Parte I

Set Theory

Capítulo 1

A Concepção Iterativa

1.1 Extensionalidade

O primeiro ponto a notar é que os conjuntos são individuados pelos seus membros. Mais precisamente: sth:story:extensionality:sec

Extensionalidade (Extensionalidade). Se os conjuntos A e B têm os mesmos membros, então A e B são o mesmo conjunto.

$$\forall A \forall B \left(\forall x \left(x \in A \leftrightarrow x \in B\right) \rightarrow A = B\right)$$

Assumimos isto ao longo de **??**. Mas vale a pena repetir. O axioma de extensionalidade exprime a ideia fundamental de que um conjunto é determinado pelos seus membros. (Assim, os conjuntos podem contrastar-se com os *conceitos*, nos quais precisamente os mesmos objetos podem cair sob muitos conceitos diferentes.)

Por que aceitar este princípio? Ora, é plausível dizer que qualquer recusa da extensionalidade é uma decisão de abandonar tudo o que possa ser chamado *teoria dos conjuntos*. A teoria dos conjuntos não é mais nem menos do que a teoria de coleções extensionais.

O verdadeiro desafio na Parte I, contudo, é estabelecer princípios que nos digam *que conjuntos existem*. E acaba por se verificar que a única resposta verdadeiramente "óbvia" a esta questão é provadamente errada.

1.2 Paradoxo de Russell (de novo)

Na **??**, trabalhamos com uma teoria ingênua dos conjuntos. Mas, segundo uma concepção *muito* ingênua, os conjuntos são apenas as extensões dos predicados. Este pensamento ingênuo imporia o seguinte princípio: sth:story:rus:sec

> *Compreensão ingênua.* $\{x : \varphi(x)\}$ existe para qualquer fórmula φ.

Por tentador que seja este princípio, é provadamente inconsistente. Vimo-lo na **??**, mas o resultado é tão importante, e tão direto, que vale a pena repetir. Ipsis verbis.

Teorema 1.1 (Paradoxo de Russell). *Não existe conjunto* $R = \{x : x \notin x\}$

Prova. Se $R = \{x : x \notin x\}$ existisse, então $R \in R$ sse $R \notin R$, o que é uma contradição. □

Russell descobriu este resultado em junho de 1901. (Não colocou, porém, o paradoxo exatamente na forma em que o acabamos de apresentar, pois estava a considerar a teoria dos conjuntos de Frege, tal como delineada em *Grundgesetze*. Voltaremos a isto na Seção 1.6.) Russell escreveu a Frege a 16 de junho de 1902, explicando a inconsistência no sistema de Frege. Para a correspondência, e um pouco de contexto, ver Heijenoort (1967, pp. 124–8).

Vale a pena enfatizar que esta prova de duas linhas é um resultado de *lógica pura*. De fato, usamos implicitamente um axioma (não lógico?) de extensionalidade na nossa notação $\{x : x \notin x\}$; pois $\{x : \varphi(x)\}$ deve ser *o único* (pela extensionalidade) conjunto dos φs, se algum existir. Mas podemos evitar até o vestígio da extensionalidade, bastando enunciar o resultado assim: *não existe conjunto cujos membros sejam exatamente os conjuntos que não são membros de si próprios*. E isto pouco tem a ver com conjuntos. Como o próprio Russell observou, raciocínio rigorosamente análogo leva-nos a concluir: *nenhum homem barbeia exatamente os homens que não se barbeiam a si próprios*. Ou: *nenhum pug cheira exatamente os pugs que não se cheiram a si próprios*. E assim por diante. Esquematicamente, a forma do resultado é apenas:

$$\neg\exists x\forall z(Rzx \leftrightarrow \neg Rzz).$$

E isto não passa de um teorema (esquema) da lógica de primeira ordem. Consequentemente, não podemos evitar o paradoxo de Russell apenas mexendo na nossa teoria dos conjuntos; ele surge antes sequer de *chegarmos* à teoria dos conjuntos. Se formos usar lógica (clássica) de primeira ordem, temos simplesmente de *aceitar* que não existe conjunto $R = \{x : x \notin x\}$.

A consequência é esta. Se quisermos aceitar a compreensão ingênua enquanto *evitamos* a inconsistência, não basta mexer na *teoria dos conjuntos*. Teríamos, em vez disso, de reformular a nossa *lógica*.

É claro que já foram apresentadas teorias dos conjuntos com lógicas não clássicas. Mas são—no mínimo—não standard. A abordagem usual ao paradoxo de Russell é tratá-lo como uma prova direta de não existência e depois tentar aprender a viver com ela. É essa a abordagem que seguiremos.

1.3 Predicativo e Impredicativo

sth:story:predicative:sec

O conjunto de Russell, R, foi definido via $\{x : x \notin x\}$. Dito com mais detalhe, R seria o conjunto que contém todos e apenas aqueles conjuntos que não são

membros de si próprios. Assim, ao definir R, quantificamos sobre o domínio que conteria R (se este existisse).

Isto é uma definição *impredicativa*. Mais em geral, podemos dizer que uma definição é impredicativa sse quantifica sobre um domínio que contém o objeto que está a ser definido.

Na sequência dos paradoxos, Whitehead, Russell, Poincaré e Weyl rejeitaram tais definições impredicativas como "viciosamente circulares":

> Uma análise dos paradoxos a evitar mostra que todos eles resultam de uma espécie de círculo vicioso. Os círculos viciosos em questão surgem ao supor que uma coleção de objetos pode conter membros que só podem ser definidos por meio da coleção como um todo[. . . . ¶]
>
> O princípio que nos permite evitar totalidades ilegítimas pode enunciar-se do seguinte modo: "Tudo o que envolve *todos* os membros de uma coleção não pode ser um dos membros da coleção"; ou, inversamente: "Se, supondo que uma certa coleção tivesse um todo, ela teria membros só definíveis em termos desse todo, então a dita coleção não tem todo." Chamaremos a isto o "princípio do círculo vicioso", porque nos permite evitar os círculos viciosos envolvidos na suposição de totalidades ilegítimas. (Whitehead and Russell, 1910, p. 37)

Se os acompanharmos na rejeição das definições impredicativas motivada pelo *princípio do círculo vicioso*, então podemos tentar substituir o desastroso esquema de compreensão ingênua (de Seção 1.2) por algo deste gênero:

> *Compreensão predicativa.* Para toda a fórmula φ que quantifica apenas sobre conjuntos: existe o conjunto′ $\{x : \varphi(x)\}$.

Enquanto os conjuntos′ não forem conjuntos, não se seguirá contradição.

Infelizmente, a compreensão predicativa não é muito *abrangente*. Afinal, introduz-nos novas entidades, conjuntos′. Logo teremos de considerar fórmulas que quantificam sobre conjuntos′. Se estas derem sempre um conjunto′, então o paradoxo de Russell surgirá de novo, bastando considerar o conjunto′ de todos os conjuntos′ que não são membros de si próprios. Assim, a seguir o mesmo fio de ideias, temos de dizer que uma fórmula que quantifica sobre conjuntos′ produz um conjunto″ correspondente. E então precisaremos de conjuntos‴, conjuntos⁗, etc. Para evitar uma enxurrada de primos, será mais fácil pensar nestes como conjuntos$_0$, conjuntos$_1$, conjuntos$_2$, conjuntos$_3$, conjuntos$_4$,. . . . E isto dar-nos-ia entrada na teoria (simples) dos tipos.

Há algumas objeções óbvias a tal teoria (embora não seja óbvio que sejam objeções *esmagadoras*). Em resumo: a teoria resultante é pouco manejável; é prolixa ao postular diferentes tipos de objetos; e não está claro, no fim, que as definições impredicativas sejam sequer *assim tão más*.

Para ilustrar o último ponto, consideremos esta observação de Ramsey:

> podemos referir-nos a um homem como o mais alto de um grupo, identificando-o por meio de uma totalidade da qual ele próprio é membro sem que haja círculo vicioso. (Ramsey, 1925)

O ponto de Ramsey é que "o homem mais alto do grupo" *é* uma definição impredicativa; mas é obviamente perfeitamente legítima.

Alguém poderá responder que, neste caso, poderíamos identificar a pessoa mais alta por meios *predicativos*. Por exemplo, talvez pudéssemos simplesmente apontar para o homem em questão. A objeção às definições impredicativas, então, teria claramente de se limitar a entidades que *só* possam ser identificadas impredicativamente. Mas mesmo assim, seria preciso ouvir mais, sobre por que tal "impredicatividade essencial" seria tão grave.[1]

Admitidamente, as definições impredicativas são péssimas notícias, se quisermos que as definições nos forneçam algo como uma receita para *criar* um objeto. Pois, dada uma definição impredicativa, estar-se-ia genuinamente preso a um círculo vicioso: para criar o objeto especificado impredicativamente, seria preciso *primeiro* criar todos os objetos (incluindo o objeto especificado impredicativamente), uma vez que este é especificado em termos de todos os objetos; logo seria preciso criar o objeto especificado impredicativamente antes de o ter criado. Mas, de novo, isto só é uma objeção séria a conjuntos especificados de modo "essencialmente impredicativo", se pensarmos nos conjuntos como coisas que *criamos*. E nós (provavelmente) não os criamos.

Assim—para o bem ou para o mal—a abordagem que se tornou comum não envolve tomar uma posição rígida sobre (im)predicatividade. Envolve antes o que hoje se considera a abordagem cumulativa-iterativa. No fim, isto permitir-nos-á estratificar os conjuntos em "estágios"—um *pouco* como a abordagem predicativa estratifica entidades em conjuntos$_0$, conjuntos$_1$, conjuntos$_2$, ...—mas não postularemos diferença de natureza entre eles.

1.4 A Abordagem Cumulativa-Iterativa

sth:story:approach:sec

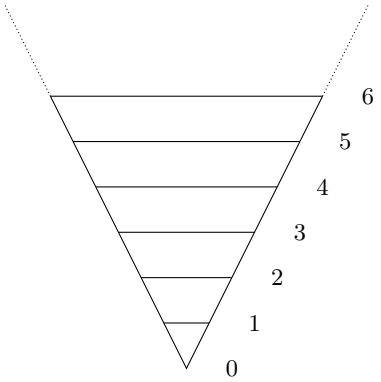
Eis um enunciado um pouco mais completo de como estratificaremos os conjuntos em estágios:

> Os conjuntos formam-se em *estágios*. Para cada estágio S, há certos estágios que são *anteriores* a S. No estágio S, cada coleção constituída por conjuntos formados em estágios anteriores a S é formada num conjunto. Não há conjuntos além dos que são formados nos estágios. (Shoenfield, 1977, p. 323)

Isto é um esboço da *concepção cumulativa-iterativa do conjunto*. Servirá de base à teoria formal dos conjuntos que apresentamos em Parte I.

[1] Para mais, ver Linnebo (2010).

Exploremos isto com um pouco mais de detalhe. Como Shoenfield descreve o processo, em cada estágio formamos novos conjuntos a partir dos conjuntos que tínhamos disponíveis nos estágios anteriores. Assim, na imagem de Shoenfield, no estágio inicial, estágio 0, não há estágios *anteriores*, e portanto *a fortiori* não há conjuntos disponíveis a partir de estágios anteriores.[2] Logo formamos apenas um conjunto: o conjunto sem membros $\emptyset$. No estágio 1, está exatamente um conjunto disponível a partir de estágios anteriores, logo apenas um conjunto novo é $\{\emptyset\}$. No estágio 2, dois conjuntos estão disponíveis a partir de estágios anteriores, e formamos dois conjuntos novos $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$. No estágio 3, quatro conjuntos estão disponíveis a partir de estágios anteriores, logo formamos doze conjuntos novos. . . . Assim, a imagem cumulativa-iterativa dos conjuntos ficará algo assim (com números a indicar estágios):



Então: por que deveríamos aceitar esta narrativa?

Uma razão é que é uma narrativa agradável e tratável. Dado o fim da narrativa mais óbvia, isto é, a compreensão ingênua, precisamos de algo de substância.

Mas a narrativa não é *apenas* agradável. Temos boa razão para acreditar que qualquer teoria dos conjuntos baseada nesta narrativa será *consistente*. Eis a razão.

Dada a concepção cumulativa-iterativa do conjunto, formamos conjuntos em estágios; e os seus membros têm de ser objetos que já estavam disponíveis. Assim, para qualquer estágio S, podemos formar o conjunto

$$R_S = \{x : x \notin x \text{ e } x \text{ já estava disponível antes de } S\}$$

O raciocínio envolvido na prova do paradoxo de Russell estabelece agora que o próprio R_S não está disponível antes do estágio S. E isso não é uma contradição. Além disso, se aceitarmos a concepção cumulativa-iterativa do conjunto, nem sequer deveríamos ter *esperado* poder formar o próprio conjunto de Russell. Pois esse seria o conjunto de todos os conjuntos que não são membros

[2] Por que deveríamos supor que *existe* um primeiro estágio? Ver a nota de rodapé a *Estágios-são-ordenados* em Seção 2.1.

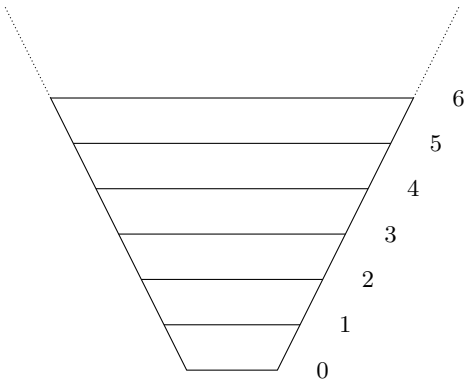
de si próprios que "alguma vez estarão disponíveis". Em resumo: o fato de, provadamente, não podermos formar o conjunto de Russell não é *surpreendente*, dada a narrativa cumulativa-iterativa; é antes *previsível*.

1.5 Urelementos ou Não?

sth:story:urelements:sec

Nos próximos capítulos, tentaremos extrair axiomas da concepção cumulativa-iterativa do conjunto. Mas, antes de avançar mais, precisamos de dizer algo mais sobre os *urelementos*.

A imagem de Seção 1.4 só nos permitia formar novos conjuntos a partir de *conjuntos* antigos. Contudo, podemos querer admitir que certos *não-conjuntos*—vacas, porcos, grãos de areia, ou o que seja—possam ser membros de conjuntos. Nesse caso, começaríamos com certos elementos básicos, *urelementos*, e diríamos que em cada estágio S formaríamos "todos os possíveis" conjuntos constituídos por urelementos ou conjuntos formados em estágios anteriores a S (em qualquer combinação). A imagem resultante parecer-se-ia mais com isto:



Temos pois uma decisão a tomar: *devemos admitir urelementos?*

Do ponto de vista filosófico, faz sentido incluir urelementos na nossa teorização. A principal razão é tornar a teoria dos conjuntos *aplicável*. Para ilustrar, recordemos de **??** que dizemos que dois conjuntos A e B têm o mesmo tamanho, isto é, $A \approx B$, sse existe uma bijeção entre eles. Agora, se as vacas no campo e os porcos no chiqueiro constituem ambos conjuntos, podemos oferecer um tratamento conjunto-teórico da afirmação "há tantas vacas como porcos". Mas se proibirmos urelementos, de modo que as vacas e os porcos *não* constituem conjuntos, esse tratamento conjunto-teórico deixará de estar disponível. De fato, não teremos capacidade direta de aplicar a teoria dos conjuntos a mais nada além dos próprios conjuntos. (Para mais razões para incluir urelementos, ver Potter 2004, pp. vi, 24, 50–1.)

Matematicamente, contudo, é bastante raro admitir urelementos. Em parte, porque é *ligeiramente* mais fácil formular a teoria dos conjuntos sem urelemen-

tos. Mas, ocasionalmente, encontram-se justificações mais interessantes para excluir urelementos da teoria dos conjuntos:

> De acordo com a convicção de que a teoria dos conjuntos é o fundamento da matemática, devemos ser capazes de captar toda a matemática apenas falando de conjuntos, pelo que as nossas variáveis não devem quantificar sobre objetos como vacas e porcos. (Kunen, 1980, p. 8)

Assim: um foco na aplicabilidade sugeriria *incluir* urelementos; um foco num objetivo fundacional redutivo (reduzir a matemática à teoria pura dos conjuntos) poderia sugerir *excluí-los*. Uma ligeira preguiça também aponta no sentido de excluir urelementos.

Seguiremos o caminho mais preguiçoso. Em parte, há também uma justificação pedagógica. O nosso objetivo é introduzir os elementos da teoria dos conjuntos de que precisa para começar na filosofia da teoria dos conjuntos. E a maior parte dessa literatura filosófica discute teorias dos conjuntos formuladas *sem* urelementos. Logo este livro será, talvez, mais útil se se mantiver bastante próximo dessa literatura.

1.6 Apêndice: Lei Básica V de Frege

sth:story:blv:sec

Na Seção 1.2, explicamos que Russell formulou o paradoxo como um problema para o sistema que Frege delineou nos seus *Grundgesetze*. O sistema de Frege não incluía uma formulação direta da compreensão ingênua. Logo, neste apêndice, explicaremos muito sumariamente o que o sistema de Frege *incluía*, como se relaciona com a compreensão ingênua e como se relaciona com o paradoxo de Russell.

O sistema de Frege é de *segunda ordem* e foi concebido para formular a noção de *extensão de um conceito*.[3] Usando notação inspirada em Frege, escreveremos $\epsilon x\, F(x)$ para *a extensão do conceito* F. Este é um dispositivo que toma um *predicado*, "F", e transforma-o num *termo* (de primeira ordem), "$\epsilon x\, F(x)$". Com este dispositivo, Frege propôs a seguinte *definição* de pertença:

$$a \in b =_{\mathrm{df}} \exists G(b = \epsilon x\, G(x) \wedge Ga)$$

grosso modo: $a \in b$ sse a cai sob um conceito cuja extensão é b. (Note que o quantificador "$\exists G$" é de segunda ordem.) Frege também sustentava o seguinte princípio, conhecido como *Lei básica V*:

$$\epsilon x\, F(x) = \epsilon x\, G(x) \leftrightarrow \forall x(Fx \leftrightarrow Gx)$$

grosso modo: conceitos têm extensões idênticas sse são coextensivos. (De novo, tanto "F" como "G" estão em posição de predicado.) Um princípio simples liga agora a pertença à satisfação de propriedades:

[3] Estritamente falando, Frege tenta formalizar uma noção mais geral: o "valor de curso" de uma função. As extensões de conceitos são um caso especial da noção mais geral. Ver Heck (2012, pp. 8–9) para pormenores.

sth:story:blv:
lem:Fregeextensions

Lema 1.2 (em *Grundgesetze*). $\forall F \forall a(a \in \epsilon x\, F(x) \leftrightarrow Fa)$

Prova. Fixe F e a. Ora $a \in \epsilon x\, F(x)$ sse $\exists G(\epsilon x\, F(x) = \epsilon x\, G(x) \wedge Ga)$ (pela definição de pertença) sse $\exists G(\forall x(Fx \leftrightarrow Gx) \wedge Ga)$ (pela lei básica V) sse Fa (por lógica elementar de segunda ordem). □

E disto resulta quase de imediato a compreensão ingênua:

Lema 1.3 (em *Grundgesetze*.). $\forall F \exists s \forall a(a \in s \leftrightarrow Fa)$

Prova. Fixe F; agora Lema 1.2 dá $\forall a(a \in \epsilon x\, F(x) \leftrightarrow Fa)$; logo $\exists s \forall a(a \in s \leftrightarrow Fa)$ por generalização existencial. O resultado segue-se, pois F era arbitrário. □

O paradoxo de Russell segue tomando F dado por $\forall x(Fx \leftrightarrow x \notin x)$.

Capítulo 2

Passos rumo a Z

2.1 A história com mais pormenor

sth:z:story:sec

Na Seção 1.4, citamos a descrição de Shoenfield do processo de formação de conjuntos. Queremos agora escrever mais alguns princípios, para tornar esta história um pouco mais precisa. Eis-os:

> *Estágios-são-chave.* Cada conjunto forma-se por algum estágio.
>
> *Estágios-são-ordenados.* Os estágios estão ordenados: alguns vêm *antes* de outros.[1]
>
> *Estágios-acumulam.* Para qualquer estágio S, e para quaisquer conjuntos que se formaram *antes* do estágio S: forma-se, no estágio S, um conjunto cujos membros são exatamente esses conjuntos. Mais nada se forma no estágio S.

Estes são princípios informais, mas poderemos usá-los para justificar vários dos axiomas da teoria de conjuntos de Zermelo.

(Convém uma palavra de cautela. Embora vamos apresentar alguns axiomas completamente standard, com nomes completamente standard, os princípios em itálico que acabamos de apresentar não têm nomes particulares na literatura. São apenas alcunhas que esperamos serem úteis.)

2.2 Separação

sth:z:sep:sec

Começamos com um princípio que substitui a compreensão ingênua:

Esquema de Separação (Esquema de Separação). Para cada fórmula $\varphi(x)$, isto é um axioma: para qualquer A, o conjunto $\{x \in A : \varphi(x)\}$ existe.

[1] Assumiremos de fato—tacitamente—que os estágios estão *bem ordenados*. O que isto significa explica-se no Capítulo 3. É um pressuposto substancial. De fato, usando uma técnica muito engenhosa devida a Scott (1974), este pressuposto pode ser *evitado* e depois *deduzido*. (Isto também explicará por que devemos pensar que existe um estágio inicial.) Não podemos aprofundar isso aqui; para mais, veja Button (2021).

Note que isto não é um único axioma. É um *esquema* de axiomas. Há *infinitamente muitos* axiomas de Separação; um para cada fórmula $\varphi(x)$. O esquema pode igualmente ser (e normalmente é) escrito do seguinte modo:

> Para qualquer fórmula $\varphi(x)$ que não contenha "S", isto é um axioma:
>
> $$\forall A \exists S \forall x (x \in S \leftrightarrow (\varphi(x) \wedge x \in A)).$$

Em conformidade com a convenção assinalada no início da Parte I, as fórmulas φ nos axiomas de Separação podem ter parâmetros.[2]

A Separação justifica-se de imediato pela concepção cumulativa iterativa de conjuntos que vamos expondo. Para ver por que, seja A um conjunto. Então A forma-se por algum estágio S (por *Estágios-são-chave*). Uma vez que A se formou no estágio S, todos os membros de A formaram-se antes do estágio S (por *Estágios-acumulam*). Consideremos em particular todos os conjuntos que são membros de A e que também satisfazem φ; claramente todos estes conjuntos também se formaram antes do estágio S. Logo formam-se num conjunto $\{x \in A : \varphi(x)\}$ também no estágio S (por *Estágios-acumulam*).

Ao contrário da compreensão ingênua, isto evita o paradoxo de Russell. Pois não podemos simplesmente afirmar a existência do conjunto $\{x : x \notin x\}$. Pelo contrário, *dado* algum conjunto A, podemos afirmar a existência do conjunto $R_A = \{x \in A : x \notin x\}$. Mas isto só prova que $R_A \notin R_A$ e $R_A \notin A$, o que não é preocupante.

Contudo, a Separação tem uma consequência imediata e marcante:

sth:z:sep: thm:NoUniversalSet

Teorema 2.1. *Não existe conjunto* universal*, isto é,* $\{x : x = x\}$ *não existe.*

Prova. Por redução ao absurdo, suponhamos que V é um conjunto universal. Então, por Separação, $R = \{x \in V : x \notin x\} = \{x : x \notin x\}$ existe, o que contradiz o paradoxo de Russell. □

A ausência de um conjunto universal—de fato, a abertura da hierarquia de conjuntos—é uma das ideias mais fundamentais por detrás da concepção cumulativa iterativa. Por isso vale a pena ver que, intuitivamente, poderíamos chegar lá por outro caminho. Um conjunto universal teria de ser um membro de si próprio. Mas, na nossa concepção cumulativa iterativa, cada conjunto aparece (pela primeira vez) na hierarquia no primeiro estágio imediatamente a seguir a todos os seus membros. Isto implica que *nenhum* conjunto pertence a si próprio. Pois qualquer conjunto que pertencesse a si próprio teria de ocorrer pela primeira vez imediatamente depois do estágio em que ocorreu pela primeira vez, o que é absurdo. (Veremos na Definição 4.15 como tornar esta explicação mais rigorosa, usando a noção de "posto" de um conjunto. Contudo, precisaremos de mais alguns axiomas para o fazer.)

Eis mais algumas consequências da Separação e da Extensionalidade.

[2] Para uma explicação do que isto significa, veja a discussão imediatamente a seguir a **??**.

Proposição 2.2. *Se existe algum conjunto, então $\emptyset$ existe.* sth:z:sep: prop:emptyexists

Prova. Se A é um conjunto, $\emptyset = \{x \in A : x \neq x\}$ existe por Separação. □

Proposição 2.3. *$A \setminus B$ existe quaisquer que sejam os conjuntos A e B*

Prova. $A \setminus B = \{x \in A : x \notin B\}$ existe por Separação. □

Também se verifica que existem (quase) interseções arbitrárias:

Proposição 2.4. *Se $A \neq \emptyset$, então $\bigcap A = \{x : (\forall y \in A)x \in y\}$ existe.* sth:z:sep: prop:intersectionsexist

Prova. Seja $A \neq \emptyset$, logo existe algum $c \in A$. Então $\bigcap A = \{x : (\forall y \in A)x \in y\} = \{x \in c : (\forall y \in A)x \in y\}$, que existe por Separação. □

Note, porém, a condição de que $A \neq \emptyset$; pois $\bigcap \emptyset$ seria o conjunto universal, vacuamente, o que contradiz Teorema 2.1.

2.3 União

Proposição 2.4 deu-nos interseções. Mas, se quisermos que existam uniões arbitrárias, precisamos de enunciar outro axioma: sth:z:union: sec

União (União). Para qualquer conjunto A, o conjunto $\bigcup A = \{x : (\exists b \in A)x \in b\}$ existe.

$$\forall A \exists U \forall x (x \in U \leftrightarrow (\exists b \in A) x \in b)$$

Este axioma também se justifica pela concepção cumulativa iterativa. Seja A um conjunto, logo A forma-se por algum estágio S (por *Estágios-são-chave*). Cada membro de A formou-se *antes* de S (por *Estágios-acumulam*); logo, raciocinando de modo análogo, cada membro de cada membro de A formou-se antes de S. Assim, todos *esses* conjuntos estão disponíveis antes de S, para serem reunidos num conjunto em S. E esse conjunto é precisamente $\bigcup A$.

2.4 Pares

O próximo axioma a considerar é o seguinte: sth:z:pairs: sec

Pares (Pares). Quaisquer que sejam os conjuntos a, b, o conjunto $\{a, b\}$ existe.

$$\forall a \forall b \exists P \forall x (x \in P \leftrightarrow (x = a \vee x = b))$$

Eis como justificar este axioma à luz da concepção iterativa. Suponhamos que a está disponível no estágio S, e b no estágio T. Seja M o que quer que seja dos estágios S e T que ocorre mais tarde. Então, uma vez que a e b estão ambos disponíveis no estágio M, o conjunto $\{a, b\}$ é uma coleção possível disponível em qualquer estágio depois de M (o que quer que seja o posterior).

Mas espera! Porquê assumir que *existem* estágios depois de M? Se não existir nenhum, a nossa justificação falha. Por isso, para justificar Pares, teremos de acrescentar outro princípio à história que contamos na Seção 2.1, nomeadamente:

> *Estágios-prosseguem.* Não há último estágio.

Este princípio está justificado? Nada na história de Shoenfield afirmava *explicitamente* que não há último estágio. Ainda assim, mesmo que seja (estritamente falando) um acréscimo à nossa história, encaixa bem na ideia básica de que os conjuntos se formam em estágios. Aceitá-lo-emos simplesmente no que se segue. E, assim, aceitaremos também o Axioma dos Pares.

Armados com este novo axioma, podemos provar a existência de muitos mais conjuntos. Por exemplo:

sth:z:pairs: prop:pairsconsequences

Proposição 2.5. *Quaisquer que sejam os conjuntos a e b, existem os seguintes conjuntos:*

sth:z:pairs: singleton
1. $\{a\}$

sth:z:pairs: binunion
2. $a \cup b$

sth:z:pairs: tuples
3. $\langle a, b\rangle$

Prova. (1). Por Pares, $\{a, a\}$ existe, o que é $\{a\}$ por Extensionalidade.

(2). Por Pares, $\{a, b\}$ existe. Ora, $a \cup b = \bigcup\{a, b\}$ existe por União.

(3). Por (1), $\{a\}$ existe. Por Pares, $\{a, b\}$ existe. Ora, $\{\{a\}, \{a, b\}\} = \langle a, b\rangle$ existe, de novo por Pares. □

Problema 2.1. Mostre que, quaisquer que sejam os conjuntos a, b, c, o conjunto $\{a, b, c\}$ existe.

Problema 2.2. Mostre que, quaisquer que sejam os conjuntos $a_1, \ldots, a_n$, o conjunto $\{a_1, \ldots, a_n\}$ existe.

2.5 Conjuntos potência

sth:z:power: sec

Prosseguiremos com outro axioma:

Conjuntos potência (Conjuntos potência). Para qualquer conjunto A, existe o conjunto $\wp(A) = \{x : x \subseteq A\}$.

$$\forall A \exists P \forall x (x \in P \leftrightarrow (\forall z \in x) z \in A)$$

A nossa justificação é bastante direta. Suponhamos que A se forma no estágio S. Então todos os membros de A estavam disponíveis antes de S (por *Estágios-acumulam*). Logo, raciocinando como na justificação da Separação, cada subconjunto de A forma-se até ao estágio S. Estão todos disponíveis, para serem reunidos num único conjunto, em qualquer estágio depois de S.

E sabemos que existe algum tal estágio, pois S não é o último estágio (por *Estágios-prosseguem*). Logo $\wp(A)$ existe.

Eis uma boa consequência dos conjuntos potência:

Proposição 2.6. *Dados quaisquer conjuntos A, B, o seu produto cartesiano $A \times B$ existe.*

Prova. O conjunto $\wp(\wp(A \cup B))$ existe por Conjuntos potência e Proposição 2.5. Logo, por Separação, existe este conjunto:

$$C = \{z \in \wp(\wp(A \cup B)) : (\exists x \in A)(\exists y \in B) z = \langle x, y \rangle\}.$$

Agora, para quaisquer $x \in A$ e $y \in B$, o conjunto $\langle x, y \rangle$ existe por Proposição 2.5. Além disso, uma vez que $x, y \in A \cup B$, temos $\{x\}, \{x, y\} \in \wp(A \cup B)$, e $\langle x, y \rangle \in \wp(\wp(A \cup B))$. Logo $A \times B = C$. □

Nesta prova, o axioma dos conjuntos potência interage com a Separação. E isso não surpreende. Sem Separação, o princípio dos conjuntos potência não seria muito *poderoso*. Afinal, a Separação nos diz que subconjuntos de um conjunto existem e, por conseguinte, determina quão "gordo" é cada conjunto potência.

Problema 2.3. Mostre que, quaisquer que sejam os conjuntos A, B: (i) existe o conjunto de todas as relações com domínio A e contradomínio B; e (ii) existe o conjunto de todas as funções de A para B.

Problema 2.4. Seja A um conjunto, e seja $\sim$ uma relação de equivalência em A. Prove que existe o conjunto das classes de equivalência sob $\sim$ em A, isto é, $A/_\sim$.

2.6 Infinito

sth:z:infinity-again:sec

Já temos axiomas suficientes para garantir que há infinitamente muitos conjuntos (se é que existe algum). De fato, suponhamos que algum conjunto existe; então $\emptyset$ existe (por Proposição 2.2). Agora, para qualquer conjunto x, o conjunto $x \cup \{x\}$ existe por Proposição 2.5. Logo, aplicando isto algumas vezes, obtemos conjuntos como se segue:

0. $\emptyset$
1. $\{\emptyset\}$
2. $\{\emptyset, \{\emptyset\}\}$
3. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
4. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$

e podemos verificar que cada um destes conjuntos é distinto.

Começamos a numeração em 0, por várias razões. Mas uma delas é esta. Não é difícil verificar que o conjunto que rotulamos "n" tem exatamente n membros e que (intuitivamente) se forma no n-ésimo estágio.

Contudo. Isto nos dá *infinitamente muitos* conjuntos, mas não garante que exista um conjunto *infinito*, isto é, um conjunto com infinitamente muitos membros. E isto importa deveras: a menos que encontremos um conjunto infinito de Dedekind, não podemos construir uma álgebra de Dedekind. Mas queremos uma álgebra de Dedekind, para a podermos tratar como o conjunto dos números naturais. (Compare-se com **??**.)

Importa que os axiomas que estabelecemos até aqui *não* garantem a existência de nenhum conjunto infinito. Por isso temos de enunciar um novo axioma:

Infinito (Infinito). Existe um conjunto, I, tal que $\emptyset \in I$ e $x \cup \{x\} \in I$ sempre que $x \in I$.

$$\exists I((\exists o \in I)\forall x\ x \notin o \wedge \\ (\forall x \in I)(\exists s \in I)\forall z(z \in s \leftrightarrow (z \in x \vee z = x)))$$

É fácil ver que o conjunto I que nos é dado pelo Axioma do Infinito é infinito de Dedekind. O seu elemento distinguido é $\emptyset$, e a injeção em I é dada por $s(x) = x \cup \{x\}$. Agora, **??** mostrou como extrair uma álgebra de Dedekind de um conjunto infinito de Dedekind; e trataremos isso como o nosso conjunto de números naturais. Mais precisamente:

sth:z:infinity-again: defnomega

Definição 2.7. Seja I qualquer conjunto que nos seja dado pelo Axioma do Infinito. Seja s a função $s(x) = x \cup \{x\}$. Seja $\omega = \mathrm{clo}_s(\emptyset)$. Chamamos *números naturais* aos membros de ω, e dizemos que n é o resultado de n aplicações de s a $\emptyset$.

Pode agora voltar atrás e verificar que o conjunto rotulado "n", há uns parágrafos, será tratado *como* o número n.

Discutiremos o significado desta estipulação na Seção 2.8. Por ora, permite-nos provar um resultado intuitivo:

sth:z:infinity-again: naturalnumbersarentinfinite

Proposição 2.8. *Nenhum número natural é infinito de Dedekind.*

Prova. A prova é por indução, isto é, **??**. Claramente $0 = \emptyset$ não é infinito de Dedekind. Para o passo indutivo, estabeleceremos a contrapositiva: se (absurdamente) $s(n)$ for infinito de Dedekind, então n é infinito de Dedekind.

Suponhamos, pois, que $s(n)$ é infinito de Dedekind, isto é, que existe alguma injeção f com $\mathrm{Im}(f) \subsetneq \mathrm{dom}(f) = s(n) = n \cup \{n\}$. Há dois casos a considerar.

Caso 1: $n \notin \mathrm{Im}(f)$. Então $\mathrm{Im}(f) \subseteq n$, e $f(n) \in n$. Seja $g = f\restriction_n$; agora $\mathrm{Im}(g) = \mathrm{Im}(f) \setminus \{f(n)\} \subsetneq n = \mathrm{dom}(g)$. Logo n é infinito de Dedekind.

Caso 2: $n \in \mathrm{Im}(f)$. Fixemos $m \in \mathrm{dom}(f) \setminus \mathrm{Im}(f)$, e definamos uma função h com domínio $s(n) = n \cup \{n\}$:

$$h(x) = \begin{cases} f(x) & \text{se } f(x) \neq n \\ m & \text{se } f(x) = n \end{cases}$$

Assim h e f coincidem em toda a parte, exceto que $h(f^{-1}(n)) = m \neq n = f(f^{-1}(n))$. Uma vez que f é uma injeção, $n \notin \mathrm{Im}(h)$; e $\mathrm{Im}(h) \subsetneq \mathrm{dom}(h) = s(n)$. Logo n é infinito de Dedekind, pelo argumento do Caso 1. □

A questão que permanece é como poderíamos *justificar* o Axioma do Infinito. A resposta curta é que precisaremos de acrescentar outro princípio à história que vamos contando. Esse princípio é o seguinte:

> *Estágios-atingem-o-infinito.* Há um estágio infinito. Isto é, há um estágio que (a) não é o primeiro estágio, e que (b) tem alguns estágios antes de si, mas que (c) não tem predecessor imediato.

O Axioma do Infinito segue-se diretamente deste princípio. Sabemos que o número natural n se forma no estágio n. Logo o conjunto ω forma-se no primeiro estágio infinito. E o próprio ω testemunha o Axioma do Infinito.

Isto, porém, apenas nos leva de volta à questão de como justificar *Estágios-atingem-o-infinito*. Tal como *Estágios-prosseguem*, não fazia parte explícita da história que contamos sobre a hierarquia cumulativa iterativa. Mas mais do que isso: nada na própria ideia de uma hierarquia iterativa, em que os conjuntos se formam estágio a estágio, nos obriga a pensar que o processo envolve um estágio *infinito*. Parece perfeitamente coerente pensar que os estágios estão ordenados como os números naturais.

Isto, contudo, levanta um problema óbvio. Na **??**, consideramos a "prova" de Dedekind de que existe um conjunto infinito de Dedekind (de pensamentos). Isto poderá não lhe ter parecido muito satisfatório. Mas se *Estágios-atingem-o-infinito* não nos é "imposto" pela concepção iterativa de conjunto (nem pelas "leis do pensamento"), continuamos sem uma justificação intrínseca para a afirmação de que existe um conjunto infinito de Dedekind.

Há muito mais a dizer aqui, naturalmente. Mas esperamos que esteja agora num ponto em que possa começar a refletir sobre o que poderá *custar* justificar um axioma (ou um princípio). No que se segue tomaremos simplesmente *Estágios-atingem-o-infinito* como concedido.

2.7 $\mathbf{Z}^-$: um marco

sth:z:milestone:sec

Voltaremos a *Estágios-atingem-o-infinito* na parte seguinte. Contudo, com o Axioma do Infinito, atingimos um marco importante. Temos agora todos os axiomas necessários para a teoria $\mathbf{Z}^-$. Em detalhe:

Definição 2.9. A teoria $\mathbf{Z}^-$ tem estes axiomas: Extensionalidade, União, Pares, Conjuntos potência, Infinito, e todas as instâncias do esquema de Separação.

O nome abrevia *Zermelo* (*menos* algo que abordaremos mais tarde). Zermelo merece a honra, pois formulou essencialmente esta teoria no seu trabalho de 1908.[3]

Esta teoria é bastante poderosa para permitir-nos fazer uma quantidade enorme de matemática. Em particular, *deverá* voltar atrás na **??** e convencer-se de que tudo o que fizemos, ingenuamente, pode ser feito de modo mais formal dentro de $\mathbf{Z}^-$. (Depois de o fazer durante algum tempo, poderá querer avançar e ler a Seção 2.9.) Por isso, daqui em diante, e sem mais comentários, assumiremos estar a trabalhar em $\mathbf{Z}^-$ (pelo menos).

2.8 A escolher os números naturais

sth:z:nat:sec

Na Definição 2.7, definimos explicitamente a expressão "números naturais". Como deve entender esta estipulação? Não é uma afirmação metafísica, mas apenas uma decisão de *tratar* certos conjuntos como os números naturais. Já abordamos razões para pensar assim na **??**, na **??** e na **??**. Mas podemos tornar essas razões ainda mais nítidas.

O nosso Axioma do Infinito segue von Neumann (1925). Mas eis outro axioma, que poderíamos ter adotado em alternativa:

> *Axioma do Infinito de Zermelo 1908.* Existe um conjunto A tal que $\emptyset \in A$ e $(\forall x \in A)\{x\} \in A$.

Se tivéssemos usado o axioma de Zermelo em vez do nosso Axioma do Infinito (inspirado em von Neumann), ter-nos-iam sido dado igualmente um conjunto infinito de Dedekind e, portanto, uma álgebra de Dedekind. Na abordagem de Zermelo, o elemento distinguido da nossa álgebra seria de novo $\emptyset$ (o nosso sucedâneo de 0), mas a injeção seria dada pela aplicação $x \mapsto \{x\}$, em vez de $x \mapsto x \cup \{x\}$. A consequência mais simples é que Zermelo trata 2 como $\{\{\emptyset\}\}$, ao passo que nós (com von Neumann) tratamos 2 como $\{\emptyset, \{\emptyset\}\}$.

Porquê escolher um axioma do Infinito em vez do outro? A razão prática principal é que a abordagem de von Neumann "escala" bastante bem para números transfinitos. Exploraremos isto a partir do Capítulo 3 em diante. Porém, na simples perspectiva de *fazer aritmética*, ambas as abordagens serviriam igualmente bem. Por isso, se alguém lhe disser que os números naturais *são* conjuntos, a pergunta óbvia é: *Que conjuntos são eles?*

Esta pergunta precisa foi tornada célebre por Benacerraf (1965). Mas vale a pena sublinhar que é apenas o exemplo mais famoso de um fenómeno que já encontramos muitas vezes. O ponto essencial é este. A teoria dos conjuntos nos dá uma maneira de *simular* vários tipos de entidades "intuitivas": os reais, os racionais, os inteiros e os naturais, sim; mas também pares ordenados, funções e relações. Contudo, a teoria dos conjuntos nunca nos fornece uma escolha

[3] Para comentários interessantes sobre a história e os pormenores técnicos, veja Potter (2004, Apêndice A).

única de simulação. Há *sempre* alternativas que—de modo direto—nos teriam servido tão bem.

2.9 Apêndice: Fechamento, compreensão e interseção

sth:z:arbintersections:sec

Na Seção 2.7, sugerimos que voltasse atrás no trabalho ingênuo da **??** e verificasse que este pode ser realizado em $\mathbf{Z}^-$. Se seguiu esse conselho, *um* ponto poderá tê-lo feito tropeçar: o uso da *interseção* no tratamento por Dedekind dos *fechamentos*.

Recordemos, de **??**, que

$$\mathrm{clo}_f(o) = \bigcap\{X : o \in X \text{ e } X \text{ é } f\text{-fechado}\}.$$

A forma geral disto é uma definição da forma:

$$C = \bigcap\{X : \varphi(X)\}.$$

Mas isto deve fazer soar o alarme: uma vez que a compreensão ingênua falha, não há garantia de que $\{X : \varphi(X)\}$ exista. Parece, então, perigosamente, que tais definições são *truques*.

Felizmente, não são truques; ou melhor, se *o forem* tal como estão, então podemos empenhar-nos honestamente para as tornar legítimas. Esse trabalho honesto foi antecipado na Proposição 2.4, quando explicamos por que $\bigcap A$ existe para qualquer $A \neq \emptyset$. Mas vamos explicitá-lo.

Dada a Extensionalidade, se tentarmos definir C como $\bigcap\{X : \varphi(X)\}$, tudo o que realmente pedimos é um objeto C que satisfaça o seguinte:

$$\forall x(x \in C \leftrightarrow \forall X(\varphi(X) \to x \in X)) \tag{*}$$

sth:z:arbintersections:bicondelimarbintersection

Suponhamos, agora, que existe *algum* conjunto, S, tal que $\varphi(S)$. Então, para satisfazer Eq. (*), podemos simplesmente definir C por *Separação*, do seguinte modo:

$$C = \{x \in S : \forall X(\varphi(X) \to x \in X)\}.$$

Deixamos como exercício verificar que esta definição produz Eq. (*), como desejado. E esta estratégia geral permitir-nos-á contornar qualquer uso aparente da compreensão ingênua na definição de interseções. No caso particular que nos levou a esta linha de raciocínio, nomeadamente o de $\mathrm{clo}_f(o)$, eis como isso funcionaria. Começamos a prova de **??** ao notar que $o \in \mathrm{Im}(f) \cup \{o\}$ e que $\mathrm{Im}(f) \cup \{o\}$ é f-fechado. Assim, podemos definir o que queremos assim:

$$\mathrm{clo}_f(o) = \{x \in \mathrm{Im}(f) \cup \{o\} : (\forall X \ni o)(X \text{ é } f\text{-fechado} \to x \in X)\}.$$

Capítulo 3

Ordinais

3.1 Introdução

sth:ordinals:intro:sec

No Capítulo 2, postulamos que existe um estágio infinito da hierarquia, na forma de *Estágios-atingem-o-infinito* (ver também o nosso axioma do Infinito). Contudo, dado *Estágios-prosseguem*, não podemos parar no estágio infinito; temos de continuar. Assim: no estágio seguinte ao primeiro estágio infinito, formamos todas as coleções possíveis de conjuntos que estavam disponíveis no primeiro estágio infinito; e repetimos; e repetimos; e repetimos; ...

Implicitamente, o que aqui aconteceu foi começarmos a invocar uma noção "intuitiva" de número, segundo a qual podem existir números *depois* de todos os números naturais. Em particular, a noção em causa é a de *ordinal transfinito*. O objetivo deste capítulo é tornar esta ideia mais rigorosa. Exploraremos a noção geral de ordinal e depois definiremos explicitamente certos conjuntos para serem os nossos ordinais.

3.2 A Ideia Geral de um Ordinal

sth:ordinals:idea:sec

Considere os números naturais, na sua ordem habitual:

$$0 \ < \ 1 \ < \ 2 \ < \ 3 \ < \ 4 \ < \ 5 \ < \cdots$$

Chamamos a isto, na gíria, uma ω-sucessão. E, de fato, esta ordenação geral espelha-se na nossa construção inicial dos estágios da hierarquia de conjuntos. Mas suponha agora que movemos 0 para o fim desta sucessão, de modo que fica depois de todos os outros números:

$$1 \ < \ 2 \ < \ 3 \ < \ 4 \ < \ 5 \ < \cdots < \ 0$$

Temos aqui as mesmas entidades, mas ordenadas de modo fundamentalmente diferente: a nossa primeira ordenação não tinha último elemento; a nova tem. De fato, a nova ordenação consiste numa ω-sucessão de entidades $(1, 2, 3, 4, 5, \ldots)$, seguida de outra entidade. Será uma sucessão do tipo $\omega + 1$.

Podemos gerar ainda mais tipos de ordenação, usando apenas estas entidades. Por exemplo, considere todos os números pares (na sua ordem natural) seguidos de todos os ímpares (na sua ordem natural):

$$0 \;<\; 2 \;<\; 4 \;<\; \cdots \;<\; 1 \;<\; 3 \;<\; \cdots$$

Isto é uma ω-sucessão seguida de outra ω-sucessão; uma sucessão do tipo $\omega+\omega$.

Pois bem, podemos continuar. Mas o que gostaríamos é de ter uma forma geral de entender esta linguagem sobre *ordenações*.

3.3 Boas Ordenações

A noção fundamental é a seguinte: sth:ordinals:wo:sec

Definição 3.1. A relação $<$ *bem ordena* A sse cumpre estas duas condições:

1. $<$ é conexa, isto é, para todos $a, b \in A$, ou $a < b$ ou $a = b$ ou $b < a$;
2. todo o subconjunto não vazio de A tem um membro $<$-minimal, isto é, se $\emptyset \neq X \subseteq A$ então $(\exists m \in X)(\forall z \in X) z \not< m$

É fácil ver que os três exemplos que acabamos de considerar eram de fato relações de boa ordenação.

Problema 3.1. Seção 3.2 apresentou três ordenações exemplo sobre os números naturais. Verifique que cada uma é uma boa ordenação.

Eis algumas observações elementares mas extremamente importantes sobre boa ordenação.

Proposição 3.2. *Se $<$ bem ordena A, então todo o subconjunto não vazio de A tem um único membro $<$-mínimo, e $<$ é irreflexiva, assimétrica e transitiva.* sth:ordinals:wo:wo:strictorder

Prova. Se X é um subconjunto não vazio de A, tem um membro $<$-minimal m, isto é, $(\forall z \in X) z \not< m$. Como $<$ é conexa, $(\forall z \in X) m \leq z$. Logo m é o membro $<$-mínimo de X.

Para a irreflexividade, fixe $a \in A$; o membro $<$-mínimo de $\{a\}$ é a, logo $a \not< a$. Para a transitividade, se $a < b < c$, então como $\{a, b, c\}$ tem um membro $<$-mínimo, $a < c$. A assimetria segue da irreflexividade e da transitividade □

Proposição 3.3. *Se $<$ bem ordena A, então para qualquer fórmula $\varphi(x)$:* sth:ordinals:wo:propwoinduction

$$\text{se } (\forall a \in A)((\forall b < a)\varphi(b) \to \varphi(a)), \text{ então } (\forall a \in A)\varphi(a).$$

Prova. Provaremos a contrapositiva. Suponha $\neg(\forall a \in A)\varphi(a)$, isto é, que $X = \{x \in A : \neg\varphi(x)\} \neq \emptyset$. Então X tem um membro $<$-minimal, a. Logo $(\forall b < a)\varphi(b)$ mas $\neg\varphi(a)$. □

Esta última propriedade deve recordar-lhe o princípio de indução forte nos naturais, isto é: se $(\forall n \in \omega)((\forall m < n)\varphi(m) \to \varphi(n))$, então $(\forall n \in \omega)\varphi(n)$. E esta propriedade torna a boa ordenação numa noção muito *robusta*.[1]

3.4 Isomorfismos de Ordem

sth:ordinals:iso:sec

Para explicar *quão* robusta é a boa ordenação, começaremos por introduzir um método para comparar boas ordenações.

Definição 3.4. Uma *boa ordenação* é um par $\langle A, < \rangle$, tal que $<$ bem ordena A. As boas ordenações $\langle A, < \rangle$ e $\langle B, \lessdot \rangle$ são *isomorfas por ordem* sse existe uma bijeção $f\colon A \to B$ tal que: $x < y$ sse $f(x) \lessdot f(y)$. Neste caso, escrevemos $\langle A, < \rangle \cong \langle B, \lessdot \rangle$, e dizemos que f é um *isomorfismo de ordem*.

Daqui em diante, por brevidade, falaremos em "isomorfismos" em vez de "isomorfismos de ordem". Intuitivamente, os isomorfismos são bijeções que preservam estrutura. Eis alguns fatos simples sobre isomorfismos.

sth:ordinals:iso:isoscompose

Lema 3.5. *Composições de isomorfismos são isomorfismos, isto é: se $f\colon A \to B$ e $g\colon B \to C$ são isomorfismos, então $(g \circ f)\colon A \to C$ é um isomorfismo.*

Problema 3.2. Prove Lema 3.5.

Prova. Fica como exercício. □

sth:ordinals:iso:ordisoisequiv

Corolário 3.6. *$X \cong Y$ é uma relação de equivalência.*

sth:ordinals:iso:ordisounique

Proposição 3.7. *Se $\langle A, < \rangle$ e $\langle B, \lessdot \rangle$ são boas ordenações isomorfas, então o isomorfismo entre elas é único.*

Prova. Sejam f e g isomorfismos $A \to B$. Provaremos o resultado por indução, isto é, usando Proposição 3.3. Fixe $a \in A$, e suponha (para indução) que $(\forall b < a) f(b) = g(b)$. Fixe $x \in B$.

Se $x \lessdot f(a)$, então $f^{-1}(x) < a$, logo $g(f^{-1}(x)) \lessdot g(a)$, invocando o fato de f e g serem isomorfismos. Mas como $f^{-1}(x) < a$, pela suposição $x = f(f^{-1}(x)) = g(f^{-1}(x))$. Logo $x \lessdot g(a)$. Analogamente, se $x \lessdot g(a)$ então $x \lessdot f(a)$.

Generalizando, $(\forall x \in B)(x \lessdot f(a) \leftrightarrow x \lessdot g(a))$. Segue que $f(a) = g(a)$ por **??**. Logo $(\forall a \in A) f(a) = g(a)$ por Proposição 3.3. □

Isto dá alguma ideia de que as boas ordenações são robustas. Mas para continuar a explicar isto, convém introduzir mais notação.

Definição 3.8. Quando $\langle A, < \rangle$ é uma boa ordenação com $a \in A$, seja $A_a = \{x \in A : x < a\}$. Dizemos que A_a é um *segmento inicial* próprio de A (e permitimos que o próprio A seja um segmento inicial impróprio de A). Seja $<_a$ a restrição de $<$ ao segmento inicial, isto é, $<\restriction_{A_a^2}$.

[1] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação em contrário).

Com esta notação, podemos enunciar e provar que nenhuma boa ordenação é isomorfa a nenhum dos seus segmentos iniciais próprios.

Lema 3.9. *Se $\langle A, <\rangle$ é uma boa ordenação com $a \in A$, então $\langle A, <\rangle \ncong \langle A_a, <_a\rangle$* sth:ordinals:iso:wellordnotinitial

Prova. Por redução ao absurdo, suponha $f\colon A \to A_a$ um isomorfismo. Como f é uma bijeção e $A_a \subsetneq A$, usando Proposição 3.2 seja $b \in A$ o membro $<$-mínimo de A tal que $b \neq f(b)$. Mostraremos que $(\forall x \in A)(x < b \leftrightarrow x < f(b))$, donde seguirá, por **??**, que $b = f(b)$, completando a redução ao absurdo.

Suponha $x < b$. Logo $x = f(x)$, pela escolha de b. E $f(x) < f(b)$, por f ser um isomorfismo. Logo $x < f(b)$.

Suponha $x < f(b)$. Logo $f^{-1}(x) < b$, por f ser um isomorfismo, e portanto $f^{-1}(x) = x$ pela escolha de b. Logo $x < b$. □

O nosso resultado seguinte mostra, grosso modo, que um "segmento inicial" de um isomorfismo é um isomorfismo:

Lema 3.10. *Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Se $f\colon A \to B$ é um isomorfismo e $a \in A$, então $f\restriction_{A_a} : A_a \to B_{f(a)}$ é um isomorfismo.* sth:ordinals:iso:wellordinitialsegment

Prova. Como f é um isomorfismo:

$$\begin{aligned} f[A_a] &= f[\{x \in A : x < a\}] \\ &= f[\{f^{-1}(y) \in A : f^{-1}(y) < a\}] \\ &= \{y \in B : y \lessdot f(a)\} \\ &= B_{f(a)} \end{aligned}$$

E $f\restriction_{A_a}$ preserva a ordem porque f preserva. □

Os nossos dois resultados seguintes estabelecem que as boas ordenações são sempre comparáveis:

Lema 3.11. *Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Se $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{b_1}, \lessdot_{b_1}\rangle$ e $\langle A_{a_2}, <_{a_2}\rangle \cong \langle B_{b_2}, \lessdot_{b_2}\rangle$, então $a_1 < a_2$ sse $b_1 \lessdot b_2$* sth:ordinals:iso:lemordsegments

Prova. Provaremos da *esquerda para a direita*; a outra direção é análoga. Suponha ambos $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{b_1}, \lessdot_{b_1}\rangle$ e $\langle A_{a_2}, <_{a_2}\rangle \cong \langle B_{b_2}, \lessdot_{b_2}\rangle$, com $f\colon A_{a_2} \to B_{b_2}$ o nosso isomorfismo. Seja $a_1 < a_2$; então $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{f(a_1)}, \lessdot_{f(a_1)}\rangle$ por Lema 3.10. Logo $\langle B_{b_1}, \lessdot_{b_1}\rangle \cong \langle B_{f(a_1)}, \lessdot_{f(a_1)}\rangle$, e portanto $b_1 = f(a_1)$ por Lema 3.9. Ora, $b_1 \lessdot b_2$ pois o domínio de f é B_{b_2}. □

Teorema 3.12. *Dadas quaisquer duas boas ordenações, uma é isomorfa a um segmento inicial (não necessariamente próprio) da outra.* sth:ordinals:iso:thm:woalwayscomparable

Prova. Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Usando a Separação, seja

$$f = \{\langle a, b\rangle \in A \times B : \langle A_a, <_a\rangle \cong \langle B_b, \lessdot_b\rangle\}.$$

Por Lema 3.11, $a_1 < a_2$ sse $b_1 \lessdot b_2$ para todos $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in f$. Logo $f\colon \mathrm{dom}(f) \to \mathrm{Im}(f)$ é um isomorfismo.

Se $a_2 \in \mathrm{dom}(f)$ e $a_1 < a_2$, então $a_1 \in \mathrm{dom}(f)$ por Lema 3.10; logo $\mathrm{dom}(f)$ é um segmento inicial de A. Analogamente, $\mathrm{Im}(f)$ é um segmento inicial de B. Por redução ao absurdo, suponha que ambos são segmentos iniciais *próprios*. Então seja a o membro $<$-mínimo de $A \setminus \mathrm{dom}(f)$, de modo que $\mathrm{dom}(f) = A_a$, e seja b o membro $\lessdot$-mínimo de $B \setminus \mathrm{Im}(f)$, de modo que $\mathrm{Im}(f) = B_b$. Logo $f\colon A_a \to B_b$ é um isomorfismo, e portanto $\langle a, b\rangle \in f$, contradição. □

3.5 Construção de Von Neumann dos Ordinais

sth:ordinals:vn:sec

Teorema 3.12 sugere uma ideia. Poderíamos introduzir certos objetos, chamados *tipos de ordem*, para servirem de representantes das boas ordenações. Escrevendo $\mathrm{ord}(A, <)$ para o tipo de ordem da boa ordenação $\langle A, <\rangle$, gostaríamos de garantir os dois princípios seguintes:

$$\mathrm{ord}(A, <) = \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B, \lessdot\rangle$$
$$\mathrm{ord}(A, <) < \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B$$

Além disso, poderíamos esperar introduzir tipos de ordem *como certos conjuntos*, tal como podemos introduzir os números naturais como certos conjuntos.

A forma mais comum de o fazer—e a abordagem que seguiremos—é definir estes tipos de ordem via certos conjuntos bem ordenados *canónicos*. Estes conjuntos canónicos foram introduzidos pela primeira vez por von Neumann:

Definição 3.13. O conjunto A é *transitivo* sse $(\forall x \in A)x \subseteq A$. Então A é um *ordinal* sse A é transitivo e bem ordenado por $\in$.

Daqui em diante, usaremos letras gregas para ordinais. Segue-se imediatamente da definição que, se α é um ordinal, então $\langle \alpha, \in_\alpha\rangle$ é uma boa ordenação, onde $\in_\alpha = \{\langle x, y\rangle \in \alpha^2 : x \in y\}$. Assim, abusando um pouco da notação, podemos dizer que o próprio α *é* uma boa ordenação.

Eis os primeiros ordinais:

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$$

Repare que estes são precisamente os primeiros ordinais que encontramos no nosso Axioma do Infinito, isto é, na definição de von Neumann de ω (ver Seção 2.6). Isto não é coincidência. A definição de von Neumann dos ordinais trata os números naturais como ordinais, mas permite também ordinais transfinitos.

Como sempre, podemos agora perguntar: *são* estes os ordinais? Ou von Neumann deu-nos apenas alguns conjuntos que podemos *tratar* como os ordinais? O tipo de discussões que se podem ter sobre esta questão é semelhante

às que tivemos na **??**, **??**, **??**, e Seção 2.8, pelo que não insistiremos no ponto. Em vez disso, daqui em diante usaremos "os ordinais" para falar dos "ordinais de von Neumann".

3.6 Propriedades Básicas dos Ordinais

Observamos que os primeiros ordinais são os números naturais. A razão principal para desenvolver uma teoria dos ordinais é alargar o princípio de indução que vale nos números naturais. Iremos construir isso através duma sucessão de resultados elementares. sth:ordinals:basic:sec

Lema 3.14. *Todo o membro de um ordinal é um ordinal.* sth:ordinals:basic:ordmemberord

Prova. Seja α um ordinal com $b \in \alpha$. Como α é transitivo, $b \subseteq \alpha$. Logo $\in$ bem ordena b pois $\in$ bem ordena α.

Para ver que b é transitivo, suponha $x \in c \in b$. Logo $c \in \alpha$ pois $b \subseteq \alpha$. Outra vez, como α é transitivo, $c \subseteq \alpha$, de modo que $x \in \alpha$. Logo $x, c, b \in \alpha$. Mas $\in$ bem ordena α, logo $\in$ é uma relação transitiva em α por Proposição 3.2. Logo, como $x \in c \in b$, temos $x \in b$. Generalizando, $c \subseteq b$ □

Corolário 3.15. $\alpha = \{\beta \in \alpha : \beta \text{ é um ordinal}\}$, *para qualquer ordinal* α sth:ordinals:basic:ordissetofsmallerord

Prova. Imediato a partir de Lema 3.14. □

A ideia grosseira dos dois resultados principais seguintes, Teorema 3.16 e Teorema 3.17, é que os ordinais eles próprios são bem ordenados por pertença:

Teorema 3.16 (Indução Transfinita). *Para qualquer fórmula* $\varphi(x)$*:* sth:ordinals:basic:ordinductionschema

$$\text{se } \exists\alpha\varphi(\alpha), \text{ então } \exists\alpha(\varphi(\alpha) \wedge (\forall\beta \in \alpha)\neg\varphi(\beta))$$

onde os quantificadores exibidos ficam implicitamente restritos a ordinais.

Prova. Suponha $\varphi(\alpha)$, para algum ordinal α. Se $(\forall\beta \in \alpha)\neg\varphi(\beta)$, terminamos. Caso contrário, como α é um ordinal, tem um membro $\in$-mínimo que verifica φ, e este é um ordinal por Lema 3.14. □

Repare que podemos exprimir igualmente Teorema 3.16 como o esquema:

$$\text{se } \forall\alpha((\forall\beta \in \alpha)\varphi(\beta) \to \varphi(\alpha)), \text{ então } \forall\alpha\varphi(\alpha)$$

tomando simplesmente $\neg\varphi(\alpha)$ no Teorema 3.16, e depois fazendo manipulações lógicas elementares.

Teorema 3.17 (Tricotomia). $\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$, *para quaisquer ordinais* α *e* β*.* sth:ordinals:basic:ordtrichotomy

Prova. A prova é por dupla indução, isto é, usando Teorema 3.16 duas vezes. Diga-se que x é *comparável* com y sse $x \in y \vee x = y \vee y \in x$.

Para a indução, suponha que todo o ordinal em α é comparável com *todo* o ordinal. Para uma segunda indução, suponha que α é comparável com todo o ordinal em β. Mostraremos que α é comparável com β. Por indução em β, seguirá que α é comparável com todo o ordinal; e por indução em α, *todo* o ordinal é comparável com *todo* o ordinal, como pretendido. Basta supor que $\alpha \notin \beta$ e $\beta \notin \alpha$, e mostrar que $\alpha = \beta$.

Para mostrar que $\alpha \subseteq \beta$, fixe $\gamma \in \alpha$; este é um ordinal por Lema 3.14. Logo, pela primeira hipótese de indução, γ é comparável com β. Mas se $\gamma = \beta$ ou $\beta \in \gamma$ então $\beta \in \alpha$ (invocando a transitividade de α se necessário), contra a suposição; logo $\gamma \in \beta$. Generalizando, $\alpha \subseteq \beta$.

Raciocínio exatamente análogo, usando a segunda hipótese de indução, mostra que $\beta \subseteq \alpha$. Logo $\alpha = \beta$. □

Assim, por vezes escreveremos $\alpha < \beta$ em vez de $\alpha \in \beta$, já que $\in$ se comporta como relação de ordem. Não há razões profundas para além da familiaridade, e porque é mais fácil escrever $\alpha \leq \beta$ do que $\alpha \in \beta \vee \alpha = \beta$.[2]

Eis duas consequências rápidas dos últimos resultados, a primeira das quais põe a nova notação em prática:

sth:ordinals:basic: ordordered

Corolário 3.18. *Se $\exists\alpha\varphi(\alpha)$, então $\exists\alpha(\varphi(\alpha) \wedge \forall\beta(\varphi(\beta) \to \alpha \leq \beta))$. Além disso, para quaisquer ordinais α, β, γ, tanto $\alpha \notin \alpha$ como $\alpha \in \beta \in \gamma \to \alpha \in \gamma$.*

Prova. Tal como Proposição 3.2. □

Problema 3.3. Complete o raciocínio "exatamente análogo" na prova de Teorema 3.17.

sth:ordinals:basic: corordtransitiveord

Corolário 3.19. *A é um ordinal sse A é um conjunto transitivo de ordinais.*

Prova. Da esquerda para a direita. Por Lema 3.14. *Da direita para a esquerda.* Se A é um conjunto transitivo de ordinais, então $\in$ bem ordena A por Teorema 3.16 e Teorema 3.17. □

Agora, descrevemos Teorema 3.16 e Teorema 3.17 como dizendo que $\in$ bem ordena os ordinais. Contudo, temos de ser *muito cautelosos* com este tipo de afirmação, graças ao resultado seguinte:

sth:ordinals:basic: buraliforti

Teorema 3.20 (Paradoxo de Burali-Forti). *Não existe conjunto de todos os ordinais*

Prova. Por redução ao absurdo, suponha O o conjunto de todos os ordinais. Se $\alpha \in \beta \in O$, então α é um ordinal, por Lema 3.14, logo $\alpha \in O$. Logo O é transitivo, e portanto O é um ordinal por Corolário 3.19. Daí $O \in O$, contradizendo Corolário 3.18. □

[2] Poderíamos escrever $\alpha \subsetneq \beta$; mas isso seria totalmente não convencional.

Este resultado deve o nome a Burali-Forti. Mas foi Cantor em 1899—numa carta a Dedekind—quem viu pela primeira vez com clareza a *contradição* em supor que existe um conjunto de todos os ordinais. Como van Heijenoort explica:

> O próprio Burali-Forti considerou a contradição como estabelecendo, por *reductio ad absurdum*, o resultado de que a ordenação natural dos ordinais é apenas uma ordenação parcial. (Heijenoort, 1967, p. 105)

Deixando de lado o erro de Burali-Forti, podemos resumir o precedente como segue. Os ordinais são conjuntos que individualmente são bem ordenados por pertença, e coletivamente são bem ordenados por pertença (sem coletivamente constituírem um conjunto).

Para concluir, eis mais propriedades básicas dos ordinais que seguem de Teorema 3.16 e Teorema 3.17.

Proposição 3.21. *Toda a sucessão estritamente descendente de ordinais é finita.*

Prova. Toda a sucessão infinita estritamente descendente de ordinais $\alpha_0 > \alpha_1 > \alpha_2 > \ldots$ não tem membro $<$-mínimo, contradizendo Teorema 3.16. □

Proposição 3.22. *$\alpha \subseteq \beta \vee \beta \subseteq \alpha$, para quaisquer ordinais α, β.* sth:ordinals:basic: ordinalsaresubsets

Prova. Se $\alpha \in \beta$, então $\alpha \subseteq \beta$ pois β é transitivo. Analogamente, se $\beta \in \alpha$, então $\beta \subseteq \alpha$. E se $\alpha = \beta$, então $\alpha \subseteq \beta$ e $\beta \subseteq \alpha$. Logo, por Teorema 3.17 terminamos. □

Proposição 3.23. *$\alpha = \beta$ sse $\alpha \cong \beta$, para quaisquer ordinais α, β.* sth:ordinals:basic: ordisoidentity

Prova. Os ordinais são boas ordenações; logo isto é imediato da Tricotomia (Teorema 3.17) e de Lema 3.9. □

Problema 3.4. Prove que, se cada membro de X é um ordinal, então $\bigcup X$ é um ordinal. sth:ordinals:basic: probunionordinalsordinal

3.7 Substituição

Na Seção 3.5, motivamos a introdução dos ordinais ao sugerir que os poderíamos tratar como tipos de ordem, isto é, como representantes canónicos de boas ordenações. Para que isso funcione, seria preciso provar que *toda a boa ordenação é isomorfa a algum ordinal*. Isso permitiria definir $\mathrm{ord}(A, <)$ como o ordinal α tal que $\langle A, < \rangle \cong \alpha$. sth:ordinals:replacement: sec

Infelizmente, *não* podemos provar o resultado desejado apenas com os axiomas introduzidos até aqui. (Veremos por que em Seção 5.2, mas por agora basta: não podemos.) Precisamos de uma ideia nova, e eis-a:

Esquema de Substituição (Esquema de Substituição). Para qualquer fórmula $\varphi(x, y)$, o seguinte é um axioma:

> para qualquer A, se $(\forall x \in A)\exists! y\, \varphi(x, y)$, então $\{y : (\exists x \in A)\varphi(x, y)\}$ existe.

Como na Separação, isto é um esquema: produz infinitamente muitos axiomas, um para cada uma das infinitas φ distintas. E pode igualmente ser (e normalmente é) escrito assim:

Para qualquer fórmula $\varphi(x, y)$ que não contenha "B", o seguinte é um axioma:

$$\forall A[(\forall x \in A)\exists! y\, \varphi(x, y) \to \exists B \forall y(y \in B \leftrightarrow (\exists x \in A)\varphi(x, y))]$$

À primeira vista, contudo, esta é uma fórmula bastante intrincada. A consequência imediata seguinte da Substituição dá provavelmente uma expressão *mais clara* à ideia intuitiva com que trabalhamos:[3]

Corolário 3.24. *Para qualquer termo $\tau(x)$, e qualquer conjunto A, este conjunto existe:*

$$\{\tau(x) : x \in A\} = \{y : (\exists x \in A)y = \tau(x)\}.$$

Prova. Como τ é um *termo*, $\forall x \exists! y\, \tau(x) = y$. *A fortiori*, $(\forall x \in A)\exists! y\, \tau(x) = y$. Logo $\{y : (\exists x \in A)\tau(x) = y\}$ existe pela Substituição. □

Isto sugere que "Substituição" é um bom nome para o axioma: dado um conjunto A, pode formar um novo conjunto, $\{\tau(x) : x \in A\}$, substituindo cada membro de A pela sua imagem sob τ. De fato, seguindo a notação para a imagem de um conjunto sob uma função, poderíamos escrever $\tau[A]$ para $\{\tau(x) : x \in A\}$.

O essencial, porém, é que τ é um *termo*. Não tem de ser (um nome de) uma *função*, no sentido de **??**, isto é, um certo conjunto de pares ordenados. Afinal, se f é uma função (nesse sentido), então o conjunto $f[A] = \{f(x) : x \in A\}$ é apenas um subconjunto particular de $\mathrm{Im}(f)$, e isso já está garantido a existir apenas com os axiomas de $\mathbf{Z}^-$.[4] A Substituição, em contraste, é um acréscimo *poderoso* aos nossos axiomas, como veremos no Capítulo 5.

[3] Um termo é uma expressão que designa exatamente um objeto (em qualquer instanciação das suas variáveis livres). Por exemplo, "$\emptyset$" é um termo que designa o conjunto vazio; "$\{x\}$" é um termo que designa o singular de x (seja qual for x); "$x \cup y$" é um termo que designa a união de x e de y (sejam quais forem).

[4] Baste considerar $\{y \in \bigcup\bigcup f : (\exists x \in A)y = f(x)\}$.

3.8 ZF$^-$: um marco

sth:ordinals:zfm:sec

A questão de como justificar o Esquema de Substituição (se é que o justificamos) não é linear. Como tal, a reservamos para o Capítulo 5. No entanto, com a adição da Substituição, atingimos outro marco importante. Dispomos agora de todos os axiomas necessários para a teoria **ZF**$^-$. Em detalhe:

Definição 3.25. A teoria **ZF**$^-$ tem estes axiomas: Extensionalidade, União, Pares, Conjuntos das Partes, Infinito, e todas as instâncias dos esquemas de Separação e Substituição. Por outras palavras, **ZF**$^-$ acrescenta a Substituição a **Z**$^-$.

Isto designa a teoria de conjuntos de *Zermelo–Fraenkel* (*menos* algo que veremos mais adiante). Fraenkel recebe a honra, uma vez que lhe é atribuída a formulação da Substituição em 1922, embora a primeira formulação precisa seja devida a Skolem (1922).

3.9 Ordinais como Tipos de Ordem

sth:ordinals:ordtype:sec

Armados com a Substituição, e portanto trabalhando agora em **ZF**$^-$, podemos finalmente provar o resultado a que vimos aspirando:

Teorema 3.26. *Toda a boa ordenação é isomorfa a um único ordinal.*

sth:ordinals:ordtype:thmOrdinalRepresentation

Prova. Seja $\langle A, <\rangle$ uma boa ordenação. Por Proposição 3.23, é isomorfa no máximo a um ordinal. Logo, por redução ao absurdo, suponha que $\langle A, <\rangle$ não é isomorfa a *nenhum* ordinal. Começaremos por "tornar $\langle A, <\rangle$ o mais pequena possível". Em detalhe: se algum segmento inicial próprio $\langle A_a, <_a\rangle$ não for isomorfo a nenhum ordinal, existe um $a \in A$ mínimo com essa propriedade; então seja $B = A_a$ e $\lessdot = <_a$. Caso contrário, seja $B = A$ e $\lessdot = <$.

Por definição, todo o segmento inicial próprio de B é isomorfo a algum ordinal, que é único como acima. Logo, pela Substituição, o conjunto seguinte existe, e é uma função:

$$f = \{\langle \beta, b\rangle : b \in B \text{ e } \beta \cong \langle B_b, \lessdot_b\rangle\}$$

Para completar a redução ao absurdo, mostraremos que f é um isomorfismo $\alpha \to B$, para algum ordinal α.

É óbvio que $\mathrm{Im}(f) = B$. E por Lema 3.11, f preserva a ordenação, isto é, $\gamma \in \beta$ sse $f(\gamma) \lessdot f(\beta)$. Para mostrar que $\mathrm{dom}(f)$ é um ordinal, por Corolário 3.19 basta mostrar que $\mathrm{dom}(f)$ é transitivo. Fixe então $\beta \in \mathrm{dom}(f)$, isto é, $\beta \cong \langle B_b, \lessdot_b\rangle$ para algum b. Se $\gamma \in \beta$, então $\gamma \in \mathrm{dom}(f)$ por Lema 3.10; generalizando, $\beta \subseteq \mathrm{dom}(f)$. □

Este resultado autoriza a definição seguinte, que queríamos apresentar desde Seção 3.5:

Definição 3.27. Se $\langle A, <\rangle$ é uma boa ordenação, então o seu tipo de ordem, $\mathrm{ord}(A, <)$, é o único ordinal α tal que $\langle A, <\rangle \cong \alpha$.

Além disso, esta definição autoriza dois princípios convenientes:

sth:ordinals:ordtype:ordtypesworklikeyouwant

Corolário 3.28. *Sendo $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações:*

$$\mathrm{ord}(A, <) = \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B, \lessdot\rangle$$
$$\mathrm{ord}(A, <) \in \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B$$

Prova. A identidade vale por Proposição 3.23. Para provar a segunda afirmação, seja $\mathrm{ord}(A, <) = \alpha$ e $\mathrm{ord}(B, \lessdot) = \beta$, e seja $f : \beta \to \langle B, \lessdot\rangle$ o nosso isomorfismo. Então:

$$\begin{aligned}\alpha \in \beta \text{ sse } & f\restriction_\alpha : \alpha \to B_{f(\alpha)} \text{ é um isomorfismo}\\ \text{sse } & \langle A, <\rangle \cong \langle B_{f(\alpha)}, \lessdot_{f(\alpha)}\rangle\\ \text{sse } & \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B\end{aligned}$$

por Proposição 3.7, Lema 3.10, e Corolário 3.15. □

3.10 Ordinais Sucessores e Limites

sth:ordinals:opps:sec

Nos próximos capítulos, usaremos muito os ordinais. Por isso convém introduzir algumas noções simples.

Definição 3.29. Para qualquer ordinal α, o seu *sucessor* é $\alpha^+ = \alpha \cup \{\alpha\}$. Dizemos que α é um ordinal *sucessor* se $\beta^+ = \alpha$ para algum ordinal β. Dizemos que α é um ordinal *limite* sse α não é nem vazio nem um ordinal sucessor.

O resultado seguinte mostra que esta é a noção certa de *sucessor*:

Proposição 3.30. *Para qualquer ordinal α:*

1. *$\alpha \in \alpha^+$;*
2. *α^+ é um ordinal;*
3. *não existe ordinal β tal que $\alpha \in \beta \in \alpha^+$.*

Prova. Trivialmente, $\alpha \in \alpha \cup \{\alpha\} = \alpha^+$. Igualmente, α^+ é um conjunto transitivo de ordinais, e portanto um ordinal por Corolário 3.19. E é impossível que $\alpha \in \beta \in \alpha^+$, pois então ou $\beta \in \alpha$ ou $\beta = \alpha$, contradizendo Corolário 3.18. □

Isto autoriza também uma variante de prova por indução transfinita:

sth:ordinals:opps:simpletransrecursion

Teorema 3.31 (Indução Transfinita Simples). *Seja $\varphi(x)$ uma fórmula tal que:*

1. *$\varphi(\emptyset)$; e*

2. *para qualquer ordinal α, se $\varphi(\alpha)$ então $\varphi(\alpha^+)$; e*

3. *se α é um ordinal limite e $(\forall \beta \in \alpha)\varphi(\beta)$, então $\varphi(\alpha)$.*

Então $\forall \alpha \varphi(\alpha)$.

Prova. Provamos a contrapositiva. Logo, suponha que existe algum ordinal para o qual vale $\neg\varphi$; seja γ o menor tal ordinal. Então ou $\gamma = \emptyset$, ou $\gamma = \alpha^+$ para algum α tal que $\varphi(\alpha)$; ou γ é um ordinal limite e $(\forall \beta \in \gamma)\varphi(\beta)$. □

Um último bocado de notação será útil mais adiante:

Definição 3.32. Se X é um conjunto de ordinais, então $\operatorname{lsub}(X) = \bigcup_{\alpha \in X} \alpha^+$. sth:ordinals:opps:defsupstrict

Aqui, "lsub" abrevia "least strict upper bound" (majorante superior estrito mínimo).[5] O resultado seguinte explica isto:

Proposição 3.33. *Se X é um conjunto de ordinais,* $\operatorname{lsub}(X)$ *é o menor ordinal estritamente maior do que todo o ordinal em X.*

Prova. Seja $Y = \{\alpha^+ : \alpha \in X\}$, de modo que $\operatorname{lsub}(X) = \bigcup Y$. Como os ordinais são transitivos e todo o membro de um ordinal é um ordinal, $\operatorname{lsub}(X)$ é um conjunto transitivo de ordinais, e portanto um ordinal por Corolário 3.19.

Se $\alpha \in X$, então $\alpha^+ \in Y$, logo $\alpha^+ \subseteq \bigcup Y = \operatorname{lsub}(X)$, e portanto $\alpha \in \operatorname{lsub}(X)$. Logo $\operatorname{lsub}(X)$ é estritamente maior do que todo o ordinal em X.

Inversamente, se $\alpha \in \operatorname{lsub}(X)$, então $\alpha \in \beta^+ \in Y$ para algum $\beta \in X$, de modo que $\alpha \leq \beta \in X$. Logo $\operatorname{lsub}(X)$ é o majorante superior estrito *mínimo* de X. □

[5] Alguns livros usam "$\sup(X)$" para isto. Mas outros usam "$\sup(X)$" para o majorante superior *não estrito* mínimo, isto é, simplesmente $\bigcup X$. Se X tem um maior elemento, α, estas noções divergem: o majorante superior estrito mínimo é α^+, enquanto o majorante superior não estrito mínimo é apenas α.

Capítulo 4

Estágios e postos

4.1 Definindo os estágios como os V_α

sth:spine:valpha:sec

No Capítulo 3, definimos boas ordenações e os ordinais (de von Neumann). Neste capítulo, usaremos isto para caracterizar a própria hierarquia de conjuntos. Para tal, recordemos que na Seção 3.10 definimos a noção de ordinal sucessor e ordinal limite. Usamos estas ideias na definição seguinte:

sth:spine:valpha:defValphas

Definição 4.1.

$$\begin{aligned} V_\emptyset &= \emptyset \\ V_{\alpha^+} &= \wp(V_\alpha) && \text{para qualquer ordinal } \alpha \\ V_\alpha &= \bigcup_{\gamma<\alpha} V_\gamma && \text{quando } \alpha \text{ é um ordinal limite} \end{aligned}$$

Será uma definição por *recursão transfinita* nos ordinais. A este respeito, convém comparar com definições recursivas de funções nos números naturais.[1] Como ao tratar dos números naturais, define-se um caso base e casos sucessor; mas ao tratar de ordinais, também precisamos de descrever o comportamento nos casos *limite*.

Esta definição dos V_α será um marco importante. Motivamos informalmente a nossa hierarquia de conjuntos como formando conjuntos por *estágios*. Os V_α são, em efeito, precisamente esses estágios. Importa, contudo, que se trata de uma caracterização *interna* dos estágios. Em vez de sugerir um possível *modelo* da teoria, teremos definido os estágios *dentro* da nossa teoria dos conjuntos.

4.2 Teorema(s) de recursão transfinita

sth:spine:recursion:sec

O primeiro passo é, contudo, confirmar que Definição 4.1 é uma definição bem sucedida. De modo mais geral, precisamos de provar que qualquer tentativa de

[1] Cf. as definições de adição, multiplicação e exponenciação em **??**.

definir por recursão transfinita (transfinita) terá êxito. Esse é o objetivo deste texto.

Aviso: este material é delicado. A lição geral, no entanto, é bem simples: a indução transfinita mais o Esquema de Substituição garantem a legitimidade de (várias versões da) recursão transfinita.[2]

Definição 4.2. Seja $\tau(x)$ um termo; seja f uma função; seja α um ordinal. Dizemos que f é uma *aproximação de ordem* α para τ sse $\mathrm{dom}(f) = \alpha$ e $(\forall \beta \in \alpha) f(\beta) = \tau(f{\restriction_\beta})$.

Lema 4.3 (Recursão limitada). *Para qualquer termo $\tau(x)$ e qualquer ordinal α, existe uma única aproximação de ordem α para τ.* *sth:spine:recursion:transrecursionfun*

Prova. Mostraremos que, para qualquer $\gamma \leq \alpha$, existe uma única aproximação de ordem γ.

Começamos por estabelecer a unicidade. Sejam g e h (respetivamente) aproximações de ordem γ e δ. Uma indução transfinita nos seus argumentos mostra que $g(\beta) = h(\beta)$ para qualquer $\beta \in \mathrm{dom}(g) \cap \mathrm{dom}(h) = \gamma \cap \delta = \min(\gamma, \delta)$. Logo as aproximações são únicas (se existem) e coincidem em todos os valores.

Para estabelecer a existência, usamos agora uma indução transfinita simples (Teorema 3.31) nos ordinais $\delta \leq \alpha$.

A função vazia é trivialmente uma aproximação de ordem $\emptyset$.

Se g é uma aproximação de ordem γ, então $g \cup \{\langle \gamma, \tau(g)\rangle\}$ é uma aproximação de ordem γ^+.

Se γ é um ordinal limite e g_δ é uma aproximação de ordem δ para todo o $\delta < \gamma$, seja $g = \bigcup_{\delta\in\gamma} g_\delta$. Isto é uma função, pois as várias g_δ coincidem em todos os valores. E se $\delta \in \gamma$ então $g(\delta) = g_{\delta^+}(\delta) = \tau(g_{\delta^+}{\restriction_\delta}) = \tau(g{\restriction_\delta})$.

Isto completa a prova por indução transfinita. □

Se nos permitirmos definir um *termo* em vez de uma função, podemos retirar a cota α do resultado anterior. No enunciado e na prova do resultado seguinte, quando σ é um termo, definimos $\sigma{\restriction_\alpha} = \{\langle \beta, \sigma(\beta)\rangle : \beta \in \alpha\}$.

Teorema 4.4 (Recursão geral). *Para qualquer termo $\tau(x)$, podemos definir explicitamente um termo $\sigma(x)$ tal que $\sigma(\alpha) = \tau(\sigma{\restriction_\alpha})$ para qualquer ordinal α.* *sth:spine:recursion:transrecursionschema*

[2] Lembrete: todas as fórmulas e termos podem ter parâmetros (salvo indicação em contrário).

Prova. Para cada α, por Lema 4.3 existe uma única aproximação de ordem α, f_α, para τ. Definimos $\sigma(\alpha)$ como $f_{\alpha^+}(\alpha)$. Ora:

$$\begin{aligned}\sigma(\alpha) &= f_{\alpha^+}(\alpha)\\ &= \tau(f_{\alpha^+}{\restriction_\alpha})\\ &= \tau(\{\langle \beta, f_{\alpha^+}(\beta)\rangle : \beta \in \alpha\})\\ &= \tau(\{\langle \beta, f_{\beta^+}(\beta)\rangle : \beta \in \alpha\})\\ &= \tau(\sigma{\restriction_\alpha})\end{aligned}$$

notando que $f_{\beta^+}(\beta) = f_{\alpha^+}(\beta)$ para todo o $\beta < \alpha$, como no Lema 4.3. □

Notemos que Teorema 4.4 é um *esquema*. Crucialmente, não podemos esperar que σ defina uma função, isto é, um certo tipo de *conjunto*, pois então $\mathrm{dom}(\sigma)$ seria o conjunto de todos os ordinais, contradizendo o paradoxo de Burali-Forti (Teorema 3.20).

Ainda falta mostrar, contudo, que Teorema 4.4 justifica a nossa definição dos V_α. Isto pode não ser óbvio de imediato; mas tornar-se-á claro com uma última versão simples da recursão transfinita.

sth:spine:recursion:simplerecursionschema

Teorema 4.5 (Recursão simples). *Para quaisquer termos $\tau(x)$ e $\theta(x)$ e qualquer conjunto A, podemos definir explicitamente um termo $\sigma(x)$ tal que:*

$$\begin{aligned}\sigma(\emptyset) &= A && \\ \sigma(\alpha^+) &= \tau(\sigma(\alpha)) && \text{para qualquer ordinal } \alpha\\ \sigma(\alpha) &= \theta(\mathrm{Im}(\sigma{\restriction_\alpha})) && \text{quando } \alpha \text{ é um ordinal limite}\end{aligned}$$

Prova. Começamos por definir um termo, $\xi(x)$, do seguinte modo:

$$\xi(x) = \begin{cases} A & \text{se } x \text{ não é uma função cujo}\\ & \quad \text{domínio é um ordinal; caso contrário:}\\ \tau(x(\alpha)) & \text{se } \mathrm{dom}(x) = \alpha^+\\ \theta(\mathrm{Im}(x)) & \text{se } \mathrm{dom}(x) \text{ é um ordinal limite}\end{cases}$$

Por Teorema 4.4, existe um termo $\sigma(x)$ tal que $\sigma(\alpha) = \xi(\sigma{\restriction_\alpha})$ para todo o ordinal α; além disso, $\sigma{\restriction_\alpha}$ é uma função com domínio α. Mostramos que σ tem as propriedades pretendidas, por indução transfinita simples (Teorema 3.31).

Primeiro, $\sigma(\emptyset) = \xi(\emptyset) = A$.

Segundo, $\sigma(\alpha^+) = \xi(\sigma{\restriction_{\alpha^+}}) = \tau(\sigma{\restriction_{\alpha^+}}(\alpha)) = \tau(\sigma(\alpha))$.

Por fim, $\sigma(\alpha) = \xi(\sigma{\restriction_\alpha}) = \theta(\mathrm{Im}(\sigma{\restriction_\alpha}))$, quando α é limite. □

Ora, para justificar Definição 4.1, basta tomar $A = \emptyset$, $\tau(x) = \wp(x)$ e $\theta(x) = \bigcup x$. Por fim, isto justifica a definição dos V_α!

4.3 Propriedades básicas dos estágios

Para evidenciar a importância fundacional da definição dos V_α, apresentaremos alguns resultados básicos sobre eles. Começamos com uma definição:[3] sth:spine:Valphabasic:sec

Definição 4.6. O conjunto A é *potente* sse $\forall x((\exists y \in A)x \subseteq y \to x \in A)$.

Lema 4.7. *Para cada ordinal α:* sth:spine:Valphabasic:Valphabasicprops

1. *Cada V_α é transitivo.* sth:spine:Valphabasic:Valphatrans
2. *Cada V_α é potente.* sth:spine:Valphabasic:Valphapotent
3. *Se $\gamma \in \alpha$, então $V_\gamma \in V_\alpha$ (e portanto também $V_\gamma \subseteq V_\alpha$, por (1))* sth:spine:Valphabasic:Valphacum

Prova. Provamos isto por indução transfinita (simultânea). Para a indução, supomos que (1)–(3) valem para cada ordinal $\beta < \alpha$.

O caso $\alpha = \emptyset$ é trivial.

Suponhamos $\alpha = \beta^+$. Para mostrar (3), se $\gamma \in \alpha$ então $V_\gamma \subseteq V_\beta$ por hipótese, logo $V_\gamma \in \wp(V_\beta) = V_\alpha$. Para mostrar (2), suponhamos $A \subseteq B \in V_\alpha$, isto é, $A \subseteq B \subseteq V_\beta$; então $A \subseteq V_\beta$, logo $A \in V_\alpha$. Para mostrar (1), notemos que se $x \in A \in V_\alpha$ temos $A \subseteq V_\beta$, logo $x \in V_\beta$, logo $x \subseteq V_\beta$ pois V_β é transitivo por hipótese, e assim $x \in V_\alpha$.

Suponhamos que α é um ordinal limite. Para mostrar (3), se $\gamma \in \alpha$ então $\gamma \in \gamma^+ \in \alpha$, de modo que $V_\gamma \in V_{\gamma^+}$ por hipótese, logo $V_\gamma \in \bigcup_{\beta\in\alpha} V_\beta = V_\alpha$. Para mostrar (1) e (2), basta observar que uma união de conjuntos transitivos (respetivamente, potentes) é transitiva (respetivamente, potente). □

Lema 4.8. *Para cada ordinal α, $V_\alpha \notin V_\alpha$.* sth:spine:Valphabasic:Valphanotref

Prova. Por indução transfinita. Evidentemente $V_\emptyset \notin V_\emptyset$.

Se $V_{\alpha^+} \in V_{\alpha^+} = \wp(V_\alpha)$, então $V_{\alpha^+} \subseteq V_\alpha$; e como $V_\alpha \in V_{\alpha^+}$ por Lema 4.7, temos $V_\alpha \in V_\alpha$. Reciprocamente: se $V_\alpha \notin V_\alpha$ então $V_{\alpha^+} \notin V_{\alpha^+}$

Se α é limite e $V_\alpha \in V_\alpha = \bigcup_{\beta\in\alpha} V_\beta$, então $V_\alpha \in V_\beta$ para algum $\beta \in \alpha$; mas então também $V_\beta \in V_\alpha$, logo $V_\beta \in V_\beta$ por Lema 4.7 (duas vezes). Reciprocamente, se $V_\beta \notin V_\beta$ para todo o $\beta \in \alpha$, então $V_\alpha \notin V_\alpha$. □

Corolário 4.9. *Para quaisquer ordinais α, β: $\alpha \in \beta$ sse $V_\alpha \in V_\beta$*

Prova. Lema 4.7 dá um sentido. Reciprocamente, suponhamos $V_\alpha \in V_\beta$. Então $\alpha \neq \beta$ por Lema 4.8; e $\beta \notin \alpha$, pois caso contrário teríamos $V_\beta \in V_\alpha$ e logo $V_\beta \in V_\beta$ por Lema 4.7 (duas vezes), contradizendo Lema 4.8. Logo $\alpha \in \beta$ por tricotomia. □

[3] Não há terminologia padrão para ≪potente≫; este é o nome usado por Button (2021).

Tudo isto permite pensar em cada V_α como o α-ésimo estágio da hierarquia. Eis a razão.

Certamente os nossos V_α podem ser vistos como formados num processo *iterativo*, pois o uso de ordinais acompanha a noção de iteração. Além disso, se um estágio é formado antes do outro, isto é, $V_\beta \in V_\alpha$, isto é, $\beta \in \alpha$, então o nosso processo de formação é *cumulativo*, pois $V_\beta \subseteq V_\alpha$. Finalmente, estamos de fato a formar *todas* as coleções possíveis de conjuntos que estavam disponíveis em qualquer estágio anterior, pois qualquer estágio sucessor V_{α^+} é o conjunto potência do seu predecessor V_α.

Em resumo: com $\mathbf{ZF}^-$, estamos *quase* a terminar de articular a nossa visão da hierarquia cumulativa e iterativa de conjuntos. (Embora, naturalmente, ainda precisemos de justificar o Esquema de Substituição.)

4.4 Fundação

sth:spine:foundation:sec

Estamos apenas *quase* concluídos—e não *totalmente* concluídos—porque nada em $\mathbf{ZF}^-$ garante que *todo* o conjunto está em algum V_α, isto é, que todo o conjunto é formado em algum estágio.

Há, contudo, um sentido (matemático) bastante direto em que não *importa* se existem conjuntos fora da hierarquia. (Se os houver, podemos simplesmente ignorá-los.) Mas motivamos o nosso *conceito* de conjunto com a ideia de que todo o conjunto é formado em algum estágio (ver *Estágios-são-chave* na Seção 2.1). Logo queremos excluir a possibilidade de conjuntos que caem fora da hierarquia. Por conseguinte, devemos acrescentar um novo axioma, que assegura que todo o conjunto surge em algum lugar da hierarquia.

Uma vez que os V_α são os nossos estágios, poderíamos simplesmente considerar acrescentar o seguinte como axioma:

> *Regularidade.* $\forall A \exists \alpha\, A \subseteq V_\alpha$

Seria uma abordagem perfeitamente razoável. Contudo, por razões que se explicarão adiante, adotaremos antes um axioma alternativo:

Fundação (Fundação). $(\forall A \neq \emptyset)(\exists B \in A) A \cap B = \emptyset$.

Com algum trabalho, podemos mostrar (em $\mathbf{ZF}^-$) que a Fundação implica a Regularidade:

Definição 4.10. Para cada conjunto A, definimos:

$$\begin{aligned} \mathrm{cl}_0(A) &= A, \\ \mathrm{cl}_{n+1}(A) &= \bigcup \mathrm{cl}_n(A), \\ \mathrm{trcl}(A) &= \bigcup_{n<\omega} \mathrm{cl}_n(A). \end{aligned}$$

Chamamos a $\mathrm{trcl}(A)$ o *fecho transitivo* de A.

O nome ≪fecho transitivo≫ é adequado:

Proposição 4.11. *$A \subseteq \operatorname{trcl}(A)$ e $\operatorname{trcl}(A)$ é um conjunto transitivo.* sth:spine:foundation:subsetoftrcl

Prova. Evidentemente $A = \operatorname{cl}_0(A) \subseteq \operatorname{trcl}(A)$. E se $x \in b \in \operatorname{trcl}(A)$, então $b \in \operatorname{cl}_n(A)$ para algum n, logo $x \in \operatorname{cl}_{n+1}(A) \subseteq \operatorname{trcl}(A)$. □

Lema 4.12. *Se A é um conjunto transitivo, então existe algum α tal que $A \subseteq V_\alpha$.* sth:spine:foundation:lem:TransitiveWellFounded

Prova. Recordando a definição de ≪$\operatorname{lsub}(X)$≫ em Definição 3.32, definimos dois conjuntos:

$$D = \{x \in A : \forall \delta\ x \nsubseteq V_\delta\}$$
$$\alpha = \operatorname{lsub}\{\delta : (\exists x \in A)(x \subseteq V_\delta \wedge (\forall \gamma \in \delta) x \nsubseteq V_\gamma)\}$$

Suponhamos $D = \emptyset$. Se $x \in A$, então existe algum δ tal que $x \subseteq V_\delta$ e, pela boa ordenação dos ordinais, $(\forall \gamma \in \delta) x \nsubseteq V_\gamma$; logo $\delta \in \alpha$ e assim $x \in V_\alpha$ por Lema 4.7. Logo $A \subseteq V_\alpha$, como pretendido.

Basta pois mostrar que $D = \emptyset$. Por redução ao absurdo, suponhamos o contrário. Pela Fundação, existe algum $B \in D \subseteq A$ tal que $D \cap B = \emptyset$. Se $x \in B$ então $x \in A$, pois A é transitivo, e como $x \notin D$, segue que $\exists \delta\ x \subseteq V_\delta$. Seja agora

$$\beta = \operatorname{lsub}\{\delta : (\exists x \in B)(x \subseteq V_\delta \wedge (\forall \gamma < \delta) x \nsubseteq V_\gamma)\}.$$

Como antes, $B \subseteq V_\beta$, contradizendo a afirmação de que $B \in D$. □

Teorema 4.13. *A Regularidade vale.* sth:spine:foundation:zfentailsregularity

Prova. Fixemos A; agora $A \subseteq \operatorname{trcl}(A)$ por Proposição 4.11, que é transitivo. Logo existe algum α tal que $A \subseteq \operatorname{trcl}(A) \subseteq V_\alpha$ por Lema 4.12 □

Estes resultados mostram que $\mathbf{ZF}^-$ prova a implicação *Fundação* ⇒ *Regularidade*. Em Proposição 4.22, mostraremos que $\mathbf{ZF}^-$ prova *Regularidade* ⇒ *Fundação*. Como tal, a Fundação e a Regularidade são *equivalentes* (módulo $\mathbf{ZF}^-$). Mas isto significa que, dado $\mathbf{ZF}^-$, podemos justificar a Fundação notando que é equivalente à Regularidade. E podemos justificar a Regularidade de imediato com base em *Estágios-são-chave*.

4.5 Z e ZF: um marco

Com a Fundação, atingimos outro marco importante. Consideramos as teorias $\mathbf{Z}^-$ e $\mathbf{ZF}^-$, que dissemos ser certas teorias ≪menos≫ alguma coisa. Essa coisa é a Fundação. Logo: sth:spine:zf:sec

Definição 4.14. A teoria **Z** acrescenta a Fundação a $\mathbf{Z}^-$. Os seus axiomas são Extensionalidade, União, Pares, Conjuntos das Partes, Infinito, Fundação, e todas as instâncias do esquema de Separação.

A teoria **ZF** acrescenta a Fundação a $\mathbf{ZF}^-$. Por outras palavras, **ZF** acrescenta todas as instâncias de Substituição a **Z**.

Ainda assim, uma pergunta pode ter surgido. Se a Regularidade é equivalente sobre $\mathbf{ZF}^-$ à Fundação, e a justificação da Regularidade é clara, por que dar voltas e tomar a Fundação como axioma básico, em vez da Regularidade?

Deixando de lado razões históricas (quem formulou o quê e quando), a razão essencial é que a Fundação pode ser apresentada sem recorrer à definição dos V_α. Essa definição dependeu de todo o trabalho na Seção 4.2: foi preciso provar a recursão transfinita, para mostrar que era legítima. Mas a nossa prova da recursão transfinita usou o *Esquema de Substituição*. Logo, embora a Fundação e a Regularidade sejam equivalentes módulo $\mathbf{ZF}^-$, não são equivalentes módulo $\mathbf{Z}^-$.

De fato, a questão é mais grave do que esta observação simples sugere. Embora ultrapasse o âmbito deste livro, verifica-se que tanto $\mathbf{Z}^-$ como **Z** são demasiado fracas para definir os V_α. Logo, se se trabalha apenas em **Z**, então a Regularidade (tal como a formulamos) nem sequer faz *sentido*. É por isso que o nosso axioma oficial é a Fundação, e não a Regularidade.

Daqui em diante, trabalharemos em **ZF** (salvo indicação em contrário), sem mais comentários.

4.6 Posto

sth:spine:rank:sec

Tendo definido os estágios como os V_α e sabendo que todo o conjunto é subconjunto de algum estágio, podemos definir o *posto* de um conjunto. Intuitivamente, o posto de A é o primeiro momento em que A é formado. Com mais precisão:

sth:spine:rank:defnsetrank

Definição 4.15. Para cada conjunto A, $\mathrm{posto}(A)$ é o menor ordinal α tal que $A \subseteq V_\alpha$.

sth:spine:rank:ranksexist

Proposição 4.16. $\mathrm{posto}(A)$ *existe, para qualquer* A.

Prova. Fica como exercício. □

Problema 4.1. Prove Proposição 4.16.

A boa ordenação dos postos permite provar alguns resultados importantes:

sth:spine:rank:valphalowerrank

Proposição 4.17. *Para qualquer ordinal* α, $V_\alpha = \{x : \mathrm{posto}(x) \in \alpha\}$.

Prova. Se $\mathrm{posto}(x) \in \alpha$ então $x \subseteq V_{\mathrm{posto}(x)} \in V_\alpha$, logo $x \in V_\alpha$ pois V_α é potente (invocando Lema 4.7 várias vezes). Reciprocamente, se $x \in V_\alpha$ então $x \subseteq V_\alpha$, logo $\mathrm{posto}(x) \leq \alpha$; agora uma indução transfinita simples mostra que $x \notin V_\alpha$.□

Problema 4.2. Complete a indução transfinita simples mencionada na Proposição 4.17.

Proposição 4.18. *Se $B \in A$, então* $\operatorname{posto}(B) \in \operatorname{posto}(A)$.

sth:spine:rank: rankmemberslower

Prova. $A \subseteq V_{\operatorname{posto}(A)} = \{x : \operatorname{posto}(x) \in \operatorname{posto}(A)\}$ por Proposição 4.17. □

Com este fato, podemos estabelecer um resultado que nos permite provar afirmações sobre *todos os conjuntos* por uma forma de indução:

Teorema 4.19 (Esquema de indução-$\in$). *Para qualquer fórmula φ:*

$$\forall A((\forall x \in A)\varphi(x) \to \varphi(A)) \to \forall A \varphi(A).$$

Prova. Provaremos a contrapositiva. Suponhamos, pois, $\neg\forall A\varphi(A)$. Pela indução transfinita (Teorema 3.16), existe algum não-φ de posto mínimo possível; isto é, algum A tal que $\neg\varphi(A)$ e $\forall x(\operatorname{posto}(x) \in \operatorname{posto}(A) \to \varphi(x))$. Ora, se $x \in A$ então $\operatorname{posto}(x) \in \operatorname{posto}(A)$, por Proposição 4.18, logo $\varphi(x)$; isto é, $(\forall x \in A)\varphi(x) \wedge \neg\varphi(A)$. □

Eis uma forma informal de interpretar este resultado poderoso. Digamos que φ é *hereditária* sse sempre que todo o membro de um conjunto é φ, o próprio conjunto é φ. Então a indução-$\in$ diz o seguinte: se φ é hereditária, todo o conjunto é φ.

Para concluir a discussão dos postos (por agora), provaremos algumas afirmações que já antecipamos várias vezes.

Proposição 4.20. $\operatorname{posto}(A) = \operatorname{lsub}_{x\in A} \operatorname{posto}(x)$.

sth:spine:rank: ranksupstrict

Prova. Seja $\alpha = \operatorname{lsub}_{x\in A} \operatorname{posto}(x)$. Por Proposição 4.18, $\alpha \leq \operatorname{posto}(A)$. Mas se $x \in A$ então $\operatorname{posto}(x) \in \alpha$, logo $x \in V_\alpha$ por Proposição 4.17, e portanto $A \subseteq V_\alpha$, isto é, $\operatorname{posto}(A) \leq \alpha$. Logo $\operatorname{posto}(A) = \alpha$. □

Corolário 4.21. *Para qualquer ordinal α,* $\operatorname{posto}(\alpha) = \alpha$.

sth:spine:rank: ordsetrankalpha

Prova. Suponhamos, por indução transfinita, que $\operatorname{posto}(\beta) = \beta$ para todo o $\beta \in \alpha$. Ora, $\operatorname{posto}(\alpha) = \operatorname{lsub}_{\beta\in\alpha} \operatorname{posto}(\beta) = \operatorname{lsub}_{\beta\in\alpha} \beta = \alpha$ por Proposição 4.20. □

Finalmente, eis uma prova rápida do resultado prometido no fim de Seção 4.4, a saber que $\mathbf{ZF}^-$ prova a implicação *Regularidade* $\Rightarrow$ *Fundação*. (Notemos que a noção de «posto» e Proposição 4.18 estão disponíveis para uso nesta prova pois—como indicamos no início deste texto—podem ser apresentadas usando $\mathbf{ZF}^-$ + Regularidade.)

Proposição 4.22 (trabalhando em $\mathbf{ZF}^-$ + Regularidade). *A Fundação vale.*

sth:spine:rank: zfminusregularityfoundation

Prova. Fixemos $A \neq \emptyset$, e algum $B \in A$ de posto mínimo possível. Se $c \in B$ então $\operatorname{posto}(c) \in \operatorname{posto}(B)$ por Proposição 4.18, logo $c \notin A$ pela escolha de B. □

Capítulo 5

Substituição

5.1 Introdução

sth:replacement:intro:sec

A Substituição é o esquema axiomático que distingue **ZF** de **Z**. Recorremos a ele ao longo de Capítulos 3 a 4. Neste capítulo, abordaremos finalmente a questão: a Substituição está justificada?

Para tornar a questão precisa, convém observar que a Substituição é realmente bastante *forte*. Teremos uma ideia de quão forte é ao longo deste capítulo (e de novo na Seção 8.5). Isto sugere que uma justificação é de fato necessária.

Discutiremos dois tipos de justificação. Em traços largos: uma justificação *extrínseca* é uma tentativa de justificar um axioma pelos seus frutos; uma justificação *intrínseca* é uma tentativa de justificar um axioma sugerindo que ele é vindicado pelos conceitos matemáticos em causa. Teremos uma ideia mais clara do que isto significa ao longo deste capítulo, mas não passa da ponta de um icebergue. Para mais pormenores, veja em particular Maddy (1988a e 1988b).

5.2 A Força da Substituição

sth:replacement:strength:sec

Começamos com uma observação simples sobre a força da Substituição: a menos que ultrapassemos **Z**, não podemos provar a existência de qualquer ordinal de von Neumann maior ou igual a $\omega + \omega$.

Eis um esboço do porquê. Trabalhando em **ZF**, consideremos o conjunto $V_{\omega+\omega}$. Este conjunto serve como domínio de um *modelo* para **Z**. Para ver isto, introduzimos alguma notação para a *relativização* de uma fórmula:

sth:replacement:strength:formularelativization

Definição 5.1. Para qualquer conjunto M, e qualquer fórmula φ, seja φ^M a fórmula que resulta de restringir todos os quantificadores de φ a M. Isto é, substituir "$\exists x$" por "$(\exists x \in M)$", e substituir "$\forall x$" por "$(\forall x \in M)$".

Pode mostrar-se que, para todo o axioma φ de **Z**, tem-se $\mathbf{ZF} \vdash \varphi^{V_{\omega+\omega}}$. Mas $\omega + \omega$ não está *em* $V_{\omega+\omega}$, por Corolário 4.21. Logo **Z** é consistente com a não existência de $\omega + \omega$.

Foi por isso que dissemos, na Seção 3.7, que Teorema 3.26 não pode ser provado sem Substituição. Pois é fácil, dentro de **Z**, definir uma boa ordenação explícita que intuitivamente *deveria* ter tipo de ordem $\omega + \omega$. De fato, demos um exemplo informal disto em Seção 3.2, quando apresentamos a ordenação nos números naturais dada por:

$$\begin{aligned} n \lessdot m \text{ sse ou } & n < m \text{ e } m - n \text{ é par,} \\ & \text{ou } n \text{ é par e } m \text{ é ímpar.} \end{aligned}$$

Mas se $\omega + \omega$ não existe, esta boa ordenação não é isomorfa a nenhum ordinal. Logo **Z** *não* prova Teorema 3.26.

Invertendo o prisma: a Substituição permite provar a existência de $\omega + \omega$, e portanto tem de permitir provar a existência de $V_{\omega+\omega}$. E não só. Para *qualquer* boa ordenação que possamos definir, Teorema 3.26 nos diz que existe algum α isomorfo com essa boa ordenação, e portanto que V_α existe. De forma direta, então, a Substituição garante que a hierarquia de conjuntos tem de ser *muito alta*.

Nas próximas partes do capítulo, e de novo em Seção 8.5, teremos uma ideia mais clara de quão *alta* a Substituição força a hierarquia a ser. O ponto simples, por agora, é que a Substituição *precisa* mesmo de justificação!

5.3 Considerações Extrínsecas sobre a Substituição

sth:replacement:extrinsic:sec

Começamos por considerar uma tentativa *extrínseca* de justificar a Substituição. Boolos sugere uma, como segue.

> [...] a razão para adotar os axiomas da substituição é bastante simples: têm muitas consequências desejáveis e (aparentemente) nenhuma indesejável. Para além de teoremas sobre a concepção iterativa, as consequências incluem uma teoria satisfatória, embora não ideal, dos números infinitos, e um resultado altamente desejável que justifica definições indutivas em relações bem fundadas. (Boolos, 1971, 229)

A ideia central de Boolos é que devemos justificar a Substituição pelos seus frutos. E os frutos específicos que menciona são os que temos discutido nos últimos capítulos. A Substituição permitiu-nos provar que os ordinais de von Neumann eram excelentes sucedâneos da ideia de um tipo de boa ordenação (isto é a nossa "teoria satisfatória, embora não ideal, dos números infinitos"). A Substituição permitiu-nos também definir os V_α, estabelecer a noção de posto e provar a indução-$\in$ (isto corresponde aos nossos "teoremas sobre a concepção iterativa"). Por fim, a Substituição permite provar o teorema de recursão transfinita (isto são as "definições indutivas em relações bem fundadas").

São, de fato, consequências desejáveis. Mas estas consequências desejáveis bastam para *justificar* a Substituição? *Não.* Ou pelo menos, não de forma direta.

Eis um problema simples. Embora tenhamos enunciado algumas consequências desejáveis da Substituição, muitas delas poderiam ter sido obtidas por outras vias. Isto não é tão conhecido como devia, pelo que convém explicar a situação.

Existe uma teoria simples de conjuntos, a Teoria dos Níveis, ou **LT** abreviadamente.[1] Os axiomas de **LT** são apenas Extensionalidade, Separação e a afirmação de que todo o conjunto é subconjunto de algum *nível*, onde "nível" é definido de modo astuto para que os níveis se comportem como os nossos amigos, os V_α. Logo **ZF** prova **LT**; mas **LT** é *muito* mais fraca que **ZF**. De fato, **LT** não dá Pares, Conjuntos potencia, Infinito nem Substituição. Seja **Zr** o resultado de acrescentar Infinito e Conjuntos potencia a **LT**; isto fornece também Pares, logo **Zr** é pelo menos tão forte quanto **Z**. Mas, de fato, **Zr** é estritamente mais forte que **Z**, pois acrescenta a afirmação de que todo o conjunto tem posto (daí a sugestão de o chamar **Zr**). De fato, **Zr** fornece: uma teoria perfeitamente satisfatória dos ordinais; resultados que estratificam a hierarquia em estágios bem ordenados; uma prova da indução-$\in$; e uma *versão* da recursão transfinita.

Em resumo: embora Boolos não soubesse disto, todas as consequências desejáveis que menciona poderiam ter sido obtidas *sem* Substituição; bastaria usar **Zr** em vez de **Z**.

(Diante disto, por que seguimos a rota convencional, ensinando-lhe **ZF** em vez de **LT** e **Zr**? Há duas razões. Primeiro: por razões puramente históricas, começar por **LT** é pouco standard; queríamos dotá-lo de ferramentas para ler discussões mais standard de teoria de conjuntos. Segundo: quando estiver preparado para apreciar **LT** e **Zr**, pode simplesmente ler Potter 2004 e Button 2021.)

Naturalmente, como **Zr** é estritamente mais fraca que **ZF**, há resultados que **ZF** prova e que **Zr** deixa em aberto. Logo alguém poderia tentar justificar a Substituição em bases extrínsecas apontando para um desses resultados. Mas, uma vez que saiba usar **Zr**, é bastante difícil encontrar muitos exemplos de coisas que (a) ficam decididas pela Substituição mas não de outro modo, e (b) são intuitivamente verdadeiras. (Para mais sobre isto, veja Potter 2004, §13.2.)

A conclusão é esta. Para fornecer uma justificação extrínseca convincente da Substituição, seria preciso encontrar um resultado que *não* possa ser obtido sem Substituição. E isso não é empresa fácil.

Consideremos um problema adicional que surge para qualquer tentativa de oferecer uma justificação puramente extrínseca da Substituição. (Este problema é talvez mais fundamental que o primeiro.) Boolos não se limita a observar que a Substituição tem muitas consequências desejáveis. Afirma também que a Substituição "(aparentemente) não tem" consequências indesejáveis. Mas

[1] As primeiras versões de **LT** são apresentadas por Montague (1965) e Scott (1974); foi simplificada e recebeu tratamento de livro por Potter (2004); e Button (2021) simplificou recentemente ainda mais **LT**.

esta ressalva entre parênteses, "aparentemente", é seguramente absolutamente crucial.

Relembre como chegamos aqui: a Compreensão ingênua encontrou inconsistência, e respondemos a essa inconsistência abraçando a concepção cumulativa-iterativa de conjunto. Esta concepção vem equipada com uma narrativa que, esperamos, nos assegura a sua consistência. Mas se não pudermos justificar a Substituição dentro dessa narrativa, então não temos (ainda) razão para crer que **ZF** é consistente. Ou melhor: não temos razão para crer que **ZF** é consistente, para além do fato (talvez meramente contingente) de que ninguém descobriu ainda uma contradição. Exatamente nesse sentido, o comentário de Boolos parece reduzir-se a isto: "(aparentemente) **ZF** é consistente". Deveríamos exigir maior garantia de consistência do que isto.

Esta questão afecta qualquer tentativa *puremente* extrínseca de justificar a Substituição, isto é, qualquer justificação formulada unicamente em termos das consequências (conhecidas) de **ZF**. Como tal, convém procurar uma justificação *intrínseca* da Substituição, isto é, uma justificação que sugira que a narrativa que contamos sobre conjuntos de algum modo "já" nos compromete com a Substituição.

5.4 Limitação de Tamanho

Talvez a tentativa mais comum de oferecer uma justificação "intrínseca" da Substituição passe pela seguinte noção: sth:replacement:limofsize:sec

> *Limitação-de-tamanho.* Quaisquer coisas formam um conjunto, desde que não haja demasiadas.

Este princípio vindicará de imediato a Substituição. Afinal, qualquer conjunto formado por Substituição não pode ser maior do que o conjunto a partir do qual foi formado. Enunciado com precisão: suponha que forma um conjunto $\tau[A] = \{\tau(x) : x \in A\}$ usando Substituição; então $\tau[A] \preceq A$; logo, se os membroos de A não eram demasiado numerosos para formar um conjunto, as suas imagens não são demasiado numerosas para formar $\tau[A]$.

A dificuldade óbvia em invocar *Limitação-de-tamanho* para justificar a Substituição é que *ainda* não estabelecemos qualquer princípio como *Limitação-de-tamanho*. Além disso, quando contamos a nossa história sobre a concepção cumulativa-iterativa de conjunto em Capítulos 1 a 2, nada *sugeriu* a direção de *Limitação-de-tamanho*. Isto é, de fato, precisamente a razão pela qual Boolos escreveu num dado momento: "Talvez se possa concluir que há pelo menos dois pensamentos 'por detrás' da teoria de conjuntos" (1989, p. 19). Por um lado, as ideias em torno da concepção cumulativa-iterativa de conjunto destinam-se a vindicar **Z**. Por outro, *Limitação-de-tamanho* visa vindicar a Substituição.

Mas a questão não é apenas termos estado até aqui *em silêncio* sobre *Limitação-de-tamanho*. Antes, a questão é que *Limitação-de-tamanho* (tal como acabamos de o formular) parece assentar mal com a noção cumulativa-iterativa

de conjunto. Afinal, não menciona nada sobre a ideia de conjuntos formados em *estágios*.

Isto não surpreende muito, dada a história destes "dois pensamentos" (isto é, a concepção cumulativa-iterativa de conjunto, e *Limitação-de-tamanho*). Estes "dois pensamentos" acabam por ser dois projetos bastante diferentes para bloquear os paradoxos da teoria de conjuntos. A noção cumulativa-iterativa de conjunto bloqueia o paradoxo de Russell dizendo, em traços largos: *nunca deveríamos ter esperado que existisse um conjunto de Russell, porque não seria "formado" em nenhum estágio*. Por contraste, *Limitação-de-tamanho* visa excluir o conjunto de Russell, dizendo, em traços largos: *nunca deveríamos ter esperado que existisse um conjunto de Russell, porque seria demasiado grande*.

Posto assim, sejamos diretos: considerada como resposta aos paradoxos, *Limitação-de-tamanho* carece de *muito* mais justificação. Considere, por exemplo, esta versão do paradoxo de Russell: *nenhum pug fareja exatamente os pugs que não se cheiram a si próprios* (ver Seção 1.2). Se perguntar "por que não há tal pug?", não é boa resposta dizer-lhe que tal pug teria de cheirar demasiados pugs. Logo por que seria boa explicação intuitiva, da não existência de um conjunto de Russell, que teria de ser "demasiado grande" para existir?

Em suma, é perdoável estar um pouco perplexo quanto à motivação "intuitiva" para *Limitação-de-tamanho*.

5.5 Substituição e "Infinito Absoluto"

sth:replacement:absinf:sec

Deixamos agora *Limitação-de-tamanho* para trás e exploramos uma outra família de tentativas (intrínsecas) de justificar a Substituição, que levam a sério a ideia de conjuntos formados em estágios.

Quando delineamos pela primeira vez o processo iterativo, oferecemos alguns princípios que explicam o que acontece em cada estágio. Foram *Estágios-são-chave*, *Estágios-são-ordenados*, e *Estágios-acumulam*. Mais tarde, acrescentamos alguns princípios que nos dizem algo sobre o número de estágios: *Estágios-prosseguem* disse-nos que o processo de formação de conjuntos nunca termina, e *Estágios-atingem-o-infinito* disse-nos que o processo passa por um estágio infinito-ésimo.

É razoável sugerir que estes dois últimos princípios decorrem de algum princípio mais amplo, como:

> *Estágios-são-inesgotáveis*. Há absolutamente infinitamente muitos estágios; a hierarquia é tão alta quanto possível.

Obviamente isto é um princípio informal. Mas mesmo que não seja imediatamente *implicado* pela concepção cumulativa-iterativa de conjunto, certamente parece *consonante* com ela. Pelo menos, e ao contrário de *Limitação-de-tamanho*, retém a ideia de que os conjuntos são formados estágio a estágio.

A esperança, agora, é alavancar *Estágios-são-inesgotáveis* numa justificação da Substituição. Vejamos como isso poderia fazer-se.

Na Seção 3.2, vimos que é fácil construir uma boa ordenação que (moralmente) deveria ser isomorfa a $\omega + \omega$. Dito de outro modo, podemos facilmente imaginar um processo iterativo estágio a estágio, cujo tipo de ordem (moralmente) é $\omega + \omega$. Como tal, se aceitamos *Estágios-são-inesgotáveis*, então deveríamos certamente aceitar que há pelo menos um estágio $\omega + \omega$-ésimo da hierarquia, isto é, $V_{\omega+\omega}$, pois a hierarquia seguramente *poderia* continuar até aqui.

Este pensamento generaliza-se como segue: para qualquer boa ordenação, o processo de construir a hierarquia iterativa deveria correr pelo menos tão longe quanto essa boa ordenação. E poderíamos garantir isto tratando Teorema 3.26 como um *axioma*. Isto diria-nos que toda a boa ordenação é isomorfa a um ordinal de von Neumann. Como cada ordinal de von Neumann será igual ao seu próprio posto, Teorema 3.26 dir-nos-á então que, sempre que possamos descrever uma boa ordenação na nossa teoria de conjuntos, o processo iterativo de formação de conjuntos tem de ultrapassar essa boa ordenação.

Esta ideia parece certamente um corolário de *Estágios-são-inesgotáveis*. Infelizmente, se o nosso objetivo é extrair a Substituição desta ideia, enfrentamos um obstáculo simples e técnico: a Substituição é estritamente mais forte que Teorema 3.26. (Esta observação é feita por Potter (2004, §13.2); prová-lo-emos na Seção 5.8.)

A conclusão é que, se vamos entender *Estágios-são-inesgotáveis* de modo a obter a Substituição, então não pode *meramente* dizer que a hierarquia ultrapassa qualquer boa ordenação. Tem de fazer uma afirmação mais forte. Com este fim, Shoenfield (1977) propôs um reforço muito natural da ideia, como segue: a hierarquia não é *cofinal* com nenhum conjunto.[2] Com um pouco mais de pormenor: se τ é um mapeamento que envia conjuntos para estágios da hierarquia, a imagem de qualquer conjunto A sob τ não esgota a hierarquia. Dito de outro modo (esquematicamente):

> *Estágios-são-supercofinais.* Se A é um conjunto e $\tau(x)$ é um estágio para todo o $x \in A$, então existe um estágio que vem depois de cada $\tau(x)$ para $x \in A$.

É óbvio que **ZF** prova uma versão adequadamente formalizada de *Estágios-são-supercofinais*. Reciprocamente, podemos argumentar informalmente que *Estágios-são-supercofinais* justifica a Substituição.[3] De fato, suponha $(\forall x \in A)\exists! y\, \varphi(x, y)$. Então, para cada $x \in A$, seja $\sigma(x)$ o y tal que $\varphi(x, y)$, e seja $\tau(x)$ o estágio em que $\sigma(x)$ é formado pela primeira vez. Por *Estágios-são-supercofinais*, existe um estágio V tal que $(\forall x \in A)\tau(x) \in V$. Ora, como cada $\tau(x) \in V$ e $\sigma(x) \subseteq \tau(x)$, por Separação podemos obter $\{y \in V : (\exists x \in A)\sigma(x) = y\} = \{y : (\exists x \in A)\varphi(x, y)\}$.

[2] Gödel parece ter proposto um pensamento semelhante; ver Potter (2004, p. 223). Para discussão de Gödel e Shoenfield, ver Incurvati (2020, 90–5).

[3] Seria mais difícil provar a Substituição usando alguma formalização de *Estágios-são-supercofinais*, pois **Z** por si só não é forte o suficiente para definir os estágios, logo não é claro como se formalizaria *Estágios-são-supercofinais*. Uma opção, contudo, é trabalhar nalguma extensão de **LT**, como discutido na Seção 5.3.

Problema 5.1. Apresente uma formalização de *Estágios-são-supercofinais* em **ZF**.

Logo *Estágios-são-supercofinais* vindica a Substituição. E é pelo menos plausível que *Estágios-são-inesgotáveis* vindique *Estágios-são-supercofinais*. De fato, suponha que *Estágios-são-supercofinais* falha. Logo a hierarquia é cofinal com algum conjunto A, isto é, temos uma aplicação τ tal que para qualquer estágio S existe algum $x \in A$ tal que $S \in \tau(x)$. Nesse caso, temos de fato uma forma de apreender o suposto "infinito absoluto" da hierarquia: ele é *esgotado* pela imagem de τ aplicada a A. E isso compromete a ideia de que a hierarquia é "absolutamente infinita". Contrapondo: *Estágios-são-inesgotáveis* implica *Estágios-são-supercofinais*, que por sua vez justifica a Substituição.

Isto representa uma tentativa genuinamente promissora de fornecer uma justificação intrínseca da Substituição. Mas se funciona ultimamente ou não, teremos de deixar para si decidir.

5.6 Substituição e Reflexão

sth:replacement:ref:sec

A nossa última tentativa de justificar a Substituição, via *Estágios-são-inesgotáveis*, começa com um resultado profundo e elegante:[4]

sth:replacement:ref:reflectionschema

Teorema 5.2 (Esquema de reflexão). *Para qualquer fórmula φ:*

$$\forall\alpha\exists\beta > \alpha(\forall x_1 \ldots, x_n \in V_\beta)(\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi^{V_\beta}(x_1, \ldots, x_n))$$

Como na Definição 5.1, φ^{V_β} é o resultado de restringir todos os quantificadores de φ ao conjunto V_β. Assim, intuitivamente, a Reflexão diz o seguinte: se φ é verdadeira em toda a hierarquia, então φ é verdadeira em arbitrariamente muitos *segmentos iniciais* da hierarquia.

Montague (1961) e Lévy (1960) mostraram que (formulações adequadas da) Substituição e da Reflexão são equivalentes, módulo **Z**, de modo que acrescentar qualquer uma delas dá **ZF**. (Provamos estes resultados na Seção 5.7.) Dada esta equivalência, poder-se-á esperar justificar a Reflexão e a Substituição via *Estágios-são-inesgotáveis* do seguinte modo: dado *Estágios-são-inesgotáveis*, a hierarquia deverá ser muito, muito alta; tão alta, de fato, que nada do que podemos dizer sobre ela é suficiente para limitar a sua altura. E podemos entender isto como a ideia de que, se qualquer sentença φ é verdadeira em toda a hierarquia, então é verdadeira em arbitrariamente muitos segmentos iniciais da hierarquia. E isso é precisamente a Reflexão.

De novo, isto parece uma tentativa genuinamente promissora de fornecer uma justificação intrínseca da Substituição. Mas há demasiado a dizer sobre o assunto aqui. Cabe-lhe agora decidir por si se tem êxito.[5]

[4] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação explícita em contrário).

[5] Poderá, no entanto, querer continuar lendo Incurvati (2020, 95–100).

5.7 Apêndice: Resultados sobre Substituição

A seguir, provaremos a Reflexão dentro de **ZF**. Provaremos também em que sentido a Reflexão é equivalente à Substituição. E provaremos uma consequência interessante de tudo isto, relativa à força da Reflexão/Substituição. *Aviso: isto é, de longe, a parte mais avançada de matemática deste manual.* sth:replacement:refproofs:sec

Começamos com um lema que, por brevidade, recorre ao expediente notacional do *sobrelinhado* para lidar com sequências de variáveis ou objetos. Assim: "$\overline{a}_k$" abrevia "$a_{k_1}, \ldots, a_{k_n}$", onde n é determinado pelo contexto.

Lema 5.3. *Para cada $1 \leq i \leq k$, seja $\varphi_i(\overline{v}_i, x)$ uma fórmula. Então, para cada α existe algum $\beta > \alpha$ tal que, para quaisquer $\overline{a}_1, \ldots, \overline{a}_k \in V_\beta$ e cada $1 \leq i \leq k$:* sth:replacement:refproofs:lemreflection

$$\exists x \varphi_i(\overline{a}_i, x) \to (\exists x \in V_\beta)\varphi_i(\overline{a}_i, x)$$

Prova. Definimos um termo μ como segue: $\mu(\overline{a}_1, \ldots, \overline{a}_k)$ é o estágio mínimo, V, que satisfaz todos os seguintes condicionais, para $1 \leq i \leq k$:

$$\exists x \varphi_i(\overline{a}_i, x) \to (\exists x \in V)\varphi_i(\overline{a}_i, x))$$

É fácil verificar que $\mu(\overline{a}_1, \ldots, \overline{a}_k)$ existe para todos $\overline{a}_1, \ldots, \overline{a}_k$. Ora, usando a Substituição e o nosso teorema de recursão, definimos:

$$\begin{aligned} S_0 &= V_{\alpha+1} \\ S_{n+1} &= S_n \cup \bigcup \{\mu(\overline{a}_1, \ldots, \overline{a}_k) : \overline{a}_1, \ldots, \overline{a}_k \in S_n\} \\ S &= \bigcup_{m<\omega} S_n. \end{aligned}$$

Cada S_n, e portanto o próprio S, é um estágio depois de V_α. Fixemos $\overline{a}_1$, $\ldots$, $\overline{a}_k \in S$; logo existe algum $n < \omega$ tal que $\overline{a}_1$, $\ldots$, $\overline{a}_k \in S_n$. Fixemos algum $1 \leq i \leq k$, e suponhamos que $\exists x \varphi_i(\overline{a}_i, x)$. Então $(\exists x \in \mu(\overline{a}_1, \ldots, \overline{a}_k))\varphi_i(\overline{a}_i, x)$ por construção, logo $(\exists x \in S_{n+1})\varphi_i(\overline{a}_i, x)$ e portanto $(\exists x \in S)\varphi_i(\overline{a}_i, x)$. Logo S é o nosso V_β. □

Podemos agora provar Teorema 5.2 de forma bastante direta:

Prova. Fixemos α. Sem perda de generalidade, podemos assumir que os únicos conectivos de φ são $\exists$, $\neg$ e $\wedge$ (pois estes são expressivamente adequados). Sejam $\psi_1, \ldots, \psi_k$ uma enumeração de cada uma das subfórmulas de φ por ordem de complexidade, de modo que $\psi_k = \varphi$. Por Lema 5.3, existe um $\beta > \alpha$ tal que, para qualquer $\overline{a}_i \in V_\beta$ e cada $1 \leq i \leq k$:

$$\exists x \psi_i(\overline{a}_i, x) \to (\exists x \in V_\beta)\psi_i(\overline{a}_i, x) \tag{*}$$

Por indução na complexidade de ψ_i, mostraremos que $\psi_i(\overline{a}_i) \leftrightarrow \psi_i^{V_\beta}(\overline{a}_i)$, para qualquer $\overline{a}_i \in V_\beta$. Se ψ_i é atómica, isto é trivial. A bicondicional estabelece

também que, quando ψ_i é uma negação ou conjunção de subfórmulas que satisfazem esta propriedade, a própria ψ_i satisfaz esta propriedade. Logo o único caso interessante é o da quantificação. Fixemos $\overline{a}_i \in V_\beta$; então:

$$\begin{aligned}
(\exists x \psi_i(\overline{a}_i, x))^{V_\beta} &\text{ sse } (\exists x \in V_\beta)\psi_i^{V_\beta}(\overline{a}_i, x) && \text{por definição}\\
&\text{sse } (\exists x \in V_\beta)\psi_i(\overline{a}_i, x) && \text{por hipótese}\\
&\text{sse } \exists x \psi_i(\overline{a}_i, x) && \text{por (*)}
\end{aligned}$$

Isto completa a indução; o resultado segue pois $\psi_k = \varphi$. □

Provamos a Reflexão em **ZF**. A nossa prova seguiu essencialmente Montague (1961). Queremos agora provar em **Z** que a Reflexão implica a Substituição. A prova segue Lévy (1960), com uma simplificação.

Como trabalhamos em **Z**, não podemos apresentar a Reflexão exatamente na forma dada acima. Afinal, formulamos a Reflexão usando a notação "V_α", e isso não pode ser definido em **Z** (ver Seção 4.5). Em vez disso, ofereceremos uma formulação aparentemente mais fraca da Substituição, como segue:

> *Reflexão fraca.* Para qualquer fórmula φ, existe um conjunto transitivo S tal que 0, 1 e quaisquer parâmetros de φ são membroos de S, e $(\forall \overline{x} \in S)(\varphi \leftrightarrow \varphi^S)$.

Para usar isto na prova da Substituição, seguiremos primeiro Lévy (1960, primeira parte do Teorema 2) e mostraremos que podemos "refletir" duas fórmulas de uma vez:

sth:replacement:refproofs: lem:reflect

Lema 5.4 (em Z + Reflexão fraca.). *Para quaisquer fórmulas ψ, χ, existe um conjunto transitivo S tal que* 0 *e* 1 *(e quaisquer parâmetros das fórmulas) são membroos de S, e $(\forall \overline{x} \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))$.*

Prova. Seja φ a fórmula $(z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)$.

Aqui usamos uma abreviatura; devemos explicitar "$z = 0$" como "$\forall t\, t \notin z$" e "$z = 1$" como "$\forall s(s \in z \leftrightarrow \forall t\, t \notin s)$". Mas como $0, 1 \in S$ e S é transitivo, estas fórmulas são *absolutas* para S; isto é, aplicam-se ao mesmo objeto quer restrinjamos os seus quantificadores a S.[6]

Pela Reflexão fraca, temos algum S adequado tal que:

$$\begin{aligned}
&(\forall z, \overline{x} \in S)(\varphi \leftrightarrow \varphi^S)\\
\text{isto é } &(\forall z, \overline{x} \in S)(((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)) \leftrightarrow\\
&\qquad ((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi))^S)\\
\text{isto é } &(\forall z, \overline{x} \in S)(((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)) \leftrightarrow\\
&\qquad ((z = 0 \wedge \psi^S) \vee (z = 1 \wedge \chi^S)))\\
\text{isto é } &(\forall \overline{x} \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))
\end{aligned}$$

[6] Mais formalmente, seja ξ qualquer uma destas fórmulas; então $\xi(z) \leftrightarrow \xi^S(z)$.

A segunda afirmação implica a terceira porque "$z = 0$" e "$z = 1$" são absolutas para S; a quarta segue pois $0 \neq 1$. □

Podemos agora obter a Substituição, seguindo e simplificando Lévy (1960, Teorema 6):

Teorema 5.5 (em Z + Reflexão fraca). *Para qualquer fórmula $\varphi(v, w)$, e qualquer A, se $(\forall x \in A)\exists! y\, \varphi(x, y)$, então $\{y : (\exists x \in A)\varphi(x, y\}$ existe.*

Prova. Fixemos A tal que $(\forall x \in A)\exists! y\, \varphi(x, y)$, e definimos fórmulas:

$$\psi \text{ é } (\varphi(x, z) \wedge A = A)$$
$$\chi \text{ é } \exists y\, \varphi(x, y)$$

Usando Lema 5.4, como A é um parâmetro de ψ, existe um conjunto transitivo S tal que $0, 1, A \in S$ (juntamente com quaisquer outros parâmetros), e tal que:

$$(\forall x, z \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))$$

Logo, em particular:

$$(\forall x, z \in S)(\varphi(x, z) \leftrightarrow \varphi^S(x, z))$$
$$(\forall x \in S)(\exists y \varphi(x, y) \leftrightarrow (\exists y \in S)\varphi^S(x, y))$$

Combinando isto, e observando que $A \subseteq S$ pois $A \in S$ e S é transitivo:

$$(\forall x \in A)(\exists y \varphi(x, y) \leftrightarrow (\exists y \in S)\varphi(x, y))$$

Ora, $(\forall x \in A)(\exists! y \in S)\varphi(x, y)$, porque $(\forall x \in A)\exists! y\, \varphi(x, y)$. Ora, a Separação dá $\{y \in S : (\exists x \in A)\varphi(x, y)\} = \{y : (\exists x \in A)\varphi(x, y)\}$. □

5.8 Apêndice: Axiomatizabilidade finita

Terminamos este capítulo extraindo alguns resultados da Substituição. O primeiro resultado é devido a Montague (1961); note que não é uma prova *dentro* de **ZF**, mas uma prova *sobre* **ZF**:

sth:replacement:finiteaxiomatizasec

Teorema 5.6. **ZF** *não é finitamente axiomatizável. Mais geralmente: se* **T** *é finita e* $\mathbf{T} \vdash \mathbf{ZF}$*, então* **T** *é inconsistente.*

sth:replacement:finiteaxiomatizabzfnotfinitely

(Aqui nos restringimos tacitamente a sentenças de primeira ordem cujo único primitivo não lógico é $\in$, e escrevemos $\mathbf{T} \vdash \mathbf{ZF}$ *para indicar que* $\mathbf{T} \vdash \varphi$ *para todo o* $\varphi \in \mathbf{ZF}$*.)*

Prova. Fixemos **T** finita tal que $\mathbf{T} \vdash \mathbf{ZF}$. Logo **T** prova a Reflexão, isto é, Teorema 5.2. Como **T** é finita, podemos reescrevê-la como uma única conjunção, θ. Refletindo com esta fórmula, $\mathbf{T} \vdash \exists\beta(\theta \leftrightarrow \theta^{V_\beta})$. Como trivialmente $\mathbf{T} \vdash \theta$, obtemos $\mathbf{T} \vdash \exists\beta\ \theta^{V_\beta}$.

Ora, seja $\psi(X)$ uma abreviatura de:

$$\theta^X \wedge X \text{ é transitivo} \wedge (\forall Y \in X)(Y \text{ é transitivo} \to \neg\theta^Y)$$

isto diz, em traços largos: X é um modelo transitivo de θ, e $\in$-minimal a esse respeito. Ora, recordando que $\mathbf{T} \vdash \exists\beta\ \theta^{V_\beta}$, por fatos básicos sobre postos dentro de **ZF** e portanto dentro de **T**, temos:

$$\mathbf{T} \vdash \exists M \psi(M). \tag{*}$$

Usando o primeiro conjunto de $\psi(X)$, sempre que $\mathbf{T} \vdash \sigma$, temos $\mathbf{T} \vdash \forall X(\psi(X) \to \sigma^X)$. Logo, por (*):

$$\mathbf{T} \vdash \forall X(\psi(X) \to (\exists N \psi(N))^X)$$

Usando isto, e (*) de novo:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \psi(N))^M)$$

Em particular, então:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \in M)((N \text{ é transitivo})^N \wedge (\theta^N)^M))$$

Logo, por raciocínio elementar sobre transitividade:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \in M)(N \text{ é transitivo} \wedge \theta^N))$$

Logo **T** é inconsistente.[7] □

Eis um resultado semelhante, assinalado por Potter (2004, 223):

replacement:finiteaxiomatizability: finiteextensionofZ

Proposição 5.7. *Seja* **T** *uma extensão de* **Z** *com um número finito de novos axiomas. Se* $\mathbf{T} \vdash$ **ZF**, *então* **T** *é inconsistente. (Aqui usamos as mesmas restrições tácitas que para Teorema 5.6.)*

Prova. Usemos θ para a conjunção de todos os axiomas de **T** *exceto* as (infinitas) instâncias de Separação. Definindo ψ a partir de θ como no Teorema 5.6, podemos mostrar que $\mathbf{T} \vdash \exists M \psi(M)$.

Como no Teorema 5.6, podemos estabelecer o esquema de que, sempre que $\mathbf{T} \vdash \sigma$, temos $\mathbf{T} \vdash \forall X(\psi(X) \to \sigma^X)$. Terminamos a prova exatamente como no Teorema 5.6.

No entanto, estabelecer o esquema envolve um pouco mais de trabalho do que no Teorema 5.6. Afinal, as instâncias de Separação estão em **T**, mas não são conjuntos de θ. Contudo, podemos ultrapassar este obstáculo provando que $\mathbf{T} \vdash \forall X(X \text{ é transitivo} \to \sigma^X)$, para toda a instância de Separação σ. Deixamos isto ao leitor. □

[7] Este "raciocínio elementar" envolve provar certos "fatos de absolutidade" para conjuntos transitivos.

Problema 5.2. Mostre que, para toda a instância de Separação σ, tem-se: $\mathbf{Z} \vdash \forall X(X \text{ é transitivo} \to \sigma^X)$. (Usamos este esquema na Proposição 5.7.)

Problema 5.3. Mostre que, para todo o $\varphi \in \mathbf{Z}$, tem-se $\mathbf{ZF} \vdash \varphi^{V_{\omega+\omega}}$.

Problema 5.4. Confirme os restantes resultados esquemáticos invocados nas provas de Teorema 5.6 e Proposição 5.7.

Como observamos na Seção 5.5, isto mostra que a Substituição é estritamente mais forte que Teorema 3.26. Ou, um pouco mais precisamente: se $\mathbf{Z}$ + "toda a boa ordenação é isomorfa a um ordinal único" for consistente, então não prova alguma instância da Substituição.

Capítulo 6

Aritmética Ordinal

6.1 Introdução

sth:ord-arithmetic:intro:sec

No Capítulo 3, desenvolvemos uma teoria dos números ordinais. Vimos no Capítulo 4 que podemos pensar nos ordinais como uma espinha dorsal em torno da qual se constrói o restante da hierarquia. Mas esse não é o único papel dos ordinais. Há também a tarefa de efetuar a aritmética ordinal.

Já aludimos a isto, em Seção 3.2, quando falamos de ω, $\omega + 1$ e $\omega + \omega$. Na altura falamos informalmente; chegou a altura de o expor com rigor. Devemos contudo mencionar que não há muita filosofia neste capítulo; apenas desenvolvimentos técnicos, juntamente com uma observação (ligeiramente) interessante de que podemos fazer a mesma coisa de duas maneiras diferentes.

6.2 Adição Ordinal

sth:ord-arithmetic:add:sec

Suponha-se que se pretende somar α e β. Pode simplesmente colocar-se uma cópia de β imediatamente a seguir a uma cópia de α. (É preciso tomar *cópias*, pois sabemos por Proposição 3.22 que ou $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$.) O efeito intuitivo disto é percorrer uma α-sucessão de passos, *e depois* percorrer uma β-sucessão. A sucessão resultante fica bem ordenada; logo, por Teorema 3.26 é isomorfa a um ordinal (único). Esse ordinal pode considerar-se a *soma* de α e β.

Esta é a ideia intuitiva por detrás da adição ordinal. Para a definir com rigor, começa-se pela ideia de tomar *cópias* de conjuntos. A ideia é usar etiquetas arbitrárias, 0 e 1, para saber de onde veio cada objeto:

sth:ord-arithmetic:add:defdissum

Definição 6.1. A *soma disjunta* de A e B é $A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$.

Define-se em seguida uma ordem em pares de ordinais:

Definição 6.2. Para quaisquer ordinais $\alpha_1, \alpha_2, \beta_1, \beta_2$, diga-se que:

$$\langle \alpha_1, \alpha_2 \rangle \lhd \langle \beta_1, \beta_2 \rangle \text{ sse ou } \alpha_2 \in \beta_2$$
$$\text{ou tanto } \alpha_2 = \beta_2 \text{ como } \alpha_1 \in \beta_1$$

Trata-se de uma ordem *lexicográfica inversa*, pois ordena-se pelo segundo elemento e depois pelo primeiro. Recorde-se que se pretendia definir $\alpha + \beta$ como o tipo de ordem de uma cópia de α seguida de uma cópia de β. Para o conseguir, define-se:

Definição 6.3. Para quaisquer ordinais α, β, a sua soma é $\alpha+\beta = \mathrm{ord}(\alpha \sqcup \beta, \lhd)$. sth:ord-arithmetic:add:defordplus

Note-se que aqui se abusou ligeiramente da notação; estritamente deveria escrever-se "$\{\langle x, y\rangle \in \alpha \sqcup \beta : x \lhd y\}$" em lugar de "$\lhd$". Por brevidade, contudo, continuaremos a abusar da notação deste modo no que se segue.

O resultado seguinte, juntamente com Teorema 3.26, confirma que a nossa definição está bem formada:

Lema 6.4. *$\langle \alpha \sqcup \beta, \lhd\rangle$ é um bom ordenamento, para quaisquer ordinais α e β.* sth:ord-arithmetic:add:ordsumlessiswo

Prova. Obviamente $\lhd$ é conexa em $\alpha \sqcup \beta$. Para mostrar que é bem fundada, fixe-se um $X \subseteq \alpha \sqcup \beta$ não vazio. Seja Y o subconjunto de X cuja segunda coordenada é a menor possível, isto é, $Y = \{\langle \gamma, i\rangle \in X : (\forall \langle \delta, j\rangle \in X) i \leq j\}$. Escolha-se agora o elemento de Y com menor primeira coordenada. □

Temos assim uma definição explícita e clara da adição ordinal. Eis um fato não surpreendente (recorde-se que $1 = \{0\}$, por Definição 2.7):

Proposição 6.5. *$\alpha + 1 = \alpha^+$, para qualquer ordinal α.*

Prova. Considere-se o isomorfismo f de $\alpha^+ = \alpha \cup \{\alpha\}$ para $\alpha \sqcup 1 = (\alpha \times \{0\}) \sqcup (\{0\} \times \{1\})$ dado por $f(\gamma) = \langle \gamma, 0\rangle$ para $\gamma \in \alpha$, e $f(\alpha) = \langle 0, 1\rangle$. □

Além disso, é fácil mostrar que a adição obedece a certas condições recursivas:

Lema 6.6. *Para quaisquer ordinais α, β, tem-se:* sth:ord-arithmetic:add:ordadditionrecursion

$$\begin{aligned} \alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \\ \alpha + \beta &= \operatorname*{lsub}_{\delta<\beta}(\alpha + \delta) \qquad \text{se } \beta \text{ é um ordinal limite} \end{aligned}$$

Prova. Verifica-se caso a caso; primeiro:

$$\begin{aligned} \alpha + 0 &= \mathrm{ord}((\alpha \times \{0\}) \cup (0 \times \{1\}), \lhd) \\ &= \mathrm{ord}((\alpha \times \{0\}) \cup \{0\}, \lhd) \\ &= \alpha \\ \alpha + (\beta + 1) &= \mathrm{ord}((\alpha \times \{0\}) \cup (\beta^+ \times \{1\}), \lhd) \\ &= \mathrm{ord}((\alpha \times \{0\}) \cup (\beta \times \{1\}), \lhd) + 1 \\ &= (\alpha + \beta) + 1 \end{aligned}$$

Seja agora $\beta \neq \emptyset$ um limite. Se $\delta < \beta$ então também $\delta + 1 < \beta$, logo $\alpha + \delta$ é um segmento inicial próprio de $\alpha + \beta$. Logo $\alpha + \beta$ é um majorante estrito de $X = \{\alpha + \delta : \delta < \beta\}$. Além disso, se $\alpha \leq \gamma < \alpha + \beta$, então claramente $\gamma = \alpha + \delta$ para algum $\delta < \beta$. Logo $\alpha + \beta = \operatorname{lsub}_{\delta<\beta}(\alpha + \delta)$. □

Mas eis um fato marcante. Para definir a adição ordinal, poder-se-ia *em alternativa* ter usado simplesmente o teorema da recursão transfinita, e estipulado as equações recursivas, exatamente como em Lema 6.6 (embora com "β^+" em vez de "$\beta + 1$").

Há, pois, duas maneiras diferentes de definir operações nos ordinais. Podem definir-se *sinteticamente*, construindo explicitamente um conjunto bem ordenado e considerando o seu tipo de ordem. Ou podem definir-se *recursivamente*, apenas estipulando as equações recursivas. Feito corretamente, porém, o resultado é idêntico. De fato, Teorema 3.26 garante que estas equações recursivas determinam ordinais *únicos*.

Em muitos aspectos, a aritmética ordinal comporta-se como a adição dos números naturais. Por exemplo, pode provar-se o seguinte:

sth:ord-arithmetic:add:ordinaladditionisnice
sth:ord-arithmetic:add:ordaddition1
sth:ord-arithmetic:add:ordaddition2
sth:ord-arithmetic:add:ordaddition3
sth:ord-arithmetic:add:ordaddition4

Lema 6.7. *Se α, β, γ são ordinais, então:*

1. *se $\beta < \gamma$, então $\alpha + \beta < \alpha + \gamma$*
2. *se $\alpha + \beta = \alpha + \gamma$, então $\beta = \gamma$*
3. *$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, isto é, a adição é associativa*
4. *Se $\alpha \leq \beta$, então $\alpha + \gamma \leq \beta + \gamma$*

Prova. Provamos (3), deixando o resto como exercício. A prova é por indução transfinita simples em γ, usando Lema 6.6. Quando $\gamma = 0$:

$$(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0)$$

Quando $\gamma = \delta + 1$, suponha-se por indução que $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$; usando Lema 6.6 três vezes:

$$\begin{aligned}(\alpha + \beta) + (\delta + 1) &= ((\alpha + \beta) + \delta) + 1 \\ &= (\alpha + (\beta + \delta)) + 1 \\ &= \alpha + ((\beta + \delta) + 1) \\ &= \alpha + (\beta + (\delta + 1))\end{aligned}$$

Quando γ é um ordinal limite, suponha-se por indução que se $\delta \in \gamma$ então $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$; então:

$$\begin{aligned}(\alpha + \beta) + \gamma &= \operatorname*{lsub}_{\delta<\gamma}((\alpha + \beta) + \delta) \\ &= \operatorname*{lsub}_{\delta<\gamma}(\alpha + (\beta + \delta)) \\ &= \alpha + \operatorname*{lsub}_{\delta<\gamma}(\beta + \delta) \\ &= \alpha + (\beta + \gamma)\end{aligned}$$

□

Problema 6.1. Prove o resto de Lema 6.7.

Deste modo, a adição ordinal deve parecer muito familiar. Há contudo um ponto crucial em que a adição ordinal *não* se parece com a adição nos naturais.

Proposição 6.8. *A adição ordinal* não *é comutativa;* $1 + \omega = \omega < \omega + 1$. sth:ord-arithmetic:add:ordsumnotcommute

Prova. Note-se que $1 + \omega = \operatorname{lsub}_{n<\omega}(1 + n) = \omega \in \omega \cup \{\omega\} = \omega^+ = \omega + 1$. □

Embora isto possa surpreender à primeira vista, *não devia*. Por um lado, ao considerar $1 + \omega$, pensa-se no tipo de ordem que se obtém colocando um elemento extra *antes* de todos os números naturais. Raciocinando como com o Hotel de Hilbert em **??**, intuitivamente esse primeiro elemento extra não altera o tipo de ordem global. Por outro lado, ao considerar $\omega+1$, pensa-se no tipo de ordem que se obtém colocando um elemento extra *depois* de todos os números naturais. E isso é algo radicalmente diferente!

6.3 Usando Adição Ordinal

Com a adição nos ordinais, podemos calcular explicitamente os postos de vários conjuntos, no sentido de Definição 4.15: sth:ord-arithmetic:using-additionsec

Lema 6.9. *Se* $\operatorname{posto}(A) = \alpha$ *e* $\operatorname{posto}(B) = \beta$*, então:* sth:ord-arithmetic:using-additionrankcomputation

1. $\operatorname{posto}(\wp(A)) = \alpha + 1$ sth:ord-arithmetic:using-additionexrankpow
2. $\operatorname{posto}(\{A, B\}) = \max(\alpha, \beta) + 1$ sth:ord-arithmetic:using-additionexrankpair
3. $\operatorname{posto}(A \cup B) = \max(\alpha, \beta)$ sth:ord-arithmetic:using-additionexrankcup
4. $\operatorname{posto}(\langle A, B\rangle) = \max(\alpha, \beta) + 2$ sth:ord-arithmetic:using-additionexranktuple
5. $\operatorname{posto}(A \times B) \leq \max(\alpha, \beta) + 2$ sth:ord-arithmetic:using-additionexranktimes
6. $\operatorname{posto}(\bigcup A) = \alpha$ *quando* α *é vazio ou limite;* $\operatorname{posto}(\bigcup A) = \gamma$ *quando* $\alpha = \gamma + 1$ sth:ord-arithmetic:using-additionexrankunion

Prova. Ao longo de todo o raciocínio, invocamos repetidamente Proposição 4.20.

(1). Se $x \subseteq A$ então $\operatorname{posto}(x) \leq \operatorname{posto}(A)$. Logo $\operatorname{posto}(\wp(A)) \leq \alpha + 1$. Como em particular $A \in \wp(A)$, tem-se $\operatorname{posto}(\wp(A)) = \alpha + 1$.

(2). Por Proposição 4.20

(3). Por Proposição 4.20.

(4). Por (2), duas vezes.

(5). Note-se que $A \times B \subseteq \wp(\wp(A \cup B))$, e invoque (4).

(6). Se $\alpha = \gamma + 1$, existe algum $c \in A$ com $\operatorname{posto}(c) = \gamma$, e nenhum membro de A tem posto superior; logo $\operatorname{posto}(\bigcup A) = \gamma$. Se α é um ordinal limite, então A tem membros com posto arbitrariamente próximo (mas estritamente inferior) de α, pelo que $\bigcup A$ também tem membros com posto arbitrariamente próximo (mas estritamente inferior) de α, e portanto $\operatorname{posto}(\bigcup A) = \alpha$. □

Deixamos como exercício mostrar por que (5) envolve uma *des*igualdade.

Problema 6.2. Exiba conjuntos A e B tais que $\operatorname{posto}(A\times B) = \max(\operatorname{posto}(A), \operatorname{posto}(B))$.
Exiba conjuntos A e B tais que $\operatorname{posto}(A \times B) = \max(\operatorname{posto}(A), \operatorname{posto}(B)) + 2$.
São possíveis outros postos?

Estamos também agora em condições de mostrar que várias noções razoáveis do que possa significar descrever um ordinal como "finito" ou "infinito" coincidem:

sth:ord-arithmetic:using-addition:ordinfinitycharacter

Lema 6.10. *Para qualquer ordinal α, as seguintes afirmações são equivalentes:*

1. $\alpha \notin \omega$, *isto é,* α *não é um número natural*
2. $\omega \leq \alpha$
3. $1 + \alpha = \alpha$
4. $\alpha \approx \alpha + 1$, *isto é,* α *e* $\alpha + 1$ *são equipotentes*
5. α *é infinito de Dedekind*

sth:ord-arithmetic:using-addition:ord:notinomega
sth:ord-arithmetic:using-addition:ord:omegaplus
sth:ord-arithmetic:using-addition:ord:oneplus
sth:ord-arithmetic:using-addition:ord:plusone
sth:ord-arithmetic:using-addition:ord:infinite

Temos assim cinco formas provavelmente equivalentes de precisar o que exige que um ordinal seja (in)finito.

Prova. *(1)* $\Rightarrow$ *(2).* Por tricotomia.

(2) $\Rightarrow$ *(3).* Fixe $\alpha \geq \omega$. Por indução transfinita, existe um ordinal γ mínimo (possivelmente 0) tal que existe um ordinal limite β com $\alpha = \beta + \gamma$. Ora:

$$1 + \alpha = 1 + (\beta + \gamma) = (1 + \beta) + \gamma = \operatorname*{lsub}_{\delta<\beta}(1 + \delta) + \gamma = \beta + \gamma = \alpha.$$

(3) $\Rightarrow$ *(4).* Existe claramente uma bijeção $f\colon (\alpha \sqcup 1) \to (1 \sqcup \alpha)$. Se $1 + \alpha = \alpha$, existe um isomorfismo $g\colon (1 \sqcup \alpha) \to \alpha$. Considere-se $g \circ f$.

(4) $\Rightarrow$ *(5).* Se $\alpha \approx \alpha + 1$, existe uma bijeção $f\colon (\alpha \sqcup 1) \to \alpha$. Defina $g(\gamma) = f(\gamma, 0)$ para cada $\gamma < \alpha$; esta injeção mostra que α é infinito de Dedekind, pois $f(0, 1) \in \alpha \setminus \operatorname{Im}(g)$.

(5) $\Rightarrow$ *(1).* Isto é Proposição 2.8. □

6.4 Multiplicação Ordinal

sth:ord-arithmetic:mult:sec

Passamos agora à multiplicação ordinal, abordando-a de forma muito semelhante à adição ordinal. Suponha-se que se pretende multiplicar α por β. Pode imaginar-se uma grelha retangular, com largura α e altura β; o produto de α e β é então o resultado de percorrer cada linha e depois passar à linha seguinte... até percorrer toda a grelha. Dito de outro modo, o produto de α e β obtém-se substituindo *cada* elemento de β por uma cópia de α.

Para formalizar, usa-se simplesmente a ordem lexicográfica inversa no produto cartesiano de α e β:

Definição 6.11. Para quaisquer ordinais α, β, o seu produto $\alpha \cdot \beta = \mathrm{ord}(\alpha \times \beta, \lhd)$.

É preciso de novo confirmar que esta definição está bem formada:

Lema 6.12. *$\langle \alpha \times \beta, \lhd \rangle$ é um bom ordenamento, para quaisquer ordinais α e β.* sth:ord-arithmetic:mult:ordtimeslessiswo

Prova. Exatamente como para Lema 6.4. □

E não é difícil provar que a multiplicação se comporta assim:

Lema 6.13. *Para quaisquer ordinais α, β:* sth:ord-arithmetic:mult:ordtimesrecursion

$$\begin{aligned} \alpha \cdot 0 &= 0 \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \beta &= \operatorname{lsub}_{\delta < \beta}(\alpha \cdot \delta) \qquad \text{quando } \beta \text{ é um ordinal limite.} \end{aligned}$$

Prova. Deixado como exercício. □

De fato, tal como no caso da adição, poderíamos ter definido a multiplicação ordinal por estas equações recursivas, em vez de dar uma definição direta. Tal como na adição, certo comportamento é familiar:

Lema 6.14. *Se α, β, γ são ordinais, então:* sth:ord-arithmetic:mult:ordinalmultiplicationisnice

1. *se $\alpha \neq 0$ e $\beta < \gamma$, então $\alpha \cdot \beta < \alpha \cdot \gamma$;* sth:ord-arithmetic:mult:ordtimes1
2. *se $\alpha \neq 0$ e $\alpha \cdot \beta = \alpha \cdot \gamma$, então $\beta = \gamma$;* sth:ord-arithmetic:mult:ordtimes2
3. *$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$;* sth:ord-arithmetic:mult:ordtimes3
4. *Se $\alpha \leq \beta$, então $\alpha \cdot \gamma \leq \beta \cdot \gamma$;* sth:ord-arithmetic:mult:ordtimes4
5. *$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.* sth:ord-arithmetic:mult:ordtimes5

Prova. Deixado como exercício. □

Pode provar-se (ou consultar) outros resultados, à vontade. Mas, dado Proposição 6.8, o que se segue não deve surpreender:

Proposição 6.15. *A multiplicação ordinal não é comutativa: $2 \cdot \omega = \omega < \omega \cdot 2$*

Prova. $2 \cdot \omega = \operatorname{lsub}_{n<\omega}(2 \cdot n) = \omega \in \operatorname{lsub}_{n<\omega}(\omega + n) = \omega + \omega = \omega \cdot 2$. □

De novo, a justificação intuitiva é direta. Para calcular $2 \cdot \omega$, substitui-se cada número natural por duas entidades. Obtém-se o mesmo tipo de ordem se simplesmente se inserirem todos os números "meios" nos naturais, isto é, se se considerar a ordem natural em $\{n/2 : n \in \omega\}$. Assim posto, o tipo de ordem é claramente o mesmo que o de ω em si. Mas, para calcular $\omega \cdot 2$, dispõem-se duas cópias de ω, uma a seguir à outra.

Problema 6.3. Prove Lema 6.12, Lema 6.13, e Lema 6.14

6.5 Exponenciação Ordinal

sth:ord-arithmetic:expo:sec

Passamos agora à exponenciação ordinal. Infelizmente, não há uma definição *simpática* sintética para a exponenciação ordinal.

Certo que *existem* definições sintéticas explícitas. Eis uma. Seja $\mathrm{finfun}(\alpha, \beta)$ o conjunto de todas as funções $f\colon \alpha \to \beta$ tais que $\{\gamma \in \alpha : f(\gamma) \neq 0\}$ é equipotente a algum número natural. Defina-se um bom ordenamento em $\mathrm{finfun}(\alpha, \beta)$ por $f \sqsubset g$ sse $f \neq g$ e $f(\gamma_0) < g(\gamma_0)$, onde $\gamma_0 = \max\{\gamma \in \alpha : f(\gamma) \neq g(\gamma)\}$. Então pode definir-se $\alpha^{(\beta)}$ como $\mathrm{ord}(\mathrm{finfun}(\alpha, \beta), \sqsubset)$. Potter usa esta definição explícita e explica de seguida:

> A escolha desta ordenação determina-se unicamente pelo desejo de obter uma definição da exponenciação ordinal que obedeça à condição recursiva adequada. . . , e é muito mais difícil de visualizar do que a soma ou o produto ordenados. (Potter, 2004, p. 199)

Exatamente. Explicamos a adição como "uma cópia de α seguida de uma cópia de β", e a multiplicação como "uma β-sucessão de cópias de α". Mas não temos nada de sucinto a dizer sobre $\mathrm{finfun}(\alpha, \gamma)$. Por isso, apresentaremos a definição da exponenciação ordinal apenas *por* recursão transfinita, isto é:

sth:ord-arithmetic:expo:ordexporecursion

Definição 6.16.

$$\begin{aligned} \alpha^{(0)} &= 1 \\ \alpha^{(\beta+1)} &= \alpha^{(\beta)} \cdot \alpha \\ \alpha^{(\beta)} &= \bigcup_{\delta<\beta} \alpha^{(\delta)} \qquad \text{quando } \beta \text{ é um ordinal limite} \end{aligned}$$

Se trabalhássemos *como* teoristas de conjuntos, poderíamos querer explorar algumas propriedades da exponenciação ordinal. Mas pouco mais temos a acrescentar, salvo notar o fato pouco surpreendente de que a exponenciação ordinal não comuta. Assim $2^{(\omega)} = \bigcup_{\delta<\omega} 2^{(\delta)} = \omega$, enquanto $\omega^{(2)} = \omega \cdot \omega$. Mas então não se deve *esperar* que comute, pois já não comuta nos naturais: $2^{(3)} = 8 < 9 = 3^{(2)}$.

Problema 6.4. Usando indução transfinita, prove que, se se define $\alpha^{(\beta)} = \mathrm{ord}(\mathrm{finfun}(\alpha, \beta), \sqsubset)$, obtêm-se as equações recursivas de Definição 6.16.

Capítulo 7

Cardinais

7.1 Princípio de Cantor

sth:cardinals:cp:sec

Volte o pensamento a Seção 3.5. Estávamos a discutir conjuntos bem ordenados e sugerimos que seria desejável ter objetos que funcionem como representantes dos bons ordenamentos. Com isto em mente, introduzimos os ordinais e depois mostramos em Corolário 3.28 que estes se comportam como desejamos, isto é:

$$\mathrm{ord}(A, <) = \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, < \rangle \cong \langle B, \lessdot \rangle.$$

Volte ainda mais atrás, a **??**. Ali, trabalhando ingenuamente, introduzimos a noção de "tamanho" de um conjunto. Especificamente, dissemos que dois conjuntos são equipotentes, $A \approx B$, precisamente quando existe uma bijeção $f\colon A \to B$. Esta noção é intrinsecamente mais simples do que a de um bom ordenamento: interessam-nos apenas as bijeções, e não (como com os isomorfismos de ordem) se as bijeções "preservam alguma estrutura".

Tudo isto sugere um pensamento óbvio. Tal como introduzimos certos objetos, *ordinais*, para calibrar bons ordenamentos, podemos introduzir certos objetos, *cardinais*, para calibrar tamanho. Esse é o objetivo deste capítulo.

Antes de dizer o que serão estes cardinais, convém enunciar um princípio que devem satisfazer. Escrevendo $|X|$ para a cardinalidade do conjunto X, desejaríamos que obedecessem a:

$$|A| = |B| \text{ sse } A \approx B.$$

Chamaremos a isto o Princípio *de Cantor*, já que Cantor foi provavelmente o primeiro a tê-lo claramente presente. (Diremos mais sobre a sua relação com o Princípio de *Hume* na Seção 7.5.) O nosso objetivo é definir $|X|$, para cada X, de modo a que satisfaça o Princípio de Cantor.

7.2 Cardinais como Ordinais

sth:cardinals:cardsasords:sec

De fato, a nossa teoria dos cardinais fará uso (descarado) da nossa teoria dos ordinais. Ou seja: definiremos os cardinais como certos ordinais específicos. Em particular, proporemos o seguinte:

sth:cardinals:cardsasords:defcardinalasordinal

Definição 7.1. Se A pode ser bem ordenado, então $|A|$ é o menor ordinal γ tal que $A \approx \gamma$. Para qualquer ordinal γ, diz-se que γ é um *cardinal* sse $\gamma = |\gamma|$.

Acabamos de usar a locução "A pode ser bem ordenado". Como quase sempre em matemática, a locução modal aqui é apenas um atalho para uma asserção existencial: dizer "A pode ser bem ordenado" é dizer "existe uma relação que bem ordena A".

Há contudo um problema com Definição 7.1. Gostaríamos que *todo* o conjunto tivesse um tamanho, isto é, que $|A|$ existisse para todo A. A definição que acabamos de dar, porém, começa por uma condicional: "*Se* A pode ser bem ordenado…". Se existir algum conjunto A que não possa ser bem ordenado, a nossa definição simplesmente deixa de definir um objeto $|A|$.

Logo, para usar Definição 7.1, precisamos de uma garantia de que todo o conjunto pode ser bem ordenado. Infelizmente, essa garantia não está disponível em **ZF**. Assim, se queremos usar Definição 7.1, não há alternativa senão acrescentar um novo axioma, tal como:

Bom ordenamento (Bom ordenamento). Todo o conjunto pode ser bem ordenado.

Discutiremos se o axioma do bom ordenamento é aceitável em Capítulo 9. Daqui em diante, porém, simplesmente o admitiremos. E, com ele, é bastante direto provar que os cardinais (tal como definidos na Definição 7.1) existem e comportam-se bem:

sth:cardinals:cardsasords:lem:CardinalsExist
sth:cardinals:cardsasords:cardaexists
sth:cardinals:cardsasords:cardaapprox
sth:cardinals:cardsasords:cardaidem

Lema 7.2. *Para todo o conjunto A:*

1. $|A|$ *existe e é único;*
2. $|A| \approx A$*;*
3. $|A|$ *é um cardinal, isto é,* $|A| = ||A||$*;*

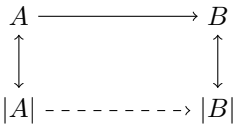
Prova. Fixe A. Pelo Bom ordenamento, existe um bom ordenamento $\langle A, R\rangle$. Por Teorema 3.26, $\langle A, R\rangle$ é isomorfo a um único ordinal, β. Logo $A \approx \beta$. Por indução transfinita, existe um único ordinal mínimo, γ, tal que $A \approx \gamma$. Logo $|A| = \gamma$, o que estabelece (1) e (2). Para (3), note-se que se $\delta \in \gamma$ então $\delta \prec A$, pela escolha de γ, logo também $\delta \prec \gamma$ pois a equipotência é uma relação de equivalência (**??**). Logo $\gamma = |\gamma|$. □

O resultado seguinte garante o Princípio de Cantor, e mais ainda. (Note-se que os cardinais herdam a ordem dos ordinais, isto é, $\mathfrak{a} < \mathfrak{b}$ sse $\mathfrak{a} \in \mathfrak{b}$. Ao formular isto, usaremos letras Fraktur para objetos que sabemos serem cardinais. Isto é bastante usual. Uma alternativa comum é usar letras gregas, já que os cardinais são ordinais, escolhendo-as do meio do alfabeto, por exemplo κ, λ.):

Lema 7.3. *Para quaisquer conjuntos A e B:* sth:cardinals:cardsasords:lem:CardinalsBehaveRight

$$A \approx B \text{ sse } |A| = |B|$$
$$A \preceq B \text{ sse } |A| \leq |B|$$
$$A \prec B \text{ sse } |A| < |B|$$

Prova. Provaremos o sentido da esquerda para a direita da segunda afirmação (os outros casos são semelhantes e ficam como exercício). Considere-se o diagrama seguinte:



As setas duplas indicam bijeções, cuja existência é garantida por Lema 7.2. Ao supor $A \preceq B$, existe uma injeção $A \to B$. Seguindo as setas de $|A|$ para A, para B e para $|B|$, obtém-se uma injeção $|A| \to |B|$ (a seta tracejada). □

Pode ainda usar-se Lema 7.3 para voltar a provar Cantor–Bernstein. Trata-se da afirmação de que se $A \preceq B$ e $B \preceq A$ então $A \approx B$. A enunciamos como **??**, mas a provamos primeiro—com algum esforço—em **??**. Considere-se:

Nova prova de Schröder-Bernstein. Se $A \preceq B$ e $B \preceq A$, então $|A| \leq |B|$ e $|B| \leq |A|$ por Lema 7.3. Logo $|A| = |B|$ e $A \approx B$ por tricotomia e Lema 7.3.□

Embora seja uma prova muito simples, apoia-se implicitamente na Substituição (para assegurar Teorema 3.26) e no Bom ordenamento (para garantir Lema 7.3). Em contraste, a prova na **??** era muito mais autônoma (de fato, pode efetuar-se em $\mathbf{Z}^-$).

7.3 ZFC: um marco

Com a adição do axioma do bom ordenamento, atingimos o último marco teórico. Dispomos agora de todos os axiomas necessários para **ZFC**. Em detalhe: sth:cardinals:zfc:sec

Definição 7.4. A teoria **ZFC** tem estes axiomas: Extensionalidade, União, Pares, Conjuntos potência, Infinitude, Fundação, Bom ordenamento e todas as instâncias dos esquemas de Separação e Substituição. Dito de outro modo, **ZFC** acrescenta o Bom ordenamento a **ZF**.

ZFC significa teoria de conjuntos de *Zermelo–Fraenkel* com *Escolha*. Isto pode parecer ligeiramente estranho, pois o axioma que adicionamos se chama "Bom ordenamento", não "Escolha". Mas, quando mais tarde formularmos a *Escolha*, verificar-se-á que o Bom ordenamento lhe é equivalente (módulo **ZF**) (ver Teorema 9.6). Logo, qual tomar como axioma "básico" é indiferente. E o nome "**ZFC**" é inteiramente standard na literatura.

7.4 Finito, Enumerável, Não Enumerável

sth:cardinals:classing:sec

Agora que fomos introduzidos aos cardinais, vale a pena dedicar um pouco de tempo a variedades de cardinais; nomeadamente, cardinais finitos, enumerável e não enumerável.

Os nossos dois primeiros resultados implicam que os cardinais finitos serão exatamente os ordinais finitos, que definimos como os nossos *números naturais* em Definição 2.7:

sth:cardinals:classing:finitecardisoequal

Proposição 7.5. *Sejam $n, m \in \omega$. Então $n = m$ sse $n \approx m$.*

Prova. O sentido *da esquerda para a direita* é trivial. Para provar *da direita para a esquerda*, suponha-se $n \approx m$ embora $n \neq m$. Por tricotomia, ou $n \in m$ ou $m \in n$; suponha-se, sem perda de generalidade, $n \in m$. Então $n \subsetneq m$ e existe uma bijeção $f : m \to n$, logo m é infinito de Dedekind, o que contradiz Proposição 2.8. □

sth:cardinals:classing:naturalsarecardinals

Corolário 7.6. *Se $n \in \omega$, então n é um cardinal.*

Prova. Imediato. □

Segue-se também que várias noções razoáveis do que possa significar descrever um cardinal como "finito" ou "infinito" coincidem:

sth:cardinals:classing:generalinfinitycharacter

Teorema 7.7. *Para qualquer conjunto A, as seguintes afirmações são equivalentes:*

sth:cardinals:classing:card:notinomega
1. *$|A| \notin \omega$, isto é, A não é um número natural;*

sth:cardinals:classing:card:omegaplus
2. *$\omega \leq |A|$;*

sth:cardinals:classing:card:infinite
3. *A é infinito de Dedekind.*

Prova. Por Lema 6.10, Lema 7.3, e Corolário 7.6. □

Isto autoriza a seguinte *definição* de algumas noções que usamos de forma informal na **??**:

sth:cardinals:classing:defnfinite

Definição 7.8. Diz-se que A é *finito* sse $|A|$ é um número natural, isto é, $|A| \in \omega$. Caso contrário, diz-se que A é *infinito*.

Note-se que esta definição é apresentada no contexto de **ZFC**. Afinal, precisamos do Bom ordenamento para garantir que todo o conjunto tem uma cardinalidade. E, de fato, sem o Bom ordenamento, pode existir um conjunto que nem é finito nem infinito de Dedekind. Voltaremos a este tipo de questão no Capítulo 9. Por ora, continuamos a assumir o Bom ordenamento.

Passemos agora dos cardinais finitos aos cardinais infinitos. Eis dois pontos elementares:

sth:cardinals:classing:omegaisacardinal

Corolário 7.9. *ω é o menor cardinal infinito.*

Prova. ω é um cardinal, pois ω é infinito de Dedekind e se $\omega \approx n$ para algum $n \in \omega$ então n seria infinito de Dedekind, contrariando Proposição 2.8. Ora, ω é o menor cardinal infinito por definição. □

Corolário 7.10. *Todo o cardinal infinito é um ordinal limite.*

Prova. Seja α um ordinal sucessor infinito, logo $\alpha = \beta + 1$ para algum β. Por Proposição 7.5, β também é infinito, logo $\beta \approx \beta + 1$ por Lema 6.10. Ora, $|\beta| = |\beta + 1| = |\alpha|$ por Lema 7.3, logo $\alpha \neq |\alpha|$. □

Já na **??**, assinalamos que podemos distinguir conjuntos infinitos enumerável de conjuntos infinitos não enumerável. Essa definição conduz naturalmente ao seguinte:

Proposição 7.11. *A é enumerável sse $|A| \leq \omega$, e A é não enumerável sse $\omega < |A|$.*

Prova. Por tricotomia, as duas afirmações são equivalentes, bastando provar que A é enumerável sse $|A| \leq \omega$. Para *da direita para a esquerda*: se $|A| \leq \omega$, então $A \preceq \omega$ por Lema 7.3 e Corolário 7.9. Para *da esquerda para a direita*: suponha-se A enumerável; então, por **??**, há três casos possíveis:

1. se $A = \emptyset$, então $|A| = 0 \in \omega$, por Corolário 7.6 e Lema 7.3.
2. se $n \approx A$, então $|A| = n \in \omega$, por Corolário 7.6 e Lema 7.3.
3. se $\omega \approx A$, então $|A| = \omega$, por Corolário 7.9.

Em todos os casos, $|A| \leq \omega$. □

De fato, ω tem um lugar especial. Embora existam muitos ordinais contáveis:

Corolário 7.12. *ω é o único cardinal infinito enumerável.*

Prova. Seja $\mathfrak{a}$ um cardinal infinito enumerável. Como $\mathfrak{a}$ é infinito, $\omega \leq \mathfrak{a}$. Como $\mathfrak{a}$ é um cardinal infinito enumerável, $\mathfrak{a} = |\mathfrak{a}| \leq \omega$. Logo $\mathfrak{a} = \omega$ por tricotomia. □

Claro que existem infinitos cardinais. Poderíamos perguntar: *Quantos cardinais há?* Os resultados seguintes mostram que convém reconsiderar essa pergunta.

Proposição 7.13. *Se todo o membro de X é um cardinal, então $\bigcup X$ é um cardinal.*

sth:cardinals:classing: unioncardinalscardinal

Prova. É fácil verificar que $\bigcup X$ é um ordinal. Seja $\alpha \in \bigcup X$ um ordinal; então $\alpha \in \mathfrak{b} \in X$ para algum cardinal $\mathfrak{b}$. Como $\mathfrak{b}$ é um cardinal, $\alpha \prec \mathfrak{b}$. Como $\mathfrak{b} \subseteq \bigcup X$, tem-se $\mathfrak{b} \preceq \bigcup X$, e portanto $\alpha \not\approx \bigcup X$. Generalizando, $\bigcup X$ é um cardinal. □

Teorema 7.14. *Não existe um cardinal máximo.*

sth:cardinals:classing: lem:NoLargestCardinal

Prova. Para qualquer cardinal $\mathfrak{a}$, o teorema de Cantor (**??**) e Lema 7.2 implicam que $\mathfrak{a} < |\wp(\mathfrak{a})|$. □

Teorema 7.15. *O conjunto de todos os cardinais não existe.*

Prova. Por redução ao absurdo, suponha-se $C = \{\mathfrak{a} : \mathfrak{a} \text{ é um cardinal}\}$. Ora, $\bigcup C$ é um cardinal por Proposição 7.13, logo por Teorema 7.14 existe um cardinal $\mathfrak{b} > \bigcup C$. Por definição $\mathfrak{b} \in C$, logo $\mathfrak{b} \subseteq \bigcup C$, donde $\mathfrak{b} \leq \bigcup C$, uma contradição. □

Compare isto com o paradoxo de Russell e com Burali-Forti.

7.5 Apêndice: Princípio de Hume

sth:cardinals:hp:sec

Na Seção 7.1, descrevemos o Princípio de Cantor. Era:

$$|A| = |B| \text{ sse } A \approx B.$$

Isto é muito semelhante ao que hoje se chama *Princípio de Hume*, que diz:

$$\#x\, F(x) = \#x\, G(x) \text{ sse } F \sim G$$

onde '$F \sim G$' abrevia que há tantos F quantos G, isto é, os F podem pôr-se em bijeção com os G, isto é:

$$\begin{aligned} &\exists R(\forall v \forall y(Rvy \to (Fv \wedge Gy)) \wedge \\ &\quad \forall v(Fv \to \exists! y\, Rvy) \wedge \\ &\quad \forall y(Gy \to \exists! v\, Rvy)) \end{aligned}$$

Mas há uma diferença de tipo entre o Princípio de Hume e o Princípio de Cantor. No enunciado do Princípio de Cantor, as variáveis "A" e "B" são termos de primeira ordem que denotam *conjuntos*. No enunciado do Princípio de Hume, "F", "G" e "R" *não* são termos de primeira ordem; estão em *posição de predicado*. (Talvez denotem *propriedades*.) Assim, o Princípio de Hume pode parafrasear-se em português: o número de Fs é o número de Gs sse os Fs estão em bijeção com os Gs. Chama-se *Princípio de Hume* porque Hume escreveu o seguinte:

> Quando dois números se combinam de tal modo que a cada unidade de um corresponde sempre uma unidade do outro, dizemos que são iguais. (Hume, 1740, Pt.III Bk.1 §1)

E o Princípio de Hume foi trazido à proeminência matemático-lógica contemporânea por Frege (1884, §63), que citou esta passagem de Hume antes de (em efeito) esboçar (o que chamamos) Princípio de Hume.

Note a semelhança estrutural entre o Princípio de Hume e a Lei Básica V. A formulamos na Seção 1.6 do seguinte modo:

$$\epsilon x\, F(x) = \epsilon x\, G(x) \text{sse } \forall x\, (F(x) \leftrightarrow G(x)).$$

E, neste ponto, alguns comentários e comparações podem ajudar.

Há duas maneiras de entender um princípio como o Princípio de Hume ou a Lei Básica V: *predicativamente* ou *impredicativamente* (recorde Seção 1.3). Na leitura impredicativa da Lei Básica V, para cada F, o objeto $\epsilon x\, F(x)$ pertence ao domínio de quantificação usado na própria formulação da Lei Básica V. Do mesmo modo, na leitura impredicativa do Princípio de Hume, para cada F, o objeto $\#x\, F(x)$ pertence ao domínio de quantificação usado na formulação do Princípio de Hume. Em contraste, na compreensão *predicativa*, os objetos $\epsilon x\, F(x)$ e $\#x\, F(x)$ seriam entidades de um domínio *diferente*.

Agora, se a Lei Básica V se lê impredicativamente, conduz à inconsistência, via Compreensão ingênua (para pormenores, ver Seção 1.6). Tal como a Compreensão ingênua, pode tornar-se consistente se se lê *predicativamente*. Mas provavelmente não fará tudo o que desejávamos.

O Princípio de Hume, porém, *pode* ser lido de modo consistente impredicativamente. E, assim lido, é bastante poderoso.

Para ilustrar: considere-se o predicado "$x \neq x$", que obviamente nada satisfaz. O Princípio de Hume fornece agora um objeto $\#x(x \neq x)$. Podemos tratá-lo como o número 0. Agora, na compreensão *impredicativa*—mas *só* na impredicativa—esta entidade 0 pertence ao nosso domínio original de quantificação. Logo podemos aplicar sensatamente o Princípio de Hume com o predicado "$x = 0$" para obter um objeto $\#x(x = 0)$. Podemos tratá-lo como o número 1. Além disso, o Princípio de Hume implica que $0 \neq 1$, pois não pode haver bijeção dos objetos não auto-idênticos para os objetos idênticos a 0 (não há dos primeiros, mas há um dos segundos). Agora, de novo impredicativamente, 1 pertence ao domínio original de quantificação. Logo podemos aplicar o Princípio de Hume com o predicado "$(x = 0 \vee x = 1)$" para obter um objeto $\#x(x = 0 \vee x = 1)$. Podemos tratá-lo como o número 2, e mostrar que $0 \neq 2$ e $1 \neq 2$, e assim por diante.

Em suma, tomado impredicativamente, o Princípio de Hume implica que há *infinitamente muitos objetos*. E isto encorajou os *logicistas neo-fregeanos* a tomar o Princípio de Hume como fundação da aritmética.

O próprio Frege, contudo, não tomou o Princípio de Hume como fundação da aritmética. Em vez disso, Frege provou o Princípio de Hume a partir de uma definição explícita: $\#x\, F(x)$ é definido como a extensão do conceito $F \sim \Phi$. Em termos modernos, poder-se-ia tentar render isto como $\#x\, F(x) = \{G : F \sim G\}$; mas isto volta a arrastar-nos para os problemas da Compreensão ingênua.

Capítulo 8

Aritmética Cardinal

8.1 Definindo as Operações Básicas

sth:card-arithmetic:opps:sec

Como não precisamos de controlar a ordem, a aritmética cardinal é bastante mais fácil de definir do que a aritmética ordinal. Definiremos adição, multiplicação e exponenciação simultaneamente.

Definição 8.1. Quando $\mathfrak{a}$ e $\mathfrak{b}$ são cardinais:

$$\begin{aligned} \mathfrak{a} \oplus \mathfrak{b} &= |\mathfrak{a} \sqcup \mathfrak{b}| \\ \mathfrak{a} \otimes \mathfrak{b} &= |\mathfrak{a} \times \mathfrak{b}| \\ \mathfrak{a}^{\mathfrak{b}} &= \left|{}^{\mathfrak{b}}\mathfrak{a}\right| \end{aligned}$$

onde ${}^{X}Y = \{f : f \text{ é uma função } X \to Y\}$. (É fácil mostrar que ${}^{X}Y$ existe para quaisquer conjuntos X e Y; deixamos isto como exercício.)

Problema 8.1. Prove em $\mathbf{Z}^-$ que ${}^{X}Y$ existe para quaisquer conjuntos X e Y. Trabalhando em **ZF**, calcule posto$({}^{X}Y)$ a partir de posto(X) e posto(Y), à maneira de Lema 6.9.

Pode ajudar explicar esta definição. Quanto à adição: usa-se a noção de soma disjunta, $\sqcup$, tal como definida em Definição 6.1; e é fácil ver que esta definição dá o resultado certo nos casos finitos. Quanto à multiplicação: **??** nos diz que, se A tem n membros e B tem m membros, então $A \times B$ tem $n \cdot m$ membros, pelo que a nossa definição generaliza simplesmente a ideia à multiplicação transfinita. A exponenciação é semelhante: estamos simplesmente a generalizar o pensamento do finito para o transfinito. De fato, sob certos aspectos, a aritmética cardinal transfinita parece muito mais a aritmética "ordinária" do que a aritmética ordinal transfinita:

sth:card-arithmetic:opps:cardplustimescommute

Proposição 8.2. *$\oplus$ e $\otimes$ são comutativas e associativas.*

Prova. Para a comutatividade, por Lema 7.3 basta observar que $(\mathfrak{a} \sqcup \mathfrak{b}) \approx (\mathfrak{b} \sqcup \mathfrak{a})$ e $(\mathfrak{a} \times \mathfrak{b}) \approx (\mathfrak{b} \times \mathfrak{a})$. Deixamos a associatividade como exercício. □

Problema 8.2. Prove que $\oplus$ e $\otimes$ são associativas.

Proposição 8.3. *A é infinito se e só se $|A| \oplus 1 = 1 \oplus |A| = |A|$.*

Prova. Como em Teorema 7.7, a partir de Lema 6.10 e Lema 7.3. □

Isto explica porque precisamos de símbolos distintos para adição/multiplicação ordinal versus cardinal: são operações genuinamente *diferentes*. Este par de resultados mostra que a exponenciação ordinal versus cardinal também são operações distintas. (Recordar que Definição 2.7 implica que $2 = \{0, 1\}$):

Lema 8.4. *$|\wp(A)| = 2^{|A|}$, para qualquer A.*

sth:card-arithmetic:opps:lem:SizePowerset2Exp

Prova. Para cada subconjunto $B \subseteq A$, seja $\chi_B \in {}^A2$ dado por:

$$\chi_B(x) = \begin{cases} 1 & \text{se } x \in B \\ 0 & \text{caso contrário.} \end{cases}$$

Seja agora $f(B) = \chi_B$; isto define uma bijeção $f\colon \wp(A) \to {}^A2$. Logo $\wp(A) \approx {}^A2$. Daí $\wp(A) \approx {}^{|A|}2$, pelo que $|\wp(A)| = \left|{}^{|A|}2\right| = 2^{|A|}$. □

Esta prova sucinta subsume essencialmente a discussão em **??**. Ali, mostramos como "reduzir" a não enumerabilidade de $\wp(\omega)$ à não enumerabilidade do conjunto das sequências binárias infinitas, $\mathbb{B}^\omega$. Na prática, $\mathbb{B}^\omega$ é apenas ${}^\omega 2$; e a prova precedente mostrou que o raciocínio que seguimos na **??** continua a valer usando qualquer conjunto A no lugar de ω. O resultado também fornece um fato rápido sobre exponenciação cardinal:

Corolário 8.5. *$\mathfrak{a} < 2^{\mathfrak{a}}$ para qualquer cardinal $\mathfrak{a}$.*

sth:card-arithmetic:opps:cantorcor

Prova. Pelo Teorema de Cantor (**??**) e Lema 8.4. □

Logo $\omega < 2^\omega$. Mas nota: isto é um resultado sobre exponenciação *cardinal*. Deve contrastar-se com a exponenciação *ordinal*, pois neste último caso $\omega = 2^{(\omega)}$ (ver Seção 6.5).

Enquanto estamos no tema da exponenciação cardinal, podemos também ser um pouco mais precisos sobre a "maneira" pela qual $\mathbb{R}$ é não enumerável.

Teorema 8.6. $|\mathbb{R}| = 2^\omega$

sth:card-arithmetic:opps:continuumis2aleph0

Esboço de prova. Há muitas maneiras de provar isto. A mais direta é argumentar que $\wp(\omega) \preceq \mathbb{R}$ e $\mathbb{R} \preceq \wp(\omega)$, e depois usar Schröder-Bernstein para inferir que $\mathbb{R} \approx \wp(\omega)$, e Lema 8.4 para inferir que $|\mathbb{R}| = 2^\omega$. Deixamos como exercício (esclarecedor) definir injecções $f\colon \wp(\omega) \to \mathbb{R}$ e $g\colon \mathbb{R} \to \wp(\omega)$. □

Problema 8.3. Complete a prova de Teorema 8.6, mostrando que $\wp(\omega) \preceq \mathbb{R}$ e $\mathbb{R} \preceq \wp(\omega)$.

8.2 Simplificando Adição e Multiplicação

sth:card-arithmetic:simp:sec

Acontece que a adição e a multiplicação cardinais transfinitas são *extremamente* fáceis. Isto segue do fato de os cardinais serem (certos) ordinais, logo bem ordenados, e poderem ser manipulados de certa forma. Mostrar isto, porém, *não* é tão fácil. Para começar, precisamos de uma definição hábil:

Definição 8.7. Definimos uma *ordenação canónica*, $\lhd$, em pares de ordinais, estipulando que $\langle \alpha_1, \alpha_2\rangle \lhd \langle \beta_1, \beta_2\rangle$ se e só se se verifica uma das seguintes condições:

1. $\max(\alpha_1, \alpha_2) < \max(\beta_1, \beta_2)$; ou
2. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 < \beta_1$; ou
3. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 = \beta_1$ e $\alpha_2 < \beta_2$

Lema 8.8. *$\langle \alpha \times \alpha, \lhd\rangle$ é uma boa ordem, para qualquer ordinal α.*

Prova. Evidentemente $\lhd$ é conexa em $\alpha \times \alpha$. De fato, suponhamos que nem $\langle \alpha_1, \alpha_2\rangle$ nem $\langle \beta_1, \beta_2\rangle$ é menor do que a outra no sentido de $\lhd$. Então $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 = \beta_1$ e $\alpha_2 = \beta_2$, pelo que $\langle \alpha_1, \alpha_2\rangle = \langle \beta_1, \beta_2\rangle$.

Para mostrar que é boa ordem, seja $X \subseteq \alpha \times \alpha$ não vazio. Como α é um ordinal, algum δ é o menor membro de $\{\max(\gamma_1, \gamma_2) : \langle \gamma_1, \gamma_2\rangle \in X\}$. Descartemos agora todos os pares de $\{\langle \gamma_1, \gamma_2\rangle \in X : \max(\gamma_1, \gamma_2) = \delta\}$ exceto os de primeira coordenada mínima; entre estes, o par de segunda coordenada mínima é o elemento $\lhd$-mínimo de X. □

Segue-se uma observação mínima, mas simples:

sth:card-arithmetic:simp:simplecardproduct

Proposição 8.9. *Se $\alpha \approx \beta$, então $\alpha \times \alpha \approx \beta \times \beta$.*

Prova. Basta deixar que $f\colon \alpha \to \beta$ induza $\langle \gamma_1, \gamma_2\rangle \mapsto \langle f(\gamma_1), f(\gamma_2)\rangle$. □

E agora aplicaremos tudo isto para provar um lema crucial:

sth:card-arithmetic:simp:alphatimesalpha

Lema 8.10. *$\alpha \approx \alpha \times \alpha$, para qualquer ordinal infinito α*

Prova. Por redução ao absurdo, seja α o menor ordinal infinito para o qual isto falha. **??** mostra que $\omega \approx \omega \times \omega$, logo $\omega \in \alpha$. Além disso, α é um cardinal: suponhamos o contrário, por redução ao absurdo; então $|\alpha| \in \alpha$, pelo que $|\alpha| \approx |\alpha| \times |\alpha|$, por hipótese; e $|\alpha| \approx \alpha$ por definição; logo $\alpha \approx \alpha \times \alpha$ por Proposição 8.9.

Ora, para cada $\langle \gamma_1, \gamma_2\rangle \in \alpha \times \alpha$, consideremos o segmento:

$$\mathrm{Seg}(\gamma_1, \gamma_2) = \{\langle \delta_1, \delta_2\rangle \in \alpha \times \alpha : \langle \delta_1, \delta_2\rangle \lhd \langle \gamma_1, \gamma_2\rangle\}$$

Seja $\gamma = \max(\gamma_1, \gamma_2)$; note-se que $\langle \gamma_1, \gamma_2 \rangle \lhd \langle \gamma + 1, \gamma + 1 \rangle$. Assim, quando γ é infinito, observe-se:

$$\begin{aligned} \operatorname{Seg}(\gamma_1, \gamma_2) &\precsim ((\gamma + 1) \cdot (\gamma + 1)) \\ &\approx (\gamma \cdot \gamma), \text{ por Lema 6.10 e Proposição 8.9} \\ &\approx \gamma, \text{ pela hipótese de indução} \\ &\prec \alpha, \text{ pois } \alpha \text{ é um cardinal} \end{aligned}$$

Logo $\operatorname{ord}(\alpha \times \alpha, \lhd) \leq \alpha$, e portanto $\alpha \times \alpha \preceq \alpha$. Como obviamente $\alpha \preceq \alpha \times \alpha$, o resultado segue por Schröder-Bernstein. □

Finalmente, chegamos ao nosso resultado simplificador:

Teorema 8.11. *Se $\mathfrak{a}, \mathfrak{b}$ são cardinais infinitos, então:* sth:card-arithmetic:simp:cardplustimesmax

$$\mathfrak{a} \otimes \mathfrak{b} = \mathfrak{a} \oplus \mathfrak{b} = \mathit{max}(\mathfrak{a}, \mathfrak{b}).$$

Prova. Sem perda de generalidade, suponhamos $\mathfrak{a} = \max(\mathfrak{a}, \mathfrak{b})$. Então, invocando Lema 8.10, $\mathfrak{a} \otimes \mathfrak{a} = \mathfrak{a} \leq \mathfrak{a} \oplus \mathfrak{b} \leq \mathfrak{a} \oplus \mathfrak{a} \leq \mathfrak{a} \otimes \mathfrak{a}$. □

Do mesmo modo, se $\mathfrak{a}$ é infinito, uma união de cardinalidade $\mathfrak{a}$ de conjuntos de cardinalidade $\leq \mathfrak{a}$ tem cardinalidade $\leq \mathfrak{a}$:

Proposição 8.12. *Seja $\mathfrak{a}$ um cardinal infinito. Para cada ordinal $\beta \in \mathfrak{a}$, seja X_β um conjunto com $|X_\beta| \leq \mathfrak{a}$. Então $\left|\bigcup_{\beta \in \mathfrak{a}} X_\beta\right| \leq \mathfrak{a}$.* sth:card-arithmetic:simp:kappaunionkappasize

Prova. Para cada $\beta \in \mathfrak{a}$, fixe uma injeção $f_\beta \colon X_\beta \to \mathfrak{a}$.[1] Defina uma injeção $g \colon \bigcup_{\beta \in \mathfrak{a}} X_\beta \to \mathfrak{a} \times \mathfrak{a}$ por $g(v) = \langle \beta, f_\beta(v) \rangle$, onde $v \in X_\beta$ e $v \notin X_\gamma$ para qualquer $\gamma \in \beta$. Ora, $\bigcup_{\beta \in \mathfrak{a}} X_\beta \preceq \mathfrak{a} \times \mathfrak{a} \approx \mathfrak{a}$ por Teorema 8.11. □

8.3 Algumas Simplificações com Exponenciação Cardinal

Embora definir $\lhd$ fosse um pouco trabalhoso, o resultado é um teorema útil sobre adição e multiplicação cardinais, Teorema 8.11. A exponenciação transfinita, porém, não se simplifica tão diretamente. Para explicar por que, começamos por um resultado que prolonga um padrão familiar do caso finitário (embora a sua prova esteja a um nível elevado de abstração): sth:card-arithmetic:expotough:sec

Proposição 8.13. *$\mathfrak{a}^{\mathfrak{b} \oplus \mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \otimes \mathfrak{a}^{\mathfrak{c}}$ e $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b} \otimes \mathfrak{c}}$, para quaisquer cardinais $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$.* sth:card-arithmetic:expotough:simplecardexpo

[1] Como são estes "fixos"? Ver Seção 9.5.

Prova. Para a primeira afirmação, considere-se uma função $f\colon (\mathfrak{b}\sqcup\mathfrak{c}) \to \mathfrak{a}$. Ora, "parta-se" isto, definindo $f_{\mathfrak{b}}(\beta) = f(\beta, 0)$ para cada $\beta \in \mathfrak{b}$, e $f_{\mathfrak{c}}(\gamma) = f(\gamma, 1)$ para cada $\gamma \in \mathfrak{c}$. A aplicação $f \mapsto (f_{\mathfrak{b}} \times f_{\mathfrak{c}})$ é uma bijeção ${}^{\mathfrak{b}\sqcup\mathfrak{c}}\mathfrak{a} \to ({}^{\mathfrak{b}}\mathfrak{a} \times {}^{\mathfrak{c}}\mathfrak{a})$.

Para a segunda afirmação, considere-se uma função $f\colon \mathfrak{c} \to ({}^{\mathfrak{b}}\mathfrak{a})$; assim, para cada $\gamma \in \mathfrak{c}$ temos alguma função $f(\gamma)\colon \mathfrak{b} \to \mathfrak{a}$. Ora, defina-se $f^*(\beta, \gamma) = (f(\gamma))(\beta)$ para cada $\langle \beta, \gamma\rangle \in \mathfrak{b} \times \mathfrak{c}$. A aplicação $f \mapsto f^*$ é uma bijeção ${}^{\mathfrak{c}}({}^{\mathfrak{b}}\mathfrak{a}) \to {}^{\mathfrak{b}\otimes\mathfrak{c}}\mathfrak{a}$. □

O que gostaríamos *mesmo* era de uma maneira fácil de calcular $\mathfrak{a}^{\mathfrak{b}}$ quando tratamos de cardinais infinitos. Eis um passo útil nessa direção:

sth:card-arithmetic:expotough:cardexpo2reduct

Proposição 8.14. *Se $2 \leq \mathfrak{a} \leq \mathfrak{b}$ e $\mathfrak{b}$ é infinito, então $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$*

Prova.

$$\begin{aligned} 2^{\mathfrak{b}} &\leq \mathfrak{a}^{\mathfrak{b}}, \text{ pois } 2 \leq \mathfrak{a} \\ &\leq (2^{\mathfrak{a}})^{\mathfrak{b}}, \text{ por Lema 8.4} \\ &= 2^{\mathfrak{a}\otimes\mathfrak{b}}, \text{ por Proposição 8.13} \\ &= 2^{\mathfrak{b}}, \text{ por Teorema 8.11} \end{aligned}$$ □

Não devemos esperar poder simplificar mais além disto, pois $\mathfrak{b} < 2^{\mathfrak{b}}$ por Lema 8.4. Contudo, isto não nos diz o que afirmar sobre $\mathfrak{a}^{\mathfrak{b}}$ quando $\mathfrak{b} < \mathfrak{a}$. Naturalmente, se $\mathfrak{b}$ é *finito*, sabemos o que fazer.

Proposição 8.15. *Se $\mathfrak{a}$ é infinito e $n \in \omega$, então $\mathfrak{a}^n = \mathfrak{a}$*

Prova. $\mathfrak{a}^n = \mathfrak{a} \otimes \mathfrak{a} \otimes \ldots \otimes \mathfrak{a} = \mathfrak{a}$, por Teorema 8.11. □

Adicionalmente, nalguns outros casos, podemos controlar o tamanho de $\mathfrak{a}^{\mathfrak{b}}$:

Proposição 8.16. *Se $2 \leq \mathfrak{b} < \mathfrak{a} \leq 2^{\mathfrak{b}}$ e $\mathfrak{b}$ é infinito, então $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$*

Prova. $2^{\mathfrak{b}} \leq \mathfrak{a}^{\mathfrak{b}} \leq (2^{\mathfrak{b}})^{\mathfrak{b}} = 2^{\mathfrak{b}\otimes\mathfrak{b}} = 2^{\mathfrak{b}}$, raciocinando como na Proposição 8.14. □

Para além deste ponto, as coisas tornam-se bastante mais subtis.

8.4 A Hipótese do Contínuo

sth:card-arithmetic:ch:sec

O resultado anterior sugere (corretamente) que a exponenciação cardinal seria bastante *fácil*, se os cardinais infinitos estivessem garantidos a "comportar-se de forma simples" com potências de 2, isto é, (por Lema 8.4) com a operação de tomar conjuntos potência. Mas não podemos supor que os cardinais infinitos *se comportem* de forma simples com os conjuntos potência.

Começando a desdobrar isto, introduzimos uma notação conveniente.

Definição 8.17. Onde $\mathfrak{a}^{\oplus}$ é o menor cardinal estritamente maior do que $\mathfrak{a}$, definimos duas sequências infinitas:

$$\begin{aligned} \aleph_0 &= \omega & \beth_0 &= \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^{\oplus} & \beth_{\alpha+1} &= 2^{\beth_\alpha} \\ \aleph_\alpha &= \bigcup_{\beta<\alpha} \aleph_\beta & \beth_\alpha &= \bigcup_{\beta<\alpha} \beth_\beta \end{aligned} \qquad \text{quando } \alpha \text{ é um ordinal limite.}$$

A definição de $\mathfrak{a}^{\oplus}$ faz sentido, pois Teorema 7.14 nos diz que, para cada cardinal $\mathfrak{a}$, existe algum cardinal maior do que $\mathfrak{a}$, e a Indução Transfinita garante que existe um cardinal *mínimo* maior do que $\mathfrak{a}$. O resto da definição é fornecido pela recursão transfinita.

Cantor introduziu esta notação "$\aleph$"; trata-se do *alef*, a primeira letra do alfabeto hebraico e a primeira letra da palavra hebraica para "infinito". Peirce introduziu a notação "$\beth$"; trata-se do *beth*, a segunda letra do alfabeto hebraico.[2] Estas notações fornecem-nos cardinais infinitos.

Proposição 8.18. *$\aleph_\alpha$ e $\beth_\alpha$ são cardinais, para todo o ordinal α.*

Prova. Ambos os resultados valem por uma indução transfinita simples. $\aleph_0 = \beth_0 = \omega$ é um cardinal por Corolário 7.9. Supondo que $\aleph_\alpha$ e $\beth_\alpha$ são ambos cardinais, $\aleph_{\alpha+1}$ e $\beth_{\alpha+1}$ estão explicitamente definidos como cardinais. E a união de um conjunto de cardinais é um cardinal, por Proposição 7.13. □

Além disso, todo o cardinal infinito é um $\aleph$:

Proposição 8.19. *Se $\mathfrak{a}$ é um cardinal infinito, então $\mathfrak{a} = \aleph_\gamma$ para um certo γ único.*

Prova. Por indução transfinita nos cardinais. Para a indução, suponhamos que se $\mathfrak{b} < \mathfrak{a}$ então $\mathfrak{b} = \aleph_{\gamma_\mathfrak{b}}$. Se $\mathfrak{a} = \mathfrak{b}^{\oplus}$ para algum $\mathfrak{b}$, então $\mathfrak{a} = (\aleph_{\gamma_\mathfrak{b}})^{\oplus} = \aleph_{\gamma_\mathfrak{b}+1}$. Se $\mathfrak{a}$ não é o sucessor de nenhum cardinal, então, por serem os cardinais ordinais, $\mathfrak{a} = \bigcup_{\mathfrak{b}<\mathfrak{a}} \mathfrak{b} = \bigcup_{\mathfrak{b}<\mathfrak{a}} \aleph_{\gamma_\mathfrak{b}}$, logo $\mathfrak{a} = \aleph_\gamma$ onde $\gamma = \bigcup_{\mathfrak{b}<\mathfrak{a}} \gamma_\mathfrak{b}$. □

Como todo o cardinal infinito é um $\aleph$, surge naturalmente a pergunta: será que todo o cardinal infinito é um $\beth$? Certamente que, se isso *se verificasse*, os cardinais infinitos "comportar-se-iam de forma simples" com a operação de tomar conjuntos potência. De fato, teríamos o seguinte:

> *Hipótese Generalizada do Contínuo* (HGC). $\aleph_\alpha = \beth_\alpha$, para todo o α.

[2] Peirce usou esta notação numa carta a Cantor de dezembro de 1900. Infelizmente, Peirce também apresentou ali um mau argumento de que $\beth_\alpha$ não existe para $\alpha \geq \omega$.

Além disso, se a HGC valesse, poderíamos simplificar bastante a exponenciação cardinal. Em particular, poderíamos mostrar que, quando $\mathfrak{b} < \mathfrak{a}$, o valor de $\mathfrak{a}^{\mathfrak{b}}$ fica encerrado entre $\mathfrak{a} \leq \mathfrak{a}^{\mathfrak{b}} \leq \mathfrak{a}^{\oplus}$. Poderíamos então dar condições precisas que determinam qual das duas possibilidades se verifica (isto é, se $\mathfrak{a} = \mathfrak{a}^{\mathfrak{b}}$ ou $\mathfrak{a}^{\mathfrak{b}} = \mathfrak{a}^{\oplus}$).[3]

Mas a HGC é uma *hipótese*, não um *teorema*. De fato, Gödel (1938) provou que, se **ZFC** for consistente, então também o é **ZFC** + HGC. Mas mais tarde verificou-se que podemos acrescentar igualmente ¬HGC a **ZFC**. De fato, considere-se a *instância* não trivial mais simples da HGC, nomeadamente:

Hipótese do Contínuo (HC). $\aleph_1 = \beth_1$.

Cohen (1963) provou que, se **ZFC** for consistente, então também o é **ZFC** + ¬HC. Logo a Hipótese do Contínuo é independente de **ZFC**.

A Hipótese do Contínuo chama-se assim porque "o contínuo" é outro nome para a reta real, $\mathbb{R}$. Teorema 8.6 nos diz que $|\mathbb{R}| = \beth_1$. Assim, a Hipótese do Contínuo afirma que não há cardinal entre a cardinalidade dos números naturais, $\aleph_0 = \beth_0$, e a cardinalidade do contínuo, $\beth_1$.

Dada a *independência* da (H)HC relativamente a **ZFC**, o que devemos dizer sobre a sua *verdade*? Há *muito* a dizer. De fato, muito trabalho recente e fecundo em teoria dos conjuntos tem sido dedicado a estas questões. Mas dois pontos rápidos valem certamente a pena enfatizar.

Primeiro: não se segue *imediatamente* destes resultados formais de independência que a HGC ou a HC sejam *indeterminadas* no valor de verdade. Afinal, talvez bastem mais axiomas, que nos pareçam naturais, para decidir a questão num sentido ou noutro. O próprio Gödel sugeriu que essa era a resposta adequada.

Segundo: a independência da HC relativamente a **ZFC** é certamente *notável*, mas não é *inacreditável* (no sentido literal). O ponto é simplesmente que, para tudo o que **ZFC** nos diz, passar de um cardinal ao seu sucessor pode envolver uma ferramenta menos direta do que simplesmente tomar conjuntos potência.

Feitas estas duas observações, quem quiser saber mais terá de recorrer aos vários filósofos e matemáticos com cavalos na corrida.[4]

8.5 Pontos Fixos de $\aleph$

sth:card-arithmetic:fix:sec

No Capítulo 4, sugerimos que o Esquema de Substituição carece de justificação, pois força a hierarquia a ser bastante alta. Tendo feito alguma aritmética cardinal, podemos dar uma pequena ilustração da altura da hierarquia.

Evidentemente $0 < \aleph_0$, e $1 < \aleph_1$, e $2 < \aleph_2 \ldots$ e, de fato, a diferença de tamanho só fica *maior* a cada passo. Assim, é tentador conjecturar que $\kappa < \aleph_\kappa$ para todo o ordinal κ.

[3] A condição é ditada pela *cofinalidade*.

[4] Embora possa querer começar por ler Potter (2004, §15.6).

Mas esta conjectura é *falsa*, em **ZFC**. De fato, podemos provar que existem *pontos fixos de* $\aleph$, isto é, cardinais κ tais que $\kappa = \aleph_\kappa$.

Proposição 8.20. *Existe um ponto fixo de* $\aleph$. *sth:card-arithmetic:fix:alephfixed*

Prova. Por recursão, defina-se:

$$\begin{aligned} \kappa_0 &= 0 \\ \kappa_{n+1} &= \aleph_{\kappa_n} \\ \kappa &= \bigcup_{n<\omega} \kappa_n \end{aligned}$$

Ora, κ é um cardinal por Proposição 7.13. Mas então:

$$\kappa = \bigcup_{n<\omega} \kappa_{n+1} = \bigcup_{n<\omega} \aleph_{\kappa_n} = \bigcup_{\alpha<\kappa} \aleph_\alpha = \aleph_\kappa$$

□

Boolos escreveu um artigo sobre precisamente o ponto fixo de $\aleph$ que acabamos de construir. Depois de notar a existência de κ, no início do artigo, disse:

> [κ é] um número *bastante grande*, aos olhos de quem não teve contato prévio com a teoria dos conjuntos, tão grande, me parece, que põe em causa a verdade de qualquer teoria que, entre as suas afirmações, inclua a de que existem pelo menos κ objetos. (Boolos, 2000, p. 257)

E concluiu o artigo perguntando:

> [será que] suspeitamos que, seja qual for o começo da história, quando chegamos tão longe as rodas giram no vazio e já não estamos a ouvir uma descrição de coisa alguma que seja o caso? (Boolos, 2000, p. 268)

Se, de fato, ultrapassamos "qualquer coisa que seja o caso", então devemos apontar o dedo da culpa diretamente ao Esquema de Substituição. Pois é este axioma que permite a nossa prova funcionar. Nesse caso, supõe-se, Boolos teria de rever a afirmação que fizera, décadas antes, de que a Substituição não tem consequências "indesejáveis" (ver Seção 5.3).

Mas será a existência de κ assim tão má? Pode ajudar, aqui, considerar o *paradoxo de Tristram Shandy* de Russell. Tristram Shandy documenta a sua vida no diário, mas demora um ano a registrar um único dia. A cada ano que passa, Tristram fica cada vez mais atrasado: passado um ano, só registrou um dia, e viveu 364 dias por registrar; passados dois anos, só registrou dois dias, e viveu 728 dias por registrar; passados três anos, só registrou três dias, e viveu 1092 dias por registrar ...[5] Ainda assim, se Tristram é *imortal*, conseguirá

[5] Ignorando anos bissextos.

registrar todos os dias, pois registrará o n-ésimo dia no n-ésimo ano da sua vida. E assim, "no fim dos tempos", Tristram terá um diário completo.

Porque é que isto difere tanto da ideia de que α é menor do que $\aleph_\alpha$—e, de fato, cada vez mais, desesperadamente menor—até κ, onde nos "apanhamos" e $\kappa = \aleph_\kappa$?

Deixando isto de lado, e supondo que aceitamos **ZFC**, fechemos com um pouco mais de diversão sobre construções de pontos fixos. Os três resultados seguintes estabelecem, intuitivamente, que existe um ponto (não trivial) em que a hierarquia é tão larga como alta:

sth:card-arithmetic:fix: bethfixed

Proposição 8.21. *Existe um ponto fixo de* $\beth$*, isto é, um* κ *tal que* $\kappa = \beth_\kappa$.

Prova. Como na Proposição 8.20, usando "$\beth$" no lugar de "$\aleph$". □

sth:card-arithmetic:fix: stagesize

Proposição 8.22. $|V_{\omega+\alpha}| = \beth_\alpha$. *Se* $\omega \cdot \omega \leq \alpha$*, então* $|V_\alpha| = \beth_\alpha$.

Prova. A primeira afirmação vale por uma indução transfinita simples. A segunda segue-se, pois se $\omega \cdot \omega \leq \alpha$ então $\omega + \alpha = \alpha$. Para o estabelecer, usamos fatos sobre aritmética ordinal de Capítulo 6. Note-se primeiro que $\omega \cdot \omega = \omega \cdot (1 + \omega) = (\omega \cdot 1) + (\omega \cdot \omega) = \omega + (\omega \cdot \omega)$. Ora, se $\omega \cdot \omega \leq \alpha$, isto é, $\alpha = (\omega \cdot \omega) + \beta$ para algum β, então $\omega + \alpha = \omega + ((\omega \cdot \omega) + \beta) = (\omega + (\omega \cdot \omega)) + \beta = (\omega \cdot \omega) + \beta = \alpha$. □

Corolário 8.23. *Existe um* κ *tal que* $|V_\kappa| = \kappa$.

Prova. Seja κ um ponto fixo de $\beth$, dado por Proposição 8.21. Claramente $\omega \cdot \omega < \kappa$. Logo $|V_\kappa| = \beth_\kappa = \kappa$ por Proposição 8.22. □

Há tantos estágios abaixo de V_κ quantos membros de V_κ. Intuitivamente, então, V_κ é tão largo como alto. Isto é muito à maneira de Tristram Shandy: passamos de um estágio ao seguinte tomando *conjuntos potência*, tornando a hierarquia *muito* maior a cada passo. Mas "no fim", isto é, no estágio κ, a largura da hierarquia alcança a altura.

Alguém pode perguntar: *Com que frequência a largura da hierarquia coincide com a altura?* A resposta é: *Tantas vezes quantos os ordinais.* Mas isto precisa de uma pequena explicação.

Definimos um termo τ do seguinte modo. Para qualquer A, seja:

$$\begin{aligned} \tau_0(A) &= |A| \\ \tau_{n+1}(A) &= \beth_{\tau_n(A)} \\ \tau(A) &= \bigcup_{n<\omega} \tau_n(A) \end{aligned}$$

Como na Proposição 8.21, $\tau(A)$ é um ponto fixo de $\beth$ para qualquer A, e trivialmente $|A| < \tau(A)$. Considere-se então esta definição recursiva:

$$\begin{aligned} W_0 &= 0 \\ W_{\alpha+1} &= \tau(W_\alpha) \\ W_\alpha &= \bigcup_{\beta<\alpha} W_\beta, \text{ quando } \alpha \text{ é limite} \end{aligned}$$

A construção está definida para todos os ordinais. Intuitivamente, então, W é "uma injeção" dos ordinais nos pontos fixos de $\beth$. E, exatamente como antes, V_{W_α} é tão largo como alto, para qualquer α.

Capítulo 9

Escolha

9.1 Introdução

sth:choice:intro:sec

Em Capítulos 7 a 8, desenvolvemos uma teoria de cardinais tratando os cardinais como ordinais. Essa abordagem depende do Axioma da Boa Ordenação. Verifica-se que a Boa Ordenação é equivalente a outro princípio—o Axioma da Escolha—e houve discussão filosófica séria sobre a sua aceitabilidade. As questões deste capítulo são: Como é que o Axioma é usado, e pode ser justificado?

9.2 O Truque de Tarski–Scott

sth:choice:tarskiscott:sec

Na Definição 7.1, definimos cardinais como ordinais. Para isso, assumimos o Axioma da Boa Ordenação. Fizemo-lo apenas porque é o "padrão da indústria".

Antes de discutir questões filosóficas em torno da Boa Ordenação, importa deixar claro que *podemos* afastar-nos desse padrão e desenvolver uma teoria de cardinais *sem* assumir a Boa Ordenação. Continuamos a poder usar as definições de $A \approx B$, $A \preceq B$ e $A \prec B$, tal como apareceram no **??**. Só precisamos de uma nova noção de *cardinal*.

Uma ideia ingênua seria tentar definir a cardinalidade de A assim:

$$\{x : A \approx x\}.$$

Talvez queira comparar isto com a definição fregeana de $\#xFx$, esboçada no final de Seção 7.5. E, pelas razões que ali adumbramos, esta definição falha. Qualquer conjunto singular é equipotente com $\{\emptyset\}$. Mas novos singulares são formados em cada estágio sucessor da hierarquia (basta considerar o singular do estágio anterior). Logo $\{x : A \approx x\}$ não existe, pois não pode ter posto.

Para contornar o problema, usamos um truque devido a Tarski e Scott:[1]

[1] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação em contrário).

Definição 9.1 (Tarski–Scott). Para qualquer fórmula $\varphi(x)$, seja $[x : \varphi(x)]$ o conjunto de todos os x, de posto mínimo possível, tais que $\varphi(x)$ (ou $\emptyset$, se não houver φs).

Devemos verificar que esta definição é legítima. Trabalhando em **ZF**, Teorema 4.13 garante que posto(x) existe para todo o x. Agora, se houver entidades que satisfazem φ, podemos deixar α ser o posto mínimo tal que $(\exists x \subseteq V_\alpha)\varphi(x)$, isto é, $(\forall \beta \in \alpha)(\forall x \subseteq V_\beta)\neg\varphi(x)$. Podemos então definir $[x : \varphi(x)]$ por Separação como $\{x \in V_{\alpha+1} : \varphi(x)\}$.

Tendo justificado o truque de Tarski–Scott, podemos usá-lo para definir uma noção de cardinalidade:

Definição 9.2. A TS-cardinalidade de A é $\mathrm{tsc}(A) = [x : A \approx x]$.

A definição de TS-cardinal não usa a Boa Ordenação. Mas, mesmo sem esse Axioma, podemos mostrar que os TS-*cardinais* se comportam de modo semelhante aos *cardinais* tal como definidos na Definição 7.1. Por exemplo, se reformularmos Lema 7.3 e Lema 8.4 em termos de TS-cardinais, as provas funcionam em **ZF**, sem assumir a Boa Ordenação.

Enquanto estamos no assunto, vale a pena notar que também podemos desenvolver uma teoria de ordinais usando o truque de Tarski–Scott. Onde $\langle A, <\rangle$ é uma boa ordenação, seja $\mathrm{tso}(A, <) = [\langle X, R\rangle : \langle A, <\rangle \cong \langle X, R\rangle]$. Para mais sobre este tratamento de cardinais e ordinais, ver Potter (2004, chs. 9–12).

9.3 Comparabilidade e Lema de Hartogs

Isto é o lado positivo. Eis o lado negativo. Sem Escolha, as coisas ficam *complicadas*. Para ver por que, eis um belo resultado devido a Hartogs (1915): sth:choice:hartogs:sec

Lema 9.3 (*em* ZF). *Para qualquer conjunto A, existe um ordinal α tal que $\alpha \not\preceq A$* sth:choice:hartogs:HartogsLemma

Prova. Se $B \subseteq A$ e $R \subseteq B^2$, então $\langle B, R\rangle \subseteq V_{\mathrm{posto}(A)+4}$ por Lema 6.9. Logo, usando Separação, considere-se:

$$C = \{\langle B, R\rangle \in V_{\mathrm{posto}(A)+5} : B \subseteq A \text{ e } \langle B, R\rangle \text{ é uma boa ordenação}\}$$

Usando Substituição e Teorema 3.26, forme-se o conjunto:

$$\alpha = \{\mathrm{ord}(B, R) : \langle B, R\rangle \in C\}.$$

Por Corolário 3.19, α é um ordinal, pois é um conjunto transitivo de ordinais. De fato, se $\gamma \in \beta \in \alpha$, então $\beta = \mathrm{ord}(B, R)$ para algum $B \subseteq R$, donde $\gamma = \mathrm{ord}(B_b, R_b)$ para algum $b \in B$ por Lema 3.10, logo $\gamma \in \alpha$.

Por redução ao absurdo, suponhamos que existe uma injeção $f\colon \alpha \to A$. Então, onde:

$$B = \mathrm{Im}(f)$$
$$R = \{\langle f(\alpha), f(\beta)\rangle \in A \times A : \alpha \in \beta\}.$$

Claramente $\alpha = \mathrm{ord}(B, R)$ e $\langle B, R\rangle \in C$. Logo $\alpha \in \alpha$, o que é contradição. □

Isto implica um resultado profundo:

Teorema 9.4 (*em* ZF). *As afirmações seguintes são equivalentes:*

sth:choice:hartogs:equivwo
1. *O Axioma da Boa Ordenação*

sth:choice:hartogs:equivcompare
2. *Ou $A \preceq B$ ou $B \preceq A$, para quaisquer conjuntos A e B*

Prova. *(1) ⇒ (2).* Fixem-se A e B. Invocando (1), existem boas ordenações $\langle A, R\rangle$ e $\langle B, S\rangle$. Invocando Teorema 3.26, sejam $f\colon \alpha \to \langle A, R\rangle$ e $g\colon \beta \to \langle B, S\rangle$ isomorfismos. Por Proposição 3.22, ou $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$. Se $\alpha \subseteq \beta$, então $g \circ f^{-1}\colon A \to B$ é uma injeção, logo $A \preceq B$; analogamente, se $\beta \subseteq \alpha$ então $B \preceq A$.

(2) ⇒ (1). Fixe-se A; por Lema 9.3 existe algum ordinal β tal que $\beta \not\preceq A$. Invocando (2), temos $A \preceq \beta$. Logo existe alguma injeção $f\colon A \to \beta$, e podemos usar esta injecção para bem ordenar os elementos de A, definindo uma ordem $\{\langle a, b\rangle \in A \times A : f(a) \in f(b)\}$. □

Como consequência imediata: se a Boa Ordenação falha, então alguns conjuntos são *literalmente incomparáveis* quanto ao tamanho. Assim, se a Boa Ordenação falha, a aritmética cardinal transfinita ficará complicada. Por exemplo, teremos de abandonar a ideia de que, se A e B são infinitos, então $A \sqcup B \approx A \times B \approx M$, onde M é o maior de A e B (ver Teorema 8.11). O problema é simples: se não podemos *comparar* o tamanho de A e B, então não faz sentido perguntar qual é o maior.

9.4 O Problema da Boa Ordenação

sth:choice:woproblem:sec
Evidentemente que muito depende de aceitarmos ou não a Boa Ordenação. Mas a discussão deste princípio tendeu a concentrar-se num equivalente, o Axioma da Escolha. Voltemos então a atenção para esse axioma (e provemos a equivalência).

Em 1883, Cantor exprimiu o seu apoio ao Axioma da Boa Ordenação, chamando-lhe "uma lei do pensamento que me parece fundamental, rica nas suas consequências e particularmente notável pela sua generalidade" (citado em Potter 2004, p. 243). Mas Cantor acabou por convencer-se de que o "Axioma" precisava de prova. A comunidade matemática também.

O problema foi "resolvido" por Zermelo em 1904. Para explicar a solução, precisamos de algumas definições.

Definição 9.5. Uma função f é uma *função de escolha* sse $f(x) \in x$ para todo o $x \in \mathrm{dom}(f)$. Dizemos que f é uma *função de escolha para A* sse f é uma função de escolha com $\mathrm{dom}(f) = A \setminus \{\emptyset\}$.

Intuitivamente, para cada conjunto (não vazio) $x \in A$, uma função de escolha para A *escolhe* um elemento particular, $f(x)$, de x. O Axioma da Escolha é então:

Escolha (Escolha). Todo o conjunto tem uma função de escolha.

Zermelo mostrou que a Escolha implica a boa ordenação, e vice-versa:

Teorema 9.6 (em ZF). *A Boa Ordenação e a Escolha são equivalentes.* *sth:choice:woproblem: thmwochoice*

Prova. Da esquerda para a direita. Seja A um conjunto de conjuntos. Então $\bigcup A$ existe pelo Axioma da União, e logo, pela Boa Ordenação, existe alguma relação $<$ que bem ordena $\bigcup A$. Seja agora $f(x) =$ o membro $<$-mínimo de x. Isto é uma função de escolha para A.

Da direita para a esquerda. Fixe-se A. Pela Escolha, existe uma função de escolha, f, para $\wp(A) \setminus \{\emptyset\}$. Usando Recursão Transfinita, defina-se uma função:

$$g(0) = f(A)$$
$$g(\alpha) = \begin{cases} \text{parar!} & \text{se } A = g[\alpha] \\ f(A \setminus g[\alpha]) & \text{caso contrário} \end{cases}$$

A indicação "parar!" é apenas uma abreviatura para o que seria de outro modo uma definição mais longa. Ou seja, quando $A = g[\alpha]$ pela primeira vez, seja $g(\delta) = A$ para todo o $\delta \leq \alpha$. Agora, em primeiro lugar, só podemos ter a certeza de que isto define um *termo* (ver as observações após Teorema 4.4); mas mostraremos que de fato temos uma função.

Como f é função de escolha, para cada α (quando definido) temos $g(\alpha) = f(A \setminus g[\alpha]) \in A \setminus g[\alpha]$; isto é, $g(\alpha) \notin g[\alpha]$. Logo, se $g(\alpha) = g(\beta)$ então $g(\beta) \notin g[\alpha]$, isto é, $\beta \notin \alpha$, e analogamente $\alpha \notin \beta$. Logo $\alpha = \beta$, por Tricotomia. Assim, g é injetiva.

Observe-se a seguir que de fato paramos!, isto é, que existe algum ordinal mínimo α tal que $A = g[\alpha]$. De fato, suponhamos o contrário; então, como g é injetiva, teríamos $\alpha \prec \wp(A) \setminus \{\emptyset\}$ para todo o ordinal α, contradizendo Lema 9.3. Daí também $\mathrm{Im}(g) = A$.

Reunindo estes fatos, g é uma bijeção de algum ordinal para A. Agora, g pode ser usada para bem ordenar A. □

Assim, a Boa Ordenação e a Escolha estão de pé ou caem juntas. Mas a questão permanece: estão de pé ou caem?

9.5 Escolha Enumerável

É fácil provar, sem usar Escolha/Boa Ordenação, que: *sth:choice:countablechoice: sec*

Lema 9.7 (em $\mathbf{Z}^-$). *Todo o conjunto finito tem uma função de escolha.*

Prova. Seja $a = \{b_1, \ldots, b_n\}$. Suponhamos, por simplicidade, que cada $b_i \neq \emptyset$. Logo existem objetos $c_1, \ldots, c_n$ tais que $c_1 \in b_1, \ldots, c_n \in b_n$. Agora, por Proposição 2.5, o conjunto $\{\langle b_1, c_1\rangle, \ldots, \langle b_n, c_n\rangle\}$ existe; e isto é uma função de escolha para a. □

Mas a situação complica-se logo que consideramos conjuntos infinitos. Por exemplo, considere-se esta extensão "mínima" do resultado acima:

> *Escolha Enumerável.* Todo o conjunto *enumerável* tem uma função de escolha.

Isto é um caso particular da Escolha. E verifica-se que este princípio foi invocado com alguma frequência, sem uma consciência óbvia do seu uso. Eis dois bons exemplos.[2]

Exemplo 9.8. Eis um pensamento natural: para qualquer conjunto A, ou $\omega \preceq A$, ou $A \approx n$ para algum $n \in \omega$. Esta é uma maneira de exprimir a ideia intuitiva de que todo o conjunto é finito ou infinito. Cantor, e muitos outros matemáticos, fizeram esta afirmação sem a provar. Com a cautela que nos caracteriza, a provamos em Teorema 7.7. Mas nessa prova estávamos a trabalhar em **ZFC**, pois assumíamos que qualquer conjunto A pode ser bem ordenado, e logo que $|A|$ está garantidamente definido. Ou seja: assumimos explicitamente a Escolha.

De fato, Dedekind (1888) ofereceu a sua própria prova desta afirmação, do seguinte modo:

Teorema 9.9 (em $\mathbf{Z}^- +$ Escolha Enumerável). *Para qualquer A, ou $\omega \preceq A$ ou $A \approx n$ para algum $n \in \omega$.*

Prova. Suponhamos $A \not\approx n$ para todo o $n \in \omega$. Então, em particular, para cada $n < \omega$ existe um subconjunto $A_n \subseteq A$ com exatamente 2^n elementos. Usando esta sequência $A_0, A_1, A_2, \ldots$, definimos para cada n:

$$B_n = A_n \setminus \bigcup_{i<n} A_i.$$

Note-se o seguinte

$$\begin{aligned}\left|\bigcup_{i<n} A_n\right| &\leq |A_0| + |A_1| + \ldots + |A_{n-1}| \\ &= 1 + 2 + \ldots + 2^{n-1} \\ &= 2^n - 1 \\ &< 2^n = |A_n|\end{aligned}$$

[2] Devidos a Potter (2004, §9.4) e Luca Incurvati.

Logo cada B_n tem pelo menos um membro, c_n. Além disso, os B_n são dois a dois disjuntos; assim, se $c_n = c_m$ então $n = m$. Mas cada $c_n \in A$. Logo a função $f(n) = c_n$ é uma injecção $\omega \to A$. □

Dedekind não assinalou que tinha usado a Escolha Enumerável. Mas reparou o leitor no seu uso? Olhe de novo. (De fato: *olhe de novo.*)

A prova usou a Escolha Enumerável duas vezes. A usamos uma vez, para obter a nossa sequência de conjuntos A_0, A_1, A_2, ... Voltamos a usá-la para seleccionar os elementos c_n de cada B_n. Além disso, este uso da Escolha é irredutível. Cohen (1966, p. 138) provou que o resultado falha se não tivermos qualquer versão da Escolha. Ou seja: é consistente com **ZF** que existam conjuntos *incomparáveis* com ω.

Exemplo 9.10. Em 1878, Cantor afirmou que uma união enumerável de conjuntos enumeráveis é enumerável. Não apresentou prova, talvez por considerar a prova óbvia. Agora, com a nossa cautela, provamos uma versão mais geral deste resultado em Proposição 8.12. Mas a nossa prova assumiu explicitamente a Escolha. E mesmo a prova do resultado menos geral requer a Escolha Enumerável.

Teorema 9.11 (em $\mathbf{Z}^- + $ Escolha Enumerável). *Se A_n é enumerável para cada $n \in \omega$, então $\bigcup_{n<\omega} A_n$ é enumerável.*

Prova. Sem perda de generalidade, suponhamos que cada $A_n \neq \emptyset$. Logo, para cada $n \in \omega$ existe uma sobrejeção $f_n : \omega \to A_n$. Defina-se $f : \omega \times \omega \to \bigcup_{n<\omega} A_n$ por $f(m, n) = f_n(m)$. O resultado segue porque $\omega \times \omega$ é enumerável (**??**) e f é uma sobrejeção. □

Notou o uso da Escolha Enumerável? Serve para escolher a nossa sequência de funções f_0, f_1, f_2, ...[3] E, de novo, o resultado falha na ausência de qualquer princípio de Escolha. Especificamente, Feferman and Levy (1963) provou que é consistente com **ZF** que uma união enumerável de conjuntos enumeráveis tenha cardinalidade $\beth_1$. Mas eis uma formulação bem mais divertida do ponto, de Russell:

> Isto ilustra-se com o milionário que comprava um par de meias sempre que comprava um par de botas, e nunca noutra ocasião, e que tinha tal paixão por comprar ambos que acabou por ter $\aleph_0$ pares de botas e $\aleph_0$ pares de meias... Nas botas podemos distinguir direita e esquerda, e portanto podemos fazer uma seleção de uma em cada par, nomeadamente, podemos escolher todas as botas direitas ou todas as esquerdas; mas com as meias não se impõe qualquer princípio de seleção, e não podemos ter a certeza, a menos que assumamos o axioma multiplicativo [isto é, em efeito, a Escolha], de que existe alguma classe constituída por uma meia de cada par. (Russell, 1919, p. 126)

[3] Um uso semelhante da Escolha ocorreu em Proposição 8.12, quando demos a instrução "Para cada $\beta \in \mathfrak{a}$, fixe uma injeção f_β".

Em suma, alguma forma de Escolha é necessária para provar o seguinte: se tem uma quantidade enumerável de pares de meias, então tem (apenas) uma quantidade enumerável de meias. E, de fato, sem a Escolha Enumerável (ou algo equivalente), uma união enumerável de conjuntos enumeráveis pode deixar de ser enumerável.

A moral é que a Escolha Enumerável foi usada repetidamente, sem grande consciência por parte de quem a usava. A questão filosófica é: como poderíamos *justificar* a Escolha Enumerável?

Uma tentativa de justificação intuitiva poderia apelar a uma super-tarefa. Suponhamos que fazemos a primeira escolha em $1/2$ minuto, a segunda em $1/4$ minuto, ..., a n-ésima em $1/2^n$ minuto, ... Então, dentro de 1 minuto, teremos feito uma ω-sequência de escolhas, e definido uma função de escolha.

Mas que poderia realmente dizer-nos um tal experimento mental? Para começar, depende de tomar a ideia de "escolher" de modo bastante literal. Para além disso, parece atar a matemática a possibilidades metafísicas.

Mais importante: não nos dará justificação para a Escolha *sem reservas*, em vez da *mera* Escolha Enumerável. Porque, se precisarmos que *todo* o conjunto tenha função de escolha, então precisaremos de poder realizar uma "super-tarefa de comprimento ordinal arbitrário." Sem rodeios, essa ideia é risível.

9.6 Considerações Intrínsecas sobre a Escolha

sth:choice:justifications:sec

A questão mais ampla, então, é se a Boa Ordenação, ou a Escolha, ou de fato a comparabilidade de todos os conjuntos quanto ao tamanho—não importa qual—podem ser justificadas.

Eis uma tentativa de justificação *intrínseca*. De volta a Seção 2.1, introduzimos vários princípios sobre a hierarquia. Um deles merece ser repetido:

> *Estágios-acumulam.* Para qualquer estágio S, e para quaisquer conjuntos que foram formados *antes* do estágio S: forma-se no estágio S um conjunto cujos membros são exatamente esses conjuntos. Nada mais se forma no estágio S.

De fato, muitos autores sugeriram que o Axioma da Escolha pode ser justificado via (algo como) este princípio. Daremos brevemente um resumo dessa abordagem.

Começamos por um resultado simples, que oferece *mais uma* formulação equivalente da Escolha:

sth:choice:justifications:choiceset

Teorema 9.12 (em ZF). *A Escolha é equivalente ao princípio seguinte. Se os membros de A são disjuntos dois a dois e não vazios, então existe algum C tal que $C \cap x$ é um singular para todo o $x \in A$. (Chamamos a tal C um conjunto de escolha para A.)*

A prova deste resultado é direta, e a deixamos como exercício para o leitor.

Problema 9.1. Prove Teorema 9.12. Se tiver dificuldades, encontrará uma prova em (Potter, 2004, pp. 242–3).

O ponto essencial é que um conjunto de escolha para A é precisamente o contradomínio de uma função de escolha para A. Assim, para justificar a Escolha, podemos simplesmente tentar justificar a sua formulação equivalente, em termos da existência de conjuntos de escolha. E é exatamente isso que faremos agora.

Sejam os membros de A disjuntos dois a dois e não vazios. Por *Estágios-são-chave* (ver Seção 2.1), A é formado em algum estágio S. Note-se que todos os membros de $\bigcup A$ estão disponíveis antes do estágio S. Agora, por *Estágios-acumulam*, para *quaisquer* conjuntos formados antes de S, forma-se um conjunto cujos membros são exatamente esses conjuntos. Dito de outro modo: toda a *possível* coleção de conjuntos disponíveis mais cedo existirá em S. Mas é certamente *possível* seleccionar objetos que possam ser reunidos num conjunto de escolha para A; isso é apenas um certo subconjunto muito específico de $\bigcup A$. Logo: existe tal conjunto de escolha, como requerido.

Bem, esta é uma tentativa *muito* rápida de oferecer uma justificação da Escolha por razões intrínsecas. Mas, para aprofundar esta ideia, deve ler o desenvolvimento elegante de Potter (2004, §14.8).

9.7 Paradoxo de Banach–Tarski

sth:choice:banach:sec

Também podemos tentar justificar a Escolha, como Boolos tentou justificar a Substituição, apelando a considerações *extrínsecas* (ver Seção 5.3). Afinal, adotar a Escolha tem muitas consequências desejáveis: poder comparar qualquer par de cardinais; poder bem ordenar qualquer conjunto; poder tratar os cardinais como um tipo particular de ordinal; etc.

Por vezes, contudo, afirma-se que a Escolha tem consequências *indesejáveis*. Na maior parte dos casos, isso deve-se a um resultado de Banach and Tarski (1924).

Teorema 9.13 (Paradoxo de Banach–Tarski (em ZFC)). *Qualquer bola pode ser decomposta num número finito de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias dessa bola.*

À primeira vista, isto surpreende. Claramente as duas bolas têm *o dobro* do volume da bola original. Mas os movimentos rígidos—rotação e transporte—não alteram o volume. Parece assim que Banach–Tarski nos permite fazer aparecer matéria nova por magia.

Pior ainda.[4] Raciocínio semelhante mostra que uma ervilha pode ser cortada num número finito de peças, que depois podem ser remontadas (por rotação e transporte) de modo a formar um objeto com a forma e o tamanho do Big Ben.

[4] Ver Tomkowicz and Wagon (2016, Theorem 3.12).

Nada disto, porém, vale em **ZF** isoladamente.[5] Logo temos de decidir: rejeitar a Escolha, ou aprender a viver com o "paradoxo".

Sugerimos que devemos aprender a viver com o "paradoxo". De fato, não nos parece propriamente um paradoxo. Em particular, não vemos por que haveria de ser mais ou menos paradoxal do que qualquer um dos resultados seguintes:[6]

1. Há tantos pontos no intervalo $(0, 1)$ como em $\mathbb{R}$.
   Prova: considere-se $\tan(\pi(r - 1/2))$.

2. Há tantos pontos numa reta como num quadrado.
   Ver **??** e **??**.

3. Existem curvas que preenchem o espaço.
   Ver **??** e **??**.

Nenhum destes três resultados requer a Escolha. De fato, já os tratamos simplesmente como matemática surpreendente e bela. Talvez devêssemos adotar a mesma atitude perante o Paradoxo de Banach–Tarski.

Com certeza, é necessária aqui uma observação técnica; mas basta manter a cabeça fria. Os movimentos rígidos preservam volume. Consequentemente, as cinco[7] peças em que a bola é decomposta não podem todas ser *mensuráveis*. Grosso modo, não faz sentido atribuir volume a estas peças individualmente. Deve pensar nelas como dispersões infinitas de pontos impossíveis de visualizar. Agora, pode ser "estranho" conceber tais conjuntos "infinitamente dispersos". Mas a sua existência parece seguir da injunção, incorporada em *Estágios-acumulam*, de que se formem *todas* as coleções possíveis de conjuntos disponíveis mais cedo.

Se nada disto convence, eis um último argumento (extrínseco) a favor de abraçar o Paradoxo de Banach–Tarski. Ele implica de imediato a melhor piada matemática de sempre:

> *Pergunta.* O que é um anagrama de "Banach–Tarski"?
>
> *Resposta.* "Banach–Tarski Banach–Tarski".

9.8 Apêndice: Paradoxo de Vitali

sth:choice:vitali:sec

Para ter uma ideia real de se a construção de Banach–Tarski é aceitável ou não, devíamos examinar a sua *prova*. Infelizmente, isso exigiria muito mais

[5] Embora Banach–Tarski possa ser provado com princípios estritamente mais fracos do que a Escolha; ver Tomkowicz and Wagon (2016, 303).

[6] Potter (2004, 276–7), Weston (2003, 16), Tomkowicz and Wagon (2016, 31, 308–9) fazem pontos semelhantes, com outros exemplos.

[7] Enunciamos o Paradoxo em termos de "número finito de peças". De fato, Robinson (1947) provou que a decomposição pode ser feita com *cinco* peças (mas não menos). Para uma prova, ver Tomkowicz and Wagon (2016, pp. 66–7).

álgebra do que podemos apresentar aqui. Contudo, podemos oferecer algumas observações rápidas que talvez esclareçam a prova de Banach–Tarski,[8] concentrando-nos no resultado seguinte:

Teorema 9.14 (Paradoxo de Vitali (em ZFC)). *Qualquer círculo pode ser decomposto numa quantidade enumerável de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias desse círculo.* *sth:choice:vitali: vitaliparadox*

O Paradoxo de Vitali é muito mais fácil de provar do que o Paradoxo de Banach–Tarski. Chamamos-lhe "Paradoxo de Vitali", pois segue-se da construção, em 1905, de um conjunto não mensurável. Mas os aspectos conjuntistas da prova do Paradoxo de Vitali e do Paradoxo de Banach–Tarski são muito semelhantes. A diferença essencial entre os resultados é que Banach–Tarski considera uma decomposição *finita*, enquanto o Paradoxo de Vitali considera uma decomposição *enumerável infinita*. Como Weston (2003) diz, o Paradoxo de Vitali "certamente não é tão notável como o paradoxo de Banach–Tarski, mas ilustra que paradoxos geométricos podem ocorrer mesmo em situações 'simples'."

O Paradoxo de Vitali trata de uma figura bidimensional, um círculo. Logo trabalhamos no plano, $\mathbb{R}^2$. Seja R o conjunto das rotações (no sentido dos ponteiros do relógio) de pontos em torno da origem por valores em radianos *racionais* no intervalo $[0, 2\pi)$. Eis alguns fatos algébricos sobre R (se não compreender o enunciado do resultado, a prova esclarecerá o seu significado):

Lema 9.15. *R forma um grupo abeliano sob a composição de funções.* *sth:choice:vitali: rotationsgroupabelian*

Prova. Escrevendo 0_R para a rotação por 0 radianos, este é um elemento neutro para R, pois $\rho \circ 0_R = 0_R \circ \rho = \rho$ para qualquer $\rho \in R$.

Todo o elemento tem inverso. Onde $\rho \in R$ roda por r radianos, $\rho^{-1} \in R$ roda por $2\pi - r$ radianos, de modo que $\rho \circ \rho^{-1} = 0_R$.

A composição é associativa: $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$ para quaisquer $\rho, \sigma, \tau \in R$

A composição é comutativa: $\sigma \circ \rho = \rho \circ \sigma$ para quaisquer $\rho, \sigma \in R$. □

De fato, podemos partir o nosso grupo R ao meio e depois usar qualquer metade para recuperar o grupo inteiro:

Lema 9.16. *Existe uma partição de R em dois conjuntos disjuntos, R_1 e R_2, ambos dos quais são uma base para R.* *sth:choice:vitali: disjointgroup*

Prova. Seja R_1 o conjunto das rotações por valores racionais em radianos em $[0, \pi)$; seja $R_2 = R \setminus R_1$. Por álgebra elementar, $\{\rho \circ \rho : \rho \in R_1\} = R$. Um resultado semelhante obtém-se para R_2. □

[8] Para um tratamento bem mais completo, ver Weston (2003) ou Tomkowicz and Wagon (2016).

Usaremos este fato sobre grupos para estabelecer Teorema 9.14. Seja $\mathbf{S}$ o círculo unitário, isto é, o conjunto dos pontos exatamente a 1 unidade da origem do plano, isto é, $\{\langle r, s\rangle \in \mathbb{R}^2 : \sqrt{r^2 + s^2} = 1\}$. Partiremos $\mathbf{S}$ em partes considerando a relação seguinte em $\mathbf{S}$:

$$r \sim s \text{ sse } (\exists \rho \in R)\rho(r) = s.$$

Ou seja, os pontos de $\mathbf{S}$ estão ligados por esta relação sse se pode passar de um para o outro por uma rotação de valor racional em torno da origem. Sem surpresa:

Lema 9.17. *$\sim$ é uma relação de equivalência.*

Prova. Trivial, usando Lema 9.15. □

Invocamos agora a Escolha para obter um conjunto, C, contendo exatamente um membro de cada classe de equivalência de $\mathbf{S}$ sob $\sim$. Ou seja, consideramos uma função de escolha f no conjunto das classes de equivalência,[9]

$$E = \{[r]_\sim : r \in \mathbf{S}\},$$

e seja $C = \mathrm{Im}(f)$. Para cada rotação $\rho \in R$, o conjunto $\rho[C]$ consiste nos pontos obtidos ao aplicar a rotação ρ a cada ponto de C. Os dois resultados seguintes mostram que estes conjuntos cobrem o círculo por completo e sem sobreposição:

sth:choice:vitali: vitalicover

Lema 9.18. $\mathbf{S} = \bigcup_{\rho \in R} \rho[C]$.

Prova. Fixe-se $s \in \mathbf{S}$; existe algum $r \in C$ tal que $r \in [s]_\sim$, isto é, $r \sim s$, isto é, $\rho(r) = s$ para algum $\rho \in R$. □

sth:choice:vitali: vitalinooverlap

Lema 9.19. *Se $\rho_1 \neq \rho_2$ então $\rho_1[C] \cap \rho_2[C] = \emptyset$.*

Prova. Suponhamos $s \in \rho_1[C] \cap \rho_2[C]$. Logo $s = \rho_1(r_1) = \rho_2(r_2)$ para alguns $r_1, r_2 \in C$. Daí $\rho_2^{-1}(\rho_1(r_1)) = r_2$, e $\rho_2^{-1} \circ \rho_1 \in R$, logo $r_1 \sim r_2$. Logo $r_1 = r_2$, pois C selecciona exatamente um membro de cada classe de equivalência sob $\sim$. Logo $s = \rho_1(r_1) = \rho_2(r_1)$, e portanto $\rho_1 = \rho_2$. □

Aplicamos agora os fatos algébricos anteriores ao nosso círculo:

sth:choice:vitali: pseudobanachtarski

Lema 9.20. *Existe uma partição de $\mathbf{S}$ em dois conjuntos disjuntos, D_1 e D_2, tal que D_1 pode ser particionado numa quantidade enumerável de conjuntos que podem ser rodados de modo a formar uma cópia de $\mathbf{S}$ (e analogamente para D_2).*

[9] Como R é enumerável, cada membro de E é enumerável. Como $\mathbf{S}$ é não enumerável, segue-se de Lema 9.18 e Proposição 8.12 que E é não enumerável. Logo isto é um uso de Escolha *não* enumerável.

Prova. Usando R_1 e R_2 de Lema 9.16, seja:

$$D_1 = \bigcup_{\rho \in R_1} \rho[C] \qquad\qquad D_2 = \bigcup_{\rho \in R_2} \rho[C]$$

Isto é uma partição de $\mathbf{S}$, por Lema 9.18, e D_1 e D_2 são disjuntos por Lema 9.19. Por construção, D_1 pode ser particionado numa quantidade enumerável de conjuntos, $\rho[C]$ para cada $\rho \in R_1$. E estes podem ser rodados de modo a formar uma cópia de $\mathbf{S}$, pois $\mathbf{S} = \bigcup_{\rho \in R} \rho[C] = \bigcup_{\rho \in R_1} (\rho \circ \rho)[C]$ por Lema 9.16 e Lema 9.18. O mesmo raciocínio vale para D_2. □

Isto implica de imediato o Paradoxo de Vitali. Pois podemos gerar *duas* cópias de $\mathbf{S}$ a partir de $\mathbf{S}$, apenas partindo-o numa quantidade enumerável de peças (os vários $\rho[C]$) e depois movendo-as rigidamente (basta rodar cada peça de D_1, e primeiro transportar e depois rodar cada peça de D_2).

Recapitulemos a estratégia de prova. Começamos com fatos algébricos sobre o grupo de rotações no plano. Usamos este grupo para partir $\mathbf{S}$ em classes de equivalência. Chegamos então a um "paradoxo", usando a Escolha para seleccionar elementos de cada classe.

Usamos exatamente a mesma estratégia para provar Banach–Tarski. A principal diferença é que os fatos algébricos usados na prova de Banach–Tarski são bastante mais complicados do que os usados no Paradoxo de Vitali. Mas esses fatos algébricos nada têm a ver com a Escolha. Resumimos-os rapidamente.

Para provar Banach–Tarski, começamos por estabelecer um análogo de Lema 9.16: qualquer *grupo livre* pode ser partido em quatro peças que, intuitivamente, podemos "mover" de modo a recuperar duas cópias do grupo inteiro.[10] Mostramos depois que podemos usar duas rotações particulares em torno da origem de $\mathbb{R}^3$ para gerar um grupo livre de rotações, F.[11] (Ainda sem Escolha.) Consideramos agora pontos na superfície da esfera como "semelhantes" sse um pode obter-se do outro por uma rotação em F. *Usamos então a Escolha* para seleccionar exatamente um ponto de cada classe de equivalência de pontos "semelhantes". Aplicando a nossa divisão de F à superfície da esfera, como em Lema 9.20, partimos essa superfície em quatro peças, que podemos "mover" de modo a obter duas cópias da superfície da esfera. E isto estabelece (Hausdorff, 1914):

Teorema 9.21 (Paradoxo de Hausdorff (em ZFC)). *A superfície de qualquer esfera pode ser decomposta num número finito de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias disjuntas dessa esfera.*

[10] O fato de podermos usar *quatro* peças deve-se a Robinson (1947). Para uma prova recente, ver Tomkowicz and Wagon (2016, Theorem 5.2). Seguimos Weston (2003, p. 3) ao descrever isto como "mover" as peças do grupo.

[11] Ver Tomkowicz and Wagon (2016, Theorem 2.1).

Ainda são precisos alguns truques algébricos para obter o Teorema completo de Banach–Tarski (que não diz só respeito à superfície da esfera, mas também ao seu interior). Francamente, porém, isto é apenas a cereja no topo do bolo algébrico. Por isso Weston escreve:

> [...] o resultado sobre grupos livres é o passo *chave* na prova do paradoxo de Banach–Tarski. Deste ponto de vista, o paradoxo de Banach–Tarski não é tanto uma afirmação sobre $\mathbb{R}^3$ quanto uma afirmação sobre a complexidade do grupo [das translações e rotações em $\mathbb{R}^3$]. (Weston, 2003, p. 16)

Ou seja: podermos ou não oferecer uma decomposição *finita* (como em Banach–Tarski) ou uma decomposição *enumerável infinita* (como no Paradoxo de Vitali) resume-se a certos fatos de teoria dos grupos sobre trabalhar em duas ou três dimensões.

Admitidamente, esta última observação estraga ligeiramente a piada no final de Seção 9.7. Por ser bidimensional, "Banach–Tarski" tem de ser dividido numa *infinidade* enumerável de peças, se se quiserem rearranjar essas peças de modo a formar "Banach–Tarski Banach–Tarski". Para consertar a piada, é preciso escrever em três dimensões. Deixamos isto como exercício para o leitor.

Um último comentário. Na Seção 9.7, mencionamos que as "peças" da esfera que se obtêm não podem ser *mensuráveis*, mas têm de ser dispersões infinitas impossíveis de visualizar. O mesmo vale para o nosso uso da Escolha ao obter Lema 9.20. E tudo isto merece explicação.

De novo, devemos esboçar alguma base (mas isto é *apenas* um esboço; talvez queira consultar uma entrada de manual sobre *medida*). Definir uma medida para um conjunto X é atribuir um valor $\mu(E) \in \mathbb{R}$ a cada E nalguma "σ-álgebra" sobre X. Os detalhes aqui não são essenciais, exceto que a função μ deve obedecer ao princípio da aditividade enumerável: a medida de uma união enumerável de conjuntos disjuntos é a soma das medidas individuais, isto é, $\mu(\bigcup_{n<\omega} X_n) = \sum_{n<\omega} \mu(X_n)$ sempre que os X_n são disjuntos. Dizer que um conjunto é "não mensurável" é dizer que nenhuma medida pode ser atribuída de modo adequado. Agora, usando o nosso R de antes:

Corolário 9.22 (Vitali). *Seja μ uma medida tal que $\mu(\mathbf{S}) = 1$, e tal que $\mu(X) = \mu(Y)$ se X e Y são congruentes. Então $\rho[C]$ é não mensurável para todo o $\rho \in R$.*

Prova. Por redução ao absurso, suponhamos o contrário. Seja então $\mu(\sigma[C]) = r$ para algum $\sigma \in R$ e algum $r \in \mathbb{R}$. Para qualquer $\rho \in R$, $\rho[C]$ e $\sigma[C]$ são congruentes, logo $\mu(\rho[C]) = r$ para qualquer $\rho \in R$. Por Lema 9.18 e Lema 9.19, $\mathbf{S} = \bigcup_{\rho\in R} \rho[C]$ é uma união enumerável de conjuntos disjuntos dois a dois. Logo a aditividade enumerável dita que $\mu(\mathbf{S}) = 1$ é a soma das medidas de cada $\rho[C]$, isto é,

$$1 = \mu(\mathbf{S}) = \sum_{\rho\in R} \mu(\rho[C]) = \sum_{\rho\in R} r$$

Mas se $r = 0$ então $\sum_{\rho\in R} r = 0$, e se $r > 0$ então $\sum_{\rho\in R} r = \infty$. □

Créditos das Imagens

Referências Bibliográficas

Banach, Stefan and Alfred Tarski. 1924. Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fundamenta Mathematicae* 6: 244–77.

Benacerraf, Paul. 1965. What numbers could not be. *The Philosophical Review* 74(1): 47–73.

Boolos, George. 1971. The iterative conception of set. *The Journal of Philosophy* 68(8): 215–31.

Boolos, George. 1989. Iteration again. *Philosophical Topics* 17(2): 5–21.

Boolos, George. 2000. Must we believe in set theory? In *Between Logic and Intuition: Essays in Honor of Charles Parsons*, eds. Gila Sher and Richard Tieszen, 257–68. Cambridge: Cambridge University Press.

Burali-Forti, Cesare. 1897. Una questione sui numeri transfiniti. *Rendiconti del Circolo Matematico di Palermo* 11: 154–64.

Button, Tim. 2021. Level theory, part 1: Axiomatizing the bare idea of a cumulative hierarchy of sets. *The Bulletin of Symbolic Logic* 27(4): 436–460.

Cantor, Georg. 1878. Ein Beitrag zur Mannigfaltigkeitslehre. *Journal für die reine und angewandte Mathematik* 84: 242–58.

Cantor, Georg. 1883. *Grundlagen einer allgemeinen Mannigfaltigkeitslehre. Ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen.* Leipzig: Teubner.

Cohen, Paul J. 1963. The independence of the continuum hypothesis. *Proceedings of the National Academy of Sciences of the United States of America* 24: 556–557.

Cohen, Paul J. 1966. *Set Theory and the Continuum Hypothesis.* Reading, MA: Benjamin.

Dedekind, Richard. 1888. *Was sind und was sollen die Zahlen?* Braunschweig: Vieweg.

Ebbinghaus, Heinz-Dieter, Craig G. Fraser, and Akihiro Kanamori. 2010. *Ernst Zermelo. Collected Works*, vol. 1. Berlin: Springer-Verlag.

Feferman, Solomon and Azriel Levy. 1963. Independence results in set theory by Cohen's method II. *Notices of the American Mathematical Society* 10: 593.

Fraenkel, Abraham. 1922. Über den Begriff 'definit' und die Unabhängigkeit des Auswahlaxioms. *Sitzungsberichte der Preussischen Akadademie der Wissenschaften, Physikalisch-mathematische Klasse* 253–257.

Frege, Gottlob. 1884. *Die Grundlagen der Arithmetik: Eine logisch mathematische Untersuchung über den Begriff der Zahl*. Breslau: Wilhelm Koebner. Translation in Frege (1953).

Frege, Gottlob. 1953. *Foundations of Arithmetic*, ed. J. L. Austin. Oxford: Basil Blackwell & Mott, 2nd ed.

Gödel, Kurt. 1938. The consistency of the axiom of choice and the generalized continuum hypothesis. *Proceedings of the National Academy of Sciences of the United States of America* 50: 1143–8.

Hartogs, Friedrich. 1915. Über das Problem der Wohlordnung. *Mathematische Annalen* 76: 438–43.

Hausdorff, Felix. 1914. Bemerkung über den Inhalt von Punktmengen. *Mathematische Annalen* 75: 428–34.

Heck, Richard Kimberly. 2012. *Reading Frege's Grundgesetze*. Oxford: Oxford University Press.

Heijenoort, Jean van. 1967. *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*. Cambridge, MA: Harvard University Press.

Hume, David. 1740. *A Treatise of Human Nature*. London.

Incurvati, Luca. 2020. *Conceptions of Set and the Foundations of Mathematics*. Cambridge: Cambridge University Press.

Kunen, Kenneth. 1980. *Set Theory: An Introduction to Independence Proofs*. New York: North Holland.

Lévy, Azriel. 1960. Axiom schemata of strong infinity in axiomatic set theory. *Pacific Journal of Mathematics* 10(1): 223–38.

Linnebo, Øystein. 2010. Predicative and impredicative definitions. *Internet Encyclopedia of Philosophy* URL `http://www.iep.utm.edu/predicat/`.

Maddy, Penelope. 1988a. Believing the axioms I. *The Journal of Symbolic Logic* 53(2): 481–511.

Maddy, Penelope. 1988b. Believing the axioms II. *The Journal of Symbolic Logic* 53(3): 736–64.

Montague, Richard. 1961. Semantic closure and non-finite axiomatizability I. In *Infinitistic Methods: Proceedings of the Symposium on Foundations of Mathematics (Warsaw 1959)*, 45–69. New York: Pergamon.

Montague, Richard. 1965. Set theory and higher-order logic. In *Formal systems and recursive functions*, eds. John Crossley and Michael Dummett, 131–48. Amsterdam: North-Holland. Proceedings of the Eight Logic Colloquium, July 1963.

Potter, Michael. 2004. *Set Theory and its Philosophy*. Oxford: Oxford University Press.

Ramsey, Frank Plumpton. 1925. The foundations of mathematics. *Proceedings of the London Mathematical Society* 25: 338–384.

Robinson, Raphael. 1947. On the decomposition of spheres. *Fundamenta Mathematicae* 34(1): 246–60.

Russell, Bertrand. 1919. *Introduction to Mathematical Philosophy*. London: Allen & Unwin.

Scott, Dana. 1974. Axiomatizing set theory. In *Axiomatic Set Theory II*, ed. Thomas Jech, 207–14. American Mathematical Society. Proceedings of the Symposium in Pure Mathematics of the American Mathematical Society, July–August 1967.

Shoenfield, Joseph R. 1977. Axioms of set theory. In *Handbook of Mathematical Logic*, ed. Jon Barwise, 321–44. London: North-Holland.

Skolem, Thoralf. 1922. Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. In *Wissenschaftliche Vorträge gehalten auf dem fünften Kongress der skandanivschen Mathematiker in Helsingfors vom 4. bis zum 7. Juli 1922*, 137–52. Akademiska Bokhandeln.

Tomkowicz, Grzegorz and Stan Wagon. 2016. *The Banach-Tarski Paradox*. Cambridge: Cambridge University Press.

Vitali, Giuseppe. 1905. *Sul problema della misura dei gruppi di punti di una retta*. Bologna: Gamberini e Parmeggiani.

von Neumann, John. 1925. Eine Axiomatisierung der Mengenlehre. *Journal für die reine und angewandte Mathematik* 154: 219–40.

Weston, Tom. 2003. The Banach-Tarski paradox URL `http://people.math.umass.edu/~weston/oldpapers/banach.pdf`.

Whitehead, Alfred North and Bertrand Russell. 1910. *Principia Mathematica*, vol. 1. Cambridge: Cambridge University Press.

Zermelo, Ernst. 1904. Beweis, daß jede Menge wohlgeordnet werden kann. *Mathematische Annalen* 59: 514–516. English translation in (Ebbinghaus et al., 2010, pp. 115–119).

Zermelo, Ernst. 1908. Untersuchungen über die Grundlagen der Mengenlehre I. *Mathematische Annalen* 65: 261–81.