho(z) < \beta$. Por outro lado provamos que $\beta \in \rho(z) + 1$, e então temos dois casos:

(a) $\beta \in \rho(z)$: logo $\beta \in \rho(z)$ e $\rho(z) \in \beta$, contradição.

(b) $\beta = \rho(z)$: logo $\rho(z) \in \beta$ e $\beta = \rho(z)$, contradição.

Os dois casos nos levam a uma contradição, portanto $\rho(y) < \alpha$. Isto conclui a prova da **Parte 1**.
Parte 2: $(\rho(y) < \alpha \to y \in \mathcal{V}_\alpha)$.
Assumamos que

$$\rho(y) = \bigcup\{\rho(z) + 1 \ : \ z \in y\} < \alpha.$$

Suponha que $y \notin \mathcal{V}_\alpha = \bigcup\{\mathcal{P}(\mathcal{V}_\beta) \ : \ \beta < \alpha\}$. Aplicando a definição de $\bigcup$ obtemos:

$(***)$ para todo $\beta < \alpha$ existe $z \in y$ tal que $z \notin \mathcal{V}_\beta$

pois $y \notin \mathcal{P}(\mathcal{V}_\beta)$ sse $y \not\subseteq \mathcal{V}_\beta$. Por hipótese $\rho(y) < \alpha$ donde, por $(***)$, existe $z \in y$ tal que $z \notin \mathcal{V}_{\rho(y)}$. Dado que $z \in y$ e $\rho(z) < \rho(z) + 1$ então, por (HI), temos que $z \in \mathcal{V}_{\rho(z)+1}$. Mas $z \in y$ implica $\rho(z) < \rho(y)$, pela Proposição 13.11(iv). Logo $\rho(z)+1 < \rho(y)+1$, donde $\mathcal{V}_{\rho(z)+1} \subseteq \mathcal{V}_{\rho(y)}$, pelo **Fato 2**. De $z \in \mathcal{V}_{\rho(z)+1}$ obtemos $z \in \mathcal{V}_{\rho(y)}$, uma contradição. Portanto $y \in \mathcal{V}_\alpha$. Provamos desta maneira a **Parte 2**, obtendo portanto $\psi(y)$. Por indução transfinita temos que $\psi(x)$ vale para todo x.
(v) Dado x, então $\rho(x)$ é um ordinal, portanto $\rho(x) + 1$ é também um ordinal, e $\rho(x) < \rho(x) + 1$. Pelo item (iv) inferimos que $x \in \mathcal{V}_{\rho(x)+1}$. ■

O teorema anterior é a afirmação mais forte que podemos fazer em ZF com relação à teoria cumulativa de tipos. Provamos desta maneira que os objetos que estudamos na linguagem (reprsentados pelas variáveis livres) pertencem de fato a uma estrutura cumulativa. O ordinal $\rho(x)+1$ indica o nível da hierarquia em que o conjunto x aparece pela primeira vez; portanto o seu posto $\rho(x)$ denota exatamente o nível em que ele é concebido. Por outro lado, $\mathcal{V}_\alpha$ é a coleção de todos os conjuntos que apareceram antes do nível α. Logo $\mathcal{V}_{\alpha+1} - \mathcal{V}_\alpha$ consiste dos conjuntos criados no nível α. O fato que $\rho(x) + 1 = Min\{\beta \ : \ x \in \mathcal{V}_\beta\}$ é fácil de ser provado. Com efeito:

(a) $\rho(x) < \rho(x) + 1$ implica $x \in \mathcal{V}_{\rho(x)+1}$;
(b) $x \in \mathcal{V}_\beta$ implica $\rho(x) < \beta$ implica $\rho(x) + 1 \leq \beta$.

Assim, $\mathbf{0}$ aparece no nível 1 (pois o nível 0 é vazio); $\mathbf{1}$ é concebido no nível 1 (isto é, $\rho(\mathbf{1}) = \mathbf{1} \simeq 1$), logo só aparece no nível 2; em geral, $\mathbf{n}$ é concebido no nível $\rho(\mathbf{n}) = \mathbf{n} \simeq n$, portanto aparece pela primeira vez no nível seguinte $n + 1$. Já ω aparece no nível $\omega + 1$, pois ele é criado no nível ω ("infinito"), enquanto que $\mathcal{V}_\omega$ consiste de todos os conjuntos que apareceram em níveis finitos. Em geral, se α é um ordinal, então α é concebido no nível α, logo aparece no nível $\alpha + 1$, isto é: $\alpha \in \mathcal{V}_{\alpha+1} - \mathcal{V}_\alpha$. Cada nível (diferente do nível 0) contém exatamente um ordinal, e cada ordinal denota um nível. Neste sentido forte, os ordinais descrevem os níveis da hierarquia cumulativa de tipos.

14 Aritmética Ordinal

Continuaremos estudando nesta seção os ordinais. Primeiro de tudo provaremos que os ordinais são exatamente os conjuntos bem ordenados, dai a denominação de *ordinais*. Lembremos da Definição 6.10 que $bo(r,x)$ denota que r é uma boa ordem em x, e $min(v,r,u)$ denota $v \in u \wedge (\forall w)(w \in u \to \neg(w\ r\ v))$ (v é um elemento r-minimal de u). Introduzimos a seguinte notação:

Definição 14.1 *$bf(r,x)$ denota $(\forall u)(u \subseteq x \wedge u \neq \emptyset \to (\exists v)min(v,r,u)$*
("r é bem fundada sobre x")

Usando esta definição, é imediato que $bo(r,x) \leftrightarrow bf(r,x) \wedge con(r,x)$, em que $con(r,x)$ denota que r é conectada em x (lembre da Definição 6.1). Como foi provado nas Proposições 6.12 e 6.13, uma boa ordem r em x equivale a uma ordem estrita r em x tal que todo subconjunto de x não vazio tem r-primeiro elemento.

Lema 14.2 *Seja $E(x) = \{\langle y,z\rangle\ :\ y,z \in x \wedge y \in z\}$. Em* S *vale o seguinte:*
(i) Se x é um ordinal, então $E(x)$ é uma boa ordem em x.
(ii) Se r é bem fundada em z, então $\phi(x,y) \equiv_{def} (x,y \in z) \wedge (x\ r\ y)$ é bem fundada (lembre da Definição 13.3).

Demonstração: (i) Se x é um ordinal, então $y\ E(x)\ z$ sse $y < z$ para todo $y,z \in x$. Dado que $y < z$ é uma relação bem fundada, então $E(x)$ é bem fundada em x. Se $y,z \in x$ então y e x são ordinais. Pela lei de tricotomia para ordinais temos que $E(x)$ é conectada em x.
(ii) Seja r bem fundada em z, e considere $\phi(x,y) \equiv_{def} (x,y \in z) \wedge (x\ r\ y)$. Se $x \neq \emptyset$, queremos provar o seguinte:

$$(*) \qquad (\exists\, v \in x)(\forall\, w \in x)(w \in z \wedge v \in z \to \neg(w\ r\ v),$$

pois $\neg\phi(w,v) \leftrightarrow [w \in z \wedge v \in z \to \neg(w\ r\ v)]$. Considere $u = x \cap z \subseteq z$. Se $u = \emptyset$, então tomando $v \in x$ arbitrário (estamos assumindo que x é não vazio) obtemos $(*)$ trivialmente, pois $v \notin z$. Se $u \neq \emptyset$ então, dado que $u \subseteq z$, temos que existe $v \in u$ (portanto $v \in x$) tal que $\neg(w\ r\ v)$ para todo $w \in u$, pois r é bem fundada em z. Seja $w \in x$; se $w \in z$ e $v \in z$, isto é, se $w \in z$, então inferimos $w \in u$, donde $\neg(w\ r\ v)$. Isto prova $(*)$, e logo $\phi(x,y)$ satisfaz a primeira metade da definição de relação bem fundada. Para a segunda metade, seja x arbitrário; queremos provar que existe u tal que

$$(**) \qquad x \subseteq u \wedge (\forall\, w,y)(y \in u \wedge \phi(w,y) \to w \in u).$$

Se $x = \emptyset$, então $u = \emptyset$ satisfaz trivialmente $(**)$. Se $x \neq \emptyset$ considere

$$u = x \cup \{w\ :\ w \in z \wedge (\exists\, y \in z)(w\, r\, y)\}.$$

Temos que $u \neq \emptyset$ e $x \subseteq u$. Sejam w e y tais que $y \in u$ e $\phi(w,y)$, logo: $y,w \in z$ e $w\ r\ y$. Daqui $w \in u$, pela definição de u, portanto vale $(**)$ e então $\phi(x,y)$ é bem fundada. ■

Lema 14.3 *Em* ZF *provamos o seguinte: se* $bf(r,z)$*, então existe*

$$h(x) = \{h(y) \ : \ y \in z \ \wedge \ y\, r\, x\}$$

para todo $x \in z$.

Demonstração: Usaremos recursão transfinita para definir os conjuntos $h(x)$. Considere a fórmula

$$G(X, x_1, y) \equiv_{def} (x_1 = x_1) \wedge (y = im(X)).$$

Seja $F(x,y)$ a operação definida a partir de $G(X, x_1, y)$ por recursão transfinita na relação bem fundada $\phi(x,y) \equiv_{def} (x, y \in z) \wedge (x \ r \ y)$ (temos que $\phi(x,y)$ é bem fundada pelo Lema 14.2(ii)). Por definição

$$ANT(F, x, \phi(u,v)) = \{\langle y, F'\langle y\rangle\rangle \ : \ \phi(y,x)\}$$

portanto, fixado $x \in z$,

$$\begin{aligned} F'\langle x\rangle &= G'\langle ANT(F, x, \phi(u,v)), x\rangle \\ &= im(ANT(F, x, \phi(u,v)) \\ &= \{F'\langle y\rangle \ : \ \phi(y,x)\} \\ &= \{F'\langle y\rangle \ : \ x, y \in z \wedge y \ r \ x\} \\ &= \{F'\langle y\rangle \ : \ y \in z \wedge y \ r \ x\}. \end{aligned}$$

Desta maneira, $F(x,y)$ representa a operação $h(x)$ desejada para todo $x \in z$. ■

Teorema 14.4 (Caracterização dos Ordinais) *Em* ZF *prova-se: se* r *é uma boa ordem em* z*, então existe um ordinal* α *tal que*

$$h : z \longrightarrow \alpha, \ \ h(x) = \{h(y) \ : \ y \in z \wedge y\, r\, x\}$$

é um isomorfismo de conjuntos bem ordenados, isto é: h *é uma bijeção tal que:* $x \ r \ y$ *sse* $h(x) < h(y)$*. O ordinal* α *e o isomorfismo* h *são únicos.*

Demonstração: Seja r uma boa ordem em z; logo, $bf(r,z)$ donde existe $h(x)$ para todo $x \in z$, pelo Lema 14.3. Seja

$$r^* = (r|z) \cup \{\langle y, z\rangle \ : \ y \in z\}$$

lembrando que $r|z = \{\langle x, y\rangle \ : \ x \in z \wedge x \ r \ y\}$. Provaremos que r^* é bem fundada em $z+1$. Seja então $u \subseteq z+1$, $u \neq \emptyset$.
Caso 1: $u \subseteq z$. Como $bf(r,z)$, existe $v \in u$ tal que $\neg(w \ r \ v)$ para todo $w \in u$. Pela construção de r^*, temos que $\neg(w \ r^* \ v)$ para todo $w \in u$ pois r coincide com r^* em $z \times z$.
Caso 2: $u = \{z\} \cup u_1$ tal que $u_1 \subseteq z$. Se $u_1 = \emptyset$ então $v = z$ satisfaz: $v \in u$ e $\neg(w \ r^* \ v)$ para todo $w \in u$. Se $u_1 \neq \emptyset$ então $u_1 \subseteq z$ é não vazio, logo existe $v \in u_1$ tal que $\neg(w \ r \ v)$ para todo $w \in u_1$. Como $\neg(z \ r^* \ v)$, pela construção de

r^*, então $\neg(w\ r^*\ v)$ para todo $w \in u$.
Isto prova que $bf(r^*, z+1)$. Pelo Lema 14.3 inferimos que existe

$$h^*(x) = \{h^*(y)\ :\ (y \in z+1) \wedge (y\, r^*\, x)\}$$

para todo $x \in z+1$.
Fato 1: $h^*(x) = h(x)$ para todo $x \in z$.
Com efeito: seja $\psi(x) \equiv_{def} (x \in z \rightarrow h^*(x) = h(x))$. Fixemos y tal que

$$\text{(HI)} \qquad (\forall w)(\phi(w,y) \rightarrow \psi(w)),$$

onde $\phi(u,v) \equiv_{def} (u,v \in z) \wedge (u\ r\ v)$ é uma relação bem fundada, pelo Lema 14.2(ii).
Suponhamos que $y \in z$; logo, pela construção de r^*:

$$\begin{aligned} h^*(y) &= \{h^*(w)\ :\ (w \in z+1) \wedge (w\ r^*\ y)\} \\ &= \{h^*(w)\ :\ w \in z \wedge w\ r\ y\} \\ &= \{h^*(w)\ :\ \phi(w,y)\}. \end{aligned}$$

Por (HI) temos que $\psi(w)$ para todo w tal que $\phi(w,y)$. Como $\phi(w,y)$ implica $w \in z$, então obtemos que $h^*(w) = h(w)$ para todo w tal que $\phi(w,y)$. Daqui $h^*(y) = h(y)$. Por indução transfinita sobre $\phi(x,y)$ inferimos que $\psi(x)$ é verdadeira para todo x como queriamos, provando o **Fato 1**.
A partir do **Fato 1** e da definição de r^* obtemos

$$h^*(z) = \{h^*(y)\ :\ (y \in z+1) \wedge (y\, r^*\, z)\} = \{h^*(y)\ :\ y \in z\} = \{h(y)\ :\ y \in z\}.$$

Seja $\alpha \equiv_{def} h^*(z)$. Provaremos que α é um ordinal. Seja $x \in h(y)$, $y \in z$. Logo $x = h(w)$ tal que $w \in z$, pelas definições de $h(y)$ e $\phi(w,y)$, portanto $x \in \alpha$; daqui α é transitivo. Sejam $h(x), h(y) \in \alpha$. Como $x, y \in z$, então $y = x$ ou $y\ r\ x$ ou $x\ r\ y$. Se $x = y$ então $h(x) = h(y)$. O caso em que $y\ r\ x$ implica $h(y) \in h(x)$. Se $x\ r\ y$ então $h(x) \in h(y)$. Vemos assim que α é conectado. Daqui obtemos que α é um ordinal, portanto $h(x)$ é um ordinal para todo $x \in z$, e α é bem ordenado pela relação $E(\alpha) = <$, pelo Lema 14.2(i). A propriedade $x\ r\ y$ sse $h(x) < h(y)$ é imediata, logo $h : z \longrightarrow \alpha$ é um isomorfismo de conjuntos bem ordenados. Para provar a unicidade de α, suponha que $\langle z, r\rangle$ é isomorfo a $\langle \beta, <\rangle$ via $g : z \longrightarrow \beta$ para um outro ordinal β. Logo $g \circ h^{-1} : \alpha \longrightarrow \beta$ é um isomorfismo.
Fato 2: Sejam α e β ordinais, e $f : \alpha \longrightarrow \beta$ un isomorfismo, isto é: f é uma bijeção tal que $\gamma < \delta$ sse $f(\gamma) < f(\delta)$ para todo $\gamma, \delta \in \alpha$. Logo $f(\gamma) = \{f(\delta)\ :\ \delta < \gamma\}$, donde $f(\gamma) = \gamma$ para todo $\gamma \in \alpha$.
Com efeito, se $\delta < \gamma < \alpha$, então $f(\delta) \in f(\gamma)$. Por outro lado, seja $\theta \in f(\gamma)$; então $\theta = f(\delta)$ para $\delta \in \alpha$, pois f é sobrejetora. Daqui $f(\delta) < f(\gamma)$ implica $\delta < \gamma$, e então $\theta = f(\delta)$ com $\delta < \gamma$, isto é: $f(\gamma) = \{f(\delta)\ :\ \delta < \gamma\}$. Considerando a fórmula

$$\psi(x) \equiv_{def} x \in \alpha \rightarrow f(x) = x$$

então é agora muito simples provar por indução sobre $\in$ que $\psi(x)$ vale para todo x (exercício!), concluindo a prova do **Fato 2**.

Temos que $g \circ h^{-1} : \alpha \longrightarrow \beta$ é um isomorfismo. Pelo **Fato 2**, $g \circ h^{-1}(x) = x$ para todo $x \in \alpha$. Mas $g \circ h^{-1}$ é sobrejetora, portanto $\alpha = \beta$, e $g \circ h^{-1} = I(\alpha)$. Daqui $g = h$ (compondo à direita com h). Isto mostra que α e h são unicos para cada $\langle z, r \rangle$. ■

Pelo Lema 14.2(i) vemos que todo ordinal α é bem ordenado pela relação $<$. Reciprocamente, pelo Teorema 14.4, se z é um conjunto bem ordenado por uma relação r então existe um único ordinal α e um único isomorphismo $h : z \longrightarrow \alpha$ de conjuntos bem ordenados tal que $\langle z, r \rangle \simeq \langle \alpha, < \rangle$. O ordinal α associado com $\langle z, r \rangle$ é dito o *tipo ordinal* de $\langle z, r \rangle$. Observe que o tipo ordinal α de z depende da relação r: com efeito, z pode possuir duas estruturas de boa ordem r_1 e r_2 não isomorfas, de maneira a ter associados dois tipos ordinais, α_1 para $\langle z, r_1 \rangle$ e α_2 para $\langle z, r_2 \rangle$ com $\alpha_1 \neq \alpha_2$.

Exemplo 14.5 Considere em $\mathbb{N}$ a estrutura usual r_1 de boa ordem: $n\ r_1\ m$ sse $n < m$. Logo, $h_1 : \mathbb{N} \longrightarrow \omega$ dada por $h_1(n) = \mathbf{n}$ é o único isomorfismo de $\langle \mathbb{N}, r_1 \rangle$ em $\langle \omega, < \rangle$ tal que ω é o tipo ordinal de $\langle \mathbb{N}, r_1 \rangle$. Por outro lado, considere a seguinte relação r_2 em $\mathbb{N}$:

$$\begin{array}{ll} n\ r_2\ m & \text{se } n, m > 0 \text{ e } n < m; \\ n\ r_2\ 0 & \text{para todo } n > 0. \end{array}$$

Isto é: r_2 coincide com a boa ordem usual $<$ para todos os números naturais positivos, e 0 é colocado como r_2-último elemento de $\mathbb{N}$. É muito simples ver que r_2 é uma boa ordem em $\mathbb{N}$ (conferir!). Considere $h_2 : \mathbb{N} \longrightarrow \omega + 1$ dada por

$$h_2(n) = \begin{cases} \mathbf{n-1} & \text{se } n > 0 \\ \omega & \text{se } n = 0 \end{cases} .$$

Temos que h_2 é um isomorfismo entre $\langle \mathbb{N}, r_2 \rangle$ e $\langle \omega + 1, < \rangle$ (conferir!), portanto $\omega + 1$ é o tipo ordinal de $\langle \mathbb{N}, r_2 \rangle$, sendo que $\omega \neq \omega + 1$. Isto mostra que o tipo ordinal de um conjunto bem ordenado depende da boa ordem especificada. ■

Definição 14.6 *Sejam α e β ordinais. Definimos a soma ordinal $\alpha + \beta$ como sendo*

$$\alpha + \beta = \begin{cases} \alpha & \textit{se } \beta = \mathbf{0} \\ (\alpha + \gamma) + 1 & \textit{se } \beta = \gamma + 1 \\ \bigcup_{\gamma < \beta} (\alpha + \gamma) & \textit{se } \beta \textit{ é limite ordinal} \end{cases} .$$

Para provar que a soma está bem definida, precisamos introduzir uma relação bem fundada apropriada.

Lema 14.7 *Considere a fórmula*

$$\phi(u, v) \equiv_{def} (ord(u) \wedge ord(v)) \wedge [(\exists z)(v = z + 1 \wedge u = z) \vee (lim(v) \wedge u \in v)].$$

Então $\phi(u,v)$ é uma relação bem fundada.

Demonstração: Seja $x \neq \emptyset$. Pelo axioma da regularidade, existe $v \in x$ tal que $(\forall\, z \in x)(z \notin v)$. Logo, $v \neq z+1$ para todo $z \in x$, e então não vale $(\exists z)(v = z+1 \wedge u = z)$ para todo $u \in x$. Se v é um ordinal limite então, dado que $z \notin v$ para todo $z \in x$, inferimos que não vale $(lim(v) \wedge u \in v)$ para todo $u \in x$. Desta maneira obtemos: $u \in x \rightarrow \neg\phi(u,v)$, donde

$$x \neq \emptyset \rightarrow (\exists\, v \in x)(\forall\, w \in x)\neg\phi(w,v).$$

Para provar a segunda parte da Definição 13.3 de relação bem fundada, seja x arbitrário, e considere $u = FT(x)$, o fecho transitivo de x. Seja $y \in u$ e w tal que $\phi(w,y)$. Se z é um conjunto transitivo tal que $x \in z$ então $y \in z$, pois $y \in FT(x)$. Dado que $\phi(w,y)$, então $w \in y$ (é uma conseqüência direta da definição de ϕ), logo $w \in z$ (pois z é transitivo). Daqui $w \in FT(x) = u$, donde

$$(\exists u)(x \subseteq u \wedge (\forall\, w,y)(y \in u \wedge \phi(w,y) \rightarrow w \in u)).$$

Isto prova que $\phi(u,v)$ é uma relação bem fundada. ■

Lema 14.8 *Seja b um conjunto de ordinais, isto é: $(\forall x)(x \in b \rightarrow ord(x))$. Logo $\bigcup b$ é um ordinal.*

Demonstração: Seja $a = \bigcup b$. Considere $x \in a$ e $y \in x$. Logo, existe $z \in b$ tal que $x \in z$. Por hipótese z é um ordinal, e $y \in x$, $x \in z$; portanto $y \in z$ com $z \in b$, donde $y \in a$. Isto mostra que a é transitivo. Por outro lado, sejam $x, y \in a$; logo existem $z, w \in b$ tais que $x \in z$ e $y \in w$. Por hipótese z e w são ordinais, logo x e y são ordinais. Portanto $x = y$ ou $x \in y$ ou $y \in x$ pela lei de tricotomia para ordinais. Isto prova que a é conectado para $\in$, portanto a é um ordinal. ■

Proposição 14.9 *A soma ordinal está bem definida em* ZF, *isto é, para cada ordinal α e β, existe um único conjunto $\alpha+\beta$ definido de acordo com a Definição 14.6.*

Demonstração: Para provar que a soma ordinal está bem definida usaremos recursão transfinita sobre a relação bem fundada $\phi(u,v)$ do Lema 14.7. Considere a seguinte fórmula:

$$\begin{aligned} G(X,x_1,x_2,y) \equiv_{def} & [x_1 = \mathbf{0} \wedge y = x_2] \vee [(\exists z)(x_1 = z+1) \wedge y = (\textstyle\bigcup im(X))+1] \\ & \vee\ [lim(x_1) \wedge y = \textstyle\bigcup im(X)]. \end{aligned}$$

Logo, definimos por recursão transfinita sobre $\phi(u,v)$ uma operação $F(x_1,x_2,y)$. Temos que, se x_1 é um ordinal, então

$$ANT(F,\mathbf{0},x_2,\phi(u,v)) = \{\langle\langle w,x_2\rangle, F'\langle w,x_2\rangle\rangle\ :\ \phi(w,\mathbf{0})\} = \emptyset,$$

$$ANT(F,z+1,x_2,\phi(u,v)) = \{\langle\langle w,x_2\rangle, F'\langle w,x_2\rangle\rangle\ :\ \phi(w,z+1)\}$$

$$= \{\langle\langle z, x_2\rangle, F'\langle z, x_2\rangle\rangle\},$$

$$\begin{aligned} ANT(F, x_1, x_2, \phi(u,v)) &= \{\langle\langle w, x_2\rangle, F'\langle w, x_2\rangle\rangle \ : \ \phi(w, x_1)\} \\ &= \{\langle\langle w, x_2\rangle, F'\langle w, x_2\rangle\rangle \ : \ w \in x_1\} \end{aligned}$$

segundo o caso: $x_1 = \mathbf{0}$, $x_1 = z + 1$ ou x_1 é um ordinal limite, respectivamente. Obtemos assim em cada caso:

$$im(ANT(F, \mathbf{0}, x_2, \phi(u,v))) = \emptyset,$$

$$im(ANT(F, z+1, x_2, \phi(u,v))) = \{F'\langle z, x_2\rangle\},$$

$$im(ANT(F, x_1, x_2, \phi(u,v))) = \{F'\langle w, x_2\rangle \ : \ w \in x_1\},$$

respectivamente. Portanto, se α e β são ordinais, então

$$F'\langle \mathbf{0}, \alpha\rangle = G'\langle ANT(F, \mathbf{0}, \alpha, \phi(u,v)), \mathbf{0}, \alpha\rangle = \alpha,$$

$$\begin{aligned} F'\langle \gamma+1, \alpha\rangle &= G'\langle ANT(F, \gamma+1, \alpha, \phi(u,v)), \gamma+1, \alpha\rangle = (\bigcup\{F'\langle\gamma,\alpha\rangle\}) + 1 \\ &= (F'\langle\gamma,\alpha\rangle) + 1, \end{aligned}$$

$$F'\langle \beta, \alpha\rangle = G'\langle ANT(F, \beta, \alpha, \phi(u,v)), \beta, \alpha\rangle = \bigcup\{F'\langle\gamma,\alpha\rangle \ : \ \gamma \in \beta\}$$

segundo o caso: $\beta = \mathbf{0}$, $\beta = \gamma + 1$ ou β é um ordinal limite, respectivamente. Desta maneira $F'\langle\beta,\alpha\rangle = \alpha + \beta$ é definido de acordo com 14.6; isto é, sempre podemos definir o conjunto $\alpha + \beta$. ■

Proposição 14.10 *Sejam α e β ordinais. Então $\alpha + \beta$ é um ordinal.*

Demonstração: Considere a fórmula

$$\psi(x) \equiv_{def} ord(x) \to (\forall z)(ord(z) \to ord(z + x)).$$

Provaremos por indução sobre $\phi(u,v)$ (Lema 14.7) que $\psi(x)$ vale para todo x; logo teremos que $\alpha + \beta$ é um ordinal para todo ordinal α e β. Seja y um conjunto satisfazendo

(HI) $\qquad (\forall w)(\phi(w, y) \to \psi(w)).$

Queremos provar que vale $\psi(y)$. Suponhamos então que y é um ordinal, e seja z um ordinal. Provaremos que $z + y$ é um ordinal. Temos três casos:
(a) $y = \mathbf{0}$. Logo $z + y = z$, portanto $z + y$ é um ordinal.
(b) $y = w + 1$. Logo temos que $\phi(w, y)$, portanto vale $\psi(w)$, por (HI). Como y é um ordinal e $w \in y$, então w é um ordinal, logo $ord(z) \to ord(z + w)$. Mas z é um ordinal, portanto $z + w$ é um ordinal. Daqui inferimos que $z + y = (z + w) + 1$ é um ordinal.

(c) y é um ordinal limite. Se $w \in y$ então vale $\phi(w, y)$, donde vale $\psi(w)$ por (HI). Dado que $w \in y$ implica que w é um ordinal, então, como antes, obtemos que $z + w$ é um ordinal para todo $w \in y$. Pelo Lema 14.8 deduzimos que

$$z + y = \bigcup\{z + w \ : \ w \in y\}$$

é um ordinal.
Portanto, em todos os casos possíveis temos que $z + y$ é um ordinal, provando que (HI) implica $ord(y) \to (\forall z)(ord(z) \to ord(z+y))$, isto é, $\psi(y)$. Por indução transfinita inferimos que $\psi(x)$ vale para todo x. ■

Proposição 14.11 *Sejam α, β e γ ordinais. Então $\beta < \gamma$ implica que $\alpha+\beta < \alpha + \gamma$.*

Demonstração: Considere a fórmula

$$\psi(x) \equiv_{def} ord(x) \to (\forall y)(y < x \to (\forall z)(ord(z) \to (z + y < z + x))).$$

Por indução sobre a fórmula $\phi(u, v)$ do Lema 14.7 provaremos que $\psi(x)$ vale para todo x. Suponha que temos

(HI) $\qquad (\forall w)(\phi(w, x) \to \psi(w)).$

Queremos provar $\psi(x)$. Suponha que x é um ordinal.
(1) Se $x = \mathbf{0}$ então $y < x$ é falso para todo y, portanto

$$(\forall y)(y < x \to (\forall z)(ord(z) \to (z + y < z + x)))$$

é trivialmente verdadeiro.
(2) Se $x = w + 1$, considere $y < x$ e z um ordinal.
(2.1) Se $y = w$ então $z + w < (z + w) + 1 = z + (w + 1) = z + x$.
(2.2) Se $y \in w$ então, dado que $\phi(w, x)$, obtemos $\psi(w)$ por (HI), portanto $z + y < z + w$ (pois $y < w$). Mas $z + w < z + x$ (caso 2.1), logo $z + y < z + x$.
(3) Se x é um ordinal limite, seja $y < x$ e z um ordinal. Como $(z+y) \in (z+(y+1))$ (caso 2.1) e $y+1 \in x$, pois x é limite, então $z+y \in \bigcup\{z+w \ : \ w \in x\} = z+x$. Em todos os casos temos que $(\forall y)(y < x \to (\forall z)(ord(z) \to (z + y < z + x)))$ é verdadeiro. Portanto (HI) implica $\psi(x)$ donde $\psi(x)$ vale para todo x. ■

Proposição 14.12 $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ *para todo ordinal α, β e γ.*

Demonstração: Considere a fórmula

$$\psi(z) \equiv_{def} ord(z) \to (\forall\, x, y)(ord(x) \wedge ord(y) \to ((x + y) + z = x + (y + z))).$$

Por indução na relação $\phi(u, v)$ do Lema 14.7 provaremos que $\psi(x)$ vale para todo x. Seja z tal que

(HI) $\qquad (\forall w)(\phi(w, z) \to \psi(w)).$

Suponha que z é ordinal, e sejam x, y ordinais.
(1) Se $z = \mathbf{0}$, então $(x+y)+z = x+y = x+(y+\mathbf{0}) = x+(y+z)$.
(2) Se $z = w+1$, então temos $\phi(w,z)$, donde vale $\psi(w)$ por (HI). Daqui

$$\begin{aligned}(x+y)+z &= (x+y)+(w+1) = ((x+y)+w)+1\\ &=_{HI} (x+(y+w))+1 = x+((y+w)+1)\\ &= x+(y+(w+1)) = x+(y+z).\end{aligned}$$

(3) Se z é limite, então provaremos primeiro os seguintes
Fatos: Seja γ ordinal limite.
(a) Se $x \in \alpha+\theta$ tal que $\theta \in \beta+\gamma$ então existe $\delta < \gamma$ tal que $x \in \alpha+(\beta+\delta)$.
(b) $\beta+\gamma$ é um ordinal limite.
Com efeito, seja $x \in \alpha+\theta$ tal que $\theta \in \beta+\gamma$. Logo $\theta \in \beta+\delta$ tal que $\delta \in \gamma$. De $\theta < \beta+\delta$ inferimos que $\alpha+\theta < \alpha+(\beta+\delta)$, pela Proposição 14.11. Logo $x \in \alpha+(\beta+\delta)$ para algum $\delta \in \gamma$, provando o item (a). Para provar (b), observe que $\beta+\gamma = \bigcup\{\beta+\delta \ : \ \delta \in \gamma\}$ é não vazio. Seja $u \in \beta+\gamma$, logo $u \in \beta+\delta$ para algum $\delta \in \gamma$. Daqui $u+1 \in (\beta+\delta)+1 = \beta+(\delta+1)$, onde $\delta+1 \in \gamma$. Assim $u+1 \in \beta+\gamma$, donde $\beta+\gamma$ é um ordinal limite, por [LIM]. Isto conclui a demonstração dos **Fatos**.
Por causa dos **Fatos**(b) obtemos que $y+z$ é um ordinal limite, e pelos **Fatos**(a)

$$x+(y+z) = \bigcup\{x+w \ : \ w \in y+z\} \subseteq \bigcup\{x+(y+w) \ : \ w \in z\}.$$

Além disso, se $w \in z$ então $(y+w) \in (y+z)$ pela Proposição 14.11, logo:

$u \in x+(y+w)$ para $w \in z$ implica $u \in x+w'$ com $w' \in y+z$

implica $u \in \bigcup\{x+w \ : \ w \in y+z\}$,

donde

$$\bigcup\{x+(y+w) \ : \ w \in z\} \subseteq \bigcup\{x+w \ : \ w \in y+z\}$$

e assim

$$x+(y+z) = \bigcup\{x+w \ : \ w \in y+z\} = \bigcup\{x+(y+w) \ : \ w \in z\}.$$

Mas, para todo $w \in z$ temos que $\phi(w,z)$ é satisfeita, logo vale $\psi(w)$ por (HI), donde $x+(y+w) = (x+y)+w$ para todo $w \in z$. Portanto

$$x+(y+z) = \bigcup\{x+(y+w) \ : \ w \in z\} = \bigcup\{(x+y)+w \ : \ w \in z\} = (x+y)+z.$$

Acabamos de provar que (HI) implica $\psi(z)$. Por indução transfinita obtemos que $\psi(z)$ vale para todo z. ■

Lema 14.13 *Seja α um ordinal limite. Então $\alpha = \bigcup \alpha$.*

Demonstração: Seja $x \in \alpha$; logo, $x+1 \in \alpha$. Portanto $x \in x+1$ com $x+1 \in \alpha$, donde $x \in \bigcup \alpha$. Daqui obtemos que $\alpha \subseteq \bigcup \alpha$. Reciprocamente, seja $x \in \bigcup \alpha$; logo $x \in y$ para algum $y \in \alpha$; dado que α é transitivo, então $x \in \alpha$. Portanto $\bigcup \alpha \subseteq \alpha$. Desta maneira, temos que $\alpha = \bigcup \alpha$. ■

Proposição 14.14 *Seja α um ordinal. Vale o seguinte:*
(i) $\mathbf{0}+\alpha=\alpha$.
(ii) $\alpha+\mathbf{1}=\alpha+1$.

Demonstração: (i) Por indução na relação $\phi(u,v)$ do Lema 14.7, provaremos que $(\forall x)\psi(x)$, onde

$$\psi(x) \equiv_{def} ord(x) \rightarrow (\mathbf{0}+x=x).$$

Seja x um conjunto satisfazendo

(HI) $\qquad (\forall z)(\phi(z,x) \rightarrow \psi(z)).$

Assuma que x é um ordinal. Temos três casos para analizar:
(a) $x=\mathbf{0}$. Logo $\mathbf{0}+x=\mathbf{0}+\mathbf{0}=\mathbf{0}=x$.
(b) $x=z+1$. Logo $\phi(z,x)$ e $ord(z)$, portanto $\mathbf{0}+z=z$, por (HI). Daqui

$$\mathbf{0}+x=\mathbf{0}+(z+1)=(\mathbf{0}+z)+1=z+1=x.$$

(c) x é um ordinal limite. Se $z\in x$, então $\phi(z,x)$ e $ord(z)$, portanto $\mathbf{0}+z=z$, por (HI). Daqui

$$\mathbf{0}+x=\bigcup\{\mathbf{0}+z \ : \ z\in x\}=\bigcup\{z \ : \ z\in x\}=\bigcup x=x$$

pelo Lema 14.13. Vemos que nos três casos possíveis $\mathbf{0}+x=x$. Portanto (HI) implica $\psi(x)$ donde, por indução transfinita, obtemos que $\psi(x)$ é verdadeira para todo x.
(ii) Temos que $\mathbf{1}=\mathbf{0}+1$, pela definição de $\mathbf{1}$. Logo

$$\alpha+\mathbf{1}=\alpha+(\mathbf{0}+1)=(\alpha+\mathbf{0})+1=\alpha+1.$$

■

Definiremos agora o produto de ordinais.

Definição 14.15 *Sejam α e β ordinais. Definimos o produto ordinal $\alpha\cdot\beta$ como sendo*

$\alpha\cdot\mathbf{0}=\mathbf{0}$;
$\alpha\cdot(\beta+1)=(\alpha\cdot\beta)+\alpha$;
$\alpha\cdot\beta=\bigcup_{\gamma<\beta}\alpha\cdot\gamma$ *se β é ordinal limite.*

Como foi feito com a soma ordinal, podemos provar que $\alpha\cdot\beta$ pode ser definido, e $\alpha\cdot\beta$ é um ordinal. A relação funcional $G(X,x_1,x_2,y)$ utilizada para definir $F(x_1,x_2,y)$ tal que $F'\langle\beta,\alpha\rangle=\alpha\cdot\beta$ é dada neste caso por

$$\begin{aligned} G(X,x_1,x_2,y) \equiv_{def} & [x_1=\mathbf{0}\wedge y=\mathbf{0}]\vee[(\exists z)(x_1=z+1)\wedge y=(\textstyle\bigcup im(X))+x_2] \\ & \vee\ [lim(x_1)\wedge y=\textstyle\bigcup im(X)] \end{aligned}$$

(confira os detalhes!).

Proposição 14.16 *Seja α um ordinal. Logo $\mathbf{0} \cdot \alpha = \mathbf{0}$.*

Demonstração: Por indução na relação $\phi(u, v)$ do Lema 14.7, provaremos que $(\forall x)\psi(x)$, onde

$$\psi(x) \equiv_{def} ord(x) \to (\mathbf{0} \cdot x = \mathbf{0}).$$

Seja x um conjunto satisfazendo

$$\text{(HI)} \qquad (\forall z)(\phi(z, x) \to \psi(z)).$$

Assuma que x é um ordinal. Temos três casos para analizar:
(a) $x = \mathbf{0}$. Logo $\mathbf{0} \cdot x = \mathbf{0} \cdot \mathbf{0} = \mathbf{0}$.
(b) $x = z + 1$. Logo $\phi(z, x)$ e $ord(z)$, portanto $\mathbf{0} \cdot z = \mathbf{0}$, por (HI). Daqui

$$\mathbf{0} \cdot x = \mathbf{0} \cdot (z + 1) = (\mathbf{0} \cdot z) + \mathbf{0} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

(c) x é um ordinal limite. Se $z \in x$, então $\phi(z, x)$ e $ord(z)$, portanto $\mathbf{0} \cdot z = \mathbf{0}$, por (HI). Daqui

$$\mathbf{0} \cdot x = \bigcup\{\mathbf{0} \cdot z \ : \ z \in x\} = \bigcup\{\mathbf{0} \ : \ z \in x\} = \bigcup\{\mathbf{0}\} = \mathbf{0}.$$

Vemos que nos três casos possíveis $\mathbf{0} \cdot x = \mathbf{0}$. Portanto (HI) implica $\psi(x)$ donde, por indução transfinita, obtemos que $\psi(x)$ é verdadeira para todo x. ■

Proposição 14.17 *Seja α um ordinal. Então $\alpha \cdot \mathbf{1} = \alpha = \mathbf{1} \cdot \alpha$.*

Demonstração: Por indução na relação $\phi(u, v)$ do Lema 14.7, provaremos que $(\forall x)\psi(x)$, onde

$$\psi(x) \equiv_{def} ord(x) \to (\mathbf{1} \cdot x = x).$$

Seja x um conjunto satisfazendo

$$\text{(HI)} \qquad (\forall z)(\phi(z, x) \to \psi(z)).$$

Assuma que x é um ordinal. Temos três casos para analizar:
(a) $x = \mathbf{0}$. Logo $\mathbf{1} \cdot x = \mathbf{1} \cdot \mathbf{0} = \mathbf{0} = x$.
(b) $x = z + 1$. Logo $\phi(z, x)$ e $ord(z)$, portanto $\mathbf{1} \cdot z = z$, por (HI). Daqui

$$\mathbf{1} \cdot x = \mathbf{1} \cdot (z + 1) = (\mathbf{1} \cdot z) + \mathbf{1} = z + \mathbf{1} = z + 1 = x.$$

(c) x é um ordinal limite. Se $z \in x$, então $\phi(z, x)$ e $ord(z)$, portanto $\mathbf{1} \cdot z = z$, por (HI). Daqui

$$\mathbf{1} \cdot x = \bigcup\{\mathbf{1} \cdot z \ : \ z \in x\} = \bigcup\{z \ : \ z \in x\} = \bigcup z = z$$

pelo Lema 14.13. Daqui $\mathbf{1} \cdot x = x$ em todos os casos. Assim (HI) implica $\psi(x)$ donde, por indução transfinita, inferimos que $(\forall x)\psi(x)$. A segunda parte é provada diretamente:

$$x \cdot \mathbf{1} = x \cdot (\mathbf{0} + 1) = (x \cdot \mathbf{0}) + x = \mathbf{0} + x = x$$

pelo Lema 14.14(i). ■

Proposição 14.18 *Se $\alpha > \mathbf{0}$ e β é ordinal limite, então $\alpha \cdot \beta$ é um ordinal limite.*

Demonstração: Por definição temos que

$$\alpha \cdot \beta = \bigcup \{\alpha \cdot \gamma \ : \ \gamma \in \beta\},$$

portanto $\alpha \cdot \beta \neq \mathbf{0}$. Seja $x \in \alpha \cdot \beta$; logo $x \in \alpha \cdot \gamma$ para algum $\gamma \in \beta$, donde $x + 1 \in (\alpha \cdot \gamma) + 1$. Dado que $\alpha < \mathbf{1}$ sse $\alpha = \mathbf{0}$ então, pela lei de tricotomia dos ordinais, temos dois casos para serem analizados:
(a) $\alpha = \mathbf{1}$. Logo

$$(\alpha \cdot \gamma) + 1 = (\alpha \cdot \gamma) + \mathbf{1} = (\alpha \cdot \gamma) + \alpha = \alpha \cdot (\gamma + 1).$$

Mas $\gamma + 1 \in \beta$, pois $\gamma \in \beta$ e β é ordinal limite. Daqui $x + 1 \in \alpha \cdot \beta$.
(b) $\mathbf{1} < \alpha$. Pelo Lema 14.14(ii) e a Proposição 14.11 inferimos:

$$(\alpha \cdot \gamma) + 1 = (\alpha \cdot \gamma) + \mathbf{1} < (\alpha \cdot \gamma) + \alpha = \alpha \cdot (\gamma + 1).$$

Daqui $x + 1 \in \alpha \cdot (\gamma + 1)$ onde $\gamma + 1 \in \beta$, pois $\gamma \in \beta$ e β é um ordinal limite. Portanto $x + 1 \in \alpha \cdot \beta$. Nos dois casos possíveis para α obtemos: $x \in \alpha \cdot \beta$ implica $x + 1 \in \alpha \cdot \beta$. Isto prova que $\alpha \cdot \beta$ é um ordinal limite, pela propriedade [LIM] (introduzida logo após a Definição 12.7). ■

Por indução transfinita pode ser provado o seguinte:

Proposição 14.19 *Sejam α, β e γ ordinais. Em* ZF *vale o seguinte:*
(a) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.
(b) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

Definiremos agora a exponenciação ordinal.

Definição 14.20 *Sejam α e β ordinais. A exponenciação ordinal α^β é definida da maneira seguinte:*

$\alpha^{\mathbf{0}} = \mathbf{1}$;
$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$;
$\alpha^\beta = \bigcup_{\gamma \in \beta} \alpha^\gamma$ *se β é ordinal limite e* $\mathbf{0} < \alpha$;
$\alpha^\beta = \mathbf{0}$ *se β é ordinal limite e* $\alpha = \mathbf{0}$.

Podemos provar como antes que a definição acima é legitimada em ZF por recursão transfinita em $\phi(u, v)$ (Lema 14.7) utilizando

$$\begin{aligned} G(X, x_1, x_2, y) \equiv_{def} & [x_1 = \mathbf{0} \wedge y = \mathbf{1}] \vee [(\exists z)(x_1 = z+1) \wedge y = (\textstyle\bigcup im(X)) \cdot x_2] \\ & \vee \ [lim(x_1) \wedge x_2 \neq \mathbf{0} \wedge y = \textstyle\bigcup im(X)] \\ & \vee \ [lim(x_1) \wedge x_2 = \mathbf{0} \wedge y = \mathbf{0}] \end{aligned}$$

para definir uma operação $F(x_1, x_2, y)$ tal que $F'\langle \beta, \alpha \rangle = \alpha^\beta$ (confira os detalhes!). Por indução transfinita pode ser provado o seguinte:

Proposição 14.21 *Sejam α, β e γ ordinais. Em* ZF *valem as seguintes propriedades:*
(a) α^{β} é um ordinal.
(b) $\alpha^{\mathbf{1}} = \alpha$.
(c) Se $\beta > \mathbf{0}$ então $\mathbf{0}^{\beta} = \mathbf{0}$.
(d) $\mathbf{1}^{\alpha} = \mathbf{1}$.
(e) $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.
(f) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$.

Observação 14.22 Se bem as operações de soma, produto e exponenciação ordinal possuem propriedades análogas às propriedades das mesmas operações numéricas, existem algumas diferências notórias. Certas asimetrias (não comutatividade da soma e o produto, por exemplo) aparecem por causa das próprias definições, feitas por recursão transfinita numa só das variáveis. Podemos destacar os seguintes exemplos em que as operações são "mal comportadas":

$\mathbf{1} + \omega = \omega \neq \omega + \mathbf{1}$; logo a soma ordinal não é comutativa.

$\mathbf{2} \cdot \omega = \omega \neq \omega \cdot \mathbf{2}$, logo o produto ordinal não é comutativo.

$(\mathbf{1} + \mathbf{1}) \cdot \omega = \mathbf{2} \cdot \omega = \omega \neq (\mathbf{1} \cdot \omega) + (\mathbf{1} \cdot \omega)$;

logo o produto ordinal não é distributivo à direita da soma ordinal. ■

15 Cardinais

Finalmente estudaremos a noção de número cardinal. Os cardinais foram introduzidos originalmente por Frege e Russell para indicar o "tamanho" dos conjuntos. A idéia intuitiva é que dois conjuntos a e b "têm o mesmo tamanho" (ou seja, o cardinal de a é igual ao cardinal de b) se existe uma bijeção entre eles, isto é, se são equipolentes. Portanto a definição natural de cardinal de um conjunto a, denotado por $\overline{\overline{a}}$, é a coleção de todos os conjuntos b equipolentes com a. Isto é, a partir da relação de equivalência $\approx$ (equipolência), definimos

$$\overline{\overline{a}} = \{b \ : \ a \approx b\}.$$

Portanto o cardinal de um conjunto a, na concepção de Frege e Russell, é a classe de equivalência de a na relação $\approx$. O problema que apresenta esta definição é que $\overline{\overline{a}}$ é uma classe própria, isto é, o cardinal de a não pode ser legitimado em ZF (nem em ZFC); se $\overline{\overline{a}}$ fosse legitimado, podemos provar que $\bigcup \overline{\overline{a}}$ é o conjunto de todos os conjuntos, uma contradição. A solução para este problema é definir o cardinal de um conjunto a partir da teoria de ordinais. A definição é feita de maneira a escolher um conjunto (ordinal) equipolente a x; de fato, o ordinal escolhido será o menor ordinal equipolente com x. Como já parece evidente, a teoria de cardinais faz um uso pesado do Axioma da Escolha [AE]. A partir de [AE] poderemos provar a Lei de Tricotomia que estabelece que a relação $\preceq$ é total entre conjuntos (isto é, dados x e y, então $x \preceq y$ ou $y \preceq x$), assim como demonstrar que todo conjunto é similar a um ordinal (o teorema da boa ordem: todo conjunto x admite uma boa ordem). Na primeira parte desta exposição não utilizaremos [AE], mas ele deverá ser considerado posteriormente, fato que será oportunamente informado. Começamos reformulando a noção de conjunto finito, agora utilizando a representação dos números naturais em ZF.

Definição 15.1 *$FIN(x)$ denota $(\exists n)(n \in \omega \wedge x \approx n)$*
("x é n-finito");
$INFIN(x)$ denota $\neg FIN(x)$
("x é infinito");
$ENUM(x)$ denota $x \approx \omega$
("x é enumerável").

Antes de provar as seguintes propriedades precisamos do seguinte resultado.

Lema 15.2 *Seja α um inteiro. Então $\alpha \prec \alpha + 1$.*

Demonstração: Seja α um inteiro, e $f : \alpha \longrightarrow \alpha + 1$ dada por $f(x) = x$; logo f é injetora, portanto $\alpha \preceq \alpha + 1$, pela definição de $\preceq$. Provaremos por indução matemática que $(\forall x)\psi(x)$, onde

$$\psi(x) \equiv_{def} int(x) \rightarrow (x \not\approx x + 1).$$

É imediato que $\mathbf{0} \not\approx \mathbf{1} = \mathbf{0}+1$, portanto vale $\psi(\mathbf{0})$. Suponha que vale $\psi(y)$; para provar $\psi(y+1)$, suponha que $y+1$ é um inteiro, logo y é um inteiro, pois $y \in y+1$, portanto $y \not\approx y+1$. Suponhamos que existe uma bijeção $f : y+1 \longrightarrow (y+1)+1$; daqui inferimos que $f|y$ é uma bijeção entre y e $((y+1)+1) - \{f(y)\}$.
Fato: Seja z um conjunto, e $v \in z+1$. Portanto $(z+1) - \{v\} \approx z$.
Com efeito, se $v = z$ então $(z+1) - \{v\} = z$, e a equipolência é imediata. Por outro lado, se $v \in z$ então definimos $g : ((z+1) - \{v\}) \longrightarrow z$ como $g(u) = u$ se $u \neq z$, e $g(z) = v$. É claro que g é uma bijeção; isto conclui a prova do **Fato**.
Vemos então que, por um lado, $f|y$ é uma bijeção estabelecendo que $y \approx ((y+1)+1) - \{f(y)\}$ enquanto que, por outro lado, $((y+1)+1) - \{f(y)\} \approx y+1$, em virtude do **Fato**; portanto $y \approx y+1$, uma contradição. Daqui obtemos que $y+1 \not\approx (y+1)+1$. Desta maneira $\psi(y)$ implica $int(y+1) \rightarrow y+1 \not\approx ((y+1)+1)$, isto é, provamos que $\psi(y) \rightarrow \psi(y+1)$. Por indução matemática obtemos que $(\forall x)(int(x) \rightarrow \psi(x))$ ou, equivalentemente, $(\forall x)\psi(x)$, isto é, $\alpha \not\approx \alpha + 1$ para todo inteiro α. Como $\alpha \preceq \alpha + 1$, então deduzimos que $\alpha \prec \alpha + 1$ para todo inteiro α. ∎

Proposição 15.3 *(i) Em* S *vale o seguinte: se x e y são inteiros, então $x \preceq y$ sse $x \leq y$.*
(ii) Em Z *vale o seguinte: ω é infinito.*

Demonstração: (i) Provaremos por indução matemática que para todo x vale $\psi(x)$, onde

$$\psi(x) \equiv_{def} int(x) \rightarrow (\forall y)(int(y) \rightarrow (x \preceq y \rightarrow x \leq y)).$$

É imediato que $\psi(\mathbf{0})$ é verdadeira (confira!). Seja x tal que $\psi(x)$ é verdadeira. Para provar $\psi(x+1)$, assuma que $x+1$ é um inteiro; logo x é um inteiro, donde

$$(*) \qquad (\forall y)(int(y) \to (x \preceq y \to x \leq y))$$

pois vale $\psi(x)$. Suponha que y é um inteiro tal que $x+1 \preceq y$. Como $x \prec x+1$ (pelo Lema 15.2), então $x \prec y$; por $(*)$ inferimos que $x < y$ (não poderiamos ter $x = y$, senão $x \approx y$, o que contradiz $x \prec y$), portanto $x+1 \leq y$. Logo $\psi(x)$ implica $\psi(x+1)$. Por indução matemática obtemos que $\psi(x)$ vale para todo x, provando assim a primeira metade de (i). A outra implicação é imediata: $x \leq y$ implica $x \preceq y$ para todo ordinal x e y.
(ii) Suponhamos que ω é n-finito, isto é, existe um inteiro $\mathbf{n}$ tal que $\omega \approx \mathbf{n}$. Daqui inferimos que $\omega \approx \mathbf{n}$ e $\mathbf{n} \prec \mathbf{n}+1$, pelo Lema 15.2, logo $\omega \prec \mathbf{n}+1$. Mas $\mathbf{n}+1 = \mathbf{n}+\mathbf{1}$, logo $\mathbf{n}+1 \preceq \omega$ (pois $\mathbf{n}+\mathbf{1} \subseteq \omega$). Portanto $\mathbf{n}+1 \preceq \omega$, $\omega \prec \mathbf{n}+1$ implica $\mathbf{n}+1 \prec \mathbf{n}+1$, uma contradição. Daqui obtemos que ω é infinito. ■

Definição 15.4 *$inic(\alpha)$ denota $ord(\alpha) \wedge (\forall\beta)(\beta < \alpha \to (\alpha \not\approx \beta))$ ("α é um ordinal inicial").*

Pela Proposição 15.3(i) vemos que todo ordinal n-finito $\mathbf{n}$ é um ordinal inicial: se $\beta \approx \mathbf{n}$ então $\beta \preceq \mathbf{n}$ e $\mathbf{n} \preceq \beta$, donde $\beta \leq \mathbf{n}$ e $\mathbf{n} \leq \beta$. Pela tricotomia dos ordinais inferimos que $\beta = \mathbf{n}$, e então $\beta \not< \mathbf{n}$. Por 15.3(ii) e pela definição de ω é imediato que ω é também um ordinal inicial. Por outro lado, é simples provar que

$$\omega \approx \omega+1 \approx \omega+2 \approx \cdots \approx \omega+\omega = \omega\cdot\mathbf{2} \approx \omega\cdot\mathbf{3} \approx \cdots$$

junto com

$$\omega \approx \omega^2 \approx \omega^3 \approx \cdots \approx \omega^\omega \approx \omega^{\omega^\omega} \approx \cdots \text{ etc.}$$

(confira!). Pode ser provado que nenhuma das operações sobre ordinais consegue produzir um ordinal inicial superior a partir de ω. Para superar esta barreira devemos considerar o conjunto das partes $\mathcal{P}(x)$; uma maneira possível é através da função *aleph* de Hartogs:

Definição 15.5 *$\aleph(x)$ denota $\{\alpha \ : \ \alpha \preceq x\}$ ("o aleph de x").*

Proposição 15.6 *Em* ZF *provamos que $\aleph(x)$ é legitimado, e $\aleph(x)$ é um ordinal inicial para todo conjunto x.*

Demonstração: Dado um conjunto x, considere o seguinte conjunto:

$$z = \{r \ : \ (\exists y)(y \subseteq x \wedge r \subseteq y \times y \wedge bo(r,y))\}.$$

Dado que $z \subseteq \mathcal{P}(x \times x)$, então z é legitimado por [A2]. Por outro lado, lembrando que $F(r)$ denota o conjunto $dom(r) \cup im(r)$, considere a seguinte fórmula:

$$isom(r, \alpha) \equiv_{def} (\exists h)(bij(h, F(r), \alpha) \wedge (\forall x)(\forall y)(x, y \in F(r) \rightarrow (((x\ r\ y) \leftrightarrow h(x) < h(y)))).$$

O teorema de caracterização dos ordinais prova que se r é uma boa ordem sobre $a = F(r)$, então $(\exists! \alpha) isom(r, \alpha)$ (onde $(\exists!)$ indica existência e unicidade). Logo, a fórmula

$$\psi(r, \alpha) \equiv_{def} bo(r, F(r)) \wedge isom(r, \alpha)$$

satisfaz a condição FUN_ψ do axioma de substituição [A7], portanto existe o conjunto

$$b = \{\alpha\ :\ (\exists r)(r \in z \wedge \psi(r, \alpha))\} = \{\alpha\ :\ (\exists r)(r \in z \wedge isom(F(r), \alpha)\}.$$

Pela definição de z e dado que $(\exists! \alpha) isom(F(r), \alpha)$ para todo $r \in z$, sendo que $F(r) \subseteq x$, vemos que $b = \aleph(x)$, portanto o conjunto $\aleph(x)$ é legitimado para todo conjunto x. Para provar que $\aleph(x)$ é um ordinal basta provar que é transitivo, pois $\aleph(x)$ é um conjunto de ordinais. Considere então $\alpha \in \aleph(x)$ e $\beta < \alpha$. Logo: $\beta \subseteq \alpha$ e $\alpha \preceq x$, donde $\beta \preceq x$. Daqui $\beta \in \aleph(x)$ e $\aleph(x)$ é transitivo, sendo portanto um ordinal. Suponha que existe $\beta < \aleph(x)$ tal que $\aleph(x) \approx \beta$. Dado que $\beta \in \aleph(x)$, então obtemos que $\beta \preceq x$, donde $\aleph(x) \preceq x$. Daqui $\aleph(x) \in \aleph(x)$, uma contradição. Logo $\aleph(x)$ é um ordinal inicial. ■

Observe que, se α é um ordinal, então $\alpha \in \aleph(\alpha)$, pois $\alpha \preceq \alpha$. Portanto $\alpha < \aleph(\alpha)$. Isto significa que, para cada ordinal α, existe um ordinal inicial $\aleph(\alpha)$ maior do que α. Pelo Teorema de Cantor-Schröder-Bernstein $\aleph(\alpha)$ deve ser o *seguinte* ordinal inicial. Com efeito, suponha que β é um ordinal inicial diferente de $\aleph(\alpha)$ tal que $\alpha < \beta$. Pela lei de tricotomia para ordinais temos que $\beta < \aleph(\alpha)$ ou $\aleph(\alpha) < \beta$. Suponhamos que $\beta < \aleph(\alpha)$, logo $\beta \in \aleph(\alpha)$ e então $\beta \preceq \alpha$. Por outro lado, $\alpha < \beta$ implica $\alpha \subseteq \beta$ donde $\alpha \preceq \beta$. Pelo Teorema de Cantor-Schröder-Bernstein inferimos que $\beta \approx \alpha$, sendo que $\alpha < \beta$ e β é um ordinal inicial, contradição. Portanto $\aleph(\alpha) < \beta$, isto é: $\aleph(\alpha)$ é o mínimo ordinal inicial maior que α.

Definição 15.7 *Por recursão transfinita definimos a seguinte seqüência de ordinais iniciais infinitos:*

$\aleph_{\mathbf{0}} = \omega$*;*
$\aleph_{\alpha+1} = \aleph(\aleph_\alpha)$*;*
$\aleph_\lambda = \bigcup_{\beta<\lambda} \aleph_\beta$ *se* λ *é um ordinal limite.*

Como foi feito anteriormente, podemos provar que a definição por recursão transfinita 15.7 é legitimada em ZF, e que $\aleph_\alpha$ é um ordinal inicial infinito para todo ordinal α (conferir!). Reciprocamente, por indução transfinita podemos provar que se α é ordinal inicial infinito, então existe um ordinal β tal que $\alpha = \aleph_\beta$. Logo: $inic(\alpha) \wedge INFIN(\alpha) \leftrightarrow (\exists \beta)(\alpha = \aleph_\beta)$ é um teorema em ZF.

Definição 15.8 *Um cardinal é um ordinal inicial.*

Portanto, todo cardinal infinito é da forma $\aleph_\alpha$ para algum ordinal α. Uma notação alternativa para $\aleph_\alpha$ é ω_α. Por indução transfinita podemos provar o seguinte resultado, que utilizaremos para definir as operações aritméticas entre cardinais:

Proposição 15.9 *Em* ZF *vale o seguinte: Se α é um cardinal e $\omega \leq \alpha$, então $\alpha \approx (\alpha \times \alpha)$.*

Se α é um ordinal, então para todo ordinal β: $\beta \approx \alpha$ implica que $\beta \preceq \alpha$, portanto $\beta \in \aleph(\alpha)$. Desta maneira existe por [A2] o conjunto

$$a_\alpha = \{\beta \ : \ \beta \in \aleph(\alpha) \wedge \beta \approx \alpha\} = \{\beta \ : \ \beta \approx \alpha\}.$$

Temos que $\alpha \approx \alpha$, portanto $a_\alpha \neq \emptyset$. Daqui inferimos que existe o conjunto

$$\overline{\overline{\alpha}} = \bigcap a_\alpha = \bigcap \{\beta \ : \ \beta \approx \alpha\}.$$

O conjunto $\overline{\overline{\alpha}}$ é dito *o cardinal de* α. Pode ser provado que $\overline{\overline{\alpha}}$ é um cardinal, e que $\alpha = \overline{\overline{\alpha}}$ se α é um cardinal. Se x é um conjunto e $x \approx \alpha$ para algum ordinal α então $\beta \approx x$ sse $\beta \approx \alpha$ para todo ordinal β, portanto existe

$$\overline{\overline{x}} \equiv_{def} \bigcap \{\beta \ : \ \beta \approx x\} = \overline{\overline{\alpha}}.$$

Definição 15.10 *Seja x um conjunto. O cardinal de x é definido como*

$$\overline{\overline{x}} = \begin{cases} \bigcap \{\beta \ : \ \beta \approx x\} & \textit{se } x \approx \alpha \textit{ para algum ordinal } \alpha \\ \\ \emptyset & \textit{em caso contrário} \end{cases}.$$

Teorema 15.11 *(Princípio da Boa Ordem) Em* ZFC *(isto é, em* ZF *mais o axioma da escolha) provamos o seguinte: todo conjunto x admite uma boa ordem r em x.*

Daqui temos que para todo conjunto x existe $\overline{\overline{x}} = \bigcap \{\beta \ : \ \beta \approx x\}$. Com efeito, se x é um conjunto, então existe uma boa ordem r em x; pelo teorema de caracterização dos ordinais existe um único ordinal α isomorfo a $\langle x, r\rangle$; em particular $x \approx \alpha$. Pela Definição 15.10 obtemos que $\overline{\overline{x}} = \bigcap \{\beta \ : \ \beta \approx x\}$. Devemos observar que, de fato, o axioma da escolha é equivalente ao princípio da boa ordem. Por outro lado, o cardinal de um conjunto é determinado pelas diferentes possibilidades que existem para definir uma boa ordem r em x; cada r determina um ordinal α isomorfo a $\langle x, r\rangle$, portanto o mínimo desses ordinais corresponde à única boa ordem sobre x que o faz um cardinal.

Proposição 15.12 *Seja b um conjunto e β um ordinal tal que $b \preceq \beta$. Considere a seguinte relação em b: $x \ r \ y$ sse $f(x) < f(y)$ onde f é uma função injetora de b em β. Logo r é uma boa ordem em b tal que, se α é o tipo ordinal de $\langle b, r\rangle$, então $\alpha \leq \beta$.*

Demonstração: É imediato que r é uma boa ordem em b, pois r é computada a partir da cópia $f``b$ de b em β na relação de boa ordem $\in$. Seja $h : b \longrightarrow \alpha$ o isomorfismo entre b e o tipo ordinal α de b dado por

$$h(x) = \{h(y) \ : \ y \ r \ x\} = \{h(y) \ : \ f(y) < f(x)\}.$$

Logo, $h(x) < h(y)$ sse $x \ r \ y$ sse $f(x) < f(y)$. Definimos uma função $g : \alpha \longrightarrow \beta$ dada por $g(\gamma) = f(x)$ onde x é o único elemento de b tal que $\gamma = h(x)$. Logo g é uma função satisfazendo

$$\gamma = h(x) < h(y) = \delta \ \text{ sse } \ g(\gamma) = f(x) < f(y) = g(\delta)$$

portanto g é um isomorfismo entre α e $g``\alpha$. Logo $g(\gamma) = \gamma$ para todo $\gamma \in \alpha$ (pelo **Fato 2** na demonstração do Teorema 14.4) e então $\alpha \leq \beta$. ■

Corolário 15.13 *Sejam b e c conjuntos. Em* ZFC *vale o seguinte: se $b \subseteq c$ então $\overline{\overline{b}} \leq \overline{\overline{c}}$.*

Demonstração: Seja $x \in \overline{\overline{b}} = \bigcap\{\beta \ : \ \beta \approx b\}$. Queremos provar que $x \in \overline{\overline{c}} = \bigcap\{\beta \ : \ \beta \approx c\}$. Seja então β um ordinal equipolente com c, e considere $f : c \longrightarrow \beta$ uma bijeção. Logo $f|b$ é uma bijeção entre b e $f``b \subseteq \beta$, donde $b \preceq \beta$. Considere o ordinal $\alpha \leq \beta$ da Proposição 15.12. Logo $\alpha \approx b$ donde $x \in \alpha$, pois $x \in \overline{\overline{b}}$. Mas $\alpha \subseteq \beta$, portanto $x \in \beta$. Provamos assim que $x \in \overline{\overline{c}}$, e então $\overline{\overline{b}} \subseteq \overline{\overline{c}}$, donde $\overline{\overline{b}} \leq \overline{\overline{c}}$. ■

Definição 15.14 *Uma família de conjuntos indexada por um conjunto I é um conjunto*

$$(x_i)_{i \in I} = \{\langle i, x_i \rangle \ : \ i \in I\}$$

onde x_i é um conjunto para cada $i \in I$. Mais formalmente, uma família $(x_i)_{i\in I}$ é uma função $x : I \longrightarrow a$ tal que I e a são conjuntos, com $I \neq \emptyset$. Se $i \in I$ então $x(i)$ é denotado por x_i. Por outro lado, $\bigcup_{i\in I} x_i$ denota o conjunto

$$\{z \in \bigcup a \ : \ (\exists i)(i \in I \wedge z \in x_i)\}.$$

Isto é, $\bigcup_{i \in I} x_i = \bigcup im(x)$. O produto cartesiano de $(x_i)_{i\in I}$ é dado por

$$\prod_{i \in I} x_i = \{f \ : \ fun(I, \bigcup_{i \in I} x_i) \wedge (\forall i)(i \in I \rightarrow f(i) \in x_i)\}.$$

Definição 15.15 *Seja $(\kappa_i)_{i\in I}$ uma família indexada de cardinais.*
(i) A soma cardinal $\bigoplus_{i\in I} \kappa_i$ é o cardinal κ construído da maneira seguinte: se $(a_i)_{i\in I}$ é uma família de conjuntos dois a dois disjuntos (isto é, $a_i \cap a_j = \emptyset$ se $i \neq j$) tal que $\overline{\overline{a}}_i = \kappa_i$ para todo $i \in I$ então κ é o cardinal do conjunto $\bigcup_{i\in I} a_i$. Se $I = \{\mathbf{0}, \mathbf{1}\}$ escreveremos $\kappa_{\mathbf{0}} \oplus \kappa_{\mathbf{1}}$.
(ii) O produto cardinal $\bigodot_{i\in I} \kappa_i$ é o cardinal κ construído da maneira seguinte: se $(a_i)_{i\in I}$ é uma família de conjuntos tal que $\overline{\overline{a}}_i = \kappa_i$ para todo $i \in I$ então κ é o cardinal do conjunto $\prod_{i\in I} a_i$. Se $I = \{\mathbf{0}, \mathbf{1}\}$ escreveremos $\kappa_{\mathbf{0}} \odot \kappa_{\mathbf{1}}$.
(iii) Se κ, θ são cardinais, definimos a exponenciação cardinal κ^θ como sendo o cardinal μ dado pelo cardinal do conjunto x^y, onde $\overline{\overline{x}} = \kappa$ e $\overline{\overline{y}} = \theta$.

Vemos que sem o axioma da escolha não podemos assegurar que existem estas operações para I infinito, pois nada garante a existência dos conjuntos a_i tais que $\overline{\overline{a_i}} = \kappa_i$ para todo $i \in I$ nem a existência da soma e o produto cardinal. O axioma da escolha nos assegura que estas operações existem e são bem definidas, isto é, independem dos conjuntos escolhidos para a sua realização. Observemos que κ^θ é um caso particular de produto cardinal, em que $I = \theta$ e $\kappa_i = \kappa$ para todo $i \in \theta$. Algumas propriedades das operações entre cardinais são as seguintes (no caso em que a propriedade requer do axioma da escolha, isto é indicado acrescentando "([AE])" no início do enunciado).

Proposição 15.16 *As operações entre cardinais satisfazem as propriedades seguintes:*
(i) $\kappa \oplus \lambda = \lambda \oplus \kappa$, $\kappa \odot \lambda = \lambda \odot \kappa$.
(ii) $\kappa \oplus (\lambda \oplus \theta) = (\kappa \oplus \lambda) \oplus \theta$, $\kappa \odot (\lambda \odot \theta) = (\kappa \odot \lambda) \odot \theta$.
(iii) Se $\kappa \leq \lambda$ *então* $\kappa \oplus \theta \leq \lambda \oplus \theta$ *e* $\kappa \odot \theta \leq \lambda \odot \theta$.
(iv) $\kappa \odot (\lambda \oplus \theta) = (\kappa \odot \lambda) \oplus (\kappa \odot \theta)$.
(v) ([AE]) $\kappa \odot (\bigoplus_{i \in I} \lambda_i) = \bigoplus_{i \in I} (\kappa \odot \lambda_i)$.
(vi) ([AE]) *Se* $\kappa_i = \kappa$ *para todo* $i \in I$, *então* $\bigoplus_{i \in I} \kappa_i = \overline{\overline{I}} \odot \kappa$.
(vii) $\kappa \oplus \lambda$ *é o cardinal do ordinal* $\kappa + \lambda$, *e* $\kappa \odot \lambda$ *é o cardinal do ordinal* $\kappa \cdot \lambda$.

Suponha que β é um cardinal. Estamos interessados em encontrar o mínimo cardinal α tal que existe uma partição de β em α pedaços de cardinalidade estritamente menor do que β. Esse cardinal mínimo α é a *cofinalidade* de β, e será denotado $cf(\beta)$. No caso em que β é um cardinal tal que $cf(\beta) = \beta$ dizemos que β é *regular*. Por exemplo, ω não pode ser particionado numa quantidade finita de subconjuntos finitos; para cobrir todo ω por uma partição de subconjuntos finitos precissamos de ω subconjuntos; portanto ω é um cardinal regular.

Definição 15.17 *Sejam* α *e* β *ordinais.*
$\alpha\ cf\ \beta$ *denota* $\alpha \leq \beta \wedge (\exists f)(fun(f, \alpha, \beta) \wedge \beta = \bigcup im(f))$
("α é cofinal em β").
$cf(\beta)$ *denota* $\bigcap\{\alpha \ : \ \alpha\ cf\ \beta\}$
("a cofinalidade de β").

Dado que $\alpha\ cf\ \beta$ implica que $\alpha \leq \beta$ (donde $\alpha \in \beta + 1$) então $C_\beta = \{\alpha \ : \ \alpha\ cf\ \beta\} \subseteq \beta + 1$, portanto C_β é legitimado por [A2]. Por outro lado $\beta\ cf\ \beta$, portanto $C_\beta \neq \emptyset$ e então existe $cf(\beta)$ para todo ordinal β. Se $\alpha\ cf\ \beta$ e $f : \alpha \longrightarrow \beta$ tal que $\bigcup im(f) = \beta$ então, para cada $\gamma \in \beta$ existe $\delta \in \alpha$ tal que $\gamma \in f(\delta)$, pela definição de $\bigcup$. Ou seja, para cada $\gamma \in \beta$ existe $\delta \in \alpha$ tal que $\gamma < f(\delta)$. Em outras palavras, a imagem de f não é limitada em β, portanto f é uma seqüência em β (indexada por α) convergendo a β (a convergência é dada pela união $\bigcup$). Observe que se $\beta = \alpha + 1$ então $cf(\beta) = \mathbf{1}$. Com efeito, $\mathbf{1}\ cf\ (\alpha + 1)$ via $f(\mathbf{0}) = \alpha$.

Proposição 15.18 *Sejam* α *e* β *ordinais limites. Em* ZF *vale o seguinte:*
(i) $\alpha\ cf\ \beta$ *é uma relação transitiva.*
(ii) $cf(\beta)$ *é um cardinal.*

Definição 15.19 *Seja κ um cardinal. Dizemos que κ é regular se $cf(\kappa) = \kappa$. Em caso contrário, isto é, se $cf(\kappa) < \kappa$, então κ é dito singular.*

Proposição 15.20 *Em* ZFC *vale o seguinte:*
(i) ω é regular.
(ii) $\aleph_{\alpha+1}$ é regular para todo α.
(iii) Se λ é um ordinal limite então $cf(\aleph_\lambda) = cf(\lambda)$.

Observe que, pela proposição anterior, $cf(\aleph_\omega) = cf(\omega) = \omega$. Por exemplo, $\aleph_\omega$ pode ser atingido pela seqüência

$$\aleph_{\mathbf{0}} < \aleph_{\mathbf{1}} < \aleph_{\mathbf{2}} < \cdots \longrightarrow \aleph_\omega$$

provando que $\aleph_\omega$ é singular. Também temos que $cf(\aleph_{\aleph_\omega}) = \omega$, considerando, por exemplo, a seqüência

$$\aleph_{\aleph_{\mathbf{0}}} < \aleph_{\aleph_{\mathbf{1}}} < \aleph_{\aleph_{\mathbf{2}}} < \cdots \longrightarrow \aleph_{\aleph_\omega}.$$

Finalmente, discutiremos brevemente a *Hipótese do Contínuo* (HC). Temos duas maneiras para passar de um cardinal a outro superior: considerar $\aleph(\kappa) > \kappa$ ou, pelo teorema de Cantor, considerar $\mathbf{2}^\kappa > \kappa$. A Hipótese do Contínuo afirma o seguinte:

(HC) $\qquad \mathbf{2}^{\aleph_{\mathbf{0}}} = \aleph_{\mathbf{1}}.$

Dado que $\mathbb{R} \approx \mathbf{2}^{\aleph_{\mathbf{0}}}$ então (HC) afirma que todo subconjunto de $\mathbb{R}$ não enumerável é equipolente com $\mathbb{R}$, isto é, não existem subconjuntos de $\mathbb{R}$ de cardinalidade intermediária entre $\aleph_{\mathbf{0}}$ e a cardinalidade de $\mathbb{R}$. Portanto (HC) afirma que $\mathbf{2}^\kappa$ e $\aleph(\kappa)$ coincidem no primeiro valor $\aleph_{\mathbf{0}}$. A *Hipótese Generalizada do Contínuo* (HGC) afirma que estas funções coincidem em todo cardinal κ. Em outras palavras, para cada cardinal infinito κ não existe um cardinal estritamente entre κ e $\mathbf{2}^\kappa$. Em termos da função $\aleph$ temos que (HGC) afirma que

(HGC) $\qquad \mathbf{2}^{\aleph_\alpha} = \aleph_{\alpha+1}$

para todo ordinal α. Com a ajuda de (HGC) resolvemos todas as questões acerca das potências cardinais:

Teorema 15.21 *Assumamos* (HGC). *Em* ZFC *temos que $\aleph_\alpha^{\aleph_\beta}$ é determinado, sendo que*
(i) $\aleph_\alpha^{\aleph_\beta} = \aleph_{\beta+1}$ se $\alpha \leq \beta$;
(ii) $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$ se $\aleph_\beta < cf(\aleph_\alpha)$;
(iii) $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}$ se $cf(\aleph_\alpha) \leq \aleph_\beta \leq \aleph_\alpha$.

Em 1936 Kurt Gödel demonstrou que, se a teoria ZF é consistente, então ZFC com o acréscimo de (HC) é consistente. Por outro lado, Cohen demonstrou em 1964 (mediante a técnica de *forcing*) que, se a teoria ZF é consistente, então ZFC com o acréscimo da negação de (HC) também é consistente, portanto a

Hipótese do Contínuo é indecidível na teoria ZFC. Também foi provado por Cohen que, se a teoria ZF é consistente, então ZF com o acréscimo da negação de [AE] também é consistente. Vemos assim que, em particular, tanto ZF com o acréscimo de [AE] quanto ZF com o acréscimo da negação de [AE] são consistentes, desde que ZF seja consistente. Assim, ambas teorias de conjuntos são válidas, e a inclusão do Axioma da Escolha ou da sua negação acaba sendo uma questão de escolha.

Devemos observar, finalmente, que os famosos teoremas de incompletude de Gödel se aplicam a ZF, portanto existem sentenças de ZF que são indecidíveis em ZF. Em particular, se ZF é consistente, então ZF não pode provar a sua própria consistência.

References

[1] C.A. di Prisco, **Una Introducción a la Teoría de Conjuntos**, Coleção CLE, vol. 20, (UNICAMP), 1997.

[2] F.R. Drake, **Set Theory: an Introduction to Large Cardinals**, North Holland, 1974.

[3] H.B. Enderton, **Elements of Set Theory**, Academic Press, 1977.

[4] T. Jech, **Set Theory**, Springer Verlag (segunda edição), 2002.

[5] P. Suppes, **Axiomatic Set Theory**, Dover, 1972.