Teoria dos conjuntos

Charles Morgan*

* versão 1.0, 12/2/01

Sumário

Prefácio

Neste prefácio devo explicar porque estou escrevendo o livro e agradecer várias pessoas: Marco Antonio Fernandes e o Departemento de Matemática de UFBa (e Tania), CAPES, meus alunos no curso (particularmente Marival Julião de Araújo, Raimundo Leime Cergeuira e Taís Alves Dias de Azevedo), Regina e Davidson Fernandes dos Santos (e Bethânia), e Bia.

Capítulo 1. Introdução informal para os axiomas de ZF.*

1.1. Extensão. Nosso concepção de conjuntos vem dos conjuntos de objetos que conhecemos, como $\mathbf{N}$, $\mathbf{Q}$ e $\mathbf{R}$, e subconjuntos deles que podemos formar, que são determinados pelas propriedades dos objetos. Para dar duas exemplos muito simples:

$$\{r \in \mathbf{R} \mid 0 \leq r\} = \{r \in \mathbf{R} \mid r \text{ tem uma raiz quadrada em } \mathbf{R}\}$$

$$\{x \mid x \neq x\} = \{n \in \mathbf{N} \mid n \text{ é par, mas que 2 e um primo}\}.$$

(Esse último exemplo dá duas definicões de *conjunto vazio*, $\emptyset$).

A noção de conjunto é uma abstração da noção de propriedade. Então, se X, Y são conjuntos temos $\big(\forall x\,(\,x \in X \iff x \in Y)\big) \implies X = Y$.

Pode notar immediatemente que isso implica que o conjunto vazio é único:

1.2. Uniões. Logo que temos conjuntos como objetos podemos considerar conjuntos de conjuntos, por exemplo: $\{x_i \mid i \in I\}$ por I alguma conjunto de indices. Temos o conjunto que consiste em todos objetos que pertencem para qualquer x_i por $i \in I$. O conjunto indexando I não é relevante para nós, então $\bigcup\{x_i \mid i \in I\} = \bigcup_{i\in I} x_i$ pode ser escrito $\bigcup X$, onde $X = \{x_i \mid i \in I\}$.

Tipicamente vamos usar a, b, c, w, x, z, $\ldots$ como nomes de conjuntos, e podemos escrever $\bigcup x = \bigcup\{z \mid z \in x\} = \{w \mid \exists z \text{ tal que } w \in z \text{ e } z \in x\}$. Ou simplesmente: $\bigcup x = \{w \mid \exists z \in x\, w \in z\}$.

(Para explicar isso de novo temos

$$\bigcup_{y\in x} y = \bigcup\{y \mid y \in x\} = \bigcup\{z \mid \exists y \in x\; z \in y\}.$$

Então já mudamos nosso pensamento de pensar sobre conjuntos e elementos como coisas diferentes para pensar sobre todos conjuntos como coisas do mesmo tipo onde conjuntos pertencem para outras conjuntos.)

1.3. Conjuntos de potência Se x é um conjunto então $\mathcal{P}(X) = \{Z \mid Z \subseteq X\}$, o conjunto de todos os subconjuntos de x é também um conjunto.

Proposição. (Cantor) Não existe uma sobrejeção $f : X \longrightarrow \mathcal{P}(X)$ (uma função $f : X \longrightarrow \mathcal{P}(X)$ tal que por todos $Z \in \mathcal{P}(X)$ existe $x \in X$ tal que $f(x) = Z$.

Demonstração. Se f fosse uma tal sobrejeção poderíamos considerar $\{x \in X \mid x \notin f(x)\}, = A$, vamos falar. Como $A \subseteq X$ temos que $A \in \mathcal{P}(X)$ e logo existe $a \in X$ tal que $A = f(a)$ desde que f é uma sobrejeção. Mas olhe, agora temos $a \in A$ se e só se $a \notin A$, uma contradição!

Corolário. A coleção de todos conjuntos não é um conjunto.

* versão 1.2, 2/12/00

Demonstração. Vamos chamar a coleção de todos conjuntos por U no momento. Se U fosse um conjunto $\mathcal{P}(U)$ seria um conjunto também. Mas $\mathcal{P}(U)$ seria o conjunto de todos os subconjuntos de U, então para todos $x \in \mathcal{P}(U)$ teríamos $x \in U$ e logo teríamos $\mathcal{P}(U) \subseteq U$. Então existe uma sobrejeção $f : U \longrightarrow \mathcal{P}(U)$ dado pelo $x \mapsto x$ se $x \in \mathcal{P}(U)$ e $x \mapsto \emptyset$ se $x \notin \mathcal{P}(U)$. Contradição!

Frase de propoganda: "Não existe um conjunto universal!"

Esse corolário é as veces chamado *o paradoxo de Cantor*. O *paradoxo de Russell* pode ser obtido por botando f igual à função de identidade na demonstração de proposição em cima para ver que não existe um coleção $\{x \mid x \notin x\}$. (Isto é, se $\{x \mid x \notin x\}, = r$, vamos falar, fosse um conjunto, então a pergunta de se $c \in c$ ou $c \notin c$ daria a mesma contradição.) Claro, não são paradoxos de verdade, mas só fatos impressionantes/memoraveis.

O "paradoxo de Russell" mostra que não pode esperar para usar a extensão de todas propriedades matematicamente–algumas são inerentemente contradictória–e então dá uma razão porque vale a pena desenvolver a teoria dos conjuntos. Porém, eu deveria falar que a teoria de conjuntos começou e continua ser interessante e útil **não** para evitar paradoxos ou dar fundações ou saúde matemática, **mas** como uma parte da matemática (como as outras) com sua própria teoria, perguntas, etc., e com ligações matemáticas (no mesmo modo como as outras) com outros áreas.

1.4. Hierarquia cumulativa. Vamos ver o que podemos pegar com o conjunto vazio, conjuntos de potência e uniões, Começemos com $V_0 = \emptyset$ e apliquemos $\mathcal{P}$ repetidamente.

$$\begin{aligned}
V_0 &= \emptyset \\
V_1 &= \mathcal{P}(V_0) = \{\emptyset\} \\
V_2 &= \mathcal{P}(V_1) = \{\emptyset, \{\emptyset\}\} \\
V_3 &= \mathcal{P}(V_2) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}$$

Depois de todo estes passos finitos, juntemos tudo que já temos: $V_\omega = \bigcup\{V_n \mid n \text{ é finito}\}$.

Agora podemos começar aplicar $\mathcal{P}$ de novo: $V_{\omega+1} = \mathcal{P}(V_\omega)$, $V_{\omega+2} = \mathcal{P}(V_{\omega+1})$, ...

Pode "gerar" conjuntos em sua imaginação "para sempre."

(Os "V"s são por *von Neumann*, a primeira pessoa a pensar nissa hierarquia.)

Definição. Um *conjunto (puro)* é um membro de alguma V_α.

(Na verdade, o uso conjunto "puro" hoje parece muita antiquada – quase-ninguem fala isso e só mencionei o uso caso você encontre tal coisa num livro.)

O *universo* de conjuntos (gerado de $\emptyset$) é a coleção $V = \{x \mid \exists\alpha\,(\alpha \text{ indexa um passo na iteração } \& \; x \in V_\alpha)\}$. Como giria podemos falar que $V =$ "$\bigcup''\{V_\alpha \mid \alpha \text{ indexa um passo na iteração}\}$, mas como vimos, V não é um conjunto e este "união" não é uma união de um conjunto – temos que cada V_α é um conjunto mas não podemos tomar a união propriamente dita deles e formar V *como um conjunto*. Então temos que pensar sobre V como uma entidade não completado, e aí, V deve ser só uma abreviatura para nós – só vamos usa-la (mas tarde) nas coisas como "$x \in V$" querendo dizer "existe α tal que $x \in V_\alpha$." Mas mesmo assim é útil ter um nome na mão por esta coleção de todos conjuntos.

Proposição. Se α vem antes de β como um indice temos $V_\alpha \subseteq V_\beta$.

Demonstração. É óbvio se $\alpha = \beta$. Se V_β foi gerado pelo processo de tomar uma união também é claro (porque $V_\alpha \in \{V_\gamma \mid \gamma \text{ é antes de } \beta \text{ como um indice}\}$ e então se $x \in V_\alpha$ temos que $x \in \bigcup\{V_\gamma \mid \gamma \text{ é antes de } \beta \text{ como um índice}\}$).

Todávia, se $V_\beta = \mathcal{P}(V_\gamma)$ por alguma γ temos que saber que $V_\alpha \subseteq V_\gamma \Longrightarrow V_\alpha \subseteq \mathcal{P}(V_\gamma)$. Então vou interromper a demonstração por uma definição.

1.5 Conjuntos transitivos.

Definição. Um conjunto x é *transitivo* se $u \in v \in x \Longrightarrow u \in x$ (se e só se $u \in x \Longrightarrow u \subseteq x$, se e só se $\bigcup x \subseteq x$).

Para acabar a demonstração basta mostrar que cada V_α é transitivo. Porque, como $V_\alpha \subseteq V_\gamma$ temos $x \in V_\alpha \Longrightarrow x \in V_\gamma$, e se V_γ é transitivo temos $x \in V_\gamma \Longrightarrow x \subseteq V_\gamma$. Então $x \in V_\alpha \Longrightarrow x \subseteq V_\beta$. Mas $x \in V_\alpha \Longrightarrow x \subseteq V_\beta$ se e só se $V_\alpha \subseteq \mathcal{P}(V_\gamma)$, que é o que quisemos mostrar.

Mas todos V_α são transitivos pela proxima proposição.

Proposição. (i) $\emptyset$ é transitivo. (ii) Se x é transitivo então $\mathcal{P}(x)$ é transitivo. (iii) Uniões de conjuntos transitivos são transitivos.

Demonstração. (i) e (iii) são cada um triviais. (Pode ver porque?) (ii) Se $u \in v \in \mathcal{P}(x)$, temos $u \in v \subseteq x$ e então $u \in x$. Mas desde x é transitivo temos que $u \subseteq x$. Então $u \in \mathcal{P}(x)$.

Então podemos ver que todo V_α é transitivo indutivamente usando a proposição. E assim acabo a demonstração que se α é antes de β temos $V_\alpha \subseteq V_\beta$, por indução nos índices.

NOTA! Para falar que x é transitivo não quer dizer que $\in$ é uma relação transitivo sobre x ou qualquer coisa similar.

Usaramos implicitamente o princípio indutivo que $\forall\alpha\,\big((\forall\beta < \alpha\,\mathrm{Pr}(\beta)) \longrightarrow \mathrm{Pr}(\alpha)\big) \longrightarrow \forall\alpha\,\mathrm{Pr}(\alpha)$, onde $\mathrm{Pr}(.)$ é uma propriedade de nossos índices. Vamos usar este princípio mostrar a seguinte:

Proposição. ($\in$-induction) $\forall x\,\big((\forall u \in x\,\phi(u)) \longrightarrow \phi(x)\big) \longrightarrow \forall x\,\phi(x)$, por qualquer propriedade ϕ.

Demonstração. Mostremos por indução no α que $\forall x \in V_\alpha\,\phi(x)$. Daremos este, $\forall x \in V_\alpha\,\phi(x)$, o nome $\mathrm{Pr}(\alpha)$. Para nosso princípio é bastante mostra que para cada α temos $\forall\beta < \alpha\,\mathrm{Pr}(\beta)) \longrightarrow \mathrm{Pr}(\alpha)$.$\blacksquare$

Assim, suponha que $\forall\beta < \alpha\,\mathrm{Pr}(\beta)$. Tome $x \in V_\alpha$. Tem dois casos.

Ou $V_\alpha = \mathcal{P}(V_\beta)$ para um β menor que α, quando $x \subseteq V_\beta$ e para todos $u \in x$ temos $\phi(u)$. Então usando o antecedente para x temos $\phi(x)$. Porque x era arbitrário temos $\forall x \in V_\alpha\,\phi(x)$, *i.e.*, $\mathrm{Pr}(\alpha)$.

Ou $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, quando existe $\beta < \alpha$ tal que $x \in V_\beta$. Como já sabemos $\Pr(\beta)$ temos $\phi(x)$. De novo, porque x era arbitrário temos $\forall x \in V_\alpha\, \phi(x)$, *i.e.*, $\Pr(\alpha)$.

Como α era arbitrário temos $\forall\alpha\,\big((\forall\beta < \alpha\, \Pr(\beta)) \longrightarrow \Pr(\alpha)\big)$. E agora podemos deduzir que $\forall\alpha\, \Pr(\alpha)$, e então $\forall\alpha\, \forall x \in V_\alpha\, \phi(x)$, e assim $\forall x\, \phi(x)$.

Para evitar fazer muitas demonstrações como esta usemos um princípio, Fundação, equivalente para $\in$-indução:

$(\star)$ Se A é uma propriedade dos conjuntos e existe x tal que $A(x)$ então existe x tal que $A(x)$ e para todos $u \in x$ não temos $A(u)$. Simbôlicamente: $\exists x\, A(x) \Longrightarrow \exists x\, A(x)\ \&\ \forall y \in x\, \neg A(y)$

Nota. Temos a idéia que para qualquer coisa tem que ser um passo o mais cedo em qual a coisa acontece.

Temos mais duas problemas:

(1) Que são as propriedades da hierarquia?
(2) Quanto longe persistir a hierarquia?

Resposta para (2) (parte (a)).

1.6 Infinidade. Precisamos de alguns números naturais. Aqui estão:

$$0 = \emptyset$$
$$1 = \{0\}$$

$$
\begin{aligned}
2 &= \{0,1\} \\
3 &= \{0,1,2\} \\
&\vdots
\end{aligned}
$$

Nota que se definirmos $s(x) = x \cup \{x\}$ temos $s(n) = n+1$ para cada n.

Queríamos também um conjunto dos números naturais: $\mathbf{N} = \omega = \{0,1,2,\dots\}$. Assim gostaríamos que $\omega = \bigcap\{x \mid 0 \in x \,\&\, \forall u \in x\; s(u) \in x\}$.

Mas são quaisquer conjuntos infinitos? Bem, sim – mas temos que estipular que existem.

Infinidade. $\exists x\,(\emptyset \in x \,\&\, \forall u \in x\; s(u) \in x)$.

(Nota. V_ω é um tal x.)

Outras noções de infinidade. (1) Infinito = não finito: "$\exists x\, \forall n \in \omega\, x \not\sim n$" onde $x \sim u$ se e só se $\exists f : x \longrightarrow y$ e f é uma bijeção. (Em palavras: Existe x não numa bijeção com qualquer número natural.) Mas para falar isso precisamos de funções que até agora não temos definidas.

(2) Infinidade do tipo Dedekind: "$\exists x\, \exists u \subseteq x\, (x \neq u \,\&\, x \sim u)$." (Em palavras: Existe um conjunto com um subconjunto não igual ao conjunto mas do mesmo tamanho.)

Se um conjunto é infinito de tipo Dedekind é infinito. Na outra direção, se um conjunto é infinito, é infinito de tipo Dedekind, mas este precisa de uma pequena porção de axioma de Escolha (para mostrar que se x não é finito x conte um subconjunto enumerável).

Não se preocupa se a última frase não quis dizer muito para você agora... não é uma grande coisa e não vai ser importante para nós. Em qualquer caso, nosso axioma para estipular que temos conjuntos infinitos vai ser o primeiro que dei.

1.7. A língua da teoria dos conjuntos e propriedades. Propriedades são as propriedades que são definíveis numa língua, a língua de teoria dos conjuntos–LTC, com parâmetros entre conjuntos. Podemos escolhar a língua de teoria dos conjuntos para ser muito simples. LTC tem:

(i) variáveis: u, v, x, z, ...
(ii) símbolos para relações: $=$, $\in$
(iii) ligações de lógica das proposições: & (e), `v` (ou), $\longrightarrow$ (implica), $\neg$ (não), $\longleftrightarrow$ (se e só se)
(iv) quantificadores: $\forall x$ (para todos x), $\exists x$ (existe x).

Nota: se temos um conjunto a temos que $\{x \mid a \in x\}$ é uma propriedade e não um conjunto.

Com sorte você entende esta língua informalmente, e então pode raciocinar usando-o. (Se quer entender melhor como fazer estes tipos das coisas mais formalmente deve dar uma olhada no livro do van Dalen.)

Vamos usar algumas abreviaturas naturais:
$x \neq z$ em vez de $\neg(x = z)$
$x \notin z$ em vez de $\neg(x \in z)$

$\forall x \in z\, \phi(x)$ em vez de $\forall x\, (x \in z \longrightarrow \phi(x))$
$\exists x \in z\, \phi(x)$ em vez de $\exists x\, (x \in z \;\&\; \phi(x))$
$\exists! x\, \phi(x)$ em vez de $\exists x\, (\phi(x))\; \&\; \forall z\, (\phi(z) \longrightarrow z = x)$, e assim por diante. (Também muitas vezes usarei "ou" em vez de " $\mathtt{v}$ " para evitar confusão entre " $\mathtt{v}$ " e "v.")

Introdução de símbolos por relações e funções. Se tenho um fórmula $\phi(x)$ em LTC, pois posso introduzir um símbolo novo $R_\phi(x)$ por uma relação e um axioma $\forall x(R_\phi(x) \longleftrightarrow \phi(x))$. Isso não muda o poder de expressão da língua (o que pode falar na língua). Por exemplo: poderia bota $x \subseteq z$ se e só se $\forall u \in x\, u \in z$, onde $\subseteq$ é nosso símbolo novo.

Similarmente, se temos $\phi(x_0, \ldots, x_{k-1}, z)$ e podemos mostrar (de algumas axiomas) que, escrevendo $\overrightarrow{x}$ por $x_0, \ldots, x_{k-1}$, $\forall \overrightarrow{x}\, \exists! z\, \phi(\overrightarrow{x}, z)$, podemos introduzir um símbolo $f_\phi(z)$ por uma função e um axioma $\forall \overrightarrow{x}, y\, (\phi(\overrightarrow{x}, y) \longleftrightarrow f(\overrightarrow{x}) = y)$. De novo isso não muda o que a língua pode expressar.

Vou dar alguns exemplos do uso deste língua. Como já encontramos a majoria dos axiomas de Zermelo-Fraenkel parece uma boa coisa usá-los como nesses exemplos.

1.8 Axiomas de teoria dos conjuntos de Zermelo-Fraenkel (ZF)

Os axiomas são (em breve):

Extensão
Conjunto Vazio
Pares (se temos dois conjuntos temos também o conjunto para quem pertencem exatamente os dois conjuntos)
Infinidade
Uniões
Conjuntos de potência
Compreensão (ou formação de subconjuntos)
Coleção (até agora não discutido)
$\in$-indução **ou** Fundação: Se A não é vazio então A tem um componente que é mínimo em $\in$ ($\in$-mínimo).

Zermelo produz todos além de Coleção e então o sistema sem Coleção e chamado theoria dos conjuntos de Zermelo (Z).

Exercício. Mostrar que Z e verdadeiro em $V_{\omega+\omega}$.

E agora de novo, usando LTC, e com algumas comentarios.

Extensão. $\forall x\, \forall y\, \big(\forall z\, (z \in x \longleftrightarrow z \in y\big) \longrightarrow x = y)$.

Conjunto Vazio. $\exists x\, \forall y\, (y \notin x)$.
Por o axioma de extensão $\exists! x\, \forall y\, (y \in x)$. Assim podemos introduzir um novo símbolo por um constante $\emptyset$ tal que $\forall y\, y \notin \emptyset$. (Um constante é meramente uma função de 0 variáveis.)

Pares. $\forall x\, \forall y\, \exists! z\, \forall u\, (u \in z \longleftrightarrow u = x \;\mathtt{v}\; u = y)$.
Podemos introduzir um simbolo por uma função $\{.,.\}$ com $\forall u\, (u \in \{x, y\} \longleftrightarrow u = x \;\mathtt{v}\; u = y)$.

(A par de dois conjuntos é único por extensão.)

Agora podemos ver que $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$ e então $1 \in 2$ (introduzindo os simbolos 1 e 2 por constantes no modo óbvio por estes conjuntos).

Uniões. $\forall x\, \exists z\, (u \in z \longleftrightarrow \exists y \in x\, (u \in y))$.
De novo podemos introduzir um símbolo, $\bigcup$ por uma função e temos $\forall x\, (u \in \bigcup x \longleftrightarrow \exists y \in x\, u \in y)$.

Conjunto de potência. $\forall x\, \exists! z\, (y \in z \longleftrightarrow \forall u \in y\, (u \in x))$.
De novo vamos introduzir um símbolo $\mathcal{P}$ com efeito que $z \in \mathcal{P}(x) \longleftrightarrow z \subseteq x$.

Infinidade. $\exists x\, (\emptyset \in x \;\&\; \forall y \in x\, (y \cup \{y\} \in x))$.
Assim podemos introduzir um símbolo novo por uma função e tomar que $s(y) = y \cup \{y\}$ e ω com $u \in \omega \longleftrightarrow \forall x\, ((\emptyset \in x \;\&\; \forall y \in x\, (y \cup \{y\} \in x)) \longrightarrow u \in x)$. Com dois passos mais podemos falar que $\omega = \bigcap\{x \mid \emptyset \in x \;\&\; \forall y \in x\, (y \cup \{y\} \in x)\}$.

Compreensão e classes. Por uma propriedade de conjuntos quero dizer alguma fórmula $\phi(\overrightarrow{x}, \overrightarrow{a})$ onde $\overrightarrow{a} = a_0, \ldots, a_{n-1}$ são nomes por alguns conjuntos específicos. A propriedade é verdadeira de $b_0, \ldots, b_{m-1} = \overrightarrow{b}$ se e só se $\phi(\overrightarrow{b}, \overrightarrow{a})$ é verdadeiro. A *extensão* de uma propriedade é a coleção dos conjuntos de quais a propriedade é verdadeira. Este coleção é uma subcoleção de V, a coleção de todos conjuntos. Chamamos a extensão de uma propriedade uma classe. Assim uma classe é uma coisa de tipo $\{x \mid \phi(x, \overrightarrow{a})\}$.

Axioma de Compreensão. Para todas fórmulas $\phi(x, \overrightarrow{y})$ na língua de teoria dos conjuntos temos $\forall x \forall a_0, \ldots, \forall a_{n-1}\, \exists y\, \forall z (z \in y \longleftrightarrow z \in x \;\&\; \phi(z, \overrightarrow{a}))$.

Nota, este "axioma" é na verdade uma esquema dos axiomas: temos uma axioma para todas fórmulas $\phi(x, \overrightarrow{y})$ na LTC, e não um axioma só.

Em efeito o esquema fala que para todos x temos que cada $x \cap \{z \mid \phi(z, \overrightarrow{a})\}$ é um conjunto. Então uma classe $\{x \mid \phi(x, \overrightarrow{a})\}$ é um conjunto (no sentido que $\exists z\, \forall x\, (x \in z \longleftrightarrow \phi(x, \overrightarrow{a}))$ se e só se $\{x \mid \phi(x, \overrightarrow{a})\} \subseteq V_\alpha$ por alguma α. *I.e.*, $\{x \mid \phi(x, \overrightarrow{a})\}$ é um conjunto se e só se é limitado na hierarquia.

É muito útil (como vamos ver logo) poder usar várias classes como abreviaturas informais–todo mondo faz isso e vamos fazer isso também. Só que você deveria ficar cauteloso para o fato de que as classes são só abreviaturas e seus usos sempre podem ser eliminados em favor de falar sobre as fórmulas de LTC que define elas.

Por exemplo, se $A = \{x \mid \phi(x, \overrightarrow{a})\}$ é uma classe, pode usar $b \in A$ como abreviatura por $\phi(b, \overrightarrow{a})$ sendo verdadeiro, mas não pode pensar sobre se $A \in A$. Este ultima não é falsa, mas *não tem sentido*. Similarmente, $P(A)$ não tem sentido.

Se ainda tem perguntas ou dúvidas sobre como usar ou pensar de classes, espere um pouquinho e depois de termos usados classes um pouco acho que coisas aparecerão mas claras.

(Nota técnica: aqui tomamos fórmulas $\phi(x, \overrightarrow{y})$ na LTC tal que as variáveis $y_0, \ldots, y_{n-1}$ são *livres*, *i.e.* podemos botar $a_0, \ldots, a_{n-1}$ na fórmula em vez de $y_0, \ldots, y_{n-1}$ sem problemas. Por exemplo, cada y_i não ocorre na forma $\exists y_i \ldots$ ou $\forall y_i$. Para mais informação sobre variáveis livres e uma definição indutiva formal do que são variáveis livres veja o livro de van Dalen ou a seção mais tarde sobre lógica matemática.)

Fundação. Para todas fórmulas $\phi(x, \overrightarrow{a})$ na LTC $\exists y\, \phi(y, \overrightarrow{a}) \longrightarrow \exists y\, \phi(y, \overrightarrow{a})\ \&\ \neg\exists z \in y\, \phi(z, \overrightarrow{a})$.

Usando classes como abreviaturas este fala que se A é uma classe e não é vazio então A tem um componente que é mínimo em $\in$ ($\in$-mínimo).

Quanto alto é a hierarquia? (b) Suponha que $\forall x \in u\, \exists y\, \phi(x, y, \overrightarrow{a})$. Para cada x existe um primeiro α_x tal que $\exists y \in V_{\alpha_x}\, \phi(x, y, \overrightarrow{a})$ (isso por o axioma da fundação). Então temos uma função mandando u para $\{\alpha_x \mid x \in u\}$ dado por $x \mapsto \alpha_x$. Assim $\{\alpha_x \mid x \in u\}$ é um "conjunto" de níveis, e então existe um β tal que $\alpha_x < \beta$ para todos $x \in u$. Assim temos $V_{\alpha_x} \in V_\beta$ para todos $x \in u$. Se botarmos $v = V_\beta$ temos $\exists v\, \forall x \in u\, \exists y \in v\, \phi(x, y, \overrightarrow{a})$.

Ora! Precisamos de um axioma (bem, em verdade um esquema dos axiomas, mais uma vez) para fazer este "coleta" que dá para nós o conjunto de níveis que usamos em cima.

Axioma de Coleção. Para todas fórmulas $\phi(x, y, \overrightarrow{z})$ na LTC (com $\overrightarrow{z}$ variáveis livres) temos o seguinte:

$$\forall \overrightarrow{a}\, \forall u (\forall x \in u\, \exists y\, \phi(x, y, \overrightarrow{a}) \longrightarrow \exists v \forall x \in u\, \exists y \in v\, \phi(x, y, \overrightarrow{a})).$$

Supreendentemente este esquema implica que a hierarquia persiste por um tempo muito longe.

Princípio de Reposição Para todas fórmulas $\phi(x, y, \overrightarrow{z})$ na LTC (com $\overrightarrow{z}$ variáveis livres) temos o seguinte:

$$\forall \overrightarrow{a}\, (\forall u\, \exists! v\, \phi(u, v, \overrightarrow{a}) \longrightarrow \forall x\, \exists y\, \forall z\, (z \in y \longleftrightarrow \exists w \in x\, \phi(w, z, \overrightarrow{a}))).$$

Usando classes como abreviaturas de novo este fala "Se F é uma operação definavel no V então para todos conjuntos x temos que $F|x``x$ (a imagem da restrição de F para x) é também um conjunto."

Algumas autores preferem usar o princípio de reposição em vez de Coleção para formular os axiomas de ZF. Eu acho que é melhor usar Coleção (acho mais simples entender que está acontecendo – em parte porque não precisa usar classes para fazer uma abreviatura), mas não faz diferença formalmente pois a reposição segue de coleção e compreensão.

(**Demonstração.** Para cada $\overrightarrow{a}$ o lado esquerda dá para todos x que temos $\forall u \in x\, \exists (!) v\, \phi(u, v, \overrightarrow{a})$. Usando o axioma de coleção temos $\exists s\, \forall u \in x\, \exists v \in s\, \phi(u, v, \overrightarrow{a})$. Mas o y que precisamos é uma subcoleção definível de s e então existe para o axioma de compreensão.

1.9. Algumas noções matemáticas úteis. Agora podemos introduzir várias nocões úteis, dando definições na LTC delas.

Definição. *Pares ordenados.* $(x, y) = \{\{x\}, \{x, y\}\}$.

Proposição. (a) Para todos x e y, (x, y) é um conjunto.
(b) Para todos x, y, u e v, $(x, y) = (u, v) \longrightarrow x = u \;\&\; y = v$.

Demonstração. (a) Por o axioma de pares (aplicada três veces).
(b) Por o axioma dá extensãoalidade.

Nota: se $x = y$ a definição da que $(x, x) = \{\{x\}\}$ e temos que verificar este caso também.

Definição. *Produto cartesiano de dois conjuntos.* $x \times y = \{(a, b) \mid a \in x \,\&\, b \in y\}$.

Proposição. Para todos x e y, $x \times y$ é um conjunto.

Demonstração. Para todos x e y, $x \times y$ é uma subcoleção definível de $\mathcal{P}(\mathcal{P}(\bigcup\{x, y\}))$ e então é um conjunto para os axiomas de compreensão, conjuntos de potência, uniões e pares.

Definição. *Relações e funções.* Uma relação no produto $x \times y$ é um subconjunto de $x \times y$, *i.e.*, um componente de $\mathcal{P}(x \times y)$. Então vamos escrever, igualmente, $\mathrm{Rel}(x,y)$ por $\mathcal{P}(x \times y)$ como uma ajuda à lembrança. Funções são algumas relações. A coleção de funções de x para y é ${}^{x}y = \{f \in \mathrm{Rel}(x,y) \mid \forall a \in x\, \exists! b \in y\, (a, b) \in f\}$.

Proposição. Para todos x e y, $\mathrm{Rel}(x, y)$ e ${}^{x}y$ são conjuntos.

(Poderiamos continuar assim, por exemplo definindo $\mathrm{dom}(z) = \{a \mid \exists b\, (a, b) \in z\} \subseteq \bigcup\bigcup z$ e $\mathrm{im}(z) = \{b \mid \exists a\, (a, b) \in z\} \subseteq \bigcup\bigcup z$, e depois provar, dado que $\mathrm{Rel}(z) \longleftrightarrow \forall x \in z\, \exists a, b\, (x = (a, b))$, temos $\mathrm{Rel}(z) \longleftrightarrow z \subseteq \mathrm{dom}(z) \times \mathrm{im}(z)$.)

Vamos falar que $f : x \longrightarrow y$ quando $f \in {}^{x}y$, $\mathrm{dom}(f) = x$ e $\mathrm{im}(f) \subseteq y$. Queriamos usar a notação $f(a)$ quando $f \in {}^{x}y$, $a \in x$ e $(a, b) \in f$. Se estamos juntando um nome por uma função definível para a língua deveríamos dar um sentido para qualquer $f(x)$. Então botamos $f(a) = b$ se $a \in \mathrm{dom}(f)$, e $f(a) = \emptyset$ se $a \notin \mathrm{dom}(f)$. Aqui estamos usando f em dois sentidos, um como o nome de um conjunto (a função de x para y), e o outro como um novo símbolo numa extensão por funções definível para LTC. Logo que precisamos botar $f(a)$ (f no segundo sentido) igual 0 se $a \notin \mathrm{dom}(f)$ (f no primeiro sentido). Na prática rapidamente vemos ignorar estas distinções.

Agora podemos definir injetivo, sobrejetivo e bijetivo for funções $f \in {}^{x}y$, e então podemos escrever o axioma de infinidade por exemplo:

Infinidade. $\exists x\, \forall n \in \omega \neg \exists f \in {}^{x}n\; f$ é bijetivo.

Agora podemos introduzir também o axioma de escolha.

Axioma de Escolha. $\forall x\, ((\forall y \in x\; y \neq \emptyset) \longrightarrow \exists f \in {}^{x}\bigcup x\, \forall y \in x\; f(y) \in y)$.

Isto fala que para todos conjuntos de conjuntos não-vazios tem uma função que escolha um membro de cada um. Não vou falar mas nisso aqui, porque veremos mas sobre este axioma no cápitulo 3.

Outras coisas similares. Podemos fazer algumas outras definições úteis similares. Se I e $\{y_i \mid i \in I\}$ são conjuntos temos:

Produtos cartesianos gerais. $\Pi_{i\in I} y_i = \{ f : I \longrightarrow \bigcup\{y_i \mid i \in I\} \mid \forall i \in I\, f(i) \in Y_i \}$.

Uniões disjuntas. $\Sigma_{i\in I} y_i = \{ (i, a) \mid a \in y_i \}$. (Às veces pode ver $\dot{\bigcup}_{i\in I} y_i$ em vez de $\Sigma_{i\in I} y_i$.)

Quociente de um conjunto por um relação de equivalência. R é um relação de equivalência no x se R é reflexivo, $\forall y \in x\ (y, y) \in R$, R é simétrico $\forall y, z \in x\ (y, z) \in R \longleftrightarrow (z, y) \in R$ e R é transitivo, $\forall w, y, z \in x\ (w, y) \in R\,\&\,(y, z) \in R \longleftrightarrow (w, z) \in R$. Se R é um relação de equivalência no x temos $x/R = \{ y \in \mathcal{P}(x) \mid \exists a \in x\, \forall b\, (b \in y \longleftrightarrow (a, b) \in R) \}$.

Proposição. Cada $\Pi_{i\in I} y_i$, $\Sigma_{i\in I} y_i$ e x/R é um conjunto.

Teorema. A coleção de todos conjuntos, V, é fechado sob
(i) subconjuntos definíveis,
(ii) uniões,
(iii) produtos indexados por conjuntos,
(iv) uniões disjuntos indexados por conjuntos,
(v) espaços de funções
(vi) conjuntos de potência
(vii) quocientes
e também contem $\mathbf{N}$ – *i.e.*, um objeto $\mathbf{N}$ com uma função $s : \mathbf{N} \longrightarrow \mathbf{N}$ que satisfaz os aximas de Peano (que dão as regras que esperamos de conduta da função de sucessor nos números naturais).

Usando este teorema podemos construir mais ou menos qualquer objeto matemática (e é facil augmentar a teorema para monstrar como fazer outras consrtuções matemáticas na teoria dos conjuntos). Estes não são coisas muitas grandes como pode ver para os exemplos seguintes.

Podemos definir + e . nos números naturais indutivemente, primeiro +: $n + (m + 1) = s(n + m)$; e depois .; $n.(m+1) = n.m+n$. Depois pode definir $\mathbf{Z}$ como $\mathbf{N} \times \{0\} \dot{\cup} \{0\} \times \{1\} \dot{\cup} \mathbf{N} \times \{2\}$ ($\subseteq \mathbf{N} \times 3$), com $(i, y) < (j, z)$ se $i < j$, ou $i = j = 0$ e $z < y$, ou $i = j = 2$) e $y < z$, por exemplo. (Mas claro também pode esolhar qualquer outro esquema razoavel.) Pode dar as regras para +, . si mesmo. Podemos definir $\mathbf{Q}$ como $\mathbf{Z} \times \mathbf{N} / \sim$ onde $\sim$ é a relação $(a, b) \sim (c, d)$ se $a.d = b.c$. Depois pode definir $\mathbf{R}$ pela cortes de Dedekind. Ou também poderia definir, por exemplo, $\{r \in \mathbf{R} \mid 0 < r < 1\}$ pelo expansões binarias, ou pela frações contínuas e tomar $\mathbf{R} = \mathbf{Z} \times \{r \in \mathbf{R} \mid 0 < r < 1\}$. (Pode achar informação sobre frações contínuas em qualquer livro bom que tratar da teoria elementar dos números, como, por exemplo, Alan Baker, *A Consise Introduction to the Theory of Numbers*, Cambridge University Press, páginas 41-42.) Como pode ver estes construçõs são mais ou menos trivias e também tem muito liberdade em fazer-las

Teoria dos conjuntos: Exercícios 1.

1. Escrever uma demonstração do axioma de extensão que o conjunto vazio (se existe) é único. **Um ponto estúpido?** Suponha que (X, τ) e (Y, σ) são espaços topológicos. Mostre que $\tau \cap \sigma \neq \emptyset$. Isso é matemática?

2. É a união de uma coleção de conjuntos não vazios também não vazia? É a intersecção de uma coleção de conjuntos não vazios também um conjunto? Deduza do axioma de compreensão que a intersecção de uma classe não vazia de conjuntos é um conjunto.

3. Mostre que o axioma de compreensão com o axioma de infinidade implica que o conjunto vazio existe.

4. Mostre que se $\bigcup x \subseteq x$, então $\bigcup(\bigcup x) \subseteq x$. É o inverso verdadeiro? Mostre que as três fórmulas seguintes são equivalentes: (i) $x \subseteq \mathcal{P}(x)$, (ii) $\bigcup x \subseteq x$, (iii) $x = \bigcup\{ y \cup \{ y \} \mid y \in x \}$.

5. Quantos membros tem cada V_n por n finito? Mostre que V_ω é enumerável. Mostre que a função $x \longrightarrow \#x$, onde $\#x$ é definida por indução por "$\#x$ é o número que na expansão binária de qual os 1s ocorrem nos lugares i exatamente por estes i que são iguais para $\#y$ por alguma $y \in x$" é uma bijeção entre V_ω e $\mathbf{N}$.

6. Se x é um conjunto (puro) existe um primeiro lugar α onde $x \in V_\alpha$ e existe um primeiro lugar β tal que $x \subseteq V_\beta$. Qual é a relação entre α e β?

7. Seja x um conjunto, e sejam α o primeiro lugar tal que $\bigcup\{ \mathcal{P}(y) \mid y \in x \} \in V_\alpha$ e β o primeiro lugar onde $\mathcal{P}(\bigcup x) \in V_\beta$. Qual é a relação entre α e β?

8. Existe um conjunto x com $x \in x$? Existe uma seqüência de conjuntos $\ldots x_3 \in x_2 \in x_1 \in x_0$?

9. Um conjunto que satisfaz as condições (i)-(iii) de (4) é chamado *transitivo*. Suponha que $x = \{ x \}$. (Não considere se tem tal coisas!) É x transitivo?

10. Escrever uma demonstração, usando indução, mostrando que cada V_α é transitivo. (Que acontece nos passos limites?)

11. Considere o princípio que cada conjunto pertence a um conjunto transitivo. (Por que isso é implicado pela hierarquia de V_αs?)
    (i) Mostre que este princípio e a axioma de compreensão implicam o axioma des uniões.
    (ii) Mostre que este princípio, o axioma de compreensão e o axioma de fundação implicam o princípio de indução no $\in$. (O axioma de fundação fala: $\forall x (x \neq \emptyset \longrightarrow \exists y \in x\ (y \cap x = \emptyset))$.)

12. Sejam todos os membros de x transitivos, mostre que $\in$ é uma relação transitiva no x.

13. Mostre que o axioma de pares poderia ser substituido em ZF pelo princípio que para cada conjunto x e cada conjunto y existe um conjunto $x \cup \{ y \}$.

14. Mostre que o princípio de reposição, o axioma de conjunto vazio e o axioma de conjuntos de potência mostram o axioma de pares.

Capítulo 2. Ordinais, relações bem-fundadas.*

2.1. Relações bem-fundadas.

Vamos começar com algumas definições e rápidamente chegaremos na noção de um conjunto bem-ordenado.

Definição. Por qualquer X e qualquer relação binária $<$ sobre X, $(X, <)$ é um *conjunto parcialmente ordenado* (*conjunto p.o.*) se $<$ é uma relação anti-simétrica e transitiva no X: $\forall x \in X x \not< x$ and $\forall x \in X\, \forall y \in X\, \forall z \in X\, (x < y \,\&\, y < z \longrightarrow x < z)$. Falamos que $<$ *ordena parcialmente* X ou $<$ é um *ordenando parcial* ou *ordem parcial* de X.

$(X, <)$ é um *conjunto linearmente ordenado* (*conjunto l.o.*) ou um *conjunto totalmente ordenado* (*conjunto t.o.*) se $(X, <)$ é um conjunto parcialmente ordenado e $\forall x \in X\, \forall y \in X\, (x < y$ ou $x = y$ ou $y < x)$ também.

Definição. Agora seja $<$ qualquer relação binária sobre X. Se $Y \subseteq X$, então $(Y, <)$ é um *segmento inicial* de $(X, <)$ se $\forall x \in X\, \forall y \in X\, (x < y \,\&\, y \in Y \longrightarrow x \in Y)$. Muitas vezes falaremos apenas que Y é um segmento inicial de X quando é claro de qual relação $<$ estamos falando. $(Y, <)$ é um segmento inicial próprio de $(X, <)$ se $Y \neq X$ também. Para todos $s \in X$ e $Y \subseteq X$, falaremos que s é *um sucessor* de Y se $s \notin Y$ e $\{y \in X \mid y < s\} \subseteq Y$. E se $Y \subseteq X$ e $y \in X$ falaremos que y é *$<$-mínimo no* Y se $y \in Y$ é $\forall x \in X\, (x < y \longrightarrow x \notin Y)$.

Teorema. As seguintes condições são equivalentes para qualquer X e qualquer relação binária sobre X.

(1) Cada segmento inicial próprio de X tem um sucessor.
(2) Cada subconjunto não-vazio de X tem um elemento $<$-mínimo.
(3) O princípo de indução sobre $<$ é verdadeira:

$$\forall x \in X\, \big(\big(\forall y \in X\, (y < x \longrightarrow \phi(y))\big) \longrightarrow \phi(x)\big) \longrightarrow \forall x \in X\, \phi(x).$$

Demonstração. (2) $\Longrightarrow$ (3). Suponhamos que $\forall x \in X\, \big(\big(\forall y \in X\, (y < x \longrightarrow \phi(y))\big) \longrightarrow \phi(x)\big)$ mas $\neg\forall x \in X\, \phi(x))$. Então $\{x \in X \mid \neg\phi(x)\}$ não é vazio e, para (2), tem um membro, vamos falar x_0, que é $<$-mínimo. Mas logo temos que $\forall y < x_0\, \phi(y)$ e então $\phi(x)$, uma contradição.

(3) $\Longrightarrow$ (2). Se $Y \subseteq X$ e Y não tem um membro $<$-mínimo, então temos que $\forall x \in X\, (\forall y \in X (y < x \,\&\, y \notin Y)) \longrightarrow x \notin Y$. Aplicando (3), temos que $\forall x \in X\, x \notin Y$. Então Y é vazio.

(2) $\Longrightarrow$ (1). Se Y é um segmento inicial próprio de X, então $X \setminus Y$ $(= \{x \in X \mid x \notin Y\})$ não é vazio, e (2) fala que tem um membro, s vamos falar, que é $<$-mínimo. Logo s é um sucessor de Y.

(1) $\Longrightarrow$ (2). Para todos $x, y \in X$ seja $x <^* y$ se tem $x_0, \ldots, x_{n-1} \in X$ e $x < x_0 < \ldots < x_{n-1} < y$. $<^*$ é o fechamento transitivo de $<$: é transitivo, $< \subseteq <^*$ e se R é uma relação binária transitiva com $< \subseteq R$, então $<^* \subseteq R$.

---

* versão 1.2, 1/12/00

(Para ver que $<^*$ é transitivo tome $x <^* y$ e $y <^* z$ e suponhamos que temos isso porque $x < x_0 < \ldots < x_{n-1} < y$ e $y < y_0 < \ldots < y_{m-1} < z$ para algumas $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1} \in X$. Logo, $x < x_0 < \ldots < x_{n-1} < y < y_0 < \ldots < y_{m-1} < z$, e então $x < z$. É claro que $x < y \implies x <^* y$: tome $n = 0$ na definição de $<^*$. E se $x <^* y$ existem $x_0 < \ldots < x_{n-1}$ com $x < x_0 < \ldots < x_{n-1} < y$, então se $<\subseteq R$ temos $x\,R\,x_0\,R\,\ldots\,Rx_{n-1}\,Ry$, e logo, se R é transitivo, temos $x\,R\,y$.)

Agora suponhamos que $Y \subseteq X$ e Y não é vazio. $\{x \in X \mid x \notin Y \,\&\, \forall y \in X\,(y <^* x \longrightarrow y \notin Y)\}$, $= Z$, vamos falar, é um segmento inicial e não é próprio. Se s é um sucessor de Z temos que $s \in Y$ e s é $<$-mínimo no Y.

Definição. Uma relação binária $<$ sobre um conjunto X é *bem-fundada* se satisfaz as condições (1)-(3) do teorema em cima. Um ordenando total bem-fundado é chamado um *bem-ordenando* ou uma *bem-ordem.* $(X, <)$ é então um *conjunto bem-ordenado* (um *conjunto b.o.*).

2.2 Ordinais.

Então, um conjunto bem-ordenado é um conjunto que sobre qual podemos "contar," um passo de cada vez. Os ordinais são conjuntos bem-ordenados que serão cruciais para nós. Em fato, veremos mas tarde que qualquer conjunto bem-ordenado é isomorfico para um ordinal para um isomorfismo que preservar ordem, então pode falar que se quer "contar" tem que usar os ordinais.

Definição. Um *(número) ordinal* é um conjunto que é bem-ordenado por $\in$. (Frequentemente escrevemos $<$ em vez de $\in$ quando estamos tratando dos ordinais.)

Exemplos. 0, 1, 2, 3, $\ldots$, ω, $\ldots$ são (os primeiros) ordinais. Exercício: se isso não está aparente para você, vai confirmá-lo.

Proposição. Se α é um ordinal e $z \in \alpha$, logo z é um conjunto transitivo e então é um ordinal também.

Demonstração. Suponhamos que $x \in y \in z \in \alpha$. Temos que mostrar que $x \in z$. Mas α é transitivo, então $y \in \alpha$, então $x \in \alpha$. α também é bem-ordenado por $\in$, então $\in$ é uma relação trasitiva sobre α. Porque temos $x \in y$ e $y \in z$, então $x \in z$.

Definição. Se α é um ordinal defina $s(\alpha) = \alpha \cup \{\alpha\}$.

Proposição. Se α é um ordinal, então $s(\alpha)$ é um ordinal também.

Demonstração. Se $z \in y \in s(\alpha)$, então ou $z \in y \in \alpha$ ou $z \in y \in \{\alpha\}$. No primeiro caso $z \in \alpha$ porque $\in$ é transitivo sobre α, e no segundo caso $z \in y = \alpha$. Então, em qualquer caso $z \in s(\alpha)$. Logo $s(\alpha)$ é transitivo. E é claro que $s(\alpha)$ é bem-ordenado por $\in$.

Proposição. Se $x \neq \emptyset$ é um conjunto dos ordinais, então $\bigcap x$ é um ordinal também.

Demonstração. É claro que qualquer intersecção dos conjuntos transitivos é transitiva. E se $\alpha \in x$, então $\bigcap x \subseteq \alpha$ e deve ser bem-ordenada por $\in$ porque α é bem-ordenado por $\in$.

Proposição. Se α, β são ordinais e $\alpha \subseteq \beta$, então (a) α é um segmento inicial de β, e (b)

$\alpha \neq \beta \Longrightarrow \alpha \in \beta$.

Demonstração. (a) Se $\gamma \in \beta$, $\delta \in \alpha$ e $\gamma \in \delta$ (*i.e.*, γ vem antes do δ no b.o. do β por $\in$), então $\gamma \in \delta \in \alpha$, e então $\gamma \in \alpha$ pela transitividade do $\in$ sobre α.

(b) Se $\alpha \neq \beta$, então, pela equivalente de ser bem-fundado, existe um sucessor, vamos falar s, de α como subconjunto do β. Nota que s é único porque $\in$ é um l.o. do β. Também porque $\in$ é um l.o. do β, $\gamma \in \alpha$ implica que $\gamma \in s$, então $\alpha \subseteq s$. No outro lado, $S = \alpha \cup \{s\}$ é um segmento inicial do β e, então, é transitivo e, logo, para qualquer $\gamma \in s (\in S)$ temos $\gamma \in S$. Porque $s \notin s$ (para o axioma de fundação), $\gamma \in s$ implica $\gamma \in \alpha$ e $s \subseteq \alpha$. Então $\alpha = s, \in \beta$.

2.3. Tricotomia.

Teorema. Se α e β são ordinais um e exatamente um dos seguintes acontece: $\alpha \in \beta$ ou $\alpha = \beta$ ou $\beta < \alpha$.

Demonstração. $\alpha \cap \beta = \alpha$ ou $\alpha \cap \beta \subset \alpha$ e $\alpha \cap \beta \neq \alpha$. Similarmente $\alpha \cap \beta = \beta$ ou $\alpha \cap \beta \subset \beta$ e $\alpha \cap \beta \neq \beta$, dando quatro casos para considerar para nós.

(i) $\alpha \cap \beta = \alpha$ e $\alpha \cap \beta = \beta$. Logo $\alpha = \beta$.

(ii) $\alpha \cap \beta = \alpha$ e $\alpha \cap \beta \subset \beta$ e $\alpha \cap \beta \neq \beta$. Então a última proposição de Seção (2.2) dá imediatemente que $\alpha \in \beta$.

(iii) $\alpha \cap \beta = \beta$ e $\alpha \cap \beta \subset \alpha$ e $\alpha \cap \beta \neq \alpha$. Então a última proposição de Seção (2.2) dá que $\beta \in \alpha$.

(iv) $\alpha \cap \beta \subset \alpha, \beta$, $\alpha \cap \beta \neq \alpha$ e $\alpha \cap \beta \neq \beta$. Nota que já mostramos que $\alpha \cap \beta$ é um ordinal. Então a última proposição de Seção (2.2) dá que $\alpha \cap \beta \in \alpha$ e que $\alpha \cap \beta \in \beta$. Então $\alpha \cap \beta \in \alpha \cap \beta$, uma contradição! (Para o axioma de fundação.)

Corolário. Por todos ordinais α e β, $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$.

Demonstração. $\alpha \in \beta \Longrightarrow \alpha \subseteq \beta$ porque β é transitivo; $\beta \in \alpha \Longrightarrow \beta \subseteq \alpha$ porque α é transitivo; $\alpha = \beta \Longrightarrow \alpha \subseteq \beta \,\&\, \beta \subseteq \alpha$.

Notação. Escrevemos $\alpha \leq \beta$ se $\alpha \in \beta$ ou $\alpha = \beta$.

Corolário. A coleção de todos os ordinais é uma coleção que é bem-ordenada por $\in$.

Demonstração. É facil ver que a coleção é parcialmente ordenada por $\in$ pela a transitividade dos ordinais. A teorema da tricotomia da que $\in$ ordena a coleção totalmente. Então, vamos ver que $\in$ é bem-fundado na coleção.

Suponhamos que Z é um subconjunto da coleção dos ordinais e $Z \neq \emptyset$. Seja $\alpha \in Z$. Ou α é $\in$-mínimo (quando acabamos), ou $Y = \alpha \cap Z \neq \emptyset$. Y é um subconjunto não-vazio do α, então existe um $\beta \in Y$ que é $\in$-mínimo. Mas β deve ser $\in$-mínimo no Z também, porque se $\gamma \in \beta$ temos que $\beta \in \alpha$ e, pela transitividade do α, $\gamma \in \alpha$. Então $\gamma \in Z$.

Corolário. A coleção de todos ordinais não é um conjunto, é uma classe própria.

Demonstração. Seja a coleção um conjunto, x vamos falar, teríamos que $x \in x$ porque seria um conjunto bem-ordenado por $\in$. Isso seria uma contradição para o axioma de fundação (de novo).

Este corolário é às vezes chamado o *paradoxo de Burali-Forti*. Como você já entende, como o paradoxo de Cantor, não é um paradoxo de verdade. Ainda, como com V é útil ter um nome para a classe própria de todos os ordinais. Vamos escrever On por esta classe.

Corolário. Se x é um conjunto dos ordinais, então $\bigcup x$ é também um ordinal.

Demonstração. É claro que $\bigcup x$ é transitivo. E porque $\bigcup x \subseteq \mathrm{On}$, tricotomia dá que $\in$ ordena $\bigcup x$ totalmente. Assim, suponhamos que $\emptyset \neq Z \subseteq \bigcup x$. Tome $\alpha \in Z$. Como no corolário dois atrás, ou α já é $\in$-mínimo, ou $\alpha \cap Z$ tem um membro que é $\in$-mínimo e que é $\in$-mínimo no Z também.

2.4. Sucessors e limites. Seja α um ordinal. Temos duas coisas que podem acontecer.

Ou existe um elemento $\in$-máximo do α, *i.e.*, um $\beta \in \alpha$ tal que $\forall \gamma \in \alpha\, \gamma \leq \beta$. Neste caso $\alpha = \{\beta\} \cup \{\gamma \mid \gamma < \beta\}, = \{\beta\} \cup \beta, = s(\beta)$. Se existe β tal que $\alpha = s(\beta)$ falaremos que α e um *ordinal do tipo sucessor*.

Ou não existe um membro $\in$-máximo na ápice de α, *i.e.*, $\forall \beta \in \alpha\, \exists \gamma \in \alpha\, \beta < \gamma$. Neste caso $\alpha = \{\beta \mid \beta < \alpha\} = \{\beta \mid \exists \gamma \in \alpha\, \beta \in \gamma\} = \bigcup \alpha$. Se $\alpha = \bigcup \alpha$ falaremos que α é um *ordinal do tipo limite*.

Deveria acertar que se $\alpha = s(\beta)$, então $\beta = \bigcup \alpha$.

Exemplos. $1, 2, 3, \ldots$ são ordinais do tipo sucessor. ω é um ordinal do tipo limite. (E pela nossa definição, 0 é um ordinal do tipo limite também, embora é um caso especial e típicamente tratado em si próprio.)

Em geral, se x é um conjunto dos ordinais, $\bigcup x$ é o supremo dos ordinais no x, e se x é não vazio, $\bigcap x$ é o infimo dos ordinais no x, e também o membro mínimo de x. (Esta última é verdadeira porque já vimos que x tem um membro que é $\in$-mínimo quando $\emptyset \neq x \subseteq \mathrm{On}$, α, vamos falar, e então $\forall \beta \in x\, \alpha \leq \beta$ – *i.e.*, $\forall \beta \in x\, \alpha \in \beta$ ou $\alpha = \beta$, então $\alpha = \bigcap x$.)

2.5. Teoremas de recursão. Agora queríamos definir + e . nos ordinais, num modo similar ao que é normal fazer nos números naturais. Mas antes que podemos fazer isso precisamos saber que podemos fazer definições utlizando recursão e como fazer essas definições. Então esta seção é devotada para este tema. Talvez à primeira vista vai parecer um pouco mais técnica que as últimas, mas será muito lucrativa para nós no fim.

Teorema de recursão fraca. Sejam X, Y dois conjuntos. Seja $<$ uma relação bem-fundada sobre X, e seja $g : X \times \mathcal{P}(()Y) \longrightarrow Y$ uma função. Então existe uma única função $f : X \longrightarrow Y$ tal que $f(x) = g(x, \{f(z) \mid z < x\})$ para todos $x \in X$.

Demonstração. (Parte 1.) Falemos que $\phi : Z \longrightarrow Y$ é uma *tentativa* se Z é um segmento inicial de X e $\phi(x) = g(x, \{\phi(z) \mid z < x\})$ para todos $x \in Z$. Se $\phi_0 : Z_0 \longrightarrow Y$ e $\phi_1 : Z_1 \longrightarrow Y$ são duas tentativas, elas concordam no $Z_1 \cap Z_2$: $\phi_1 | Z_1 \cap Z_2 = \phi_2 | Z_1 \cap Z_2$. Porque $X_1 \cap X_2$ é claro um segmento inicial de X e se as tentativas não concordão existe um x_0 que é $<$-mínimo no $\{x \in Z_1 \cap Z_2 \mid \phi_1(x) \neq \phi_2(x)\}$. Mas neste caso temos $\phi_1(x_0) = g(x_0, \{\phi_0(x) \mid x < x_0\}) =$

$g(x_0, \{\, \phi_1(x) \mid x < x_0 \,\}) = \phi_2(x)$, uma contradição!

(Parte 2.) Agora seja $f = \bigcup\{\, \phi \mid \phi$ é uma tentativa$\}$, então $f(x) = \phi(x)$ se existe uma tentativa ϕ com $x \in \mathrm{dom}(\phi)$. É claro que $\mathrm{dom}(f) = \bigcup\{\, \mathrm{dom}(\phi) \mid \phi$ é uma tentativa$\}$ é um segmento inicial de X, e que f satisfaz $f(x) = g(x, \{\, f(z) \mid z < x \,\})$ para todos $x \in \mathrm{dom}(f)$. Então todo que ficar ser mostrado é que $\mathrm{dom}(f) = X$.

Mas fosse $\mathrm{dom}(f) \neq X$ existe x_0 que é $<$-mínimo no $\{\, x \in X \mid x \notin \mathrm{dom}(f) \,\}$. Para um tal x defina $\bar{f} : \mathrm{dom}(f) \cup \{\, x_0 \,\} \longrightarrow Y$ pelo $\bar{f}(x) = f(x)$ se $x \in \mathrm{dom}(f)$ e $\bar{f}(x_0) = g(x_0, \{\, f(x) \mid x < x_0 \,\})$. Seria claro que $\bar{f}$ seria uma tentativa, mas não um subconjunto de f. Contradição! Então $f : X \longrightarrow Y$ como desejamos.

Agora vamos ver um teorema de recursão mais forte que trata das classes.

Definição. Sejam A e B uns classes. Então $A \times B = \{\, (x, y) \mid x \in A \;\&\; y \in B \,\}$ é uma classe tambem, porque se $A = \{\, x \mid \phi(x, \bar{a}) \,\}$ e $B = \{\, x \mid \psi(x, \bar{b}) \,\}$ para dois fórmulas $\phi(x, \bar{a})$ e $\psi(x, \bar{b})$ na LTC, então $A \times B = \{\, z \mid z = \{\, \{\, x \,\}, \{\, x, y \,\} \,\} \;\&\; \phi(x, \bar{a}) \;\&\; \phi(y, \bar{b}) \,\}$.

Seja A uma classe. $<$ uma *Relação bem-fundada* (nota o "R" maiúscula) sobre A se $<$ é uma subclasse do $A \times A$, $\forall a \in A \, \{\, b \in A \mid b < a \,\}$ é um conjunto, é qualquer B com $\emptyset \neq B \subseteq A$ tem elementos $<$-mínimos.

Sejam A, B uns classes. $G : A \longrightarrow B$ é uma *Função* (nota o "F" maiúscula) se G é uma subclasse de $A \times B$ e para cada $x \in A$ existe um único $y \in B$ tal que $(x, y) \in G$. Se $x \in A$, $y \in B$ e $(x, y) \in G$ (naturalmente) vamos escrever $G(x) = y$. (Nota falar que G é uma (sub)classe quer dizer que existe um fórmula $\chi(z, \bar{c})$ na LTC tal que $x \in G$ se e só se $\chi(x, barc)$ é verdadeiro.)

Lembrar que conjuntos são classes também e se A e B são conjuntos, então $A \times B$ é um conjunto, $<$ é uma relação bem-fundada e G é uma função, respectivamente.

Teorema de recursão forte. Seja $<$ uma Relação bem-fundada sobre uma classe A e seja $G : A \times V \longrightarrow V$ uma Função. Então existe uma Função única $F : A \longrightarrow V$ tal que para todos $x \in A$ temos que $F(x) = G(x, \{\, F(y) \mid y < x \,\})$.

Demonstração. (Parte 1.) O primeiro parte é exatamente como na teorema de recursão fraca. Defina ϕ ser uma tentativa se $\phi : B \longrightarrow V$, onde B é um *conjunto* que é um segmento inicial de A e $\phi(x) = G(x, \{\, \phi(y) \mid y < x \,\})$. Logo quaisquer duas tentativas concordam na intersecção dos segmentos iniciais deles.

(Parte 2.) Seja $F = \bigcup\{\, \phi \mid \phi$ é uma tentativa$\}$ (isto é $(x, z) \in F$ se existe uma tentativa ϕ com $\phi(x) = z$). Nota que a ultima vez este foi um conjunto, mas agora meromente temos que $F \subseteq \mathcal{P}(A \times V)$ e não sabemos que F é um conjunto, pois não será se A não é. No outro lado ainda temos que $F(x) = G(x, \{\, F(y) \mid y < x \,\})$ para todos $x \in \mathrm{dom}(F)$. Suponhamos que $\mathrm{dom}(F) \neq A$, e escolhe a_0 que é $<$-mínimo no conjunto $A \setminus \mathrm{dom}(F)$.

Agora temos que $\forall b < a_0 \, \exists \phi \, (\phi$ é uma tentativa e $b \in \mathrm{dom}(\phi)$. Por isto podemos aplicar o axioma de coleção que dá $\exists v \, \forall b < a_0 \, \exists \phi \in v \, (\phi$ é uma tentativa e $b \in \mathrm{dom}(f)$. Então $w = v \cap \{\, \phi \mid \phi$ é uma tentativa$\}$ é um *conjunto* pelo axioma de compreensão. Claro $f = \bigcup w$ é uma tentativa e podemos considerar $\bar{f} = f \cup \{\, (a_0, G(a_0, \{\, f(b) \mid b < a_0 \,\})) \,\}$ que é uma tentativa mas não é um subconjunto do f. Assim, como na teorema de recursão fraca temos uma contradição! Então $\mathrm{dom}(F) = A$.

Talvez você quer saber porque a demostração tem algumas mudanças de nossa demonstração anterior. Bem, você teria que saber que $G(a_0, \{\, F(a) \mid a < a_0 \,\})$ faria sentido antes de definir $\bar{F} = F \cup \{\, (a_0, G(a_0, \{\, F(a) \mid a < a_0 \,\})) \,\}$. E Para saber isso temia que saber que $\{\, F(a) \mid a < a_0 \,\}$ é um conjunto, que é uma conseqüência de aplicar o princípio de reposição para o conjunto $\{\, a \mid a < a_0 \,\}$. Então pode ver que não é possível evitar usar ou coleção ou reposição.

Eu deveria prevenir que não pode evitar usar coleção na teorema de recursão mesmo se A é um conjunto se G não é, e mesmo se $<$ é uma bem-ordem sobre A e não apenas uma relação bem-fundada.

2.6 Teoremas de comparação.

Definição. Uma função $f : (X, <_X) \longrightarrow (Y, <_Y)$ é um isomorfismo que preservar ordem se f é uma bijeção entre X e Y e $\forall x,\, y \in X\ (x <_X y \longleftrightarrow f(x) <_Y f(y))$.

Nota. Se $f : (X, <_X) \longrightarrow (Y, <_Y)$ é uma função que preservar ordem, f injetivo, ento s tem que saber que f tambm uma sobrejeo para saber que f um isomorfismo.

Teorema. Para qualquer conjunto bem-ordenado $(X, <)$ existe um ordinal único α para qual existe um isomorfismo (único) do $(X, <)$ para α que preserva ordem.

Demonstração. Definir, pela teorema de recursão, uma função $f : X \longrightarrow V$ (On) que satisfaz $f(x) = \{\, f(y) \mid y < x \,\}$.

(i) $\forall x \in X\ f(x) \in \mathrm{On}$. Senão, escolhe um x_0 que é $<$-mínimo no conjunto $\{\, x \in X \mid f(x) \notin \mathrm{On} \,\}$. Suponhamos que $x \in X$ e para todos $y < x$ temos que $f(y) \in \mathrm{On}$. Então $f(x) \subseteq \mathrm{On}$ pela definição de f, e $f(x)$ é bem-ordenado pela $\in$. Mas também, se $z \in y \in f(x)$, temos que $y = f(v)$ para alguma $v < x$. Logo $z \in \{\, f(u) \mid u < v \,\}$ e existe $u < v < x$ tal que $z = f(u)$. Conseqüentemente, $z \in f(x)$, e $f(x)$ é transitivo. Então $f(x) \in \mathrm{On}$. Logo, pelo princípio de indução para $<$, temos que $\forall x \in X\ f(x) \in \mathrm{On}$.

(ii) $\mathrm{im}(f)$ é um conjunto (pelos axiomas de coleção e compreensão ou pelo princípio de reposição), e (i) mostra que $\mathrm{im}(f) \subseteq \mathrm{On}$, então $\mathrm{im}(f)$ é bem-ordenado pelo $\in$. Suponhamos que $z \in y \in \mathrm{im}(f)$, então existe $x \in X$ tal que $z \in y = f(x)$, e logo existe $v \in X$ tal que $v < x$ e$z = f(v)$. Então $z \in \mathrm{im}(f)$ e $\mathrm{im}(f) \in \mathrm{On}$.

Finalmente se $g : X \longrightarrow \beta$ é um outro isomorfismo que preserva ordem, então $f \cdot g^{-1}$ seria um isomorfismo de β para α que preserva a ordem dada pelo $\in$. Então $\beta = \alpha$ e $f \cdot g^{-1}$ é igual para a funcão de identidade pela (o primerio corolário para) tricotomia.

Teorema de Comparação. Sejam $(X, <_X)$ e $(Y, <_Y)$ dois b.o.conjuntos. Então existe um isomorfismo que preservar ordem entre um deles e um segmento inicial do outro.

Demonstração. A teorema anterior fala que existem $\alpha, \beta \in \mathrm{On}$ e isomorfismos $f : (X, <_X) \longrightarrow \alpha$ e $g : (Y, <_Y) \longrightarrow \beta$ que preservam ordem. Agora vamos aplicar tricotomia. Se $\alpha = \beta$ temos que

$g^{-1} \cdot f$ é um isomorfismo que preserva ordem entre $(X, <_X)$ e $(Y, <_Y)$. Se $\alpha \in \beta$ temos que $g^{-1} \cdot f$ é um isomorfismo que preserva ordem entre $(X, <_X)$ e um segmento inicial próprio de $(Y, <_Y)$ (do qual $g^{-1}(\alpha)$ é um sucessor). E se $\beta \in \alpha$ temos que $f^{-1} \cdot g$ é um isomorfismo que preserva ordem entre $(Y, <_Y)$ e um segmento inicial próprio de $(X, <_X)$ (do qual $f^{-1}(\beta)$ é um sucessor).

2.7. A Hierarquia do V_αs

Agora podmeos definir rigorosomente (dos axiomas) a hierarquia dos V_αs. Defina, pela teorema de recursão, uma Funcão $V : \mathrm{On} \longrightarrow V$ (a colecão de todos conjuntos) tal que $V_\alpha = \bigcup\{\mathcal{P}(V_\beta) \mid \beta < \alpha\}$.

Proposição. $\forall\alpha\, V_\alpha$ é transitivo.

Demonstração. Se não escolhe α (<-)mínimo tal que V_α não é transitivo. Já vimos (na primeira proposição de Seção (1.5)) que $\mathcal{P}(X)$ é transitivo se X é transitivo. Logo $\forall\beta < \alpha\ \mathcal{P}(V_\beta)$ é transitivo. Mas $V_\alpha = \bigcup\{\mathcal{P}(V_\beta) \mid \beta < \alpha\}$ é uma união dos conjuntos transitivos e, então, é transitivo também.

Proposição. Se $\alpha \leq \beta$ temos que $V_\alpha \subseteq V_\beta$.

Demonstração. Se $\alpha = \beta$ é trivial. Se $\alpha < \beta$, então $V_\alpha \subseteq \mathcal{P}(V_\alpha)$, porque V_α e, logo, $\mathcal{P}(V_\alpha)$ são transitivos, e $\mathcal{P}(V_\alpha) \subseteq V_\beta$.

Corolário. Se α é um ordinal do tipo sucessor, então $V_{s(\alpha)} = V_{\alpha+1} = \mathcal{P}(V_\alpha)$.

Demonstração. $V_{s(\alpha)} = \bigcup\{\mathcal{P}(V_\beta) \mid \beta \leq \alpha\} = \bigcup\{\mathcal{P}(V_\beta) \mid \beta \leq \alpha\} \cup \mathcal{P}(V_\alpha)$. Mas $V_\beta \subseteq V_\alpha$ se $\beta < \alpha$, e então $\mathcal{P}(V_\beta) \subseteq \mathcal{P}(V_\alpha)$ se $\beta < \alpha$. Logo $\bigcup\{\mathcal{P}(V_\beta) \mid \beta \leq \alpha\} \subseteq \mathcal{P}(V_\alpha)$.

Corolário. Se λ é um ordinal do tipo limite, então $V_\lambda = \bigcup\{V_\alpha \mid \alpha < \lambda\}$.

Demonstração. $\bigcup\{V_\alpha \mid \alpha < \lambda\} \subseteq V_\lambda = \bigcup\{\mathcal{P}(V_\alpha) \mid \alpha < \lambda\} = \bigcup\{V_{s(\alpha)} \mid \alpha < \lambda\} \subseteq \bigcup\{V_\alpha \mid \alpha < \lambda\}$ porque $s(\alpha) < \lambda$ se $\alpha < \lambda$.

Teorema. O axioma de fundação é equivalente para "$\forall x\, \exists\alpha \in \mathrm{On}\, x \in V_\alpha$."

Demonstração. "$\Longrightarrow$" Se não, seja x_0 $\in$-mínimo tal que $\forall\beta \in \mathrm{On}\ x \notin V_\beta$. Logo $\forall x \in x_0\, \exists\beta\, x \in V_\beta$. Se aplicamos o axioma de coleção temos $\exists v\, \forall x \in x_0\, \exists\beta \in v\ x \in V_\beta$. Seja $u = v \cap \mathrm{On}$. Logo $\forall x \in x_0\, \exists\beta \leq \sup(u)\, x \in V_\beta$, e este dá que $\forall x \in x_0\, x \in V_{\sup(u)}$. Segui que $x_0 \subseteq V_{\sup(u)}$, e então que $x_0 \in V_{s(\sup(u))}$. Contradição

"$\Longleftarrow$" Seja $A \neq \emptyset$ uma classe com $A \subseteq \bigcup\{V_\alpha \mid \alpha \in \mathrm{On}\}$. Tome α mínimo tal que $A \cap V_\alpha \neq \emptyset$. Então qualquer $a \in A \cap V_\alpha$ é $\in$-mínimo no A.

Definição. Defina uma Função $\mathrm{rk} : V \longrightarrow V$ (On) pela $\mathrm{rk}(x) = \bigcup\{s(\mathrm{rk}(y)) \mid y \in x\}$, usando a teorema de recursão.

Proposição. (i) $\forall x \in V\ \mathrm{rk}(x) \in \mathrm{On}$. (ii) $\mathrm{rk}(x) =$ o α mínimo tal que $x \subseteq V_\alpha$. (iii) $\mathrm{rk}(x) =$ o α mínimo tal que $x \in V_\alpha$.

Demonstração. Exercísio. (Usar indução sobre $(V, \in)$.)

2.8. Fechos transitivos.

Defina para cada conjunto, pela recursão sobre $(\omega, \leq)$, uma função $t(n,x)$ tal que $t(0,x) = x$ e $t(n+1,x) = t(n,x) \cup \bigcup t(n,x)$. No fim, defina $\mathrm{FT}(x) = \bigcup\{\, t(n,x) \mid n \in \omega\}$. $\mathrm{FT}(x)$ o *fecho transitivo* de x

Proposição. Para cada x, $\mathrm{FT}(x)$ é o conjunto transitivo mínimo z com $x \subseteq z$. (Isto é, se y é transitivo e $x \subseteq y$, então $\mathrm{FT}(x) \subseteq y$.)

Demonstração. Seja $u \in v \in \mathrm{FT}(x)$. Então existe $n < \omega$ tal que $u \in v \in t(n,x)$. Então $u \in \bigcup t(n,x) \subseteq t(n+1,x) \subseteq \mathrm{FT}(x)$. Logo, $\mathrm{FT}(x)$ é transitivo.

Seja y transitivo com $x \subseteq y$. Vamos mostrar pela indução sobre ω que cada $t(n,x) \subseteq y$. É claro quando $n = 0$. Suponhamos que $t(n,x) \subseteq y$. Se $z \in t(n+1,x)$ temos ou $z \in t(n,x)$, quando $z \in y$, ou $z \in \bigcup t(n,x)$. Então existe alguma $v \in t(n,x)$ tal que $z \in v$. Mas se $z \in v \in t(n,x) \subseteq y$, temos que $z \in y$ pela transitividade de y. Então temos $t(n+1,x) \subseteq y$, e logo $\mathrm{FT}(x) = \bigcup t(n,x) \subseteq y$.

Proposição. O axioma de fundação para conjuntos (cada conjunto não vazio tem um membro $\in$-mínimo) implica o axioma de fundação para classes (cada classe não vazia tem um membro $\in$-mínimo).

Demonstração. Seja A, $\neq \emptyset$, uma classe. Seja $x \in A$. Ou x é $\in$-mínimo (acabamos) ou $x \cap A \neq \emptyset$. Então $\mathrm{FT}(x) \cap A \neq \emptyset$. Seja y $\in$-mínimo no conjunto $\mathrm{FT}(x) \cap A$. (Sabemos que é um conjunto pela propsição prévia.) Temos que $y \in A$. Agora suponhamos que $z \in y$. Então $z \notin \mathrm{FT}(x) \cap A$. Mas $z \in y \in \mathrm{FT}(x)$ é $\mathrm{FT}(x)$ é transitivo, então $z \in \mathrm{FT}(x)$. Logo $z \notin A$, e temos mostrado que y é $\in$-mínimo no A.

2.9. Aritmética dos ordinais: Adio dos ordinais.

Vamos usar recursão para definir adição e multiplicação sobre On.

Definição. Defina, para α fixo e β variável, $\alpha + \beta = \alpha \cup \{\, \alpha + \gamma \mid \gamma < \beta \,\}$

Proposição. Sejam α, $\beta \in \mathrm{On}$. Então $\alpha + \beta \in \mathrm{On}$.

Demonstração. Se não, seja β_0 mínimo com $\alpha + \beta_0 \notin \mathrm{On}$. Então para todos $\gamma < \beta_0$ temos que $\alpha + \gamma \in \mathrm{On}$, então $\alpha + \beta_0 = \alpha \cup \{\, \alpha + \gamma \mid \gamma < \beta_0 \,\} \subseteq \mathrm{On}$ e, logo, é bem-ordendado pelo $\in$.

Agora vamos ver que $\alpha + \beta_0$ é transitivo, então pertence a On, dando uma contradição para a suposição que não pertence a On. Sejam $z \in y \in \alpha \cup \{\alpha + \gamma \mid \gamma < \beta_0\}$. Então, ou $y \in \alpha$, quando $z \in \alpha$, porque α é um ordinal, ou existe $\gamma < \beta$ tal que $y = \alpha + \gamma \in \mathrm{On}$, logo, de novo, $z \in \{\alpha + \delta \mid \delta < \gamma\}$. Em cada caso temos que $z \in \alpha + \{\alpha + \gamma \mid \gamma < \beta_0\}$, dando a contradição desejeda. Logo $\alpha + \beta_0 \in \mathrm{On}$.

Lema. $\forall \alpha, \beta, \gamma, \delta \in \mathrm{On}$: (i) $\beta < \gamma \Longrightarrow \alpha + \beta < \alpha + \gamma$; (ii) $\alpha \leq \delta \Longrightarrow \alpha + \beta \leq \delta + \beta$.

Demonstração. (i) Se $\beta < \gamma$, então $\alpha + \beta \in \alpha + \gamma$.
(ii) Suponhamos que o Lema é falso para alguma par α e δ, e seja β_0 mínimo tal que $\alpha+\beta \not\leq \delta+\beta$. Então $\forall\beta < \beta_0$ temos que $\alpha+\beta \leq \delta+\beta$ e logo ou $\alpha+\beta = \delta+\beta$ ou $\alpha+\beta < \delta+\beta$, *i.e.* $\alpha+\beta = \delta+\beta$ ou existe $\gamma < \beta$ tal que $\alpha+\beta = \delta+\gamma$, ou $\alpha+\beta \in \delta$. Logo $\alpha+\beta_0 = \alpha\cup\{\,\alpha+\beta \mid \beta < \beta_0\,\} \subseteq \delta\cup\{\,\delta+\gamma \mid \gamma < \beta_0\,\}$ $= \delta + \beta_0$.

Proposição. (i) $\alpha + 0 = \alpha$; (ii) $\alpha + s(\beta) = s(\alpha + \beta)$; (iii) se λ é um ordinal do tipo limite, então $\alpha + \lambda = \bigcup\{\,\alpha + \gamma \mid \gamma < \lambda\,\}$.

Demonstração. (i) Trivial.
(ii) $\alpha + s(\beta) = \alpha \cup \{\,\alpha + \gamma \mid \gamma < s(\beta)\,\} = \alpha \cup \{\,\alpha + \gamma \mid \gamma < s(\beta)\,\} = \alpha \cup \{\,\alpha + \gamma \mid \gamma < \beta\} \cup \{\,\alpha + \beta\} =$ $(\alpha + \beta) \cup \{\,\alpha + \beta\,\} = s(\alpha + \beta)$.
(iii) Se $x \in \bigcup\{\alpha + \gamma \mid \gamma < \lambda\}$ então existe $\gamma < \lambda$ tal que $x \in \alpha \cup \{\,\alpha + \beta \mid \beta < \gamma\}$. Então $x \in \alpha\cup\{\,\alpha+\beta \mid \beta < \lambda\}$. Mas sabemos que $\lambda = \bigcup\lambda = \bigcup\{\,\gamma \mid \gamma < \lambda\}$, então se $x \in \alpha\cup\{\,\alpha+\beta \mid \beta < \lambda\}$ ou $x \in \alpha$ ou $x = \alpha+\beta$ para alguma $\beta < \lambda$ e existe $\gamma < \lambda$ tal que $\beta < \gamma$. Logo $x \in \bigcup\{\,\alpha+\gamma \mid \gamma < \lambda\}$.

Teorema. Sejam α, $\beta \in \mathrm{On}$ e seja $\prec$ a ordem anti-lexicográfico sobre $\alpha \times \{\,0\} \cup \beta \times \{\,1\}$ definido pelo $(\gamma, i) \prec (\delta, j)$ se e s se ou $i < j$ ou $i = j$ e $\gamma < \delta$. Então esta ordem é isomorfico para $(\alpha + \beta\, in)$

Demonstração. Defina uma função $f : \alpha\times\{\,0\}\cup\beta\times\{\,1\} \longrightarrow \alpha+\beta$ pelo $f(\gamma, 0) = \gamma$ e $f(\delta, 1) = \alpha+\delta$. É claro que a f é sobrejetivo e também que $\prec$ é uma ordem total sobre $\mathrm{dom}(f)$. Vamos ver que $(\gamma, i) \prec (\delta, j)$ implica $f(\gamma, i) < f(\delta, j)$.

Se $i < j$ então $i = 0$ e $j = 1$, $f(\gamma, i) = \gamma$ e $f(\delta, j) = \alpha + \delta$ e temos que $\gamma < \alpha \leq \alpha + \delta$. Se $i = j = 0$, então $f(\gamma, i) = \gamma$ e $f(\delta, j) = \delta$ e temos $\gamma < \delta$. E se $i = j = 1$ temos que $\alpha + \gamma < \alpha + \delta$ pelo lemma anterior.

Nota. $1 + \omega = \omega$, enquanto $\omega + 1 = s(\omega)$, então $+$ não é comutativo em geral.

Proposição. Se $x \subseteq \mathrm{On}$ é um conjunto não vazio, então $\alpha + \bigcup x = \bigcup\{\,\alpha + \beta \mid \beta \in x\}$. ($+$ é contínuo no segundo lugar/variável.)

Demonstração. $\beta \in x$ implica que $\beta \leq \bigcup x$, e então $\forall\beta \in x\,(\alpha + \beta \leq \alpha + \bigcup x)$. Logo $\bigcup\{\,\alpha + \beta \mid \beta \in x\,\} \subseteq \alpha + \bigcup x$.

Seja $\rho = \bigcup\{\,\alpha + \beta \mid \beta \in x\}$ Se $\rho \in \alpha + \bigcup x$, então ou $\rho \in \alpha$ ou existe $\gamma \in \bigcup x$ tal que $\rho = \alpha + \gamma$. Se $\rho \in \alpha$, então $\forall\beta \in x\; \alpha + \beta \leq \rho < \alpha$, uma contradição. E se $\rho = \alpha + \gamma$ com $\gamma \in \bigcup x$, então existe $\beta \in x$ tal que $\gamma < \beta$ e então $\rho < \alpha + \beta$ e $\rho < \bigcup\{\,\alpha + \beta \mid \beta \in x\,\} = \rho$, uma contradição de novo. Logo, $\rho \notin \alpha + \bigcup x$ e temos que $\rho = \alpha + \bigcup x$.

Podemos definir subtração também, mas pela falta de comutatividade de adição não é tão útil como adição.

Definição. $\alpha - \beta = \{\gamma \,|\, \beta + \gamma < \alpha\}$. Alternativamente pode definir $\alpha - \beta$ pela recursão: $\alpha - \beta = 0$ se $\beta > \alpha$ e $\alpha - \beta = \{\alpha - \gamma \,|\, \gamma < \beta\}$ se $\beta \leq \alpha$.

Proposição. Sejam $\alpha, \beta \in \mathrm{On}$ e $\beta \leq \alpha$. Então $\beta + (\alpha - \beta) = \alpha$.

Demonstração. $\beta + (\alpha - \beta) = \beta \cup \{\beta + \gamma \,|\, \gamma < \alpha - \beta\} = \beta \cup \{\beta + \gamma \,|\, \beta + \gamma < \alpha\} \subseteq \alpha$. Suponhamos que $\beta + (\alpha - \beta) < \alpha$. Então $(\alpha - \beta) \in \{\gamma \,|\, \beta + \gamma < \alpha\} = \alpha - \beta$. Uma contradição. Logo $\beta + (\alpha - \beta) = \alpha$.

Nota. $(\alpha - \beta) + \beta \neq \alpha$ em geral. Por exemplo, $\omega - 1 = \omega$, logo $(\omega - 1) + 1 = s(\omega) \neq \omega$.

2.10 Aritmética dos ordinais: Multiplicação dos ordinais.

Pela teorema sobre recursão, definamos $\alpha.\beta = \{\alpha.\gamma + \delta \,|\, \gamma < \beta \,\&\, \delta < \alpha\}$.

Proposição. $\forall \alpha, \beta \in \mathrm{On}\ (\alpha.\beta \in \mathrm{On})$.

Demonstração. Suponhamos que $\alpha.\gamma \in \mathrm{On}$ para cada $\gamma < \beta$. Então $\alpha.\gamma + \delta \in \mathrm{On}$ para cada $\gamma < \beta$ pela proposição que $\xi + \zeta \in \mathrm{On}$ se $\xi, \zeta \in \mathrm{On}$, e temos que $\alpha.\beta \subseteq \mathrm{On}$ e logo é bem-ordenado pelo $\in$. Também para cada $\gamma < \beta$ a função $f_\gamma : \alpha \longrightarrow \{\alpha.\gamma + \delta \,|\, \delta < \alpha\}$ dado pelo $f_\gamma(\delta) = \alpha.\gamma + \delta$ tem f_γ"$\alpha = \{\alpha.\gamma + \delta \,|\, \delta < \alpha\}$, e logo $\{\alpha.\gamma + \delta \,|\, \delta < \alpha\}$, A_γ vamos falar, é um conjunto pelo princípio de reposição. Então $\alpha.\beta = \bigcup A_\gamma \gamma < \beta$ é uma união dos conjunto e é um conjunto também. Finalmente, se $x \in y \in \alpha.\beta$, então existe $\gamma < \beta$ e $\delta < \alpha$ tal que $x \in y = \alpha.\gamma + \delta$. Então ou $x \in \alpha.\gamma$ ou existe $\sigma < \delta$ tal que $x = \alpha.\gamma + \sigma$. No primeiros caso existe $\epsilon < \gamma$ e $\tau < \alpha$ tal que $x = \alpha.\epsilon + \tau$. Então em cada caso temos que $x \in \alpha.\beta$. Porque agora temos que $\forall \beta\, (\forall \gamma < \beta\, (\alpha.\gamma \in \mathrm{On}) \longrightarrow \alpha.\beta \in \mathrm{On})$ temos que $\forall \beta \in \mathrm{On}\ \alpha.\beta \in \mathrm{On}$.

Lema. $\forall \alpha \in \mathrm{On}$ (i) $0.\alpha = 0$; (ii) $1.\alpha = \alpha$; (iii) $\forall \beta, \gamma \in \mathrm{On}\ (\beta < \gamma) \Longrightarrow \alpha.\beta < \alpha.\gamma$; e (iv) $\forall \delta\ \beta \in \mathrm{On}, (\alpha \leq \delta \Longrightarrow \alpha.\beta \leq \delta.\beta)$.

Demonstração. (i)–(iii) são óbvios. (iv) Suponhamos que $\alpha, \delta \in \mathrm{On}$, $\beta \in \mathrm{On}$ e para todos $\gamma < \beta$ temos que $\alpha.\gamma \leq \delta.\gamma$. Usando o lema sobre adição na Seção (2.8), temos para todos $\gamma < \beta$ e todos $\epsilon < \alpha$ que $\alpha.\gamma + \epsilon \leq \delta.\gamma + \epsilon$. Então ou $\alpha.\gamma + \epsilon = \delta.\gamma + \epsilon$, quando $\alpha.\gamma + \epsilon \in \delta.\beta$, ou $\alpha.\gamma + \epsilon \in \delta.\gamma + \epsilon \in \delta.\beta$, e $\alpha.\gamma + \epsilon \in \delta.\beta$, pela transitividade de $\delta.\beta$. Em cada caso temos que $\alpha.\beta \subseteq \delta.\beta$ e então $\alpha.\beta \leq \delta.\beta$. Mas este mostrar que $(\forall \gamma < \beta\, \alpha.\beta \leq \delta.\gamma) \longrightarrow \alpha.\beta \leq \delta.\beta$. Então, porque $<$ é bem-fundado sobre os ordinais, $\forall \beta \in \mathrm{On}\, \alpha.\beta \leq \delta.\beta$.

Proposição. (i) $\alpha.0 = 0$; (ii) $\alpha.s(\alpha) = \alpha.\beta + \alpha$; e (iii) se $\lambda \in \mathrm{On}$ é do tipo limite, então $\alpha.\lambda = \bigcup \{\alpha.\gamma \,|\, \gamma < \lambda\}$.

Demonstração. (i) Trivial.
(ii) $\alpha.s(\beta) = \{\alpha.\gamma + \delta \,|\, \gamma \leq \beta \,\&\, \delta < \alpha\} = \{\alpha.\gamma + \delta \,|\, \gamma < \beta \,\&\, \delta < \alpha\} \cup \{\alpha.\beta + \delta \,|\, \delta < \alpha\} = \alpha.\beta + \alpha$.
Se λ é um ordinal do tipo limite, $\bigcup \{\alpha.\beta \,|\, \beta < \lambda\} = \{\alpha.\gamma + \delta \,|\, (\exists \beta < \lambda\, \gamma < \beta) \,\&\, \delta < \alpha\} = \{\alpha.\gamma + \delta \,|\, \gamma \in \bigcup \lambda \,\&\, \delta < \alpha\} = \{\alpha.\gamma + \delta \,|\, \gamma < \lambda \,\&\, \delta < \alpha\}$, com o último passo porque λ é do tipo limite.

Teorema. Sejam $\alpha, \beta \in \mathrm{On}$ e seja $\prec$ a ordem anti-lexicografico sobre $\alpha \times \beta$, definido pelo $(\delta_0, \gamma_0) \prec (\delta_1, \gamma_1)$ ou se $\gamma_0 < \gamma_1$ ou se $\gamma_0 = \gamma_1$ e $\delta_0 < \delta_1$. Então $(\alpha \times \beta, \prec)$ é isomorfico para

$(\alpha.\beta, \in)$ pelo um isomorfismo que preserva ordem.

Demonstração. Defina $f : \alpha \times \beta \longrightarrow \alpha.\beta$ pelo $f(\delta, \gamma) = \alpha.\gamma + \delta$. É claro que f é uma sobrejeção. Se $(\delta_0,\ \gamma_0) \prec (\delta_1,\ \gamma_1)$ *ou* $\gamma_0 < \gamma_1$ quando $\alpha.\gamma_0 + \delta_0 < \alpha.s(\gamma_0) \leq \alpha.\gamma_1 \leq \alpha.\gamma_1 + \delta_1$, *ou* $\gamma_0 = \gamma_1$ e $\delta_0 < \delta_1$, quando $\alpha.\gamma_0 + \delta_0 < \alpha.\gamma_0 + \delta_1$ pela lema sobre adição. Logo, f preserva ordem, é então é um isomorfismo.

Nota. $2.\omega = \omega$, $3.\omega = \omega$, $\ldots$, mas $\omega.\omega \neq \omega$. Nota também que $(\omega + 1).\omega = \omega.\omega$

Teorema. Seja $\alpha,\ \beta \in \mathrm{On}$, $\beta > 0$. Então existe únicos σ, τ com $\tau < \beta$ tal que $\alpha = \beta.\sigma + \tau$.

Demonstração. Sejam $\sigma = \{\, \gamma \,|\, \beta.s(\gamma) \leq \alpha \,\}$ e $\tau = \alpha - \beta.\sigma, = \{\, \delta \,|\, \beta.\sigma + \delta < \alpha \,\}$. Então $\alpha = \beta.\sigma + \tau$. Para ver que $\tau < \beta$, observe que se não ou $\beta = \tau$, quando $\alpha = \beta.\sigma + \beta = \beta.s(\sigma)$ ou $\beta \in \{\, \delta \,|\, \beta.\sigma + \delta < \alpha \,\}$ e, então, $\beta.\sigma + \beta = \beta.s(\sigma) < \alpha$. Logo em qualquer caso $\beta.s(\sigma) \leq \alpha$ e $\sigma \in \sigma$, uma contradição!

Proposição. Se $x \subseteq \mathrm{On}$ então $\alpha.\bigcup x = \bigcup\{\, \alpha.\beta \,|\, \beta \in x \,\}$. (Que quer dizer que . é continuo no segundo lugar/variável.)

Demonstração. $\alpha.\bigcup x = \{\, \alpha.\gamma{+}\delta \,|\, \delta < \alpha \,\&\, (\exists \beta \in x\, \gamma < \beta) \,\} = \{\, \alpha.\gamma{+}\delta \,|\, \exists \beta \in x\, (\gamma < \beta \,\&\, \delta < \alpha) \,\}$ $= \bigcup\{\, \alpha.\beta \,|\, \beta \in x \,\}$.

Nota. Na teorema prévio $\sigma = \bigcup\{\, \gamma \,|\, \beta.\gamma \leq \alpha \,\}$.

Aritmética dos ordinais: 2.11 Exponenciação dos ordinais.

Agora podemos fazer mais uma definição pelo teorema sobre recursão, da exponciação.

Definição. Seja $\alpha,\ \beta \in \mathrm{On}$. Então $\alpha^\beta = \{\, 0 \,\} \cup \{\, \alpha^\gamma.\delta + \epsilon \,|\, \gamma < \beta \;\&\; \delta < \alpha \;\&\; \epsilon < \alpha^\gamma \,\}$.

Proposição. Seja $\alpha,\ \beta \in \mathrm{On}$. Então $\alpha^\beta \in \mathrm{On}$.

Lema. $\forall \alpha,\ \beta,\ \gamma\ \delta \in \mathrm{On}$ temos (i) $\alpha^\beta.\alpha^\gamma = \alpha^{\beta+\gamma}$; (ii) $(\alpha^\beta)^\gamma = \alpha^{\beta.\gamma}$; (iii) $\beta < \gamma \Longrightarrow \alpha^\beta < \alpha^\gamma$; e (iv) $\alpha \leq \delta \Longrightarrow \alpha^\beta \leq \delta^\beta$.

Proposição. Seja $\alpha \in \mathrm{On}$. (i) $\alpha^0 = 1$; (ii) $\alpha^{s(\beta)} = \alpha^\beta.\alpha$ para cada $\beta \in \mathrm{On}$; e (iii) se λ é um ordinal do tipo limite, então $\alpha^\lambda = \bigcup\{\, \alpha^\gamma \,|\, \gamma < \lambda \,\}$.

As demonstraçes são similares para as demonstraçes dos equivalentes para .. Pode confirmá-las se quiser.

Nota. $\forall n \in \omega\, n^\omega = \omega$, mas $\omega^\omega \neq \omega$, enquanto $\omega.\omega^\omega = \omega^\omega$. E se definimos $\epsilon_0 = \bigcup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}$, então $\omega^{\epsilon_0} = \epsilon_0$.

Quando você voltar para esta Seção mas tarde você deveria lembrar que todos estes fatos são para exponenciação dos *ordinais*, que é muito diferente da teoria da exponenciação dos *cardinais* que veremos no Capítulo (4).

Teoria dos conjuntos: Exercícios 2.

1. Escrever os axiomas para uma ordem parcial e uma ordem total usando $\leq$ em vez de $<$, e mostre a equivalença com os axiomas exprimidos usando $<$.

2. Mostre que se $Y \subseteq X$ e $<$ é uma relação bem-fundada sobre X, então a restrição de $<$ para Y é também bem-fundada.

3. Mostre que se $<_0$ é bem-fundado sobre X_0 e $<_1$ é bem-fundado sobre X_1, então $<_0 \times <_1$ é bem-fundado sobre $X_0 \times X_1$, onde $(a_0, a_1)(<_0 \times <_1)(b_0, b_1)$ se e só se $a_0 <_0 b_0$ e $a_1 <_1 b_1$. Mostre que se $<_0$ e $<_1$ são bem-ordens, então $<_0 \times <_1$ é uma bem-ordem também.

4. Suponhamos que $<$ é uma bem-ordem sobre X. Construir de $<$ uma bem-ordem sobre $\mathcal{P}_{<\omega}(X)$ – o conjunto do todos os subconjuntos finitos de X.

5. (Uma olhada de "teoria de conjuntos descritivo.") Vamos escrever ${}^{<\omega}\omega$ para $\bigcup\{{}^{n}\omega \mid n \in \omega\}$, o conjunto de todos seqüências finitos dos números naturais. Defina $<$ para $u < v$ se e só se v é uma subseqüência inicial própria de u. (Nota a direção disso!)

(i) Mostre que $f : {}^{\omega}\omega \longrightarrow \omega$ é continuo (com referência para a topologia produto sobre ${}^{\omega}\omega$ que vem de a topologia discreta sobre ω) se e só se $<$ é uma relaçao bem-fundada sobre o conjunto $\{u \in {}^{<\omega}\omega \mid f$ *não* é constante sobre $\{g \in {}^{<\omega}\omega \mid g$ prolonga a seqüência $u\}\}$.

(ii) Seja $T \subseteq {}^{<\omega}\omega$ tal que $u \in T$ e $u < v$ implica $v \in T$. (Falamos que T é uma árvore.) Escreva u_i para i^o-membro de u, e defina uma relação $\prec$ sobre T por: $u \prec v$ se e só se **ou** $u < v$, **ou** existe um i mínimo com $u_i \neq v_i$, e $u_i < v_i$ para este i (na ordem usual sobre ω). Mostre que $<$ é uma relação bem-fundada sobre T se e só se $\prec$ é uma bem-ordem de T.

6. Se $X \subseteq \mathrm{On}$ é um conjunto mostre que ou $\bigcup X \in X$ ou $\bigcup X = \bigcap\{\alpha \mid \forall\beta \in X\ \beta < \alpha\}$.

7. Ache um subconjunto de $\mathbf{R}$ (com a ordem usual) que é isomorfico para $\omega+\omega$. (Se você fez pergunta (5): ache $T \subseteq^{\omega} \omega$ tal que existe um isomorfismo entre $(T, \prec)$ e $\omega + \omega$ que preserva a ordem.)

8. Defina ordens lineares sobre ω que são isomorficas sob isomorfismos que preservão as ordens com: (i) ω^2, (ii) ω^ω, (iii) $\mathbf{Q}$ com a ordem usual.

9. Mostre que $\alpha + \beta = \alpha' + \beta'$ e $\beta' > \beta$ implica $\alpha' < \alpha$, mas o inverso e falso.

10. Quando é $\alpha + \beta$ um ordinal do tipo limite? E $\alpha.\beta$?

11. Sejam α, $\beta \in \{1, \omega, \omega.\omega\}$. Quantos possibilidades são para (i) $\alpha + \beta$, (ii) $\alpha \times \beta$?

12. Mostre que sejam α, $\beta \in \mathrm{On}$, então $\alpha\beta = \beta\alpha$ se e só se $\alpha^2\beta^2 = \beta^2\alpha^2$.

13. Seja $\alpha \in \mathrm{On}$. Mostre que existe $k < \omega$ e ordinais $\gamma_0, \ldots, \gamma_k$ e nmeros naturais $n_0, \ldots, n_k$ tal que $\alpha = \omega^{\gamma_k}.n_k + \ldots + \omega^{\gamma_0}.n_0$. (Uma pista: começe para mostrando que $\alpha = \omega^\beta + \delta$ para alguma ordinal β e alguma $\delta < \omega^\beta$ e depois analise δ.)

14. Suponhamos que $f : \mathrm{On} \longrightarrow \mathrm{On}$ é aumentando estritomente ($\forall\alpha < \beta\ f(\alpha) < f(\beta)$) e contínuo

nos limites (seja λ um ordinal do tipo limite, então $f(\lambda) = \bigcup\{\, f(\alpha) \mid \alpha < \lambda \,\}$). Mostre que existe um $\zeta \in \mathrm{On}$ tal que $f(\zeta) = \zeta$. Mostre que a função f definida para $f(\alpha) = \alpha^\omega$ é aumentanda estritomente e contínua nos limites. Qual ordinal é o primeiro tal que $f(\zeta) = \zeta$?

Capítulo 3. O axioma de escolha.*

Agora vamos tratar do ultimo axioma do nosso sistema de teoria dos conjuntos, o axioma de escolha. Vamos mostrar a equivalência entre o axioma de escolha e dois outros princípios muitos úteis.

Axioma de Escolha. (AE) Se x é um conjunto de conjuntos não vazios, então existe uma função que escolha um membro de cada dos conjuntos quem pertencem a x: $f : x \longrightarrow \bigcup x \; \forall y \in x \; f(x) \in x$.

Princípio de Bem-Ordenando. (BO) Seja x um conjunto. Então existe uma bem-ordem do x.

Lema de Zorn. (LZ) Seja $(X, \leq)$ um conjunto parcialmente ordenado tal que qualquer subconjunto C que é totalmente ordenado pelo $\leq$ (*i.e.* qualquer cadeia no $(X, \leq)$) tem um limite superior. Então X tem um membro máximo.

Teorema. (AE) $\Longleftrightarrow$ (BO) $\Longleftrightarrow$ (LZ).

Demonstração. (LZ) $\Longrightarrow$ (BO). Seja X um conjunto e considerar o conjunto dos bem-ordenandos dos subconjuntos de X. É um conjunto parcialmente ordenado sob a relação de sendo um segmento inicial: $(Y, \leq) \prec (Y', \leq')$ se e só se $(Y, \leq)$ é um segmento inicial de $(Y', \leq')$. É claro que qualquer a união de qualquer cadeia é um supremo para a cadeia. Então o lema de Zorn fala que existe um elemento máximo, seja $(Z, \leq)$. Se $Z \neq X$ podemos escolhar $x \in X \setminus Z$ e ter uma bem-ordem do $Z \cup \{x\}$ pelo botando $z < x$ para todos $z \in Z$. Então $Z = X$ e $\leq$ é um bem-ordem do X.

(BO) $\Longrightarrow$ (AE). Seja x um conjunto de conjuntos não vazios. Seja $<$ uma bem-ordem do x. Podemos tomar $f(y) =$ o membro $<$-mínimo de y para cada $y \in x$.

(AE) $\longrightarrow$ (LZ). Seja $(X, \preceq)$ um conjunto parcialmente ordenado tal que qualquer cadeia tem um limite superior. Pelo axioma de escolha podemos achar uma função $f : \mathcal{P}_{\neq\emptyset}(X) \longrightarrow X$ tal que $\forall A \subseteq X \; (A \neq \emptyset \longrightarrow f(A) \in A)$. Vamos usar f para ajudar nós escolhar pela recuraão uma cadeia no $(X, \prec)$ do qual um limite superior será máximo no x.

Para qualquer $B \subseteq X$ defina $\uparrow(B) = \{x \in X \mid \forall b \in B \; b \prec x\}$. Seja $\star$ um conjunto que não pertence a x. Pela teorema de recursão (forte) defina uma Função $F : \mathrm{On} \longrightarrow X \cup \{\star\}$ tal que $F(\alpha) = f(\uparrow(\{F(\beta) \mid \beta < \alpha\}))$ se $\uparrow(\{F(\beta) \mid \beta < \alpha\}) \neq \emptyset$, and $F(\alpha) = \star$ senão.

Se $\beta < \alpha$ e $F(\alpha) \neq \star$, então $F(\beta) \prec F(\alpha)$. Logo, fosse $\star \notin \mathrm{rge}(F)$ teríamos que F seria uma injeção, e então $F^{-1} : \mathrm{im}(F) \longrightarrow \mathrm{On}$ seria uma sobrejeção. Mas $\mathrm{im}(F) \subseteq X(\cup\{\star\})$ é em qualquer caso um conjunto. Então pelo princípio de reposição teríamos que On seria um conjunto também. Uma contradição! Logo $\star \in \mathrm{im}(F)$.

Então seja α_0 mínimo tal que $F(\alpha_0) = \star$. Temos que $\{F(\beta) \mid \beta < \alpha_0\}$ é um cadeia no $(X, \prec)$ e $\uparrow(\{F(\beta) \mid \beta < \alpha_0\}) = \emptyset$. Se x_0 é um limite superior de $\{F(\beta) \mid \beta < \alpha_0\}$ então x_0 é máximo no X. (x_0 é, então, também o elemento máximo do $\{F(\beta) \mid \beta < \alpha_0\}$ e α_0 é um ordinal do tipo sucessor.)

* versão 1.0, 3/12/00

Nota. Nos exercísios deixei varias conseqüências do axioma para vocês mostrar. Entre elas é um outro equivalente do axioma de escolha: que qualquer produto cartesiano geral é não vazio.

Nota. Taís me perguntou no fim de uma aula se existe alguma coisa para a teoria dos conjuntos parecida à dicotomia entre geometria euclidiana e não-euclidiana. Para dar uma resposta razoável para esta pergunta vale a pena parar um momento para pensar sobre axiomatisação e abstração na matemática mas geralmente. Fazemos abstrações (do qual axiomatisações são um tipo) muito na matemática. Tem ao menos três razões para fazer isso. Ajuda nós entender melhor que estamos fazendo nas situações mais concretos. Este parece ser uma coisa que muitos vezes sentimos ou acreditamos é um bom para nós em se mesmo, e talvez as vezes faz sentir mais seguro. Abstrações muitos vezes esclarecem como tratar outras problemas numa área. E abstrações muitos vezes ajudam nós abrir novos áreas da matemática, criando materias interesantes novos com teoria nova e problemas novos. Quando fazemos essas abstrações nunca temos garantias que qualquer dos razão vai dar certo para nós. Porém nossa experiência é que muitos vezes vale a pena. Simultâneo para abratração temos um processo continuo das coisas abstraitos virando mais concreto com uso. Por exemplo $2^{1/2}$, os reis $\mathbf{R}$ e mesmo o cardinal ω_1 que vamos encontrar no cápitulo proximo se tornam mais concreto quando viramos acostumados para eles.

O descobrimento do geometrias não-euclidianas não foi só um resposta para uma pergunta formal sobre os axiomas de Euclid, mas foi importante porque dou muito introspecção na geometria em se mesmo, do dois na área "velha" e não sentido mais amplo que ajudou criar. Até agora parece que precisamos dos axiomas do ZF para explicar nossas idéias sobre conjuntos. Isso é que ninguem tenha tido sucesso iluminando a teoria dos conjuntos ou criando uma vista nova sobre o assunto pelo mudando ou trocando os axiomas do ZF. Não falo que não é possível, mas talvez tem menos probabilidade agora de uma revelações desta natureza depois de um século da pesquisa no assunto (muito intensificada nas ultimas 40 anos) que na epoca do descobrimento do geometrias não-euclidianas – talvez porque agora estamos mais sensível para este perguntas de axiomatizações e modelos (cf. Cápitulo 6).

Embora, talvez um analogia da dicotomia seria ZF com AE e ZF sem AE. ZF com AE é o sistema o mais importante para nós, dando para nós coisas que esperemos dos conjunto, como que produtos cartesianos não são vazio e que cada espaço vectorial tem uma base. Mas estudiando ZF sem AE com alguma outro axioma (como por exemplo o axioma de determinacidade†) pode também dá para nós introspecções úteis sobre a natureza da coleção dos conjuntos, e sobre a teoria ZF com AE. Mas falarei mais sobre este pergunta na §6.

† Veja, por exemplo, Alexander Kechris, *Classical Descriptive Set Theory*, Springer, 1995, ou Yiannis Moschovakis, *Descriptive Set Theory*, North Holland, 1980.

Teoria dos conjuntos: Exercícios 3.

1. Demonstrar que os seguintes são equivalentes do axioma de escolha.
(a) Se $f : y \longrightarrow x$ é uma sobrejeção, então existe uma função $g : x \longrightarrow y$ tal que $g(f(z)) = z$ para todos $z \in y$.
(b) Para qualquer conjunto x dos conjuntos não vazios existe um conjunto transversal t, *i.e.*, um conjunto $t \subseteq \bigcup x$ tal que $\forall y \in x\ \overline{\overline{y \cap t}} = 1$.
(c) Para qualquer x, y ou existe uma injeção do x para y, ou existe uma injeção do y para x.
(d) $\mathbf{m} \,.\, \mathbf{m} = \mathbf{m}$ para qualquer cardinal $\mathbf{m}$. (Pista: se x é um conjunto considerar os cardinalidades do x e o conjunto dado pelo aplicando o Lema de Hartog para x, *i.e.*, $\{\alpha \in \mathrm{On} \mid \alpha \prec x\}$.)

2. Use equivalentes do axioma da escolha para monstrar os seguintes.
(a) Qualquer ordem parcial sobre um conjunto pode ser estendido para uma ordem total sobre o conjunto.
(b) Qualquer espaço vetorial tem uma base.
(c) Quaisquer duas bases dum espaço vetorial tem a mesmo cardinalidade.
(d) Qualquer campo pode ser embutido num campo álgebraicamente fechado.
(e) Qualquer produto de espaços topologicos compactos é compacto.
(e) Existe um conjunto dos reais que não é medidável no sentido de Lebesgue.

3. O axioma de escolha é usado mostrar:
(a) Qualquer conjunto não finito tem um subconjunto enumerável?
(b) Um união de um conjunto enumerável dos conjuntos que são enumeráveis é enumerável?
Se sim, explicar como.

4. Para qualquer x vamos escrever $\mathcal{P}_{<\omega}(x)$ para o conjunto dos subconjuntos de x que são finitos. Mostre que se x é infinito, então $x \sim \mathcal{P}_{<\omega}$. Tem conjuntos x para qual você não precisa do axioma de escolha para mostrar isso?

5. (a) Mostre que $(\aleph_{\alpha+1})^{\aleph_\beta} = (\aleph_\alpha)^{\aleph_\beta}.\aleph_{\alpha+1}$ para qualquer α, $\beta \in \mathrm{On}$. (Pista: Considerar os casos $\alpha \leq \beta$ e $\beta < \alpha$ individualmente.)
(b) Deduzir que $(\aleph_n)^{\aleph_\beta} = 2^{\aleph_\beta}.\aleph_n$ para qualquer $n \in \omega$.
(c) Quando é $(\aleph_\omega)^{\aleph_\beta} = 2^{\aleph_\beta}.\aleph_\omega$?

6. (a) Seja I um conjunto e sejam $\{X_i \mid i \in I\}$ e $\{Y_i \mid i \in I\}$ conjuntos tal que não existe uma sobrejeção do X_i para Y_i para qualquer $i \in I$. Mostre que nao existe uma sobrejeção do $\bigcup\{X_i \mid i \in I\}$ para $\Pi\{Y_i \mid i \in I\}$. Deduzir que se κ é um cardinal e $\{\mu_\alpha \mid \alpha < \kappa\}$ e $\{\nu_\alpha \mid \alpha < \kappa\}$ são conjuntos dos cardinais tal que $\mu_\alpha < \nu_\alpha$ para todos $\alpha < \kappa$, então temos que $\Sigma\{\mu_\alpha \mid \alpha < \kappa\} < \Pi\{\mu_\alpha \mid \alpha < \kappa\}$.
(b) Mostre que qualquer cardinal κ é a soma de $\mathrm{cf}\,(\kappa)$ cardinais cada um com cardinalidade menos que κ, e logo que $\kappa < \kappa^{\mathrm{cf}\,(\kappa)}$.

7. Mostrar que se κ é regular e $2^\mu \leq \kappa$ para todos $\mu < \kappa$, então $\Sigma\{\kappa^\mu \mid \mu < \kappa\} = \kappa$.

8. Mosrar que $2^{\aleph_1} = \aleph_2$ implica que $\aleph_\omega^{\aleph_0} \neq \aleph_{\omega_1}$.

Capítulo 4. Aritmética dos cardinais.*

4.1. Noções basicos sobre cardinais.

Somos habitudos comparar o tamanho dos conjuntos pelo vindo se tem uma injeção de um para o outro, ou um bijeção entre os dois.

Definição. Sejam x, y conjuntos. Seja $x \preceq y$ se existe uma injeção (uma immersão) do x para y (*i.e.* uma função f tal que para todos $z_0,\ z_1 \in x$ temos que $f(z_0) = f(z_1) \Longrightarrow z_0 = a_1$).
E seja $x \preceq^* y$ ou se $x = \emptyset$ ou se existe uma sobrejeção do y para x (*i.e.* uma função g tal que para todos $z \in x$ existe $u \in y$ tal que $g(u) = z$).
Defina $x \sim y$ se existe uma bijeção $f : x \longrightarrow y$ (*i.e.* uma função f do x para y tal que f é uma injeção e uma sobrejeção.

Nossos dois lemas primeiros são claros.

Lema. Se $x \preceq y$, então $x \preceq^* y$

Demonstração. Se $x = \emptyset$ tem nada para mostrar. Senão seja $f : x \longrightarrow y$ uma injeção e seja u qualquer elemento arbitrário do x. Logo, se definimos $g : y \longrightarrow x$ pelo $g(z) = f^{-1}(z)$ se $z \in \mathrm{im}(f)$, e $g(z) = u$ é senão, é claro que g é uma sobrejeção.

Lema. O axioma de escolha implica que se $x \preceq^* y$, então $x \preceq y$.

Demontração. Se $g : y \longrightarrow x$ é uma sobrejeção, seja $s_v = \{u \in y \,|\, g(u) = v\}$ para todos $v \in x$ e seja $z = \{s_v \,|\, v \in x\}$. Aplicamos o axioma de escolha para z. Esse dá para nós uma função $f : z \longrightarrow \bigcup z, = y$, tal que $f(s_v) \in s_v$ para todos $s_v \in z$. Logo a função $h : x \longrightarrow y$ definida pelo $h(v) = f(s_v)$ é uma injeção, porque se temos $v_0,\ v_1 \in x$ e $h(v_0) = h(v_1)$, então $v_0 = g(h(v_0)) = g(h(v_1)) = v_1$.

Nota. Precisamos do axioma de escolha para establecer este fato. Porém, a teorema seguinte não usa o axioma de escolha.

Teorema. (Schröder-Bernstein) Se $x \preceq y$ e $y \preceq x$, então $x \sim y$.

Demonstração. Suponhamos que $i : x \longrightarrow y$ e $j : y \longrightarrow x$ são injeções. Defina $k : \mathcal{P}(x) \longrightarrow \mathcal{P}(x)$ pelo $k(a) = (x \setminus j``y) \cup j{\cdot}i``a$ para cada $a \in x$. É claro que se $a \subseteq b \subseteq x$, então $k(a) \subseteq k(b)$.

Tome $c = \bigcup\{a \subseteq x \,|\, a \subseteq k(a)\}$. Então $c \subseteq \bigcup\{k(a) \,|\, a \subseteq x \,\&\, a \subseteq k(a)\} \subseteq k(c)$, porque $a \subseteq k(a) \subseteq k(c)$ quando $a \subseteq c$. Logo $k(c) \subseteq k(k(c))$. Então $k(c) \subseteq c$, e $c = k(c)$. (Nota que até aqui só usamos que k é cresente sobre $\mathcal{P}(x)$ e nada mais.)

Defina $f : x \longrightarrow y$ pelo $f(u) = i(u)$ se $u \in c$, e $f(u) = j^{-1}(u)$ se $u \notin c$. Sejam $u_0,\ u_1 \in x$. Se do dois $u_0,\ u_1 \in c$ é claro que $f(u_0) = f(u_1)$ implica $u_0 = u_1$. Similarmente, se $u_0,\ u_1 \notin c$ temos

* versão 1.0, 3/12/00

que $f(u_0) = f(u_1)$ implica $u_0 = u_1$ também. E se $u_0 \in c$ e $u_1 \notin c$ e $f(u_1) = v$, então $v \notin \text{im}(i)$ e $f(u_0) \neq f(u_1)$. Finalmente, se $v \in y$ e não existe $u \in c$ tal que $f(u) = v$, então $j(v) \notin c$ e $v = f(j(v))$.

Definição. Uma *noção de cardinalidade* é uma Função, card : $V \longrightarrow V$, tal que $\text{card}(x) = \text{card}(y)$ se e só se $x \sim y$.

Mesmo sem o axioma de esolha existe uns tais noções. Vamos usar um, paraqual escrevemos $\overline{\overline{x}}$ em vez de $\text{card}(x)$:

$$\overline{\overline{x}} = \ \alpha \text{ onde } \alpha \in \text{On é mínimo tal que existe uma bem-ordem de } x \text{ bijetivo com } \alpha,$$
$$\text{se existe tais } \alpha\text{s, e}$$
$$\overline{\overline{x}} = \ V_\alpha \cap \{y \mid y \sim x\} \text{ onde } \alpha \text{ é mínimo tal que existe } y \in V_\alpha \text{ com } y \sim x, \text{ senão.}$$

Nota. Fazemos este definição caso não tem uma bem-ordem do x porque seria indesejável usar a classe de equivalência do x sob $\sim$, uma classe própria e portanto difícil usar nossas argumentações, em se mesma.

Com o axioma de escolha o princípio (BO) fala que qualquer conjunto pode ser bem-ordenado, então para qualquer conjunto existe um existe um ordinal com qual tem uma bijeção (cf. §2.6). Logo, com o axioma de escolha a cardinalidade de qualquer conjunto é um ordinal.

Exercício. Mostrar que $\overline{\overline{x}} \notin \text{On}$ se não existe uma bem-ordem do x.

Definição. (Para qualquer noção de cardinalidade.) Um conjunto $\mathbf{m}$ é um cardinal se existe $x \in V$ tal que $\text{card}(x) = \mathbf{m}$.

$$\mathbf{m} \leq \mathbf{n} \quad \text{se existe } x \text{ e } y \text{ tal que } \text{card}(x) = \mathbf{m} \text{ e } \text{card}(y) = \mathbf{n} \text{ e } x \preceq y.$$
$$\mathbf{m} + \mathbf{n} = \text{card}(x \times \{0\} \cup y \times \{1\}), \text{ onde } \text{card}(x) = \mathbf{m} \text{ e } \text{card}(y) = \mathbf{n}.$$
$$\mathbf{m} \,.\, \mathbf{n} \ = \text{card}(x \times y), \text{ onde } \text{card}(x) = \mathbf{m} \text{ e } \text{card}(y) = \mathbf{n}.$$
$$\mathbf{m}^\mathbf{n} \ = \text{card}({}^y x), \text{ onde } \text{card}(x) = \mathbf{m} \text{ e } \text{card}(y) = \mathbf{n}.$$

Proposição. $+$ é comutativo e associativo; . é comutativo, associativo e distributivo sobre $+$; e $\mathbf{m}^{\mathbf{n}+\mathbf{k}} = \mathbf{m}^\mathbf{n} \,.\, \mathbf{m}^\mathbf{k}$ e $(\mathbf{m}^\mathbf{n})^\mathbf{k} = \mathbf{m}^{\mathbf{n} \cdot \mathbf{k}}$.

Demonstração. Todos são imediatos das definições.

Algumas outras conseqüências são mostrável sem o axioma de escolha, mas tipicamente usam $\preceq$ e/ou $\preceq^*$.

Exemplo. Se $\mathbf{k} + \mathbf{r} = \mathbf{m} \,.\, \mathbf{n}$, então ou $\mathbf{m} \preceq \mathbf{k}$ ou $\mathbf{n} \preceq^* \mathbf{r}$.

4.2. Lema de Hartog.

Como vimos, com o axioma de escolha vamos medir cardinalidade pelos ordinais, então vale a pena establecer algumas relações entre ordinais e cardinais.

Lema de Hartog. Seja x um conjunto. Então $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ é um conjunto, e, logo, pertence a On. ($\{\alpha \in \mathrm{On} \mid \alpha \sim x\}$ é um conjunto também.) Além disso, $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\} \npreceq x$ e o ordinal mínimo com este propriedade.

Demonstração. Seja $W = \{(y, <) \mid y \subseteq x \ \& \ < \text{ é uma bem-ordem do } y\}$. Então W é um conjunto (porque é um subconjunto do $\mathcal{P}(x) \times \mathcal{P}(x \times x)$). Como vimos na §2.6, pela teorema de recursão forte e o princípio de reposição, existe uma Função, F, levando bem-ordems para os ordinais. Então $F``W = \{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ é um conjunto pelo princípio de reposição.

É claro que $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ é um segmento inicial do On, porque se $\beta < \alpha \preceq x$ enão a composição do função de identidade com a injeção do α para x é uma injeção do β para x. Logo $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ pertence a On. Seja $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\} = \beta$. Fosse $\beta \preceq x$ teríamos que $\beta \in \beta$, uma contradição! E é claro que se $\gamma < \beta$ temos $\gamma \preceq x$.

De agora vamos sempre usar nossa noção, $\overline{\overline{x}}$, de cardinalidade.

Proposição. (i) Seja $\kappa \in \mathrm{On}$ um cardinal. $\overline{\overline{\kappa}} = \kappa$. (ii) Seja $\kappa \in \mathrm{On}$ um cardinal. $\forall \alpha < \kappa \ \kappa \not\preceq \alpha$. (iii) Sejam $\alpha, \beta \in \mathrm{On}$. Então $\overline{\overline{\alpha}} \leq \beta \leq \alpha$ implica que $\overline{\overline{\beta}} = \overline{\overline{\alpha}}$.

Demonstração. (i) Lembrar que falar que κ é um cardinal quer dizer que existe alguma x com uma bem-ordem e κ é mínimo tal que $x \sim \kappa$. Escolha um tal x. $\kappa \sim \kappa$ e se $\alpha < \kappa$ e $\alpha \sim \kappa$ então $\alpha \sim x$, uma contradição para a minimalidade do κ, do dois porque $\sim$ é uma relação de equivalência. Logo porque κ se mesmo é bem-ordenado (pelo $\in$) temos $\overline{\overline{\kappa}} = \kappa$.
(ii) Se $\alpha < \kappa$ e $i : \kappa \longrightarrow \alpha$ uma injeção, então $\mathrm{im}(i) \subseteq \alpha$ é isormorfico pelo um isomorfismo que preserva ordem para um ordinal único, vamos falar $\beta, \leq \alpha$. Então $\beta < \kappa$ e $\beta \sim \kappa$.
(iii) $\beta \leq \alpha$ implica $\beta \subseteq \alpha$, logo $\beta \preceq \alpha$. Mas $\alpha \sim \overline{\overline{\alpha}} \preceq \beta$, então $\alpha \sim \beta$ pela teorema de Schröder-Bernstein.

Nota. Se $\kappa \in \omega \cup \{\omega\}$ temos que $\forall \alpha < \kappa \ \kappa \not\sim \alpha$, e logo κ é um cardinal.

Definição. Seja $\kappa \in \mathrm{On}$ um cardinal. Defina $\kappa^+ = \{\alpha \in \mathrm{On} \mid \alpha \preceq \kappa\}$.

Corolário do Lema de Hartog. Então $\kappa^+ \in \mathrm{On}$, κ^+ é um cardinal, $\kappa < \kappa^+$, e $\kappa^+ \npreceq \kappa$. É não existe $\beta \in \mathrm{On}$ tal que $\beta < \kappa^+$ e β tem estes propriedades.

Demonstração. É claro que $\kappa \in \kappa^+$. Aplice o lema de Hartog para $x = \kappa$ para ver que κ^+ é um ordinal e $\kappa^+ \npreceq \kappa$. Se $\beta < \kappa^+$ temos que $\beta \preceq \kappa$, e logo $\kappa^+ \not\sim \beta$. Então $\overline{\overline{\beta}} \leq \kappa$ e κ^+ é um cardinal. Conseqüentemente, não existe um ordinal com cardinalidade máximo porque $\overline{\overline{\alpha}} \leq \alpha < \overline{\overline{\alpha}}^+$ para qualquer $\alpha \in \mathrm{On}$.

Definição. Seja $\kappa \in \mathrm{On}$ um cardinal. Então κ^+ é o sucessor cardinal do κ. Falamos que κ é um cardinal do *tipo sucessor* se existe um cardinal μ tal que $\kappa = \mu^+$, e que κ é do *tipo limite* senão.

Agora vamos enumerar os ordinais que são cardinais. Os primeiros ω são 0, 1, 2, ..., os números naturais. Depois usamos os ordinais em se mesmo para enumerar os ordinais infinitos que são cardinais.

Definição. Pela recursão definamos $\aleph : \mathrm{On} \longrightarrow V$ (On) pelo $\aleph_\alpha = \omega \cup \{\gamma \in \mathrm{On} \mid \exists \beta < \alpha \gamma \preceq \aleph_\beta\}$. Também escrevemos ω_α em vez do $\aleph_\alpha$ para qualquer $\alpha \in \mathrm{On}$. ($\aleph$ é "alef," a primeira letra do alfabeto hebraico.)

Proposição. (i) $\aleph_0 = \omega$. (ii) $\aleph_\alpha \in \mathrm{On}$ é um cardinal para cada $\alpha \in \mathrm{On}$ (iii) Se $\kappa \in \mathrm{On}$ é um cardinal infinito então existe cada $\alpha \in \mathrm{On}$ tal que $\kappa = \aleph_\alpha$. (iv) $\forall \alpha, \beta \in \mathrm{On}$, $\alpha < \beta$ implica $\aleph_\alpha < \aleph_\beta$. (v) $\aleph_\alpha$ é um cardinal do tipo sucessor se α é um ordinal do tipo sucessor, e é um cardinal do tipo limite se α é um ordinal do tipo limite.

Demonstração. (i), (ii) quando α é um ordinal do tipo sucessor, (iv), e (v) são imediatos das definições, usando o lema de Hartog.

(ii) Se λ é um ordinal do tipo limite temos que $\aleph_\lambda = \bigcup\{\aleph_\alpha^+ \mid \alpha < \lambda\}$ é um conjunto pelos axiomas de reposição e uniões, e enão e um ordinal. E é um cardinal porque se $\gamma < \aleph_\lambda$ então existe $\alpha < \lambda$ tal que $\gamma \in \aleph_\alpha^+ = \aleph_{s(\alpha)}$, e então $\overline{\overline{\gamma}} < \aleph_\alpha^+ < \aleph_\lambda$, e logo $\gamma \not\sim \aleph_\lambda$.

(iii) Seja $\kappa \in \mathrm{On}$ um cardinal infinito. Então $\kappa = \{\gamma \in \mathrm{On} \mid \gamma < \kappa\} = \{\gamma \in \mathrm{On} \mid \gamma \preceq \kappa \ \& \ \kappa \not\preceq \gamma\} = \omega \cup \{\gamma \in \mathrm{On} \mid \exists \mu < \kappa \, \mu \text{ é um cardinal } \ \& \ \gamma \sim \mu\}$. Logo, se temos que para todos cardinais $\mu < \kappa$ são alefs, então κ é um alef. Então qualquer cardinal $\kappa \in \mathrm{On}$ é um alef pelo princípio de indução sobre os ordinais.

Nota. Sem o axioma de escolha pode ser que, por exemplo, $2^{\aleph_0}$ não é um ordinal.

4.3. Cardinais com o axioma de escolha.

Agora vamos assumir o axioma de escolha. Então cada conjunto pode ser bem-ordenado. Logo todos os cardinais são ordinais e a classe dos cardinais é bem-ordenado (como uma subclasse de On).

Proposição. Para todos conjuntos x, y, $x \preceq y$ se e só se $\overline{\overline{x}} \leq \overline{\overline{y}}$.

Demonstração. $x \preceq y$ se e só se $\overline{\overline{x}} \preceq \overline{\overline{y}}$. Fosse $\overline{\overline{y}} < \overline{\overline{x}}$ teríamos que $\overline{\overline{x}} \not\prec \overline{\overline{y}}$. Então $\overline{\overline{x}} \leq \overline{\overline{y}}$ pela tricotomia.

Corolário. (AE) implica que para quaisquer x, y ou existe uma injeção $i : x \longrightarrow y$, ou existe uma injeção $j : y \longrightarrow x$.

Demonstração. Comparar $\overline{\overline{x}}$ e $\overline{\overline{y}}$ no On.

Teorema de produtos. (AC) Seja κ um cardinal. (Equivalentemente, seja κ um alef.) Então $\kappa.\kappa = \kappa$.

Demonstração. Primeiro nota que a teorema é verdadeira para ω: definando $(k,l) \prec (m,n)$ se ou $k+l < m+n$ ou $k+l < m+n$ e $k < m$, ou $(k,l) \prec' (m,n)$ se ou $\max\{k,l\} < \max\{m,n\}$, ou $\max\{k,l\} = \max\{m,n\}$ e $l < n$, ou $\max\{k,l\} = \max\{m,n\}$, $l = n$ e $k < m$ é claro que $\prec$ e $\prec'$ são bem-ordems de $\omega \times \omega$ e exitems bijeções entre elas e $(\omega, \in)$.

Agora usamos indução. Suponhamos que a teorema é verdadeira para todos cardinais infinito menos que κ. Defina uma ordem do $\kappa \times \kappa$ pelo $(\alpha,\beta) \prec (\gamma,\delta)$ se $\alpha \cup \beta < \gamma \cup \delta$, ou $\alpha \cup \beta = \gamma \cup \delta$ e $\beta < \delta$, ou $\alpha \cup \beta = \gamma \cup \delta$, $\beta = \delta$ e $\alpha < \gamma$. Nota que $\{\,(\alpha,\beta) \mid (\alpha,\beta) \preceq (\gamma,\gamma)\,\} = (\gamma+1) \times (\gamma+1)$ para qualquer $\gamma < \kappa$

Eu afirmo que esta ordem é uma bem-ordenando. É claro que $\prec$ é uma ordem parcial. E se $(\alpha,\beta) \not\prec (\gamma,\delta)$ e $(\gamma,\delta) \not\prec (\alpha,\beta)$ então $\alpha \cup \beta = \gamma \cup \delta$, $\beta = \delta$ e $\alpha = \gamma$, logo $(\alpha,\beta) = (\gamma,\delta)$, e temos que $\prec$ é uma ordem total. Para ver que $\prec$ é bem-fundada, seja $Z \subseteq \kappa \times \kappa$ com $\emptyset \neq \emptyset$. Seja ρ mínimo tal que existe $(\alpha,\beta) \in Z$ tal que $\alpha \cup \beta = \rho$. Primeiro seja $Z_1 = \{\,(\alpha,\beta) \in Z \mid \alpha \cup \beta = \rho\,\}$. Seja β_0 mínimo tal que existe α com $(\alpha,\beta_0) \in Z_1$. Agora seja $Z_2 = \{\,(\alpha,\beta \in Z_1 \mid \beta = \beta_0\,\}$. Seja α_0 mínimo tal que $(\alpha_0,\beta_0) \in Z_2$. Logo (α_0,β_0) é $\prec$-mínimo no Z.

Então existe um único $\rho \in \mathrm{On}$ tal que $(\kappa \times \kappa, \prec)$ é isomorfico para $(\rho, \in)$ pelo uma bijeção que preserva ordem. Seja $f : (\rho, \in) \longrightarrow (\kappa \times \kappa, \prec)$ o isomorfismo. Suponhamos que $\kappa < \rho$ e que $f(\kappa) = (\alpha,\beta)$. Seja $\gamma = \alpha \cup \beta$. Então $(\alpha,\beta) \preceq (\gamma,\gamma)$ e temos uma injeção $f|\kappa : \kappa \longrightarrow (\gamma+1) \times (\gamma+1)$. Porque κ é infinito temos que $\gamma \times \gamma$ é infinito, logo γ é infinito. Mas $\gamma < \kappa$, então $\gamma + 1 < \kappa$ e $\overline{\overline{\gamma+1}} < \kappa$. Então, pela hipótese da indução, $\overline{\overline{s(\gamma)}}.\overline{\overline{s(\gamma)}} = \overline{\overline{s(\gamma)}}$. Então $\kappa \prec s(\gamma) \times s(\gamma) \sim s(\gamma) \prec \kappa$. Uma contradição. Logo $\rho = \kappa$.

Então, pelo indução nos ordinais temos mostrado que $\kappa.\kappa = \kappa$ para todos cardinais κ.

Corolário. Seja κ um cardinal infinito e sejam x_α conjuntos tal que $\overline{\overline{x_\alpha}} \leq \kappa$ para todos $\alpha < \kappa$. Então $\overline{\overline{\bigcup\{x_\alpha \mid \alpha < \kappa\}}} \leq \kappa$.

Demonstração. Vamos aplicar o axioma de escolha para $Y = \{y_\alpha \mid \alpha < \kappa\}$, onde para cada $\alpha < \kappa$ pegamos $y_\alpha = \{\,f \mid f : x_\alpha \longrightarrow \kappa \text{ é uma injeção}\,\}$. Logo existe uma função $g : Y \longrightarrow \bigcup Y$ tal que $g_\alpha : x_\alpha \longrightarrow \kappa$ é uma injeção para todos $\alpha < \kappa$. Defina $h : \bigcup\{x_\alpha \mid \alpha < \kappa\} \longrightarrow \kappa \times \kappa$ pelo $h(z) = (\alpha, g_\alpha(z))$ onde α é mínimo tal que $z \in x_\alpha$. Logo $\overline{\overline{\bigcup\{x_\alpha \mid \alpha < \kappa\}}} \leq \kappa$ pelo teorema.

Corolário. (i) Sejam κ, μ cardinais e ao menos um infinito. Então $\kappa + \mu = \max\{\kappa, \mu\}$.
(ii) Sejam κ, μ cardinais e ao menos um infinito (*i.e.*, um aleph) e nenhum dos dois 0. Então $\kappa.\mu = \max\{\kappa, \mu\}$.
(iii) Sejam κ, μ cardinais $2 \leq \kappa \leq 2^\mu$ e μ um aleph. Então $\kappa^\mu = 2^\mu$.

Demonstração. (i) Se $\kappa \leq \mu$, então $\mu \leq \kappa + \mu \leq \mu + \mu = 2.\mu \leq \mu.\mu = \mu$.
(ii) Se $0 < \kappa < \mu$, então $\mu \leq \kappa.\mu \leq \mu.\mu = \mu$.
(iii) $2^\mu \leq \kappa^\mu \leq (2^\mu)^\mu = 2^{\mu.\mu} = 2^\mu$.

Corolário. $\aleph_\alpha + \aleph_\beta = \aleph_{\alpha \cup \beta} = \aleph_\alpha.\aleph_\beta$

Demonstração. $\aleph_{\alpha\cup\beta} = \aleph_{\max(\{\,\alpha\cup\beta\,\})} = \max(\{\,\aleph_\alpha, \aleph_\beta\,\})$.

Então temos fixado + e . nos cardinais. Mas exponciação fica um mistério, e na verdade é aqui onde o assunto começe viver. Cantor soube, como nós, que $\aleph_1 \leq 2^{\aleph_0}$ e, mais geralmente que $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$ para cada $\alpha \in \mathrm{On}$, mas não pode mostrar qualquer cardinal entre eles (pares). Então ele conjeturou que o *hipótese do continuo (HC)*, que $\aleph_1 = 2^{\aleph_0}$ foi verdadeiro, e mesmo que o *hipótese do continuo geral (HCG)* , que $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ foi verdadeiro. Isso é talvez a regra o mais simples posível. Mas como veremos na §6 *não tem razão supor que é verdadeiro*, porque não é possível mostrar HC dos axiomas do ZF + AE (Cohen, 1963), nem mostrar que é falso (Gödel, 1938).

4.4. Cofinalidade.

Agora vamos ver um sentido em qual o HCG é muito simples: ele determina todos os outras regras da exponenciação. Para fazer isso precisamos de um conceito que é muito útil apesar disso também

Definição. Sejam α, $\beta \in \mathrm{On}$ e $f : \alpha \longrightarrow \beta$ uma função. f é *cofinal* (ou *leva α cofinalmente para/no β*) se $\forall \gamma < \beta\ \exists \delta < \alpha\ (\gamma \leq f(\delta))$.

Definição. Seja $\beta \in \mathrm{On}$. A *cofinalidade* de β, $\mathrm{cf}\,(\beta)$, (é o mínimo α tal que do qual existe uma função cofinal para β.

Logo, $\mathrm{cf}\,(\beta) \leq \beta$ e é um cardinal para qualquer β. E se β é um ordinal do tipo sucessor, então $\mathrm{cf}\,(\beta) = 1$ (usando a fun=ção $f(0) = \bigcup \beta$).

Proposição. Existe uma função cofinal $f : \mathrm{cf}\,(\beta) \longrightarrow \beta$ que é cresente estritamente ($\sigma < \tau < \mathrm{cf}\,(\beta) \longrightarrow f(\sigma) < f(\tau)$), para qualquer $\beta \in \mathrm{On}$.

Demonstração. Seja $g : \mathrm{cf}\,(\beta) \longrightarrow \beta$ qualquer função cofinal, e defina f pelo recursão pelo $f(\tau) = \max(\{\, g(\tau), \sup\{\, f(\sigma) \mid \sigma < \tau \,\}\})$ para $\tau < \mathrm{cf}\,(\beta)$.

Proposição. Se $\alpha \in \mathrm{On}$ é do tipo limite e $f : \alpha \longrightarrow \beta$ é cofinal e cresente estritamente, então $\mathrm{cf}\,(\alpha) = \mathrm{cf}\,(\beta)$.

Demonstração. Seja $g : \mathrm{cf}\,(\alpha) \longrightarrow \alpha$ qualquer função cofinal. Então $f \cdot g : \mathrm{cf}\,(\alpha) \longrightarrow \beta$ é cofinal. Logo $\mathrm{cf}\,(\beta) \leq \mathrm{cf}\,(\alpha)$. E se $h : \mathrm{cf}\,(\beta) \longrightarrow \beta$ é cofinal, então $k : \mathrm{cf}\,(\beta) \longrightarrow \alpha$ é cofinal, onde $k(\tau) =$ o mínimo σ tal que $h(\tau) < f(\sigma)$.

Corolário. $\mathrm{cf}\,(\mathrm{cf}\,(\beta)) = \mathrm{cf}\,(\beta)$ para qualquer $\beta \in \mathrm{On}$.

Demonstração. Imediato pelas duas proposições prévias.

Corolário. Seja α um ordinal do tipo limite. Logo $\mathrm{cf}\,(\aleph_\alpha) = \mathrm{cf}\,(\alpha)$.

Demonstração. Imediato pela última proposição usando a função $\aleph$.

Definição. Seja $\beta \in \mathrm{On}$ é um cardinal infinito. Se $\mathrm{cf}\,(\beta) = \beta$ falamos que β é *regular*. Se $\mathrm{cf}\,(\beta) < \beta$ falamos que β é *singular*.

Exemplos. ω é regular. $\aleph_\omega$ é singular (veja o corolário segundo para ver que $\mathrm{cf}\,(\aleph_\omega) = \omega$).

Até agora não tivemos usado o axioma de escolha nesta seção.

Proposição. (AE) implica κ^+ é regular para qualquer cardinal κ.

Demonstração. Fosse $f : \alpha \longrightarrow \kappa^+$ cofinal onde $\alpha < \kappa^+$, então $\kappa^+ = \bigcup\{\, f(\gamma) \mid \gamma < \alpha\}$. Mas $f(\gamma)$, $\alpha < \kappa$, então $\overline{\overline{f(\gamma)}}$, $\overline{\overline{\alpha}} < \kappa^+$ e teríamos que κ^+ seria a união de κ conjuntos cada um com cardinalidade $\leq \kappa$. Uma contradição pelo primeiro Corolário do teorema dos productos na §4.3.

(**Nota.** Sem (AE) é possível que $\mathrm{cf}\,(\omega_1) = \omega$.)

Um pergunta natural agora é se existem cardinais do tipos limites e regulares também. Se $\aleph_\alpha$ é um tal cardinal, então $\aleph_\alpha = \alpha$. Mas isso não é bastante. Por exemplo, se $\alpha = \bigcup\{\,\aleph_0, \aleph_\omega, \aleph_{\omega_\omega}, \ldots\}$ temos que $\aleph_\alpha = \alpha$ mas $\mathrm{cf}\,(\alpha) = \omega$. Então o primeiro cardinal do tipo limite que é regular é mais grande.

Definição. κ é *inacessível fracamente* se é do tipo limite e regular.

Definição. (AC) κ é *inacessível fortemente* se é regular $\forall \mu < \kappa\; 2^\mu < \kappa$.

Proposição. Se κ é inacessível fortemente, é inacessível fracamente. E (HCG) implica que se κ é inacessível fracamente, é inacessível fortemente.

Agora vamos usar a noção de cofinalidade ajudar mostrar como (HCG) simplifica a exponenciação dos cardinais.

Propsição. Seja κ um cardinal infinito e $\mathrm{cf}\,(\kappa) \leq \mu$. Então $\kappa^\mu \not\preceq^* \kappa$.

Demonstração. A demonstração é uma variante do demonstração do Cantor que $\mathcal{P}(x) \not\preceq^x$ que vimos na §1.1. Seja $f : \mu \longrightarrow \kappa$ qualquer função cofinal e $g : \kappa \longrightarrow {}^\mu\kappa$ qualquer função. Vamos mostrar que g não pode ser uma sobrejeção. Defina $h : \mu \longrightarrow \kappa$ pelo $h(\alpha) =$ o membro mínimio de $\kappa \setminus \{\, (g(\beta))(\alpha) \mid \beta < f(\alpha)\,\}$. Se $\gamma < kappa$ pode escolhar $\alpha < \mu$ tal que $\gamma < f(\alpha)$ porque f é cofinal. Assim tem $h(\alpha) \neq g(\gamma)(\alpha)$. Então $h \notin \mathrm{im}(g)$.

Corolário. (AE) Seja κ um cardinal infinito e $\mathrm{cf}\,(\kappa) \leq \mu$. Então $\kappa < \kappa^\mu$.

Demonstrção. É claro que $\kappa \preceq \kappa^\mu$, então pelo proposição e tricotomia $\kappa < \kappa^\mu$.

Corolário. (AE) Seja κ um cardinal infinito, então $\kappa < \mathrm{cf}\,(2^\kappa)$.

Demonstrção. Se $\mathrm{cf}\,(2^\kappa) \leq \kappa$ temos que $2^\kappa < (2^\kappa)^\kappa = 2^{\kappa.\kappa} = 2^\kappa$, uma contradição.

Proposição. (AE + HCG) Sejam κ, μ cardinais, $2 \leq \kappa$, μ é ao menos um do κ, μ infinito. Então, (i) $\kappa \leq \mu \longrightarrow \kappa^\mu = \mu^+$, (ii) $\mathrm{cf}\,(\kappa) \leq \mu < \kappa \longrightarrow \kappa^\mu = \kappa^+$, e (iii) $\mu < \mathrm{cf}\,(\kappa) \longrightarrow \kappa^\mu = \kappa$,

Demonstrção. (i) Já vimos (sem (HCG)) que $\kappa^\mu = 2^\mu$. (HCG) fala que $2^\mu = \mu^+$.
(ii) O primeiro corolário em cima fala que $\kappa < \kappa^\mu$. Mas $\kappa^\mu \leq \kappa^\kappa = 2^\kappa$, $= \kappa^+$ pelo (HCG).
(iii) $\mu < \mathrm{cf}\,(\kappa)$ fala que qualquer função $f : \mu \longrightarrow \kappa$ não é cofinal, então ${}^\mu\kappa = \bigcup\{\,{}^\mu\alpha \mid \alpha < \kappa\}$, e $\overline{\overline{{}^\mu\alpha}} \leq \max(\{\overline{\overline{\alpha}}, \mu\,\})^+ \leq \kappa$.

Sem o (HCG) exponenciação pode ser muito mais complicada. Tem muitos coisas que são independente do ZF + AE – não podem ser mostrados nem podem ser mostrados os contrários. (Veja §6 para ganhar um pouco mais explicação disso.) Embora existe algumas resultados que podem ser mostrados do ZF + AE, e várias perguntas abertas importantes. Por exemplo temos os seguintes.

Teorema. (Silver, 1975) Se $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ para todos $\alpha < \omega_1$, então $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$

E tem o mesmo resultado para outros cardinais κ com $\omega < \mathrm{cf}\,(\kappa) < \kappa$. No contraste, a situação é muito diferente para cardinais κ singular com $\omega = \mathrm{cf}\,(\kappa)$.

Teorema. (Gitik-Magidor, 1989) Para qualquer $\delta < \omega_1$ e possível que $2^{\aleph_n} = \aleph_{n+1}$ para todos $n < \omega$, mas $2^{\aleph_\omega} = \aleph_{\delta+1}$.

Ainda tem algumas limitações quando $\mathrm{cf}\,(\kappa) = \omega$.

Teorema. (Shelah, 1989) Se $2^{\alpha_n} < \aleph_\omega$ para cada $n < \omega$, então $2^{\aleph_\omega} < \min(\{\, \aleph_{\omega_4}, \aleph_{(2^\omega)^+} \,\})$.

Uma das perguntas mais destacadas neste parte do teoria dos conjuntos é se o "4" na teorema de Shelah em cima pode ser melhorizado, (Talvez para "1," mas em qualquer modo seria muito importante.)

Capítulo 5. Combinatória infinita*

.

5.1. Conjunto fechados e ilimitado e conjuntos parados.

Definição. Seja λ um ordinal do tipo limite. Um conjunto $D \subseteq \lambda$ é *ilimitado no* λ se $\forall \alpha < \lambda$ $\exists \beta \in D\, \alpha < \beta$. Um conjunto $C \subseteq \lambda$ é *fechado no* λ se para todos ordinais $\delta < \lambda$ do tipo limite, $C \cap \delta$ é ilimitado no δ implica que $\sup(C \cap \delta) \in C$. Um conjunto que é fechado e ilimitado no λ é muitos vezes chamado "*club*" em inglês ("club" quer dizer "*cl*osed and *un*bounded.")

Exemplos. $\{\gamma < \lambda \mid \gamma$ é um ordinal do tipo limite$\}$ e $\{\gamma < \lambda \mid \gamma$ é um limite dos ordinais do tipo limite$\}$ são fechado no λ. E são ilimitados se λ é um cardinal.

Você deveria pensar de um conjunto fechado e ilimitado como sendo "grande" em alguma sentido.

Proposição. Seja κ um cardinal regular e $\mathcal{F}$ um conjunto de funções finitárias sobre κ com $\overline{\overline{\mathcal{F}}} < \kappa$ (*i.e.*, se $f \in \mathcal{F}$ temos que $f : {}^{n(f)}\kappa \longrightarrow \kappa$ para alguma $n(f) < \omega$.) Então, $C = \{\gamma < \kappa \mid \forall f \in \mathcal{F}$ $f``{}^{n(f)}\gamma \subseteq \gamma\}$ é fechado e ilimitado.

Demonstração. É claro que C é fechado: se $\lambda < \kappa$ é um ordinal do tipo limite e $C \cap \lambda$ é ilimitado, $f \in \mathcal{F}$, $f : {}^{n(f)}\kappa \longrightarrow \kappa$ e $(\alpha_0, \ldots, \alpha_{n-1}) \in {}^{n(f)}\lambda$ então existe um $\gamma \in (C \cap \lambda) \setminus \max(\{\alpha_0, \ldots, \alpha_{n-1}\})$, e temos que $f(\alpha_0, \ldots, \alpha_{n-1}) < \gamma < \lambda$.

Para ver que C é ilimitado, defina $G_0(X) = X$, $G_{n+1}(X) = G_n(X) \cup \bigcup\{\beta \mid \exists \alpha_0, \ldots, \alpha_{n-1} \in G_n(X)$ $\exists f \in \mathcal{F}\, f(\alpha_0, \ldots, \alpha_{n-1}) = \beta\}$, para cada, $n < \omega$ e $G(X) = \bigcup_{n \in \omega} G_n(X)$ para cada subconjunto X do κ. Se $\xi < \kappa$ é claro que $\xi \subseteq G(\xi) \subseteq \kappa$ e $\overline{\overline{G(\xi)}} < \kappa$. Porque κ é regular podemos escolhar $g(\xi) = \min(\kappa \setminus \sup(G(\xi)))$. Seja $g_{n+1}(\xi) = g(g_n(\xi))$ para qualquer $\xi < \kappa$, e seja $g_\omega(\xi) = \sup\{g_n(\xi) \mid n \in \omega\}$. Então temos que $g_\omega(\xi) \in C$ e $\xi < g_\omega(\xi)$.

Definição. Se C é um conjunto fechado e ilimitado e $g : \kappa \longrightarrow C$ enumera C na ordem crescente, seja $C' = g``\{\omega\gamma \mid \gamma < \kappa\}$. C', $\subseteq C$, é o *conjunto do puntos do tipo limite de* C.

Lema. Seja C é um conjunto fechado e ilimitado e define $f : \kappa \longrightarrow \kappa$ pelo $f(\gamma) = \min(C \setminus (\gamma+1))$. Então $C' = \{\gamma < \kappa \mid f``\gamma \subseteq \gamma\}$, e logo C' é fechado e ilimitado.

Demonstração. É claro que $C' = \{\gamma < \kappa \mid f``\gamma \subseteq \gamma\}$, e, então, pela proposição prévia, é fechado e ilimitado.

Proposição. Seja κ um cardinal com $\omega < \mathrm{cf}(\kappa)$, seja $\mu < \mathrm{cf}(\kappa)$, e seja C_α fechado e ilimitado no κ para cada $\alpha < \mu$. Então $D = \bigcap\{C_\alpha \mid \alpha < \mu\}$ é fechado e ilimitado no κ.

Demonstração. É facil ver que D é fechado. Agora seja $f_\alpha(\gamma) = \min(C_\alpha \setminus \gamma + 1)$ para $\gamma < \kappa$

* versão 1.2, 19/12/00

e para todos $\alpha < \mu$. D é ilimitado porque, pela proposição prévia, $\{\gamma < \kappa \mid \forall\alpha < \mu\, f_\alpha``\gamma \subseteq \gamma\}$ é ilimitado (e fechado), e é um subconjunto do D pela lema.

Definição. Seja κ um cardinal com $\omega < \mathrm{cf}\,(\kappa)$. Un conjunto $S \subseteq \kappa$ é *parado* se $S \cap C \neq \emptyset$ para todos C que são fechado e ilimitado no κ. Un conjunto $X \subseteq \kappa$ é *não-parado* se não é parado.

Exemplos. A proposição fala que qualquer união do menos que $\mathrm{cf}\,(\kappa)$ conjuntos não-parados é não parado. Seja $\mu < \mathrm{cf}\,(\kappa)$ um cardinal do tipo regular. Então $\{\alpha < \kappa \mid \mathrm{cf}\,(\alpha) = \mu\}$ é parado, porque se C é fechado e ilimitado no κ o elemento μ^o na enumeração crescente do C tem cofinalidade μ.

Conjuntos parados são do tamanho "medio" como subconjuntos do κ e conjuntos não-parados são "pequenos" – não obstante podem ter cardinalidade κ.

Proposição. Seja $\kappa = \mu^+$ e S parado no κ. Então existe S_α para $\alpha < \kappa$ com $S = \bigcup\{S_\alpha \mid \alpha < \kappa\}$ e $S_\alpha \cap S_\beta = \emptyset$ para cada par α, $\beta < \kappa$ com $\alpha \neq \beta$.

Demonstração. Seja $f_\gamma : \gamma \longrightarrow \mu$ uma injeção para cada $\gamma < \kappa$. Defina $S_\alpha^\xi = \{\gamma \mid \alpha < \gamma < \kappa \;\&\; f_\gamma(\alpha) = \xi\} \subseteq \kappa$. Então $S_\alpha^\xi \cap S_\beta^\xi = \emptyset$ se $\alpha \neq \beta$ para cada $\xi < \mu$ porque cada f_γ é uma injeção. Também temos que $\bigcup_{\xi<\mu} S_\alpha^\xi = \{\gamma \mid \alpha < \gamma < \kappa\}$ é parado no κ. Porque uma união do menos que κ subconjuntos do κ não-parados é não-parada, deve ser que para cada α existe um $\xi_\alpha < \mu$ tal que $S_\alpha^{\xi_\alpha}$ é parado. Porque $\mu < \kappa$ existe um $\xi < \kappa$ tal que $\overline{\overline{\{\alpha < \kappa \mid \xi = \xi_\alpha\}}} = \kappa$. Seja $A = \{\alpha < \kappa \mid \xi = \xi_\alpha\}$ é $\alpha_0 = \min(A)$. Defina $S_\alpha = S_\alpha^\xi$ para $\alpha \in A \setminus \{\alpha_0\}$, e defina $S_{\alpha_0} = S \setminus \bigcup\{S_\alpha^\xi \mid \alpha \in A \setminus \{\alpha_0\}\}$ (logo $S_{\alpha_0}^\xi \subseteq S_{\alpha_0}$). Temos que $S_\alpha \subseteq S$ é parado para cada $\alpha \in A$ e $S_\alpha \neq S_\beta$ onde α, $\beta \in A$ e $\alpha \neq \beta$.

Fato. Com um pouco mais trabalho podemos mostrar a proposição para todos cardinais regulares e não só para cardinais do tipo sucessor como cá.

Proposição. (Intersecções diagonais) Seja κ um cardinal do tipo regular e seja C_α fechado e ilimitado no κ para cada $\alpha < \kappa$. Então $D = \{\beta \mid \forall\alpha < \beta\,(\beta \in C_\alpha)\}$ $(= \{\beta \mid \beta \in \bigcap_{\alpha<\beta} C_\alpha)\})$ é fechado e ilimitado no κ.

Demonstração. É facil ver que D é fechado: se λ é um ordinal do tipo limite e $D \cap \lambda$ é ilimitado no λ temos que $\forall\alpha < \lambda\, \exists\beta\, (\alpha \leq \beta < \lambda \;\&\; \forall\gamma < \beta\, \beta \in C_\gamma)$. Logo $\forall\alpha < \lambda\, \exists\beta\, (\alpha \leq \beta < \lambda \;\&\; \beta \in C_\alpha)$. Logo $C_\alpha \cap \lambda$ é ilimitado no λ para todos $\alpha < \lambda$. Então $\lambda \in \bigcap\{C_\alpha \mid \alpha < \lambda\}$.

Para ver que D é ilimitado, defina $g(\gamma) = \min(\bigcap_{\alpha<\gamma} C_\alpha \setminus \gamma)$ para todos $\gamma < \kappa$. (Nota que esta intersecção é ilimitada pela proposição que uma intersecção de menos que κ conjuntos fechados e ilimitados é fechado e ilimitado, então $g(\gamma)$ é bem-definido.) Agora sejam $\beta < \kappa$, $\beta_0 = \beta$, $\beta_{n+1} = g(\beta_n)$ para $n < \omega$, e $\beta_\omega = \sup\{\beta_n \mid n < \omega\}$. Então $\beta_\omega \in D$.

Proposição. *(Lema de Fodor)* Seja κ regular, $\omega < \kappa$, seja S um subconjunto parado do κ e seja $f : S \longrightarrow \kappa$ tal que $f(\alpha) \in \alpha$ para cada $\alpha \in S$. Então existe $\gamma < \kappa$ tal que $\{\alpha \in S \mid f(\alpha) = \gamma\}$ é parado no κ.

Demonstração. Se a conclusão fale, escolhar para cada $\gamma \in \kappa$ um conjunto C_γ que é fechado e ilimitado no κ e tal que $C_\gamma \cap f^{-1}``\{\gamma\} = \emptyset$. Seja $D = \{\beta \mid \forall\gamma < \beta\,(\beta \in C_\gamma)\}$. A proposição prévia fala que D é fechado e ilimitado no κ. Mas $D \cap S = \emptyset$, porque se $\beta \in D$ temos que $f(\beta) \neq \alpha$ para cada $\alpha < \beta$. Uma contradição para a suposição que S é parado.

5.2 Teorema de Silver.

Agora vamos utilisar estes conceitos dos conjuntos fechados e ilimitados e dos conjuntos parados para mostrar o teorema de Silver sobre exponenciação nos cardinais sigulares com cofinalidade maior que ω que foi mencionado no fim da §4.4. É útil ter mais uma definição.

Definição. Seja $\mathcal{F} \subseteq {}^{\omega_1}\omega_{\omega_1}$ chamado *(uma família) diferente finalmente* se $\forall f, g \in \mathcal{F}\,(f \neq g \longrightarrow \overline{\overline{\{\alpha \mid f(\alpha) = g(\alpha)\}}} \leq \omega$.

Teorema. (Silver, 1975) Se $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ para todos $\alpha < \omega_1$, então $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$

Demonstração. Pelo hipotese da teorema, suphonamos que $\mathcal{P}(\omega_\alpha) = \{X^\alpha_\beta \mid \beta < \omega_{\alpha+1}\}$ para todos $\alpha < \omega_1$. Então para cada $X \subseteq \omega_{\omega_1}$ e $\alpha < \omega_1$ existe uma $\beta < \omega_{\alpha+1}$ tal que $X \cap \omega_\alpha = X^\alpha_\beta$. Logo podemos definir para cada $X \subseteq \omega_{\omega_1}$ uma função $f_X : \omega_1 \longrightarrow \omega_{\omega_1}$ pelo $f_X(\alpha) = \beta$ se $X \cap \omega_\alpha = X^\alpha_\beta$ tal que $f_X(\alpha) < \omega_{\alpha+1}$. Nota que $\mathcal{F} = \{f_X \mid X \in \mathcal{P}(\omega_{\omega_1})\}$ é diferente finalmente porque $X \neq Y$ implica que existe $\alpha < \omega_1$ tal que $f_X(\alpha) \neq f_Y(\alpha)$, e $f_X(\alpha) \neq f_Y(\alpha)$ implica $f_X(\gamma) \neq f_Y(\gamma)$ para cada $\gamma \geq \alpha$.

Agora dar uma ordem parcial para $\mathcal{F}$ pelo $f < g$ se e só se $\{\alpha < \omega_1 \mid g(\alpha) \leq f(\alpha)\}$ é um conjunto não-parado no ω_1. Pelo o lema de Zorn seja $\prec$ qualquer ordem total que estende $<$. (Veja Exercício 3.2.a.) Logo se $f \prec g$ temos que $\{\alpha < \omega_1 \mid f(\alpha) < g(\alpha)\}$ é um parado no ω_1. Seja $\mathcal{F}_g = \{f \in \mathcal{F} \mid f \prec g\}$. Vamos mostrar que $\overline{\overline{\mathcal{F}_g}} \leq \omega_{\omega_1}$ para cada $g \in \mathcal{F}$, que dará a teorema.

Para fazer isso vamos usar duas lemas.

Lema. Se $\mathcal{G}$ é diferente finalmente e $\forall g \in \mathcal{G}\,\{\alpha \mid g(\alpha) < \omega_\alpha\}$ é parado, então $\overline{\overline{\mathcal{G}}} \leq \omega_{\omega_1}$.

Demonstração. Suphonamos que $f \in \mathcal{G}$. Seja $g : \{\alpha < \omega_1 \mid \alpha = \bigcup\alpha\} \longrightarrow \omega_1$ definido pelo $g(\alpha) =$ o mínimo $\gamma < \alpha$ tal que $f(\alpha) < \kappa_\gamma$. Pela lema de Fodor existe um subconjunto parado S_f de $\{\alpha < \omega_1 \mid \alpha = \bigcup\alpha\}$ e um $\gamma_f < \omega_1$ tal que $g(\alpha) = \gamma_f$ para todos $\alpha \in S_f$. Logo, se $\omega_{\omega_1} < \overline{\overline{\mathcal{G}}}$ existe um subconjunto $\mathcal{G}' \subseteq \mathcal{G}$, um $\gamma < \omega_1$, um conjunto parado $S \subseteq \omega_1$ tal que $\omega_{\omega_1} < \overline{\overline{\mathcal{G}'}}$ e $\forall f \in \mathcal{G}'\,(\gamma_f, S_f) = (\gamma, S)$. Porque $\mathcal{G}$ é diferente finalmente deve ser que $\forall f, g \in \mathcal{G}'$ $(f \neq g \longrightarrow f|S \neq g|S)$. Mas temos $\overline{\overline{{}^S\omega_\gamma}} = \omega_\gamma^{\omega_1} \leq \max(\{\omega_\gamma^{\omega_\gamma}, \omega_1^{\omega_1}\}) = \max(\{2^{\omega_\gamma}, 2^{\omega_1}\}) = \max(\{\omega_\gamma^+, \omega_2\}) \leq \kappa$. Uma contradição! Então $\overline{\overline{\mathcal{G}}} \leq \kappa$, como desejamos.

O outro lema reduze crumente o que ficar da demonstração para a situação desta lema última.

Lema. Se $f : \omega_1 \longrightarrow \omega_{\omega_1}$ é tal que $f(\alpha) < \omega_{\alpha+1}$ para cada $\alpha \in \omega_1$, $\mathcal{G}$ é diferente finalmente e $\forall g \in \mathcal{G}\,\{\alpha \mid g(\alpha) < f(\alpha)\}$ é parado, então $\overline{\overline{\mathcal{G}}} \leq \omega_{\omega_1}$.

Demonstração. Para cada $\alpha < \omega$ seja $h_\alpha : f(\alpha) \longrightarrow \omega_\alpha$ uma injeção. Para cada $g \in \mathcal{G}$ defina $g' : \omega_1 \longrightarrow \omega_{\omega_1}$ pelo $g'(\alpha) = h_\alpha(g(\alpha))$ e seja $\mathcal{G}' = \{g' \mid g \in \mathcal{G}\}$. Então $\mathcal{G}'$ satisfaz o hipotese da lema prévia. Mas porque todos as funções h_α são injeções, $g' = k' \longrightarrow g = k$. Então $\overline{\overline{\mathcal{G}'}} = \overline{\overline{\mathcal{G}'}} \leq \omega_{\omega_1}$.

Então $\overline{\overline{\mathcal{F}_g}} \leq \omega_{\omega_1}$ para cada $g \in \mathcal{F}$, e, logo, $\overline{\overline{\mathcal{F}}} \leq \omega_{\omega_1+1}$. Então $\overline{\overline{\mathcal{F}}} = 2^{\omega_{\omega_1}} = \omega_{\omega_1+1}$.

Corolário para a demonstração. Seja κ um cardinal do tipo limite e singular com $\mathrm{cf}\,(\kappa) = \theta < \kappa$

e $c : \theta \longrightarrow \kappa$ cofinal. Se existe um subconjunto parado $T \subseteq \theta$ tal que $2^{c(\mu)} = c(\mu)^+$ para todos $\mu < \theta$, então $2^\kappa = \kappa^+$.

5.3. Teorema de Ramsey.

Vamos ver na seção proxima um outro uso das noções dos conjuntos fechados e ilimitados e conjuntos parados. Este aplicação será na teoria dos grafos.

Definição. Um *grafo* é um par (X, A) onde X é um conjunto (dos *vértices* ou *nós*) e onde $A \subseteq X \times X \setminus \{ (x, x) \mid x \in X \}$ (dos *arestes*). Um outro modo de falar a mesma coisa é falar que um grafo é um conjunto X com uma relação binária A tal que A é símetrico e anti-reflexivo.[1] Somos interesados nos grafos só até isomorfismo onde $(X, A) \cong (Y, B)$ se existe uma bijeção $f : X \longrightarrow Y$ tal que $(x, y) \in A \iff (f(x), f(y)) \in B$.

Tem muitos exemplos dos grafos, do dois finitos e infinitos. Entre eles são grafos *completos*: grafos da forma (X, B) onde para cada par $\{x, y\}$ dos membros do X com $x \neq y$ tem $(x, y) \in B$. Escrevemos K_κ para o grafo completo do tamanho κ. (Claro que é único até isomorfismo.) Por exemplo, temos que K_3 é um triangulo e K_4 é um quadro com os diagonais.

Definição. $H = (Y, B)$ é um subgrafo do $G = (X, A)$ se $Y \subseteq X$ e $B = A \cap (Y \times Y)$. Então H tem todos os arestes que G tem entre vértices no Y.

Definição. Uma *coloração* de um grafo $G = (X, A)$ *com* γ *cores* é uma função $f : A \longrightarrow \gamma$.

A teorema do Ramsey na forma o mais simples fala que para qualquer coloração finita f do grafo infinito enumerável K_ω existe um subgrafo $G = (X, A)$ do K_ω tal que $G \cong K_\omega$ é todos os arestes do G tem o mesmo cor: $\overline{\overline{\{ f(e) \mid e \in A \}}} = 1$. Falamos que G é *monocromático.* Tem, também um versão finito da teorema que pode, deduzir deste versão infinito: para qualquer $n < \omega$ e $r < \omega$ existe $m < \omega$ tal que para qualquer coloração f do K_m existe um subgrafo G do K_m tal que $G \cong K_n$. Na verdade vale a pena mostrar uma extensão pequena da teorema que tem mas ou menos a mesma demonstração.

Definição. Para qualquer conjunto x e qualquer cardinal κ seja $[x]^\kappa = \{ y \subseteq x \mid \overline{\overline{y}} = \kappa \}$.

Teorema de Ramsey. (1930) Sejam n, $r < \omega$. Se $f : [\omega]^n \longrightarrow r$, existe $X \in [\omega]^\omega$ (então um subconjunto infinito do ω) e existe um $p < r$ tal que $f``[X]^n = \{ p \}$. (*I.e.*, para qualquer coloração do conjunto dos subconjuntos do tamanho n do ω com r cores existe um subconjunto infinito X do ω tal que todos os subconjuntos do X do tamanho r ganham o mesmo cor.)

Primeiramente, observe a lema seguinte que vamos usar várias vezes na demonstração.

Lema. Sejam n, $r < \omega$ e $f : [\omega]^{n+1} \longrightarrow r$. Suponhamos que $Z \in [\omega]^\omega$, $x \in [Z]^n$, e para cada $p < r$ seja $x_p = \{ s \in Z \mid s \notin x \ \& \ f(x \cup \{ s \}) = p \}$. Então ao menos um dos conjuntos x_p é infinito.

[1] Para pegar mais informação sobre a teoria de grafos posso recomendar para você os livros de Bela Bollobas, *Graph Theory: An introductory course*, Springer, 1979 (na biblioteca) ou Bela Bollobas, *Combinatorics*, Cambridge University Press, 1986? (não na biblioteca).

Demonstração da lema. Se cada x_p fosse finito teríamos que $Z \setminus x = \bigcup\{\, x_p \mid p < r\,\}$ seria uma união finita dos conjuntos finitos, logo finito. Uma contradição!

bf Demonstração da teorema de Ramsey. A demonstração é pela indução sobre n. Então o caso primeiro é $n = 1$, e neste caso temos uma $f : [\omega]^1 \longrightarrow r$. Seja $y_p = \{\, m \in \omega \mid f(\{\, m\,\}) = p\,\}$ para cada $p < r$. Então pela lema (ao menos) um dos conjuntos y_p é infinito, como precisamos.

Agora suponhamos que temos mostrado a teorema para n e qualquer $r < \omega$. Sejam $r < \omega$ e $f : [\omega]^{n+1} \longrightarrow r$. Vamos definir uma coloração $g : [\omega]^n \longrightarrow r$ usando f. Então se $x \in [\omega]^n$ seja, usando a lema, $g(x) = p$ se p é mínimo tal que existe um conjunto infinito dos $s < \omega$ tal que $f(x \cup \{\, s\,\}) = p$.

Vamos definir uma seqüência dos conjuntos infinitos X_i para $i < \omega$ com $X_0 = \omega$ e $X_{i+1} \subseteq X_i$ e definir $a_i = \min(X_i)$. Para $i < n$ seja $X_{i+1} = X_i \setminus \{\, a_i\,\}$. Na contramão suphamos que temos $\langle a_i \mid i \leq j\rangle$ e $\langle X_i \mid i \leq j\rangle$ para alguma $n - 1 \leq j < \omega$. Seja $\langle y_k \mid k < l\rangle$ uma enumeração do $[\{\, a_i \mid i < j\,\}]^n$ para alguma $l < \omega$. Vamos definir um conjunto infinito Y_k para $k \leq l$ com $Y_0 = X_j \setminus (a_j + 1)$ e $Y_{k+1} \subseteq Y_k$ e definirimos $X_{j+1} = Y_k$. Seja, pela lema de novo, $q_k < r$ mínimo tal que existe um subconjunto infinito Y do Y_k tal que para todos $b \in Y$ temos que $f(y_k \cup \{\, b\,\}) = q_k$, e seja $Y_{k+1} = \{\, b \in Y_k \mid f(y_k \cup \{\, b\,\}) = q_k\,\}$.

Seja $X = \{\, a_i \mid i < \omega\,\}$. Pelo teorema para n temos que existe um conjunto $Z \in [X]^\omega$ e um cor $q < r$ tal que $g``[Z]^n = \{\, q\,\}$. Vamos mostrar que $\overline{\overline{f``[Z]^{n+1}}} = 1$ também. Sejam $x_0,\, x_1 \in [Z]^{n+1}$ com $b_0 = \max(x_0)$ e $b_1 = \max(x_1)$, e sejam $y_0 = x_0 \setminus \{\, b_0\,\}$ e $y_1 = x_1 \setminus \{\, b_1\,\}$. Então $f(x_0) = g(y_0)$ e $f(x_1) = g(y_1)$. Mas $g(y_0) = g(y_1)$, porque $y_0,\, y_1 \in [Z]^n$, logo $f(x_0) = f(x_1)$.

5.4. Teorema de Todorcevic.

Embora, para cardinais do tipo sucessor já nos 30s Sierpinski mostrou que a analogia da teorema de Ramsey foi falsa, ao menos sob HCG. Primeiro mostramos um lema que vai ser útil.

Definição. Seja κ um cardinal. A *ordem lexicografico sobre* $\mathcal{P}(\kappa)$ é dado pelo $x < y$ se quando z é mínimo tal que $z \in (x \setminus y) \cup (y \setminus x)$ temos $z \in y$.

Nota. É claro que $<$ é uma ordem linear. Falamos a ordem lexicografico porque é lexicografico sob o isomorfismo $\chi : \mathcal{P}(\kappa) \longrightarrow {}^\kappa 2$ onde $\chi_x(n) = 1$ se e só se $n \in x$ para $x \in \mathcal{P}(\kappa)$.

Lema. Seja κ um cardinal infinito e seja seja $<$ a ordem lexicografico sobre $\mathcal{P}(\kappa)$. Não existe um subconjunto do $\mathcal{P}(\kappa)$ bem-ordenado pelo $<$ com cardinalidade maior que κ.

Demonstação. Suphamos que $\kappa < \overline{\overline{Y}}$ e $Y \subseteq \mathcal{P}(\kappa)$ é bem-ordenado pelo $<$. Então existe um ordinal ρ tal que $(Y, <) \cong (\rho, \in)$ pelo um isomofismo que preserva ordem e $\kappa^+ \leq \rho$. Seja Y_0 o segmento inicial do Y tal que $(Y_0, <) \cong (\kappa^+, \in)$ pelo um isomofismo g que preserva ordem. Seja γ_α o mínimo $\gamma < \kappa$ tal que $\forall \beta < \alpha\, \gamma_\beta < \gamma$ e existe $x \in Y_\alpha\, \gamma \in x$, seja $Y_{\alpha+1} = \{\, x \in Y_\alpha \mid \gamma_\alpha \in x\,\}$, e seja $Y_\lambda = \bigcap\{\, Y_\alpha \mid \alpha < \lambda\,\}$ para $\lambda < \kappa$ do tipo limite. E seja $a_\alpha \in Y_\alpha$ se $Y_\alpha \neq \emptyset$.

Então a função $f : \beta \longrightarrow Y_0$ definida pelo $f(\alpha) = a_\alpha$ para $\alpha < \beta$ e $\beta = \{\, \alpha \mid Y_\alpha \neq \emptyset\,\}$ é cofinal para Y_0 e temos que $g \cdot f$ mostra $\mathrm{cf}\,(\kappa^+) \leq \mathrm{cf}\,(\beta) \leq \kappa$. Uma contradição!

Proposição. (Sierpinski) Existe uma coloração f do $[\mathcal{P}(\kappa)]^2$ com 2 cores tal que não existe um subconjunto X do $\mathcal{P}(\kappa)$ da cardinalidade maior que κ com $\overline{\overline{f``[X]^2}} = 1$.

Demonstração. Seja $<$ a ordem lexicografico sobre $\mathcal{P}(\kappa)$. Sejam $\prec$ qualquer bem-ordem do $\mathcal{P}(\kappa)$. Defina $f : [\mathcal{P}(\kappa)]^2 \longrightarrow 2$ pelo se $f(\{x, y\}) = 0$ se $x < y$ e $x \prec y$ ou $y < x$ e $y \prec x$ e $f(\{x, y\}) = 1$ se $x < y$ e $y \prec x$ ou $y < x$ e $x \prec y$.

Se $H \subseteq \mathcal{P}(\kappa)$ é tal que $f``[H]^2 = \{0\}$ então $<$ é uma bem-ordem do $H$. E se $H \subseteq \mathcal{P}(\kappa)$ é tal que $f``[H]^2 = \{1\}$ então $\{\kappa \setminus x \mid x \in H\}$ é bem-ordenado pelo $<$. Então, em qualquer caso $\overline{\overline{H}} \leq \kappa$ pela lema.

Definição. Um cardinal κ é *compacto fracamente* se para qualquer coloração f do $[\kappa]^2$ com 2 cores existe um $x \in [\kappa]^\kappa$ tal que $\overline{\overline{f``[x]^\kappa}} = 1$.

Exemplo. ω é compacto fracamente pela teorema de Ramsey.

Proposição. Se κ é compacto fracamente, então κ é inacessível fortemente.

Demonstração. Se κ não é inacessível fortemente ou existe $\mu < \kappa$ tal que $\kappa \leq 2^\mu$ ou κ é singular. Se $\mu < \kappa$ e $\kappa \leq 2^\mu$ temos que existe uma coloração do $[2^\mu]^2$ com 2 cores sem um subconjunto monocromatico do 2^μ do tamanho μ^+ pela teorema de Sierpinski. Mas $\mu^+ \leq \kappa$, então a restrição desta coloração para $[\kappa]^2$ não tem um subconjunto monocromatico do cardinalidade κ.

Se κ é singular, seja $g : \mathrm{cf}(\kappa) \longrightarrow \kappa$ cofinal e cresente estritamente. Defina $f : [\kappa]^2 \longrightarrow 2$ pelo $f(\gamma, \delta) = 0$ se e só se existe $\alpha < \mathrm{cf}(\kappa)$ tal que $g(\alpha) \leq \gamma$, $\delta < f(\alpha + 1)$. Porque para cada $\alpha < \mathrm{cf}(\kappa)$ temos que $\overline{\overline{\{\gamma < \kappa \mid g(\alpha) \leq \gamma < g(\alpha + 1)\}}} < \kappa$, não existe $x \in [\kappa]^\kappa$ tal que $f``[x]^2 = \{0\}$. E não existe $x \in [\kappa]^{\mathrm{cf}(\kappa)^+}$ tal que $f``[x]^2 = \{1\}$.

Muito mais tarde Stevo Todorčević mostrou uma teorema linda que fortelece muito o resultado de Sierpinski. Este teorema servirá como uma outra ilustração do uso conjuntos fechados e ilimitados e de conjuntos parados. (A demonstração que damos aqui é uma variação por Dan Velleman da demonstração de Todorčević.)

Teorema. (Todorčević 1986[2]) Existe uma coloração f do $[\omega_1]^2$ com ω_1 cores tal que $f``[x]^2 = \omega_1$ para cada $x \in [\omega_1]^{\omega_1}$. Em outras palavras, existe uma coloração do K_{ω_1} com ω_1 cores tal que qualquer subgrafo isomorfico para K_{ω_1} deve ter arestes com todos os cores.

Demonstração. Seja $\{r_\alpha \mid \alpha < \omega_1\} \subseteq {}^\omega 2$. Também seja $e_\alpha : \alpha \longrightarrow \omega$ uma injeção para cada $\alpha < \omega_1$. Defina $\sigma(\alpha, \beta) =$ o mínimo $n < \omega$ tal que $r_\alpha(n) \neq r_\beta(n)$ para $\alpha < \beta < \omega$, e seja $f(\alpha, \beta) =$ o mínimo $\delta < \omega_1$ tal que $\alpha \leq \delta < \beta$ e $e_\beta(\delta) \leq \sigma(\alpha, \beta)$ se existe um tal δ, e $= 0$ senão.

Para demonstrar a teorema é bastante mostrar que se $Z \in [\omega_1]^{\omega_1}$, então existe um conjunto C fechado e ilimitado tal que $C \subseteq f``[Z]^2$. Para ver isso lembrar que pelo proposição imediatemente depois da definição do parado temos que existe conjuntos parados $S_i \subseteq \omega_1$ para cada $i < \omega_1$, com

[2] Stevo Todorčević, *Partitioning pairs of countable ordinals*, Acta Mathematica, **159** (1987), pp. 261-294. Este artigo ótimo tem muitos outras coisas extremementes interessantes. Recomendâ-lo muito – e o volume de Acta Mathematica é na biblioteca também!

$\omega_1 = \bigcup\{S_i \mid i < \omega_1\}$ e $S_i \cap S_j = \emptyset$ se $i,\, j < \omega_1$ e $i \neq j$. Se definimos $g(\alpha) = i$ se e só se $\alpha \in S_i$ temos que $g \cdot f``[Z]^2 = g``C_Z$ onde C_Z é fechado e ilimitado para cada $Z \in [\omega_1]^{\omega_1}$. Mas para cada $i < \omega_1$ temos que existe $\alpha_i \in S_i \cap C_Z$ porque S_i e parado. Logo se $i < \omega$ existe $\{x, y\} \in [Z]^2$ tal que $f(\{x, y\}) = \alpha$ e $g(\alpha) = i$. Então $g \cdot f$ mostrar a teorema.

Então, seja $Z \in [\omega_1]^{\omega_1}$ e para cada $g \in \bigcup\{{}^n 2 \mid n < \omega\} = {}^{<\omega}2$ seja $B_g = \{\alpha \in Z \mid g \subseteq r_\alpha\}$. Também seja $C = \{\delta < \omega_1 \mid \forall g \in {}^{<\omega}2,$ ou $B_g \subseteq \delta$ ou $(\overline{\overline{B_g}} = \omega_1$ & $\delta = \bigcup(B_g \cap \delta))\}$. Suponhamos que λ é um ordinal do tipo limite e $\bigcup C \cap \lambda = \lambda$. Se $g \in {}^{<\omega}2$ e $B_g \not\subseteq \lambda$, temos que $B_g \not\subseteq \delta$ para cada $\delta < \lambda$, e, logo, temos $\overline{\overline{B_g}} = \omega_1$, porque $C \cap \lambda \neq \emptyset$, e $\lambda = \bigcup C \cap \lambda = \bigcup(\bigcup\{B_g \cap \delta \mid \delta \in C \cap \lambda\}) = \bigcup B_g \cap \lambda$. Então C é fechado. Não é difícil ver que C também é ilimitado no ω_1. $\overline{\overline{{}^{<\omega}2}} = \omega$, então existe $\delta < \omega_1$ tal que $\bigcup(\bigcup\{B_g \mid \overline{\overline{B_g}} < \omega_1\}) < \delta$. Seja $\{B_n \mid n < \omega\} = \{B_g \mid \overline{\overline{B_g}} = \omega_1\}$. Logo dado $\alpha < \omega_1$ pode escolhar recursivemente $\beta_{\omega.n+m}$ ser o membro mínimo do B_m tal que α, δ, e $\beta_{\omega.n'+m'} < \beta_{\omega.n+m}$ se $n' < n$ ou $n' = n$ e $m' < m$. É claro que $\alpha < \gamma = \bigcup\{\beta_{\omega.n+m} \mid n,\, m \in \omega\} \in C$. Vamos ver que $C \subseteq f``[Z]^2$.

Suponhamos que $\delta \in C$ e $\beta \in Z$ com $\delta < \beta$. Vamos achar $\alpha \leq \delta$ tal que $f(\alpha, \beta) = \delta$. Seja $n = e_\beta(\delta)$ e $g = r_\beta|n$. Então $\beta \in B_g$, e logo $B_g \not\subseteq \delta$ e temos que $\overline{\overline{B_g}} = \omega_1$.

Para cada $\gamma \in B_g$ tal que $\beta < \gamma$ sejam $m_\gamma = \sigma(\beta, \gamma)$ e $h_\gamma = r_\gamma|(m_\gamma + 1)$. Nota que $h_\gamma|m_\gamma = g|m_\gamma$, mas $h_\gamma(m_\gamma) \neq g(m_\gamma)$. Porque $\overline{\overline{B_g}} = \omega_1$ existe um subconjunto $B \in [B_g]^{\omega_1}$ e existe $m < \omega$ e $h : m \longrightarrow \omega$ tal que $m = m_\gamma$ e $h = h_\gamma$ para cada $\gamma \in B$. Logo $\overline{\overline{B_h}} = \omega_1$ e pela definição do C temos que $\delta = \bigcup \delta \cap B_h$.

Seja $F = \{\epsilon < \delta \mid e_\beta(\epsilon) \leq m\}$. F é finito porque e_β é uma injeção. Então existe $\alpha \in B_h \cap \delta$ tal que $F \subseteq \alpha$. Agora temos que $\alpha \in B_h$, logo $h \subseteq r_\alpha$, e que $h|m = r_\beta|m$ e $h(m) \neq r_\beta(m)$. Logo $\sigma(\alpha, \beta) = m$. Se $\alpha \leq \epsilon < \delta$ temos que $m < e_\beta(\epsilon)$, mas $e_\beta(\delta) = m$. Logo δ é mínimo tal que $\alpha \leq \delta < \beta$ e $e_\beta(\delta) \leq m$, então $\delta = f(\alpha, \beta)$.

Seria muito interesante ter resultados similares para outro grafos além de K_{ω_1}. Pode ver o artigo recente de András Hajnal e Péter Komjáth, *Some remarks on the simultaneous chromatic number*, (até agora não publicado, mas disponível do Péter Komjáth – kope@cs.elte.hu – pelo internet) para alguma informação sobre este problema da geralização, mas ainda tem muitas oportunidades para melhoramentos do trabalho deles.

Por exemplo, falemos que $G = (X, A)$ tem *número cromático* ω_1 se ω_1 é o cardinal κ mínimo tal que existe $f : \kappa \longrightarrow X$ tal que $f(x) \neq f(y)$ se $\{x, y\} \in A$. É claro que K_{ω_1} tem número cromático ω_1.

O princípio $\diamondsuit^+$ fala que existe $\{B_{\alpha,n} \mid \alpha < \omega_1$ & $n < \omega\}$ tal que $B_{\alpha,n} \subseteq \alpha$ para cada $\alpha < \omega_1$ e $n < \omega$, e se $B \subseteq \omega_1$, então existe um conjunto, C, fechado e ilimitado tal que $\forall \gamma \in C\ \exists n < \omega\ (B \cap \gamma = B_{\gamma,n})$. Então $\diamondsuit^+$ fala que tem um sistema $\{B_{\alpha,n} \mid \alpha < \omega_1$ & $n < \omega\}$ que prediz *qualquer* subconjunto B do ω_1 certamente num grande (fechado e ilimitado) número dos lugares. $\diamondsuit^+$ é uma fortalecendo do (HC), então não demonstraável no ZF (embora que é verdadeiro se $V = L$, por exemple). Ele implica (HC) porque se $x \subseteq \omega$ existe C tal que $\forall \gamma \in C \setminus \omega$ existe $n < \omega$ com $x = x \cap \gamma = B_{\gamma,n}$. Então $2^\omega = \overline{\overline{\mathcal{P}(\omega)}} \leq \overline{\overline{\{B_{\alpha,n} \mid \alpha < \omega_1 \ \&\ n < \omega\}}} = \omega_1$.

Hajnal e Komjáth mostram que $\diamondsuit^+$ implica que se $G = (\omega_1, A)$ tem número cromático ω_1, então existe $f : A \longrightarrow \omega_1$ tal que se $X \in [\omega_1]^{\omega_1}$ e $(X, A \cap (X \times X))$ tem número cromático ω_1 temos que $f``(A \cap (X \times X)) = \omega_1$. Mas ainda esta em aberta se pode mostrar este resultado no ZF + AE, logo geralizando a teorema de Todorčević.

Capítulo 6. Lógica matemática: uma introdução super-rápida e algumas aplicações à teoria dos conjuntos.*

6.1. Línguas (formais) da ordem primeira. Neste cápitulo vamos dar uma olhada muito breve sobre lógica matemática para explicar que foi significado no fim do §4.4. quando falamos que algumas coisas, por exemple (HCG), não são mostrável na sistema ZF nem são mostrável os contrários. Este consideração da lógica matématica ajuderá explicar o que quer dizer falar que pode *demonstrar* que alguma coisa não é mostrável. O chave para isso é a relação entre que é *demonstrável* e que é *verdadeiro*. Este não é nada místico, nem filosofico, mas é uma coisa matemática porque pelo verdadeiro queremos dizer *verdadeiro num modelo* duma coleção dos axiomas. Botâ-lo num outro modo, é a relação matemática entre sintaxe e semântica. Este assunto é chamado a *teoria de modelos*. Talvez vai paracer formal no início mas é muito efetivo. Um exemplo recente do poder do assunto é o trabalho célebre de Udi Hrushovski na área da teoria dos números/geometria algebraica aritmética usando métodos da teoria dos modelos. Para pegar mais sobre a teoria de modelos veja o livro de van Dalen para uma explicação mais completo da material desta seção, e posso recomendar os livros Wilfrid Hodges, *A shorter model theory*, Cambridge University Press(?), 1996(?), ou Bruno Poizat, *A course in model theory*, Springer, 2000 (ou a versão original em francês, Bruno Poizat, *Cours de théorie de modèles*, Nur al-Mantiq wal Ma'rifah, Lyons, 1985, que pode pegar do Poizat se mesmo). Infelizmente não tem qualquer livro no português sobre o assunto. E tem um esboço bom e acessível do trabalho de Hrushovski no Ehud Hrushovski, *Geometric Model Theory*, Documenta Mathematica, Extra Volume, ICM 1998, I, pp. 281-302. (**Endereço do email de Poizat e site do artigo de Hrushovski.**)

Definição. Uma língua $\mathcal{L}$ para lógica da ordem primeira é feito de:
(i) um conjunto enumerável dos variávais v_0, v_1,... (escritos como x, y, z,... quando queremos);
(ii) um conjunto dos símbolos para funções f, g,... do várias "áridades" – um símbolo para uma função 0-ária é um símbolo para um constante c;
(iii) um conjunto dos símbolos para relações R, S,... do várias áridades, e um símbolo especial $=$ (que é binária);
(iv) algumas ligações lógicas: &, ou, $\longrightarrow$, $\neg$, $\perp$;
(v) quantificadores $\forall$, $\exists$;
(vi) sinais de pontuação como (,), ..

Os *termos* de $\mathcal{L}$ são definidos pela uma definição recursiva.
(i) Qualquer variável v é um termo;
(ii) se f é um símbolo para um função n-ária e $t_0,\ldots, t_{n-1}$ são termos, então $f(t_0,\ldots,t_{n-1})$ é um termo também.

Definamos os *variáveis livres* de um termo t, VL(t) pelo (i) VL(v) $= \{v\}$ se v é um variável, e (ii) $\mathrm{VL}(f(t_0,\ldots,t_{n-1})) = \mathrm{VL}(t_0)\cup\ldots \mathrm{VL}(t_{n-1})$.

Os *fórmulas* de $\mathcal{L}$ são definidos pela uma definição recursiva junto com a definição dos variáveis livres.

* versão 1.1, 15/12/00

(i) Se R é um símbolo para uma relação n-ária e $t_0, \ldots, t_{n-1}$ são termos, então $R(t_0, \ldots, t_{n-1})$ é um *fórmula*. $\mathrm{VL}(R(t_0, \ldots, t_{n-1})) = \mathrm{VL}(t_0) \cup \ldots \mathrm{VL}(t_{n-1})$. (Estes fórmulas são chamados *fórmulas atômicos*.)
(ii) Se ϕ e ψ são fórmulas, então $\phi \,\&\, \psi$, ϕ ou ψ, $\phi \longrightarrow \psi$, $\neg\phi$, $\perp$ são fórmulas também. $\mathrm{VL}(\phi \,\&\, \psi) = \mathrm{VL}(\phi \text{ ou } \psi) = \mathrm{VL}(\phi \longrightarrow \psi) = \mathrm{VL}(\phi) \cup \mathrm{VL}(\psi)$, $\mathrm{VL}(\neg\phi) = \mathrm{VL}(\phi)$ e $\mathrm{VL}(\perp) = \emptyset$.
(iii) Se ϕ é um fórmula e $x \in \mathrm{VL}(\phi)$, então $\forall x\, \phi$ e $\exists x\, \phi$ é um fórmula também. $\mathrm{VL}(\forall x\, \phi) = \mathrm{VL}(\exists x\, \phi) = \mathrm{VL}(\phi) \setminus \{x\}$.

Então os variáveis livres de um fórmula ϕ são os variáveis "sobre qual ϕ fala alguma coisa." Um fórmula ϕ é um *frase* se $\mathrm{VL}(\phi) = \emptyset$. Escreva $\phi(\bar{x})$ se $\bar{x}$ é o fio $x_0, \ldots, x_{n-1}$ e ϕ é um formula tal que $\mathrm{VL}(\phi) \subseteq \{x_0, \ldots, x_{n-1}\}$.

Nota. Podemos definir todos as ligações e quantificadores usando so ou, $\neg$ e $\exists$ – que economizer no tempo mas tarde – se definimos $\phi \,\&\, \psi = \neg(\neg\phi \text{ ou } \neg\psi)$, $\phi \longrightarrow \psi = (\neg\phi \text{ ou } \psi)$, $\perp = \neg(\phi \text{ ou } \neg\phi)$ e $\forall x\, \phi = \neg\exists x\, (\neg\phi)$.

Também precisamos uma definição de como substituir um termo em vez de um variável num termo ou num fórmula. Temos que ter cuidado com isso para preservar o sentido pretentido dum fórmula, porque se, por exemplo, ϕ é $\exists y\, (y = x)$ e $t = f(y)$ queremos que o resultado da substitução do t em vez de x não é $\exists y\, (y = f(y))$ mas $\exists z\, (z = f(y))$.

Então $s[t/x]$, $\phi[t/x]$, *o resulatado da substitução do t para x*, é definido pela recursão:

$$
\begin{array}{ll}
v_i[t/x] & = t \text{ se } x = v_i, \text{ e} \\
 & = v_i \text{ senão;} \\
f(s_0, \ldots, s_{n-1})[t/x] & = f(s_0[t/x], \ldots, s_{n-1}[t/x]); \\
R(s_0, \ldots, s_{n-1})[t/x] & = R(s_0[t/x], \ldots, s_{n-1}[t/x]); \\
(\neg\phi)[t/x] & = \neg(\phi[t/x]); \\
\perp [t/x] & = \perp; \\
(\phi \,\&\, \psi)[t/x] & = \phi[t/x] \,\&\, \psi[t/x]; \\
(\phi \text{ ou } \psi)[t/x] & = \phi[t/x] \text{ ou } \psi[t/x]; \\
(\phi \longrightarrow \psi)[t/x] & = \phi[t/x] \longrightarrow \psi[t/x]; \\
(\forall y\, \phi)[t/x] & = \forall y \phi \text{ se } x = y, \\
 & = \forall y\, (\phi[t/x]) \text{ se } y \neq x \text{ e } y \notin \mathrm{VL}(s), \text{ e} \\
 & = \forall z\, ((\phi[z/y])[t/x]) \text{ se } y \neq x \text{ e } y \in \mathrm{VL}(s), \text{ onde } z \\
 & \quad\quad \text{é uma escolha de alguma coisa } z \notin \mathrm{VL}(s) \cup \mathrm{VL}(\phi); \\
(\exists y\, \phi)[t/x] & = \exists y \phi \text{ se } x = y, \\
 & = \exists y\, (\phi[t/x]) \text{ se } y \neq x \text{ e } y \notin \mathrm{VL}(s), \text{ e} \\
 & = \exists z\, ((\phi[z/y])[t/x]) \text{ se } y \neq x \text{ e } y \in \mathrm{VL}(s), \text{ onde } z \\
 & \quad\quad \text{é uma escolha de alguma coisa } z \notin \mathrm{VL}(s) \cup \mathrm{VL}(\phi).
\end{array}
$$

A relação $\vdash$ de derivação sintática vem de pensar sobre arvores de dedução com hipóteses nas folhas e a conclusão na base, feito das deduções "primativas."

Formalmente definimos $\vdash$ pela recursão. A definição é para fórmulas ϕ (uma conclusão) pela recursão na estrutura de ϕ e para qualquer conjunto dos fórmulas Γ (os hipóteses), na mesma hora.

No inicio temos $\Gamma \vdash \phi$ se $\phi \in \Gamma$;

e: se $\Gamma\vdash\phi$ e $\Gamma\vdash\psi$,	então $\Gamma\vdash\phi\,\&\,\psi$;
se $\Gamma\vdash\phi\,\&\,\psi$,	então $\Gamma\vdash\phi$;
se $\Gamma\vdash\psi\,\&\,\psi$,	então $\Gamma\vdash\psi$;
ou: se $\Gamma\vdash\phi$,	então $\Gamma\vdash\phi$ ou ψ;
se $\Gamma\vdash\psi$,	então $\Gamma\vdash\phi$ ou ψ;
se $\Gamma\vdash\psi$ ou ψ, $\Gamma\cup\{\phi\}\vdash\chi$ e $\Gamma\cup\{\psi\}\vdash\chi$,	então $\Gamma\vdash\chi$;
implicação: se $\Gamma\cup\{\phi\}\vdash\psi$,	então $\Gamma\vdash\phi\longrightarrow\psi$;
se $\Gamma\vdash\phi\longrightarrow\psi$ e $\Gamma\vdash\phi$,	então $\Gamma\vdash\psi$;
não/falso: se $\Gamma\cup\{\phi\}\vdash\bot$,	então $\Gamma\vdash\neg\phi$;
se $\Gamma\vdash\bot$,	então $\Gamma\vdash\phi$ para qualquer ϕ;
se $\Gamma\vdash\phi$ e $\Gamma\vdash\neg\phi$,	então $\Gamma\vdash\bot$;
se $\Gamma\cup\{\neg\phi\}\vdash\bot$,	então $\Gamma\vdash\phi$;
tudo: se $\Gamma\vdash\phi(x)$ e $x\notin\bigcup\{\mathrm{VL}(\psi)\mid\psi\in\Gamma\}$,	então $\Gamma\vdash\forall x\,\phi(x)$;
se $\Gamma\vdash\forall x\,\phi(x)$ e t é um termo,	então $\Gamma\vdash\phi[t/x]$;
existe: se $\Gamma\vdash\phi[t/x]$,	então $\Gamma\vdash\exists x\,\phi(x)$;
se $\Gamma\vdash\exists x\,\phi(x)$ e $\Gamma\cup\{\phi(y)\}\vdash\psi$ e $y\notin\mathrm{VL}(\psi)$,	então $\Gamma\vdash\psi$.
igualidade: se s é um termo,	então $\Gamma\vdash s=s$;
se $\Gamma\vdash s=t$ e $\Gamma\vdash\phi[s/x]$,	então $\Gamma\vdash\phi[t/x]$.

E porque na definição da introdução do *tudo* não falamos só que "se $\Gamma\vdash\phi(x)$ e $x\notin\bigcup\{\mathrm{VL}(\psi)\mid\psi$ é usado na demonstração do $\phi(x)$ do $\Gamma\,\&\,\psi\in\Gamma\}$, então $\Gamma\vdash\forall x\,\phi(x)$," temos que juntar que:

se $\Delta\subseteq\Gamma$ e $\Delta\vdash\phi$, então $\Gamma\vdash\phi$.

Definição. Γ é *consistente* se $\Gamma\nvdash\bot$. Equivalentemente Γ é *consistente* se não existe um ϕ tal que $\Gamma\vdash\phi\ \&\ \neg\phi$. As vezes escrevemos $\mathrm{Con}(\Gamma)$ para querer dizer que Γ é consistente.

Depois de todos estas definições eu deveria dar algumas exemplos. Porque agora estou muito atrasado vou evitar fazer isso.

Definição. Sejam $\mathcal{L}$ uma língua da primeria ordem, Γ uma coleção das frases e ϕ uma frase no $\mathcal{L}$. d é uma *derivação do* ϕ *de* Γ se d é um liste (ou *fio*) finito dos fórmulas, $\phi_0,\ldots,\phi_n$ para alguma $n<\omega$, com $\phi=\phi_n$ e tal que para cada $m\le n$ temos ou $\phi_m\in\Gamma$ ou ϕ_m pode ser obtido pela aplicando uma das cláusulas basicas da definição do $\vdash$ para $\{\phi_i\mid i<m\}$.

6.2. Modelos é as teoremas de completude e de compacidade.

Vamos escrever $\Gamma\Longrightarrow\phi$ para nossa noção matemática informal de ϕ segue do Γ. (Por exemple muitos vezes no curso até agora temos mostrado que $\mathrm{ZF}\Longrightarrow\phi$ para ϕ uma frase sobre conjuntos.) É claro da definição do $\vdash$ que se $\Gamma\vdash\phi$, então $\Gamma\Longrightarrow\phi$. Agora vamos introduzir uma noção de "segue semânticamente."

Definição. Seja $\mathcal{L}$ uma língua da ordem primeira como no §6.1. $\mathcal{M}$ é uma estrutura para $\mathcal{L}$ se $\mathcal{M}=(M,f^{\mathcal{M}},g^{\mathcal{M}},\ldots,R^{\mathcal{M}},S^{\mathcal{M}},\ldots)$ onde M é um conjunto, $f^{\mathcal{M}}$, $g^{\mathcal{M}}$,... são funções tal que $f^{\mathcal{M}}:{}^nM\longrightarrow M$ se f é n-ário, e $R^{\mathcal{M}}$, $S^{\mathcal{M}}$,... são relações sobre M com $R^{\mathcal{M}}\subseteq{}^nM$ se R é n-ário.

Agora vamos definir quando uma estrutura pensa que uma frase é verdadeira.

Definição. Seja $\mathcal{L}$ uma língua da ordem primeira e $\mathcal{M}$ é uma estrutura para $\mathcal{L}$. Seja ϕ uma frase no $\mathcal{L}$. Definamos ϕ é verdadeiro no $\mathcal{M}$, escrevendo $\mathcal{M}\models\phi$ pela recursão sobre a forma do ϕ.

$$
\begin{array}{ll}
\mathcal{M} \models R(a_0, \ldots, a_{n-1}) & \text{se e só se } (a_0, \ldots, a_{n-1}) \in {}^nM; \\
\mathcal{M} \models \phi \,\&\, \psi & \text{se e só se } \mathcal{M} \models \phi \text{ e } \mathcal{M} \models \psi; \\
\mathcal{M} \models \phi \text{ ou } \psi & \text{se e só se } \mathcal{M} \models \phi \text{ ou } \mathcal{M} \models \psi; \\
\mathcal{M} \models \neg\phi & \text{se e só se } \mathcal{M} \not\models \phi; \\
\mathcal{M} \models \phi \longrightarrow \psi & \text{se e só se } \mathcal{M} \not\models \phi \text{ ou } \mathcal{M} \models \psi; \\
\mathcal{M} \models \exists x\, \phi(x) & \text{se e só se existe } a \in M \text{ e } \mathcal{M} \models \phi(a); \\
\mathcal{M} \models \forall x\, \phi(x) & \text{se e só se para cada } a \in M \text{ temos que } \mathcal{M} \models \phi(a).
\end{array}
$$

Nota. Sejam $\mathcal{L}$ uma língua da ordem primeira e $\mathcal{M}$ é uma estrutura para $\mathcal{L}$. Então $\mathcal{M} \not\models \perp$ pela definição do $\models$.

Por exemplo, se $\mathcal{L} = \{e,\ .,\ ^{-1}\}$, a *língua da teoria dos grupos*, e $\mathcal{M} \models (\forall x\, x.x^{-1} = e = x^{-1}.x)$ & $(\forall x\, x.e = x = e.x)$ & $(\forall x \forall y \forall z\, (x.y).z = x.(y.x))$ (logo $\mathcal{M}$ é um grupo), então pode ser ou não que $\mathcal{M} \models \forall x \forall y\, x.y = y.x$, mas certamente $\mathcal{M} \not\models \exists x\, x.x^{-1} \neq e$.

Definição. $\Gamma \models \phi$ se para todos estruturas $\mathcal{M}$ para a língua $\mathcal{L}$ temos que se $\mathcal{M} \models \psi$ para cada $\psi \in \Gamma$, então $\mathcal{M} \models \phi$.

Definição. $\mathcal{M}$ é um *modelo* de um conjunto de frases Γ para uma língua $\mathcal{L}$ se $\mathcal{M}$ é uma estrutura para $\mathcal{L}$ e $\mathcal{M} \models \phi$ para cada $\phi \in \Gamma$. Escrevemos $\mathcal{M} \models \Gamma$.

É claro pela definição do $\models$ que se $\Gamma \Longrightarrow \phi$ então $\Gamma \models \phi$. Logo temos o seguinte.

Proposição. (Teorema de saúde ("soundness" no inglês).) Se $\Gamma \vdash \phi$, então $\Gamma \models \phi$.

Corolário. Se Γ, um conjunto das frases, tem um modelo, então Γ é consistente.

Demonstração. Se Γ não é consistente, então $\Gamma \vdash \perp$, logo $\Gamma \models \perp$. Mas não existe estruturas $\mathcal{M}$ qualquer tal que $\mathcal{M} \models \perp$, pelo definição de $\models$, então não existe qualquer estrutura $\mathcal{M}$ tal que $\mathcal{M} \models \Gamma$.

Mas também temos o inverso para a proposição.

Teorema de completude. Se $\Gamma \models \phi$, então $\Gamma \vdash \phi$.

Isso é mais profundo, porque fala que tem uma tradução dum procedimento infinito (confirmindo que cada modelo do Γ, cada um do qual pode ser infinito, é um modelo do ϕ também) para um procedimento finito (uma derivação do ϕ de Γ). Para demonstrar a teorema é conveniente introduzir um par das definições.

Definição. Uma coleção das frases Δ numa língua $\mathcal{L}$ é uma teoria de tipo *Henkin* se sempre que $\exists x\, \phi(x) \in \Delta$, existe um constante $c \in \mathcal{L}$ tal que $\Delta \vdash \exists x\, \phi(x) \longrightarrow \phi(c)$. Então c é uma *testemunha* para a frase $\exists x\, \phi(x)$.

Observação. Se Δ, numa língua $\mathcal{L}$, é uma teoria de tipo Henkin, e Δ' é uma coleção de frases na mesma língua $\mathcal{L}$, $\Delta \subseteq \Delta'$, então Δ' é uma teoria do tipo Henkin.

Definição. Se Δ é uma coleção das frases numa língua $\mathcal{L}$ e $\Delta \subseteq \Delta'$, uma coleção das frases numa lingua $\mathcal{L}'$ com $\mathcal{L} \subseteq \mathcal{L}'$, falamos que Δ' é uma extensão *conservadora* de Δ se $\Delta \vdash \phi$ se e só se $\Delta' \vdash \phi$ para cada $\phi \in \mathcal{L}$. (E então Δ' é consistente se Δ é consistente, porque $\bot \in \mathcal{L}$ e, logo, $\Delta' \vdash \bot$ se e só se $\Delta \vdash \bot$.)

Proposição. Se Δ é uma coleção das frases numa língua $\mathcal{L}$, existe uma coleção das frases Δ' numa lingua $\mathcal{L}'$ tal que $\mathcal{L} \subseteq \mathcal{L}'$, $\Delta \subseteq \Delta'$, Δ' é uma teoria do tipo Henkin e com Δ' uma extensão conservadora de Δ (e com $\overline{\overline{\mathcal{L}'}} = \overline{\overline{\mathcal{L}}} + \omega$ também).

Demonstração. Seja Γ qualquer coleção das frases numa língua $\mathcal{K}$. Juntar constantes distintos c_ϕ para $\mathcal{K}$ para cada fórmula $\phi(x)$ com variável livre x no $\mathcal{K}$ para chegar no $\mathcal{K}^* = \mathcal{K} \cup \{ c_\phi \mid \phi(x) \in \mathcal{L} \}$. Seja $\Gamma^* = \Gamma \cup \{ \exists x\, \phi(x) \longrightarrow \phi(c_\phi) \mid \Gamma \vdash \exists x\, \phi(x) \}$. Vamos mostrar que Γ^* é uma extensão conservadora de Γ.

Suponhmos que $\Gamma^* \vdash \psi$ para $\psi \in \mathcal{K}$. Então existe $n < \omega$ e fórmulas ϕ_i para $i < n$ tal que $\Gamma \cup \{ \exists x\, \phi_i(x) \longrightarrow \phi_i(c_{\phi_i}) \mid i < n \} \vdash \psi$. Seja $\Gamma^m = \Gamma \cup \{ \exists x\, \phi_i(x) \longrightarrow \phi_i(c_{\phi_i}) \mid i < m \}$ para cada $m \leq n$. Mostraramos que se $\Gamma^{m+1} \vdash \psi$ temos que $\Gamma^m \vdash \psi$, para qualquer $m < n$, e,logo, pela indução, que $\Gamma = \Gamma^0 \vdash \psi$. Se $n = 0$ não tem nada fazer. Então suponhamos que $n \neq 0$ e seja $m < n$.

Se $\Gamma^{m+1} = \Gamma^m \cup \{ \exists x\, \phi_m(x) \longrightarrow \phi_m(c_{\phi_m}) \} \vdash \psi$, temos que $\Gamma^m \vdash (\exists x\, \phi_m(x) \longrightarrow \phi_m(c_{\phi_m})) \longrightarrow \psi$. Então, temos que $\Gamma^m \vdash \exists y (\exists x\, \phi_m(x) \longrightarrow \phi_m(y)) \longrightarrow \psi$ pela definição de $\vdash$, especificamente a regra para introdução dos quantificadores existenciais, porque $c_{\phi_m} \notin \mathcal{K}$ e, logo, não aparece nos fórmulas ϕ e ψ. Logo $\Gamma^m \vdash (\exists x\, \phi_m(x) \longrightarrow \exists y\, \phi_m(y)) \longrightarrow \psi$, e então $\Gamma^m \vdash \psi$.

Agora sejam $\Delta_0 = \Delta$ e $\mathcal{L}_0 = \mathcal{L}$, sejam $\Delta_{i+1} = \Delta_i^*$, $\mathcal{L}_{i+1} = \mathcal{L}_i^*$ para cada $i < \omega$, e sejam $\Delta' = \bigcup \{ \Delta_i \mid i < \omega \}$ e $\mathcal{L}' = \bigcup \{ \mathcal{L}_i \mid i < \omega \}$. Temos que Δ' é uma extensão conservadora de Δ. E Δ' é uma teoria de tipo Henkin porque se $\exists x\, \phi(x) \in \Delta$ temos que $\exists x\, \phi(x) \in \Delta_i$ para alguma $i < \omega$ e então $(\exists x\, \phi(x) \longrightarrow \phi(c_\phi)) \in \Delta_{i+1} \subseteq \Delta$.

Demonstração de teorema de completude. Seja Γ uma coleção das frases numa língua $\mathcal{L}$, e ϕ um fórmula na língua $\mathcal{L}$. Para demonstrar a teorema mostramos que se $\Gamma \nvdash \phi$ tem um modelo de $\Gamma \cup \{ \neg\phi \}$ (e então $\Gamma \not\models \phi$).

Pela proposição, seja Γ' uma teoria do tipo Henkin tal que $\Gamma \cup \{ \neg\phi \} \subseteq \Gamma'$ numa língua $\mathcal{L}'$ com $\mathcal{L} \subseteq \mathcal{L}'$ e $\overline{\overline{\mathcal{L}'}} = \overline{\overline{\mathcal{L}}} + \omega$. Considerar o conjunto das coleções das frases Δ tal que Δ é na língua $\mathcal{L}'$, Δ é consistente, e $\Gamma' \subseteq \Delta$, ordenado pelo $\Delta \leq \Delta^*$ se $\Delta \subseteq \Delta^*$. Cada cadeia na ordem tem um limite superior, então podemos usar a Lema de Zorn para escolhar uma teoria $\Gamma_{\max}$ que é maximal tal que $\Gamma_{\max}$ é na língua $\mathcal{L}'$, $\Gamma_{\max}$ é consistente, e $\Gamma' \subseteq \Gamma_{\max}$. Nota que $\Gamma_{\max}$ é do tipo Henkin (pela observação). Também, se $\Gamma_{\max} \vdash \psi$, temos que $\psi \in \Gamma_{\max}$ pela maximalidade de $\Gamma_{\max}$; se $\exists x\, \psi(x) \in \Gamma_{\max}$, então temos um constante $c \in \mathcal{L}$ tal que $\psi(c) \in \Gamma_{\max}$; se $\psi \operatorname{ou} \chi \in \Gamma_{\max}$ temos que $\psi \in \Gamma_{\max}$ ou $\chi \in \Gamma_{\max}$; e $\neg\psi \in \Gamma_{\max}$ se e só se $\psi \notin \Gamma_{\max}$.

Agora vamos usar os termos se mesmos na língua $\mathcal{L}'$ como os elementos dum modelo para $\Gamma_{\max}$. Deveria ficar certa cá que entende como estamos usando termos, coisas síntacticas, como objetos para formar uma estrutura semântica. Seja $A = \{ t \in \mathcal{L}' \mid t \text{ é um termo no } \mathcal{L}' \}$. Se f é um símbolo para uma função n-ária no $\mathcal{L}'$, seja $f^{\mathcal{A}} : {}^n A \longrightarrow A$ definido pelo $f^{\mathcal{A}}(t_0, \ldots, t_{n-1}) = f(t_0, \ldots, t_{n-1})$, um termo também. E se R é um símbolo para uma relação n-ária no $\mathcal{L}'$, define um subconjunto $R^{\mathcal{A}}$ do ${}^n A$ pelo $(t_0, \ldots, t_{n-1}) \in R^{\mathcal{A}}$ se e só se $(t_0, \ldots, t_{n-1}) \in R$.

Estamos perto ao fim da demonstração mas poderia ser que temos termos s, t tal que '$s = t$' $\in \Gamma_{\max}$, então temos que pegar o quociente de $\mathcal{A}$ sob este relação para chegar numa estructura para $\mathcal{L}'$. Logo seja $s \sim t$ se '$s = t$' $\in \Gamma_{\max}$ para $s, t \in A$, e seja $[s] = \{ t \in A \mid t \sim s \}$ para $s \in A$. Formamos uma estrutura $\mathcal{M}$ pelo tomando $M = \{ [s] \mid s \in A \}$, $f^{\mathcal{M}}([t_0], \ldots, [t_{n-1}]) = [f(t_0, \ldots, t_{n-1})]$ se f é um simbolo para uma função n-ária no $\mathcal{L}'$, e $([t_0], \ldots, [t_{n-1}]) \in R^{\mathcal{M}}$ se e só se $(t_0, \ldots, t_{n-1}) \in R^{\mathcal{A}}$ onde R é um simbolo para uma relação n-ária no $\mathcal{L}'$. Temos que $\mathcal{M} = (M, f^{\mathcal{M}}, \ldots, R^{\mathcal{M}}, \ldots)$ é uma estructura para L', e $\mathcal{M} \models \psi$ se e só se $\psi \in \Gamma_{\max}$ para $\psi \in \mathcal{L}'$ pela indução sobre a estrutura das frases, usando as observações que seguem da maximalidade de $\Gamma_{\max}$ na ultima frase do paragráfo primeiro desta demonstração. Logo $\mathcal{N} = (M, f^{\mathcal{M}}, \ldots, R^{\mathcal{M}}, \ldots \mid f \in \mathcal{L})$ é uma estructura para $\mathcal{L}$ e $\mathcal{N} \models \Gamma \cup \{\neg\phi\}$.

Corolário. (Existência de modelos). Se Γ, um conjunto das frases, é consistente, então Γ tem um modelo. Além disso, se Γ é numa lingua $\mathcal{L}$ e $\overline{\overline{\mathcal{L}}} = \kappa$, então Γ tem um modelo $\mathcal{N}$ com $\overline{\overline{N}} = \omega + \kappa$.

Demonstração. Se Γ não tem um modelo, então temos que $\mathcal{M} \models \Gamma$ implica $\mathcal{M} \models \phi$ para qualquer ϕ. Logo $\Gamma \models \phi$ para qualquer ϕ, logo $\Gamma \models \perp$. Então $\Gamma \vdash \perp$ pela teorema.

Além disso, na demonstração da teorema chegamos num modelo $\mathcal{N}$ do Γ do qual os elementos são classes de equivalência dos termos da lingua $\mathcal{L}'$. Então $\overline{\overline{N}} \leq \overline{\overline{L}}'^{<\omega} = \overline{\overline{L}}' = \overline{\overline{L}} + \omega = \kappa + \omega$.

Corolário. (Compacidade). Se Γ é um conjunto das frases e cada subconjunto finito $\Delta \subseteq \Gamma$ tem um modelo, então Γ tem um modelo também.

Demonstração. Se Γ não tem um modelo, então temos que $\Gamma \vdash \perp$ pelo corolário sobre a existência de modelos. Mas se $\Gamma \vdash \phi$ temos que existe um $\Delta \subseteq \Gamma$ finito tal que $\Delta \vdash \phi$, para qualquer ϕ, porque demonstrações são finitárias. Então existe alguma $\Delta \subseteq \Gamma$ finito tal que $\Delta \vdash \perp$. Logo Δ não tem um modelo, uma contradição para o hipótese!

Exemplo. Seja $\mathcal{L} = \{0, +, ., s, <, exp, =\}$ uma lingua da ordem primeira onde exp é binaria, seja $\mathbf{N} = (\omega, 0^{\mathbf{N}}, +^{\mathbf{N}}, .^{\mathbf{N}}, s^{\mathbf{N}}, <^{\mathbf{N}}, exp^{\mathbf{N}}, =^{\mathbf{N}})$ onde $exp(x, y) = x^y$, e seja Γ o conjunto das frases que são verdadeiras sobre aritmética, *i.e.*, para $\mathbf{N}$ (ou poderia tomar Γ ser os axiomas para a aritmética de Peano). Juntar um constante novo c para $\mathcal{L}$, chegando no $\mathcal{L}' = \mathcal{L} \cup \{c\}$, e considerar $\Gamma' = \Gamma \cup \{ s(s(\ldots(s(0)))) < c \mid n < \omega \ \& s(s(\ldots(s(0))))$ é s aplicado n vezes para $0 \}$. As frases novas no $\Gamma' \setminus \Gamma$ falam que $n < c$ para cada $n < \omega$ porque $n = 0 + 1 + 1 + \ldots + 1$ n vezes.

Afirmo que Γ' tem um modelo. Demonstração: se $\Delta \subseteq \Gamma'$ é finito temos que $\Delta \setminus \Gamma$ é finito, então existe alguma $m_\Delta < \omega$ tal que para cada frase da forma $n < c$ (*i.e.* da forma $s(s(\ldots(s(0)))) < c$ com n aplicacões do s, formalmente) tal que $n < c \in \Delta$ temos que $n \leq m_\Delta$. Logo Δ tem um modelo $\mathbf{N} = (\omega, 0^{\mathbf{N}}, +^{\mathbf{N}}, .^{\mathbf{N}}, s^{\mathbf{N}}, <^{\mathbf{N}}, exp^{\mathbf{N}}, =^{\mathbf{N}}, c_\Delta^{\mathbf{N}})$, onde $c_\Delta^{\mathbf{N}}$ é qualquer número natural maior que m_Δ. Logo Γ' tem um modelo pelo teorema de compactidade, e o modelo é um modelo para aritmética que é não-normal porque tem números naturais infinitos, então o modelo não é $\mathbf{N}$.

Exemplo. (Analyse "não-padrão".) Nos origems de calcúlo, que pode argumentar razoávelmente foi o inicio de todo matemática moderna, Newton e Liebniz e os seguidaores deles falavam e racionaciavam sobre quantidades infinitamentes pequenhos e infinitamentes grandes para chegar nos resultados deles. No seculo 19^o ninguem conseguiu no fornecendo uma formalização satisfatória destas raciocinações, e com tempo caiem do favor, sendo reposto para o método do ϵ-δ de Kronecker como sendo "mais seguro." Agora, pela teorema de compacidade podemos recobrir a possibilidade de usar estas intuições originais de Newton e Liebniz.

Seja $\mathcal{L} = \{+, -, ., <, 0, 1\}$ e seja T o conjunto das frases verdadeiras sobre os reis com a estrutura esperada, $(\mathbf{R}, +^{\mathbf{R}}, -^{\mathbf{R}}, .^{\mathbf{R}}, <^{\mathbf{R}}, 0^{\mathbf{R}}, 1^{\mathbf{R}})$, nesta língua. Seja $\mathcal{L}' = \mathcal{L} \cup \{c\}$, onde c é um símbolo novo para um constante, e seja $\Gamma = T \cup \{O < c < y \,\&\, y.(1{+}1\ldots{+}1) \mid 1{+}1{+}\ldots{+}1$ é a suma de 1 n vezes $\&\ n < \omega\}$. Como no exemplo prévio Γ tem um modelo, vamos falar $\mathbf{R}^*$, em qual existe um c tal que $0 < c$ e $c < 1/n$ para cada número natural n, isso é tal que c é infintessimal. Nota que porque $\forall x\, \exists y x.y = 1 \in T$ temos elementos infinitos do $\mathbf{R}^*$ também.

Corolário. (Extensão por definicões.) Suponhamos que $\mathcal{L}$ é uma língua, Γ um conjunto das frases para $\mathcal{L}$. (i) Se $\phi(\bar{x})$ é um fórmula, sejam $\mathcal{L}' = \mathcal{L} \cup \{R_\phi\}$ e $\Gamma' = \Gamma \cup \{\forall \bar{x}\, (\phi(\bar{x}) \longleftrightarrow R_\phi(\bar{x}))\}$. Então para cada $\psi \in \mathcal{L}$ temos que $\Gamma' \models \psi$ se e só se $\Gamma \models \psi$. (ii) Se $\phi(\bar{x}, y)$ é um fórmula e $\Gamma \vdash \forall \bar{x}\, \exists! y\, \phi(\bar{x}, y)$, sejam $\mathcal{L}' = \mathcal{L} \cup \{f_\phi\}$ e $\Gamma' = \Gamma \cup \{\forall \bar{x}\, \forall y\, (\phi(\bar{x}, y) \longleftrightarrow f_\phi(\bar{x}) = y)\}$. Então para cada $\psi \in \mathcal{L}$ temos que $\Gamma' \models \psi$ se e só se $\Gamma \models \psi$.

Demonstração. "$\Longleftarrow$" é trivial em cada caso. "$\Longrightarrow$": Seja $\mathcal{M}$ um modelo para Γ. É trivial expandir $\mathcal{M}$ para uma estrutura $\mathcal{M}'$ para $\mathcal{L}'$ que é um modelo, no caso (i), para Γ' pelo interpretando R_ϕ ser o que ϕ escolha no $\mathcal{M}$, *i.e.*, pelo tomando $R_\phi^{\mathcal{M}'} = \{\bar{a} \in M \mid \mathcal{M} \models \phi(\bar{a})\}$, e, similarmente, no caso (ii) pelo tomando $f_\phi^{\mathcal{M}'}(\bar{a}) =$ o único b tal que $\mathcal{M} \models \phi(\bar{a}, b)$. Agora, se temos $\psi \in \mathcal{L}$ e $\Gamma' \models \psi$ então temos que $\mathcal{M}' \models \psi$ (pela teorema de saúde), logo $\mathcal{M} \models \psi$, logo $\Gamma \models \psi$ (pela teorema de completude).

Nota. Pelo corolário temos que podemos fazer uma seqüência finita das extensões duma língua por definicões.

6.3. Modelos de fragmentos da teoria dos conjuntos.

Nesta seção veremos que tem modelos de vários fragmentos de ZF. Isso é, que podemos mostrar dos axiomas de ZF que existem modelos destes fragmentos. Na verdade os modelos dos fragmentos que consideramos são razoávelmente fácil definir.

ZF$\setminus\{$Infinidade$\}$ (= ZF-I).
$(V_\omega, \in) \models$ ZF - I. Pode ver isso fácilmente, confirmando os axiomas um por um. (E é claro que $(V_\omega, \in) \not\models$ Infinidade.) Logo ZF$\vdash$ Con(ZF-I).

ZF$\setminus\{$Reposição ou coleção$\}$ (= Z).
Pode mostrar fácilmente, confirmando os axiomas um por um, que para cada ordinal λ do tipo limite tal que $\omega < \lambda$ temos $(V_\lambda, \in) \models$ Z. No outro lado, como vimos na §1.7, $(V_{\omega+\omega}, \in) \not\models$ "Coleção " porque, por exemplo, $\{\omega + n \mid n \in \omega\}$ é a imagem duma Função sobre o conjunto ω, mas não é um membro do $V_{\omega+\omega}$. (Ou porque tem mais que $\omega + \omega$ bem-ordems que são membros do $V_{\omega+\omega}$, então $V_{\omega+\omega} \not\models \Phi$ se Φ é a teorema que fala que cada bem-ordem é isomorfico para um ordinal numa moda que preserva a ordem.) (Logo ZF$\vdash$ Con(Z).)

ZF$\setminus\{$Conjuntos de potência$\}$ (= ZF-P).
Se κ é um cardinal regular seja $H_\kappa = \{x \mid \overline{\overline{\mathrm{FT}(x)}} < \kappa\}$. De novo, pode confimar que $H_\kappa \models$ ZF-P. Nota que $H_{\omega_1} \not\models$ "Conjuntos de potência" porque, por exemplo, $V_{\omega+1} = \mathcal{P}(V_\omega) \notin H_{\omega_1}$ (equivalentemente, $V_{\omega+2} \not\subseteq H_{\omega_1}$). (Logo ZF$\vdash$ Con(ZF-P).)

Pode perguntar se tem modelos de outros fragmentos de ZF. Já vimos nos exercícios 11, 13 e 14 do capítulo 1 várias dependencias entre axiomas, e este reduze o número das perguntas interessantes. Todavia, ainda podemos perguntar se existem modelos de ZF$\setminus${Fundação}, e mesmo se existem modelos de todo de ZF. Embora na proxima seção mostraramos que não podemos demonstrar que existem tais modelos como uma conseqüência da teorema de incompletude.

6.4. Teorema de incompletude.

A *teorema de incompletude*, tanto quanto a teorema de completude, é uma teorema geral sobre coleções de frases numa língua da ordem primeira. Aplica para uma variedade ampla de coleções de frases (ou *teorias*) e não tem nada a ver especificamente com a teoria dos conjuntos (além de, com certeza, ZF sendo um destas coleções. outros).

Teorema de incompletude. (Gödel, 1931) Se T é uma teoria *razoável* (numa língua $\mathcal{L}$), então $T \nvdash \text{Con}(T)$.

Nota lingüística. O nome da teorema de incompletude vem do fato que mostra que T é uma teoria *incompleto*, isso é que não tem a propreidade que ou demonstra ϕ ou demonstra $\neg\phi$ para todas frases ϕ no $\mathcal{L}$. Na contramão, a teorema de completude tem tal nome porque mostra que dedução na l'ogica da primeira ordem é completo no sentido que se ϕ é verdadeiro no cada modelo do T, então tem um derivação de ϕ do T na lógica da primeira ordem. Então, apesar de soar um pouco estranho talvez, não tem problemas nenhums falar, por exemplo, que a teorema de completude e a teorema de incompletude são verdadeiras para uma teoria T.

Razoável aqui quer dizer que: (a) podemos exprimir Con(T) no $\mathcal{L}$, (b) T é consistente, (c) podemos fazer bastante combinatoria no T para codificar as manipulações de lógica dentro de T e decodificâ-los, e (d) T é recursivo – devo explicar que este quer dizer.

Precisamos de (a) porque T só pode demonstra frases no $\mathcal{L}$, logo sem (a) a conclusão da teorema seria incomprehensível. Também precisamos de (b) para esperar mostrar a teorema porque se T não é consistente temos que $T \vdash \bot$, e, então T demonstra qualquer frase. Especificamente, $T \vdash \text{Con}(T)$. Explicamos (c) e (d) mais completamente abaixo, mas esta formulação vaga de (c) jdá uma pista para como exprimir Con(T) no $\mathcal{L}$.

Exemplos de teorias 'razoáveis.' Se são consistentes, a coleção de todos os verdadeiros sobre $(\mathbf{N}, +, ., s, exp, 0, 1)$ e a aritmetica de Peano são razoáveis. Se são consistentes, ZF e ZF-I-P-Fundação são razoáveis. Muitas teorias de analyse onde tem a função de sine, e então pode definir os números naturais, são razoável se é consistente.

Explicação de (c) na definição de razoável. Se T é razoável podemos mostrar de T que podemos achar representações de várias coisas síntaticais sobre $\mathcal{L}$ e T pelo termos no $\mathcal{L}$: os símbolos do $\mathcal{L}$, os termos no $\mathcal{L}$, os fórmulas no $\mathcal{L}$ e as demonstrações do T no $\mathcal{L}$. Se a é um pedaço da sintaxe escrevemos $\#(a)$ para o termo que representa a. As vezes chamamos estes termos *códigos*.

Também, podemos achar um fórmula $Dem(x, y)$ e uma função definivel $Subst(x, y)$ no $\mathcal{L}$ tal que d é uma demonstração de ϕ do T se e só se $T \vdash Dem(\#(d), \#(\phi))$, e $\phi[a/x] = \psi$ se e só se $T \vdash Subst(\#(\phi), a) = \#(\psi)$.

Primeiro suponhamos que T é razoável neste sentido, e mostramos como demonstrar a teorema. Depois veremos como fazer a codificação para algumas teorias especificas.

Demonstração da teorema de incompletude. Observe que se $\phi(x)$ é um fórmula temos que $T\vdash$ "$Subst(\#(\phi), \#(\phi)) = \#(\psi)$" se $\psi = \phi[\#(\phi)/x]$, isto é, se ψ é o fórmula que ganhamos se substituimos o termo que representa ϕ se mesmo em vez do variável livre x do ϕ. Considere o fórmula $\neg\exists y\, Dem(y, Subst(z, z)), = \chi(z)$, vamos falar. Então, para qualquer fórmula ϕ, temos que $T\vdash \chi(\#(\phi))$ se e só se não existe um demonstração de $\phi(\#(\phi)$ do T. Logo, porque χ se mesmo é um fórmula, temos que $T\vdash \chi(\#(\chi))$ se e só se não existe um demonstração de $\chi(\#(\chi)$ do T.

Mas agora se $T\vdash \chi(\#(\chi))$ temos que d demonstra $\chi(\#(\chi))$ para alguma demonstração d, e então $T\vdash Dem(\#(d), \#(\chi(\#(\chi)))$. Logo $T\vdash \exists y Dem(y, \#(\chi(\#(\chi)))$. Logo $T\vdash \neg(\chi(\#(\chi)))$. Então T é inconsistente.

E se $T\vdash \neg(\chi(\#(\chi)))$ temos que $T\vdash \exists y Dem(y, \#(\chi(\#(\chi)))$. Assumindo que T é consistente existe uma demonstração d tal que $T\vdash Dem(\#(d), \#(\chi(\#(\chi)))$. Logo $T\vdash \chi(\#(\chi))$ e temos que T é inconsistente de novo.

Se escrevemos $\mathrm{Con}(T)$ para $\neg\exists y\, \mathrm{Dem}(\#(y), \#(z \neq z))$ e se formalizamos a argumentação dentro do T temos que $T\vdash \mathrm{Con}(T) \longrightarrow (\chi(\#(\chi))$. Logo $T\vdash \mathrm{Con}(T)$ implica $T\vdash (\chi(\#(\chi))$, e então T não é consistente. (Fim da demonstração da teorema.)

T deve ser recursivo porque precisamos ter que "d é uma demonstração de ϕ de T" e "$\phi[a/x] = \psi$" são recursivos, e então temos que existem fórmulas no $\mathcal{L}$ que definem *Dem* e *Subst*, e porque para fazer a formalização também precisamos saber que para asserções sobre demonstrações e substituções podemos usar os fórmulas no $\mathcal{L}$ para escrever frases equivalentes no $\mathcal{L}$.

Codificação.

Ainda ser feitos sobre minha explicação da teorema de incompletude:
- *Falar exactamente qual manipulações precisamos ter o poder fazer no (c).*
- *Explicar* como fazer *a formalização de argumentação dentro do T (em cima so falo que "pode").*
- *Explicar porque faço tudo essa codificação recursivamente/Explicar mas exactamente porque precisamos que T é recursivo.*
- *Dar referências. (G.Takeuti, Proof Theory, North Holland, 1969, pp. 73-81.)*

Seja $\mathcal{L} = \{f^i \mid i < \omega\} \cup \{R^i \mid i < \omega\} \cup \{=\}$. Porque fórmulas são fios finitos dos símbolos e demonstrações são arvores finitos dos fórmulas precisaramos que T dá para nós o poder manipular fios de codigos para símbolos e codigos para fios dos símbolos. Então uma parte da definição de "razoável" é que podemos *definir* funções f_n para cada $n < \omega$ e π^n_m para cada $m < n < \omega$ no $\mathcal{L}$ tal que podmemos mostrar do T que $\pi^n_m(f_n(x_0, \ldots, x_{n-1})) = x_m$. Então f_n funciona como se ele permite nós fazer "n-tuplos" e π^n_m funciona como se ele permite nós recobrir o m^o elemente dum "n-tuplo" para cada $n < \omega$ e $m < n$. Para evitar confusão é bom pedir que $\mathrm{rge}(f_n) \cap \mathrm{rge}(f_m) = \emptyset$ se $m \neq n$. *Preciso disso nesta presentação ou não?*

Definimos $\#(t)$, $\#(\phi)$ para termos t e fórmulas $\phi \in \mathcal{L}$ pela indução na estrutura do t, ϕ.

Então sejam $\langle t_i \mid i < \omega\rangle$ termos na língua $\mathcal{L}$. Sejam $\#(\&) = t_1$, $\#(\neg) = t_3$, $\#(\exists) = t_5$, $\#(() = t_7$,

$\#()) = t_9$, $\#(,) = t_{11}$ $\#(=) = t_{13}$, $\#(v_i) = t_{2i}$, $\#(f^i) = t_{4i+15}$, e $\#(R^i) = t_{4i+17}$ para $i < \omega$.

Já vimos que $\#(v_i) = t_{2i}$. Se $i < \omega$, f^i é um símbolo para uma função k-ária e $s_0, \ldots, s_{k-1}$ são termos no $\mathcal{L}$, temos que $\#(f^i(v_{j_0}, \ldots, v_{j_{k-1}})) = f_{k+3}(t_{4i+15}, t_7, \#(s_{2j_0}), \ldots, \#(s_{2j_{k-1}}), t_9)$.

Se $i < \omega$, R^i é um símbolo para uma relção k-ária e $s_0, \ldots, s_{k-1}$ são termos no $\mathcal{L}$ temos que $\#(R^i(v_{j_0}, \ldots, v_{j_{k-1}})) = f_{k+3}(t_{4i+17}, t_7, \#(s_{2j_0}), \ldots, \#(s_{2j_{k-1}}), t_9)$. Se ϕ é um fórmula temos que $\#(\neg\phi) = f_4(t_3, t_7, \#(\phi), t_9)$. Se ϕ e ψ são fórmulas temos que $\#(\phi \,\&\, \psi) = f_3(\#(\phi), t_1, \#(\psi))$. E se $\phi(x)$ é um fórmula com x um variável livre, temos que $\#(\exists x \phi(x)) = f_2(t_5, \#(\phi(x)))$.

Então para um fórmula $\phi \in \mathcal{L}$ temos $\#(\phi)$ é um termo de $\mathcal{L}$. Se d é uma demonstração de ϕ do T, então d é um arvore finito, então um fio dos fios, então podemos definir $\#(d)$, um termo no $\mathcal{L}$ também. *Hmmm. Nunca expliquei que são arvores (finitos), nem dei as ilustrações para derivação para mostrar que demonstrações são arvores.*

Exemplos. No ZF(−I−P−Fnd) podemos simplesmente usar $f_n(x_0, \ldots, x_{n-1}) = (x_0, \ldots, x_{n-1})$ e $t_i = i$ para $i < \omega$, porque se $x_0, \ldots, x_{n-1} \in V_\omega$ temos que $(x_0, \ldots, x_{n-1}) \in V_\omega$ também.

No aritmética de Peano temos que fazer um pouco mais. $f_n(x_0, \ldots, x_{n-1}) = \ldots$.
Deveria acabar com este parte da demonstração.

6.5. Aplições da teorema de incompletude para ZF.

Teorema. Se ZF é consistente não podemos demonstrar, apenas do ZF, que existe um modelo de ZF.

Demonstração. É fácil ver que ZF é "razoável" porque podemos fazer as manipulações dos fios finitos no ZF e os axiomas do ZF são um conjunto recursivo. Então a teorema é imediata da teorema de incompletude. (*Hmmm. Deveria explicar como os axiomas são um conjunto e, então podem ser recursivos ou não.*)

Teorema. ZF$\vdash$ Con(ZF$-\{$Fundação$\}$) $\longrightarrow$ Con(ZF).

Demonstração. Seja $\mathcal{U}$ um modelo de ZF$-\{$Fundação$\}$. Podemos construir a hierarquia dos V_αs sem usando fundação – lembrar que vimos depois a construção da hierarquia dos V_αs na §2.7 que o axioma de fundação é equivalente para falar que $\forall x\, \exists \alpha \in \mathrm{On}\ x \in V_\alpha$. Então, construir a hierarquia dentro do $\mathcal{U}$ e seja $\mathcal{V}$ o resultado. Usando o fato, que pode confirmir simplesmente pela indução na estrutura de fórmulas, que se $x \in \mathcal{V}$ e $\phi(y)$ é um fórmula, então $x \cap \{\, y \mid \phi(y) \,\} \cap \mathcal{V} = x \cap \{\, y \mid \phi^V(y) \,\} \cap \mathcal{U}$, onde $\phi^V(y)$ é ϕ com todos os quantificadores correndo sobre $\mathcal{V}$, podemos confirmar que $\mathcal{V} \models$ ZF. Então Con(ZF$-\{$Fundação$\}$) implica Con(ZF). Logo ZF$\vdash$ Con(ZF$-\{$Fundação$\}$) $\longrightarrow$ Con(ZF).

Corolário. Não podemos mostrar do ZF que existe um modelo do ZF$-\{$Fundação$\}$.

Demonstração. Imediato da teorema e da teorema de incompletude.

6.6. Construtabilidade e forçando. Agora podemos explicar mais exatamente o que quer dizer as observações no fim de §4.3, por exemplo, que não pode mostrar do ZF que AE é verdadeiro nem que não é verdadeiro.

Teorema. (Gödel, 1938) Con(ZF) $\Longrightarrow$ Con(ZF + AE + HCG).

Teorema. (Cohen, 1963) Con(ZF) $\Longrightarrow$ Con(ZF + $\neg$AE), e Con(ZF) $\Longrightarrow$ Con(ZF + AE + $2^{\aleph_0} = \aleph_{\alpha+1}$) para qualquer ordinal α.

Mas exprimindo coisas neste modo, como sobre consistência, talvez não dá uma impressão certa do material da teoria dos conjuntos em geral e destas teoremas especificamente. É melhor entender estas teoremas no mesmo modo que as demonstrações delas: como falandas que se temos um modelo em qual tal e tal coisas são verdadeiras, então podemos mudar para um outro modelo onde tal e tal outras coisas são verdadeiras. Isso é um exemplo de uma tema central na teoria dos conjuntos, porque a teoria se interesse, após das coisas inicias nos capítulos 1-4, nas relações entre modelos da teoria (do ZF) e nas coisas quem acontecem dentro coleções especificos dos modelos do ZF. (Embora, claro, inclusive se interesse nas propriedades de modelos especificos (coleções do tamanho um) e da coleção de todos modelos (as conseqüências síntaticas do ZF, pela a teorema do completude).) Este não deveria ser uma surpresa grande: a teoria dos grupos se interesse nas relacões entre grupos também com propriedades de coleções dos grupos, e a teoria dos espaços topologicos se interesse nas relações entre espaços também com propriedades de (coleções dos) espaços. Só tem que lembrar que nestes exemplos últimos os modelos das teorias são grupos e espaços respectivamente, enquanto no caso da teoria dos conjuntos os modelos não são chamados 'conjuntos' mas 'modelos da teoria dos conjuntos,' ou, como falamos na seção §1.4, 'universos' (modelos são universos porque se $\mathcal{M} \models$ ZF temos que $\mathcal{M} \models \forall x\, \exists \alpha \in \mathrm{On}^{\mathcal{M}}\ x \in V_\alpha^{\mathcal{M}}$).

Construtabilidade. A idéia inicial da demonstração da teorema de Gödel é parecida para a idéia da demonstraçao que damos no fim de §6.5 que se temos um modelo de ZF$-$Fundação podemos chegar num modelo de ZF. Este vez, começamos com qualquer modelo $\mathcal{M}$ de ZF e definimos dentro de $\mathcal{M}$ um modelo mas magro, L, com $L \subseteq \mathcal{M}$ e, neste caso, com do ZF + AE + HCG, $\mathrm{On}^L = \mathrm{On}^{\mathcal{M}}$. Fazemos isso pelo definindo L como um hierarquia, como V, mas nas niveis do tipo sucessor augmentando a coleção até este nivel só com subconjuntos definíveis dele em vez de todos os subconjuntos.

Definição. Pela recursão sobre $\mathrm{On}^{\mathcal{M}}$ define $L_0 = \emptyset$, $L_\lambda = \bigcup\{\, L_\alpha \mid \alpha < \lambda \,\}$ para ordinais λ do tipo limite, e $L_{\alpha+1} = \{\, x \subseteq L_\alpha \mid \exists \phi(y_0, \ldots, y_{n-1}, z) \in \mathrm{LST}$ tal que $x = \{\, a \mid \exists b_0, \ldots, b_{n-1} \in L_\alpha\ (L_\alpha, \in \cap (L_\alpha \times L_\alpha)) \models \phi(b_0, \ldots, b_{n-1}, a) \,\}\,\}$. Seja $L = \bigcup\{\, L_\alpha \mid \alpha \in \mathrm{On}^{\mathcal{M}} \,\}$.

A teorema de Gödel é, na verdade, que para qualquer $\mathcal{M}$ temos que $L \models$ ZF + AE + HCG. E além disso que se $\mathcal{M}$, $\mathcal{N}$ são modelos de ZF com $\mathrm{On}^{\mathcal{M}} \subseteq \mathrm{On}^{\mathcal{N}}$, temos que $L^{\mathcal{N}}_{\mathrm{On}^{\mathcal{M}}} = L^{\mathcal{M}}$, então, especificamente, $L \models V = L$. Mas a demonstração que o modelo L tem estas propriedades é mais súbtil. Para ver mais sobre isso veja capítulo 7.

Forçando. Para mostrar que podemos mudar dum modelo de ZF + AE + HCG para um modelo do ZF + AE em qual, por exemplo, HC fale usamos uma técnica, forçando, para expandir o modelo para chegar, neste caso, num modelo com mais subconjuntos de ω. A técnica é muito parecida para fazer uma extensão álgebraica para um campo na álgebra: fazemos um extensão formal pelo um não-conhecido, e depois tomamos um quociente. (No fato, pode mostrar que isso não é só uma analogia boa, mas tem um sentido técnico em qual forçando e fazendo extensões álgebraicas são instâncias da mesma construção categorica.)

Os livros de Kunen[1] e Kanamor[2] são do dois lugares ótimos para pegar mais informação sobre forçando, e sobre as proximas pasos na teoria dos conjuntos mais geralmente. *Talvez um cápitulo 8 destes notas também.*

6.7. Modelos de todo do ZF.

Notar que a conseqüência da teorema de incompletude no §6.5 não fala que não existem modelos de ZF, só que não pode mostrar dos axiomas de ZF sozinhos que existem modelos. Já vimos no §6.3 que $V_\lambda \models \mathrm{ZF} - \{\text{Coleção}\}$ para qualquer ordinal λ do tipo limite com $\omega < \lambda$ e que $V_\omega \models \mathrm{ZF} - \{\text{Infinidade}\}$. Pode confirmir pelas mesmas demonstrações juntos a seguinte.

Teorema. Se κ é um cardinal que é inacessível fortemente, temos $V_\kappa \models \mathrm{ZF}$.

Observação. (Paradoxo de Skolem). Se ZF é consistente pelo corolário ultimo na §6.2 ele tem um modelo, falamos $\mathcal{M}$, enumerável. Logo $\mathcal{P}(\omega)^{\mathcal{M}}$, $\omega_1^{\mathcal{M}}$, ... são enumeráveis. Isso não é um paradoxo na verdade porque apesar de podemos contar, por exemplo, $\mathcal{P}(\omega)^{\mathcal{M}}$ fora do modelo e ver que este conjunto, que é um conjunto de subconjuntos do ω é enumerável, (para "pessoas" "morando") dentro $\mathcal{M}$ não tem qualquer bijeção do ω para $\mathcal{P}(\omega)^{\mathcal{M}}$, e, logo, dentro do $\mathcal{M}$ não pode enumerar $\mathcal{P}(\omega)$.

Não obstante que, pela teorema de incompletude aplicada para a teoria ZF, não pode mostrar dos axiomas de ZF que existem cardinais que são inacessíveis fortementes, a afirmação que existem tais cardinais é uma afirmação interessante e as vezes útil sobre (modelos de) ZF. Embora que formalmente isso e suposições similares são fortelecendos do ZF, na *prática* – o punto o mais importante – não parece qualquer razão supor que são diferentes de, por exemplo, fortelecendo a teoria da aritmética de Peano com a suposição que esta teoria não é inconsistente. No contrário, na verdade, a exploração das suposições deste tipo forma uma parte muito produtiva da teoria dos conjuntos e, logo, da matemática. (Veja, particularmente, o livro de Kanamori.) Acabamos este capítulo com um exemplo deste fenômeno sobre exponenciação dos cardinais.

Definição. Para qualquer $\delta < \omega_1$, a declaração que um cardinal κ é $\kappa{+}\delta{+}1$-*forte* é um fortelecendo de falar que κ é inacessível fortemente e que κ é compacto fracamente. (Quer dizer que existe um injeção $i : V \longrightarrow \mathcal{M}$ tal que $\mathcal{M} \subseteq V$, $\mathrm{On}^{\mathcal{M}} = \mathrm{On}^V$, se $\phi(x) \in LTC$ e $a \in V$ temos que $V \models \phi(a)$ se é so se $\mathcal{M} \models \phi(i(a))$, $i(\alpha) = \alpha$ para cada $\alpha < \kappa$, $\kappa < i(\kappa)$ e $V_{\kappa+\delta+1} \subseteq \mathcal{M}$. Não deveria esperar entender agora porque este definição é mais ou menos natural, nem mesmo como formulá-la como uma suposição sobre conjuntos e não sobre classes como fizemos aqui. Veja o livro do Kanamori para estes detalhes.)

A razão para introduzuir a definição aqui é que podemos usá-la para dar a declaraç certa da teorema seguinte annunciada no fim da seção §4.4 – do qual a demonstração é uma raciocinação esperto que usa forçando.

Teorema. (Gitik-Magidor, 1989) Seja $\omega \leq \delta < \omega_1$. Con(ZF + AE + $\exists\kappa$ tal que κ é $\kappa+\delta+1$-forte) $\Longrightarrow$ Con(ZF + AE + $2^{\aleph_n} = \aleph_{n+1}$ para todos $n < \omega$, e $2^{\aleph_\omega} = \aleph_{\delta+1}$.)

[1] Ken Kunen, *Set theory: an introduction to independence proofs*, North-Holland, 1980. Não é ainda impresso, mas pode consultar uma cópia na biblioteca.

[2] Aki Kanamori, *The Higher Infinite*, Springer, 1996.

Bibliografia:

Need to rewrite this completely.

Infelizmente é difícil recomendar quaisquer livros em português para vocês. Há traduções dos livros de Halmos e Lifshutz. O de Halmos, enquanto na época (no inicio dos anos 60) não foi tão ruim, agora é muito antiquado. O de Lifshutz não serve.

Em inglês tem mais possibilidades. Entre elas eu aconselharia:

Keith Devlin, *Fundamentals of Contemporary Set Theory*, (Springer, 1979). (Acho muito bom sobre ordinais e cardinais, mas não tão bom, talvez, na parte da introdução dos axiomas.)
Herb Enderton, *Elements of Set Theory*, (Academic, 1977). (Bom, claro, mas talvez não muito vivaz.)
Andras Hajnal e Peter Hamburger, *Set Theory*. (Cambridge University Press, LMS Lecture Notes Series, vol. 48, 1999). (Claro e também interessante.)
Judy Roitman, *Introduction to Modern Set Theory*. (Wiley, 1990) (Também uma boa escolha.)

Tenho uma fotocópia do livro de Devlin que vocês podem usar e uma cópia, que botarei na biblioteca, do livro de Hamburger e Hajnal deverá chegar logo – espero no fim de semana.

Tem na biblioteca, também, uma ótima introducão para lógica matemática–para mim a melhor,

Dirk van Dalen, *Logic and Structure*, (Springer, 4^o ed. 1996?). (Ótimo. Muito interessante em se mesmo, e boa para clarificar as coisas em (5) em cima sobre quais só teremos tempo de tocar levemente.)

Kunen, Kanamori, Kechris,. . .