PUC-Rio - Certificação Digital Nº 0510534/CA

2
A Teoria de Conjuntos - Preliminares

Esse capítulo se propõe a apresentar de maneira breve os resultados da teoria de conjuntos que serão utilizados nos capítulos subseqüentes. Começamos definindo as teorias que serão discutidas à frente, fundamentadas em dois conjuntos distintos de sentenças, os axiomas de Zermelo-Fraenkel e os axiomas de Peano, seguimos estabelecendo uma equivalência entre os axiomas de Peano e SF, a teoria composta pelos axiomas de ZF mais a negação do axioma do Infinito e tecemos um breve comentário sobre a existência de modelos não-*standard* para a Aritmética de Peano. Por fim, definimos consistência e citamos os Teoremas de Incompletude de Gödel, fundamentais para a compreensão dos resultados apresentados nos capítulos subseqüentes.

2.1
Os axiomas de Zermelo Fraenkel

Oito anos depois de Hilbert enunciar seus famosos 23 problemas no Congresso Internacional de Matemática, Zermelo publicaria sua primeira tentativa na axiomatização da teoria de conjuntos, que mais tarde seria aperfeiçoada por Skolem e Fraenkel, dando origem ao que hoje conhecemos como o sistema axiomático de Zermelo Fraenkel (**ZF**).

Há mais de uma maneira de descrever ZF, todas equivalentes. Aqui apresentaremos uma delas:

1. Extensão: $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$.

2. Separação: $(\exists z \forall x (\phi(x) \rightarrow x \in z)) \rightarrow (\exists y \forall x (x \in y \leftrightarrow \phi(x)))$.

   Com o axioma 2, definimos o conjunto $\{x : \phi(x)\}$, dos elementos que satisfazem $\phi(x)$, com a sentença $\forall x (x \in \{x : \phi(x)\} \leftrightarrow \phi(x))$. Note que, definido dessa maneira, nem sempre o conjunto $\{x : \phi(x)\}$ existe. No entanto, dado um conjunto A, sempre existe o conjunto $\{x \in A : \phi(x)\}$, definido por $\forall y (y \in \{x \in A : \phi(x)\} \leftrightarrow (y \in A) \wedge \phi(y))$.

   Definimos também o conjunto vazio, $\emptyset$, pela sentença $\{x : x \neq x\}$ e a interseção $x \cap y$ como $\{z \in x : z \in y\}$.

Note que o Axioma da Separação, assim como o axioma da Substituição, representa um esquema infinito de axiomas, com um axioma para cada fórmula de primeira ordem ϕ.

3. Par: $\forall x\, \forall y\, \exists z\, (x \in z \wedge y \in z)$.

   Com o axioma do Par e Separação garantimos a existência, para a e b dados, dos conjuntos $\{a\}$ e $\{a, b\}$.

4. União: $\forall x\, \exists y\, \forall z (z \in y \leftrightarrow \exists w((z \in w) \wedge (w \in x)))$.

   Com o axioma 4 podemos definir $\bigcup x$, como $\{y : \exists z \in x(y \in z)\}$. Em particular, a notação usual $x \cup y$ nada mais é que $\bigcup\{x, y\}$.

5. Potência: $\forall x \exists y \forall z (z \subseteq x \rightarrow z \in y)$.

   Aqui a relação $y \subseteq x$ é definida por $\forall w((w \in y) \rightarrow (w \in x))$ e, no contexto do axioma 5, podemos definir $\mathcal{P}(x)$, o conjunto das partes de x, por $\{y : y \subseteq x\}$.

6. Substituição: $\forall x \exists w \forall z (z \in w \leftrightarrow (\exists y \in x(z = F(y))))$.

   Aqui notamos $F(x)$ como o único y tal que $\phi(x, y)$, para uma dada fórmula ϕ da linguagem.

7. Infinito: $\exists x((x \neq \emptyset) \wedge (\forall y(y \in x) \rightarrow (y \cup \{y\} \in x)))$.

8. Fundação: $\forall x((x \neq \emptyset) \rightarrow (\exists y \in x \forall z \in y(z \notin x)))$.

   Os oito axiomas acima descritos representam ZF. Os axiomas de ZF mais o axioma da escolha (**ZFC**) formam o sistema axiomático padrão para a matemática desenvolvida nos dias de hoje e, salvo disposição em contrário, qualquer afirmação feita sobre a demonstração ou as conseqüências de um determinado teorema pressupõe que as mesmas se dão no contexto de ZFC.

9. Escolha: $\forall a((\emptyset \notin a) \wedge (\forall x, y \in a\ (x \neq y \rightarrow x \cap y = \emptyset)) \rightarrow \exists b(\forall w \in a\, \exists z(b \cap w = \{z\})))$

   O axioma da Escolha afirma que dado um conjunto arbitrário a de conjuntos não vazios, distintos dois a dois, existe pelo menos um conjunto b que contém exatamente um elemento em comum com cada um dos conjuntos de a. A importância do axioma da escolha (e seus equivalentes) não será discutida em profundidade nesse trabalho e o leitor interessado deve buscar em (8).

PUC-Rio - Certificação Digital Nº 0510534/CA

2.2 A Aritmética de Peano

Os axiomas de Peano são um conjunto de axiomas de segunda ordem propostos por Giuseppe Peano no final do século XIX em seu *Arithmetices principia, nova methodo exposita* que determinam toda a teoria da aritmética. Tradicionalmente, ao estudar lógica, é comum trabalhar com os axiomas de Peano em lógica de primeira ordem, com o axioma de indução de segunda ordem sendo substituído por um esquema infinito de axiomas de indução em primeira ordem. A esse sistema de axiomas de primeira ordem é dado o nome de Aritmética de Peano (PA).

Nesse trabalho nós trataremos de resultados e demonstrações em PA, evitando sempre que possível sobrecarregar o texto com a notação lógica usual. Veremos em seguida em que contexto essa prática não fere o rigor proposto.

A aritmética de Peano é a teoria de primeira ordem da linguagem da aritmética $\mathfrak{L} = \{+, \cdot, <, 0, 1\}$ que consiste nos seguintes axiomas:

1. $\forall x(x + 1 \neq 0)$
2. $\forall x \forall y(x + 1 = y + 1) \rightarrow (x = y)$
3. $\forall \boldsymbol{y}(\phi(0, \boldsymbol{y}) \wedge \forall x(\phi(x, \boldsymbol{y}) \rightarrow \phi(x + 1, \boldsymbol{y}))) \rightarrow \forall z(\phi(z, \boldsymbol{y}))$
4. $\forall x \forall y(x + 0 = x) \wedge (x + (y + 1) = (x + y) + 1)$
5. $\forall x \forall y(x \cdot 0 = 0) \wedge (x \cdot (y + 1) = x \cdot y + x)$
6. $\forall x \forall y((\neg(x < 0)) \wedge (x < (y + 1) \leftrightarrow ((x < y) \vee (x = y))))$.

Note que 3 é o esquema de indução para fórmulas de primeira ordem $\phi(x, \boldsymbol{y})$ citado anteriormente, onde $\boldsymbol{y} = y_1, y_2, \ldots, y_n$ para algum n, ao passo que os axiomas 4, 5 e 6 são, respectivamente, as definições recursivas das operações $+$, $\cdot$ e da relação $<$. Com as definições *standard* de $\mathbb{N}$ e da função s definida por $s(x) = x + 1$ é possível construir as operações $+, \cdot$ e $<$. Isso não significa, no entanto, que $+$ e $\cdot$ sejam desnecessários. É fácil construir modelos para a linguagem $\{s, 0, 1\}$ que satisfaçam a versão natural dos axiomas de Peano para essa linguagem, mas que não admitam, uma operação $+$ que satisfaça o axioma 4. Por isso, para axiomatizar a aritmética em lógica de primeira ordem, precisamos ter na linguagem original os símbolos $+$ e $\cdot$. Por outro lado, o símbolo $<$ não é estritamente necessário, pois sempre podemos defini-lo com a sentença

$$\forall x \forall y(x < y) \leftrightarrow \exists z((z \neq 0) \wedge (x + z = y)).$$

PUC-Rio - Certificação Digital Nº 0510534/CA

2.3
O sistema SF e sua correspondência com PA

É freqüente associarmos os teoremas de PA com a "matemática finitista", o mundo onde residem os teoremas matemáticos que podem ser formulados em $\{+, \cdot, <, 0, 1\}$ e cuja prova não requer essencialmente o uso ou a noção de conjunto infinito.

Por muito tempo acreditou-se que PA continha uma axiomatização do conjunto de todas as *verdades* sobre números naturais e conjuntos finitos até que, em 1931, Gödel provou os Teoremas de Incompletude, que veremos na seção 2.5.

Em muitas das demonstrações presentes nesse trabalho, nos utilizamos do fato que, para afirmações sobre números naturais, PA é equivalente a SF, a teoria obtida quando tomamos os axiomas de ZF e substituindo o axioma do Infinito por sua negação.

7b. Finitude: $\nexists x((x \neq \emptyset) \wedge (\forall y((y \in x) \rightarrow (y \cup \{y\} \in x))))$.

O único dos axiomas apresentados para ZF que afirma algo sobre a existência de conjuntos é o axioma do Infinito e, ao negá-lo, damos margem para a existência de um modelo vazio de SF. Para evitar isso, acrescentamos também o axioma do Vazio.

7c. Vazio: $\exists x(x = \{y : y \neq y\})$.

Uma vez estabelecida a equivalência entre as teorias, torna-se possível demonstrar resultados em PA, realizando todo o trabalho de prova em SF e em seguida lançando mão dessa correspondência. Um fato importante desse processo, mas que requer encodificação para ser demonstrado, é o lema que segue:

Lema 1. *O símbolo $\in$, definido por*

$$k \in n \leftrightarrow \text{o } k\text{-ésimo dígito binário de } n \text{ é } 1.$$

pode ser definido usando apenas $0, 1, \cdot, +$.

Dessa maneira, se tomamos por exemplo o decimal 14, cuja expansão binária é `1110`, temos que $0 \notin 14$, $1 \in 14$, $2 \in 14$ e $3 \in 14$ e temos que $14 = \{1, 2, 3\} = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset\}, \emptyset\}\}$. Equivalentemente, vamos usar, sem demonstração, que as funções $\sigma_k : \mathbb{N} \rightarrow \{0, 1\}$ abaixo descritas podem ser definidas em PA.

PUC-Rio - Certificação Digital Nº 0510534/CA

$$\sigma_k(n) = \begin{cases} 1 & \text{se o } k\text{-ésimo dígito de } n \text{ em binário é } 1 \\ 0 & \text{caso contrário} \end{cases}$$

Um modelo natural para SF é V_ω, definido por

$$V_0 = \emptyset,\ V_{n+1} = \mathcal{P}(V_n) \text{ e } V_\omega = \bigcup_{n \in \mathbb{N}} V_n.$$

Note que isso é justamente a hierarquia de Zermelo, parando no primeiro caso ordinal limite. Assim, por exemplo, temos $V_0 = \emptyset$, $V_1 = \{\emptyset\}$, $V_2 = \{\emptyset, \{\emptyset\}\}$ e $V_3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$. É fácil ver, em ZF, que o conjunto infinito $V_\omega = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \{\{\{\emptyset\}\}\}, \ldots\}$ é, de fato, um modelo para SF. O que faremos agora é construir recursivamente uma função $f : \mathbb{N} \to V_\omega$ que faz corresponder biunivocamente um elemento de V_ω a um natural, da seguinte maneira:

$$f(n) = \{f(k) : \sigma_k(n) = 1\}$$

Assim, por exemplo, temos que $f(0) = \emptyset$, $f(1) = \{\emptyset\}$, $f(2) = \{\{\emptyset\}\}$ e $f(3) = \{\{\emptyset\}, \emptyset\}$. Segue que a teoria PA + $\in$ satisfaz todos os axiomas de SF, fato que não demonstraremos aqui. Em particular, usando a relação $\in$, todas as construções da teoria de conjuntos podem ser feitas em PA.

2.4 Modelos não-*standard* para a Aritmética do Peano

Na teoria de modelos, um modelo não-*standard* é um modelo não-isomorfo ao modelo *standard* cujo conjunto subjacente é uma extensão do apresentado pelo modelo *standard*. Pela definição de modelo, as verdades demonstráveis na teoria serão verdade em ambos os modelos, mas frases verdadeiras no modelo *standard* podem não ser verdade no modelo não-*standard*.

A existência de modelos não-*standard* para a Aritmética de Peano em primeira ordem mostra que esse sistema é de fato mais fraco que o sistema análogo em segunda ordem, uma vez que o único modelo para o sistema de axiomas de segunda ordem de Peano, a menos de isomorfismos, é o conjunto dos números naturais.

Supondo que PA é consistente, o Teorema de Löwenheim-Skolem nos garante a existência de modelos não-enumeráveis de PA. Uma pergunta que podemos nos fazer é: serão isomorfos todos os modelos enumeráveis de PA?

Segue que toda teoria consistente e não completa T que não admita modelos finitos terá modelos enumeráveis não-isomorfos. Seja A uma sentença na

PUC-Rio - Certificação Digital Nº 0510534/CA

linguagem de T. Se T não demonstra A nem $\neg A$ então existe, por Löwenheim-Skolem, um modelo enumerável $\mathfrak{M}$ de $T \cup \{A\}$ e um modelo enumerável $\mathfrak{I}$ de $T \cup \{\neg A\}$. Ambos serão modelos de T e, claramente, não são isomorfos. Veremos adiante que, se PA é consistente, então PA não é completa e, portanto, admite modelos não-*standard* enumeráveis. Em (7) Boolos demonstra que os elementos do domínio de qualquer modelo $\mathfrak{M}$ não-*standard* de PA são linearmente ordenados por uma relação $<_{\mathfrak{M}}$. Essa ordenação terá um segmento inicial isomorfo ao conjunto do naturais, seguido por um conjunto ordenado de segmentos, cada segmento sendo isomorfo ao conjunto dos inteiros. Esse conjunto ordenado não admite um primeiro ou último membro e entre quaisquer dois desses segmentos haverá sempre um terceiro. Se o domínio de $\mathfrak{M}$ é enumerável, teremos uma quantidade enumerável desses segmentos e a relação de ordem entre eles será isomorfa à ordem usual no conjunto dos racionais.

Embora esses modelos não-*standard* satisfaçam toda a teoria *standard* de números, eles também podem satisfazer novas sentenças. É possível, por exemplo, construir um modelo não-*standard* da reta real, dando origem a um ramo da Análise chamado de Análise não-*standard* e as versões não-*standard* para a Teoria da Medida, Análise Funcional, etc.

2.5 Os Teoremas de Gödel

Provados em 1931, os teoremas de incompletude de Gödel demonstraram que a meta estabelecida por Hilbert para encontrar um sistema axiomático completo e consistente para toda a matemática era, de fato, impossível de ser atingida.

2.5.1 Consistência

Um sistema Σ de axiomas de uma determinada teoria é dito *consistente* se não existe uma demonstração do absurdo obtida através dos axiomas de Σ. Do mesmo modo, podemos nos perguntar se um determinado axioma A é consistente com o sistema Σ, o que é equivalente a dizer que não existe demonstração a partir de Σ para $\neg A$. Note, no entanto, que embora a não-consistência de A possa implicar em sua negação, a consistência não torna A uma conseqüência de Σ. Por exemplo, Gödel e Cohen demonstraram que nem o axioma da escolha nem a sua negação podem ser demonstrados em ZF (a menos que ZF seja inconsistente), ou seja, o axioma da escolha é *independente* dos demais axiomas.

PUC-Rio - Certificação Digital Nº 0510534/CA

2.5.2 Incompletude

Os teoremas que seguem são uma versão simplificada dos teoremas de Incompletude de Gödel. O resultado obtido por Gödel é mais geral, abrangendo uma classe de teorias contendo aritmética. Enunciamos aqui versões restritas a PA, que nos serão úteis mais tarde.

Teorema 2 (Primeiro Teorema de Incompletude em PA)**.** *Existe em PA uma sentença ϕ que afirma a sua própria improvabilidade. Supondo que PA seja consistente temos PA $\nvdash \phi$.*

Teorema 3 (Segundo Teorema de Incompletude em PA)**.** *Seja $Con_{\mathbf{PA}}$ a sentença que afirma que PA é consistente. Se PA é consistente então PA $\nvdash Con_{\mathbf{PA}}$.*

O fato de que uma dada teoria, se consistente, é incapaz de provar sua própria consistência devastou o Programa de Hilbert: não é possível formalizar a matemática em sua totalidade uma vez que qualquer tentativa de exibir tal formalismo é fadada a omitir alguma afirmação matematicamente verdadeira, como por exemplo a consistência desse formalismo. Lançaremos mão deste resultado para, nos capítulos 3 e 4, demonstrar que certos resultados não são demonstráveis em PA. Ao leitor interessado na demonstração da versão geral do Teorema 3, recomendamos (**?**).

PUC-Rio - Certificação Digital Nº 0510534/CA