30-8-2018 A. FISHER (1)

GEOMETRIA MAT 0230

INTRO.

Neste curso, apresentamos geometria de um ponto de vista axiomatica. Isto é, temos uma lista de frases chamadas axiomas; através das leis da lógica, provamos teoremas.

Axiomas e teoremas são ambos frases verdadeiras; a diferença é que as axiomas são o ponto da partida. Se não assumimos nada, não podemos provar nada. A coleção de todos as teoremas provadas (ou que teoricamente podem ser provadas) se chame a teoria determinada pela sistema de axiomas.

Uma outra maneira de apresentar a matematica e através da intuição, por exemplo utilizando desenhos para argumentar que algo e "obvio". Na matematica informal estes argumentos estão combinado com deduções, formulas, e contas baseado em axiomas que tambem estão considerado "obvios". A advantagem da matemática rigoroso (quer dizer, com tudo provado, dentro de uma sistema axiomatica) é:

1. evitamos o perigo de assumir ou provar coisas de fato não corretas;
2. clarificamos nosso entendimento e pensamento, ambos sobe o material do curso (no curso, geometria),

sobre a lógica, e sobre a matemática moderna.

A sistema de axiomas que encontramos é basicamente a devido ao Hilbert em 1899. A proposta dele é fornecer fundamentos rigorosos para a geometria do Euclides (~ 300 AC) que representou a primeira uso do método axiomático, mas com alguns falhas e com de mais recurso aos argumentos intuitivos.

Tambem encontramos no universo outros sistemas axiomaticas, viz:

1. A lógica matematica (que é um caso muito especial)
2. A teoria dos conjuntos;

3) A idea do espaço vetorial;

4) espaço vetorial com produto interno (produto escalar);

5) Os numeros naturais, racionais, e reais; o espaço $\mathbb{R}^n$. (o ~~espaço~~ Euclideano de dimensão n).

Podemos falar rigorosamente sobre 3, 4, ~~mas~~ os tratamentos de 1, 2, e 5 vão ser por necessidade (quer dizer, não podemos fazer tudo!!!) mais informal.

Sobre espaços vetorias veja as notas de aula.

Aí temos 3 pontos que queremos destacar:

I a idea de <u>independencia</u> dos axiomas.

<u>DEF</u>: Uma sist. de axiomas e <u>independente</u> se nenhum é uma consequencia dos demais.

<u>Exemplo</u>: os axiomas para o espaço vetrial V são:

V é um conjunto com 2 operações $+$ e $\cdot$ tal que:

(1) $\exists!\, \underline{0} : \underline{0} + \underline{v} = \underline{v}$] id (+)

(2) $\underline{v} + \underline{w} = \underline{w} + \underline{v}$] comm.

(3) $(\underline{v} + \underline{w}) + \underline{u} = \underline{v} + (\underline{w} + \underline{u})$] assoc (+)

(4) $1\, \underline{v} = \underline{v}$] id. ($\cdot$)

(5) $(a\, b)\, \underline{v} = a\,(b\underline{v})$] assoc ($\cdot$)

(6) $(a + b)\, \underline{v} = a\underline{v} + b\underline{v}$

(7) $a\,(\underline{v} + \underline{w}) = a\underline{v} + a\underline{w}$.

] distr

De fato, estes são independentes, mas muitos autores colocam um extra:

(8) $\exists! \, -\underline{v} \; : \; \underline{v} + (-\underline{v}) = \underline{0}$.

<u>Prop.</u> (8) é um teorema de (1)–(7). (é uma <u>consequência</u>) então (8) não é independente dos demais.

<u>Prova</u>: Dado $\underline{v} \in V$, definamos $\underline{u} = (-1)\underline{v}$. Afirmamos que $\underline{u} + \underline{v} = \underline{0}$:

$$\underline{u} + \underline{v} \overset{\text{Def.}}{=} -1(v) + v \overset{4}{=} (-1)v + 1(v)$$

$$\overset{\text{Distr.}}{=} (-1+1)\underline{v} \overset{\text{prop dos reais}}{=} 0\underline{v} = \underline{0}$$

OPA!
Esquecemos de provar primeiro que $0\underline{v} = \underline{v}$: pois

$$0\underline{v} + \underline{v} = 0\underline{v} + 1\underline{v} = (0+1)\underline{v} = 1\underline{v} = \underline{v}$$

Aí, $0\underline{v} + \underline{v} = \underline{v}$ e (1) $\Rightarrow$ $0\underline{v} = \underline{0}$ (pois é <u>única</u> tal vetor). //

II outro ponto a destacar é que um espaço vetorial de dimensão n tem as seguintes modelos:

(1) flechas

(2) $\mathbb{R}^n$

(3) $\mathbb{P}_{n-1}$ = {polinomios com coefficientes reais de grau $\leq n-1$}.

(Veja as Notas de Aula).

Todos estes 3 são isomorficos.

Def. Um modelo de uma ~~sistema~~ axiomática é um exemplo "concreto", i.e. apresentado utilizado uma outra sistema em que "acreditamos" (que aceitamos) por exemplo, a teoria dos conjuntos,

a teoria dos numeros reais,
ou a geometria Euclideana.

Isto é, temos que provar que um determinado modelo satisfaz as axiomas. Depois isto, todos os teoremas provados na teoria também valem para o modelo.

Exemplo: um espaço vetorial de dim n fornece um modelo para os axiomas (1)-(7) de um espaço vetorial. Eles são isomorficos sse (se e somente se) eles tem a mesma dimensão. (Veja as notas).

Def: 2 modelos de uma teoria (isto é, de uma sist. de axiomas) são isomorficos sse

∃ uma bijeção entre os conjuntos tal que os conceitos correspondem. (9)

III Um terceiro ponto é interessante: uma analogia. Uma base de um espaço vetorial é linearmente independente e gera o espaço. A analogia é com axiomas e teoremas: provar um teorema é análogo ao expressar um vetor no espaço com uma combinação linear dos vetores na base; ser independente é então análogo ao ser L.I.!

A geometria do Hilbert:

Temos um conjunto X chamado <u>o espaço</u>, com elementos chamado <u>pontos</u> e determinadas subconjuntos chamados <u>retas</u>, satisfazendo (alguns das) seguintes axiomas (cada vez, ~~determinamos quais!~~)

AXIOMAS DA INCIDENCIA:

$\boxed{I1}$ Dado $A \neq B$, $\exists! \; \ell \ni A, B$

(Para dois pontos distintos, existe uma unica reta que contem os dois; isto é, "2 pontos determinam uma reta").

$\boxed{I2}$ $\forall \ell \; \exists A \neq B : A, B \in \ell$

(cada reta contem pelo menos 2 ptos distintos).

$\boxed{I3}$ $\exists$ 3 pontos não-colineares.

(não todos contidos na mesma reta.)

Prop. 2 retas $l \neq \tilde{l}$ tem no máximo 1 pto em comum.

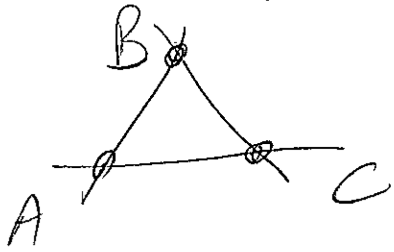
Prova: Se tem 2 ptos A, B em comum, por $\boxed{I1}$ $l = \tilde{l}$. //

Exemplo: um plano finito (número de pontos finito):

$X = \{A, B, C\}$

retas $\{A, B\}, \{B, C\}, \{A, C\}$.

exercício: verifique I1, 2, 3.

Desenho: 

(somente uma ajuda - não existem "segmentos" entre os pontos, não ~~faça~~ "parte do plano".)

Def. 2 retas $l, \tilde{l}$ são paralelos ($l \parallel \tilde{l}$) sse $l = \tilde{l}$ ou $l \cap \tilde{l} = \phi$

(identicos ou não tem nenhum ponto em comum).

$\boxed{P}$ (Axioma do Playfair) Dado l e A, $\exists$ no maximo uma reta $\tilde{l}$ com $A \in \tilde{l}$ e $l \parallel \tilde{l}$.

$\boxed{P'}$ neste caso, $\exists$ exatamente uma tal reta.

Def. Caso X satisfaz I1, 2, 3 e P' esta geometria e' um plano afim.

Prop As axiomas I1, 2, 3 e P são independentes.

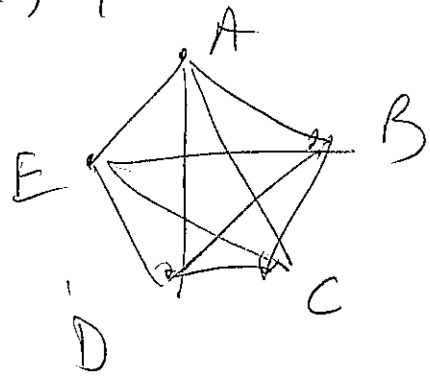
Prova. A estrategia

e de providencias modelos onde todos valem menos um. Daí, é impossível que esta seja uma consequência dos demais.

Isto foi feito na aula, mas damos uns exemplos:

exemplo: $X = \{A, B, C, D, E\}$ com retas todos os subconjuntos com 2 pontos. Aí, I1,2,3 valem mas não $\boxed{P}$.

Desenho:



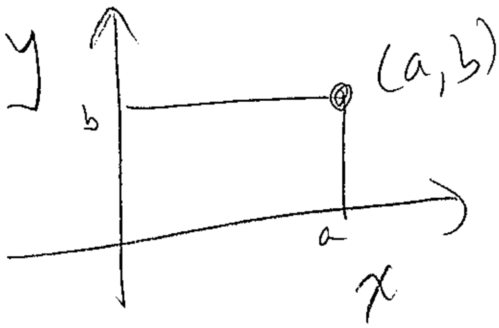
exemplo: $X = \{A, B, C\}$ retas $\{A,B\}$ $\{B,C\}$ $\{A,C\}$ $\{A\}$,
Aí valem I1, 3, P mas não vale I2.

(verifique isto, ~~e~~ ache exemplos para os outros).

Ex: $\mathbb{R}$ denote a coleção (conjunto) de numeros reais. OBS:
$(x \text{ é real}) \Leftrightarrow (x \in \mathbb{R})$.

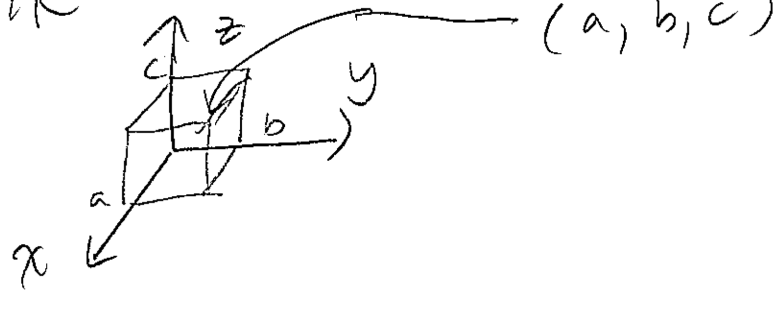
Defn: $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) : x_i \in \mathbb{R}\}$

$\mathbb{R}^2$ é o plano Euclideano, representamos geometicamete assim: o par ordenado (a,b) esta representado para um ponto (um lugar) no plano,



depois que temos escolhido (determinado) (1) o origin $(0,0)$ (2) os eixos x e y, e a orientação destas (o sentido positivo); eles estão colocado num angulo reto. (3) as unidades nos eixos: a distancia 1.

$\mathbb{R}^3$ é o espaço 3-dimensional:



verifique: (exercício) prova que: 15

$\mathbb{R}^2$ é um modelo para $\mathbb{I}$ 1, 2, 3

e $\boxed{\mathbb{P}'}$,

OBS: temos que especificar quais são as retas: o espaço é $X = \mathbb{R}^2$,

Def: uma reta é

$$\ell = \{(x,y) : ax + by + c = 0\}$$ tal que

$a, b, c \in \mathbb{R}$ e não ambos $a, b = 0$.

(Se a ou $b = 0$ temos uma reta ou vertical ou horizontal).

---

exercício: Ache todos as geometrias de incidência ($\mathbb{I}$ 1, 2, 3) possíveis para 4 pontos, até isomorfismo.

---

exercício: Provar: para uma geometria de incidência finita, # retas $\geq$ # ptos.

(...) : por

As Axiomas de "Betweenness"

Existe uma relação ternario no X (isto é, entre 3 pontos distintos) escrito $A * B * C$, "B é entre A e C" ou "B é no meio", satisfazendo:

$\boxed{B1}$ Se $A * B * C$ então A, B, C são colineares e distintos, e tambem valé $C * B * A$.

$\boxed{B2}$ Dado $A \neq B$, $\exists C$ com $A * B * C$.

$\boxed{B3}$ Dado A, B, C colinear, exatamente um está no meio.

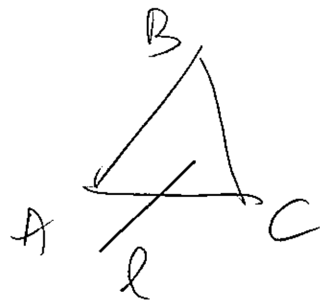
<u>Def</u>: O <u>segmento</u> $\overline{AB} = \{A, B\} \cup \{C : A * C * B\}$

<u>OBS</u>: $\overline{AB} = \overline{BA}$. (Porque??)

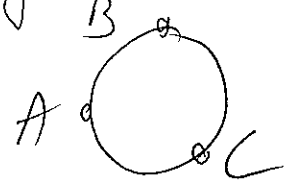
<u>Def</u>: Dado A, B, C não-colinear, o <u>triangulo</u> A, B, C, escrito ΔABC, é $\overline{AB} \cup \overline{BC} \cup \overline{AC}$.

$\boxed{B4}$ Dado A, B, C não-colinear, se uma reta l não contem A, B, C e encontra $\overline{AC}$,

então ele também encontra ou
$\overline{AB}$ ou $\overline{BC}$ mas não ambos.



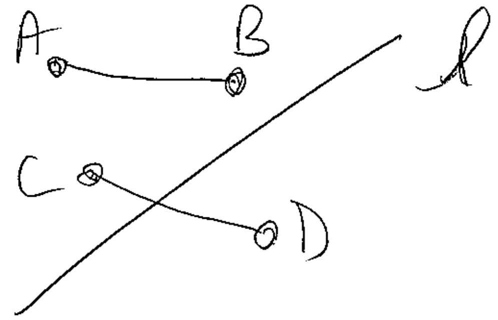
<u>Comentário</u>: $\boxed{B1}$ está dizendo que é
<u>"betweenness"</u> e não <u>ordem</u>. $\boxed{B3}$ está
dizendo que a geometria de uma reta
não é <u>"circular"</u>



$\boxed{B2}$ está
dizendo que uma reta pode ser extendido
(em ambos os sentidos), então contem
~~oo~~ pontos. $\boxed{B4}$ está dizendo que
uma reta separa um triangulo
~~com~~ um ponto num lado, os outros
2 no outro. <u>Esta idéia de "lado"</u>
agora vamos fazer rigoroso.

<u>Def</u> Dado uma reta l, definamos para $A, B \in X \setminus l$, $(A \sim B) \Leftrightarrow (\overline{AB} \cap l = \emptyset)$

Falamos que "A, B estão no mesmo lado do l" sse $A \sim B$, são nos lados opostos caso contrário, isto é, sse $\overline{AB} \cap l \neq \emptyset$.



$A \sim B$

$C \nsim D$.

<u>Prop.</u> $X \setminus l = S_1 \cup S_2$ com $S_1 \cap S_2 = \emptyset$, e com $A, B \in S_i \Leftrightarrow A \sim B$,

<u>Prova:</u> Primeiro passo:
$A \sim B$ define uma <u>relação de equivalência</u>, isto é:

(i) $A \sim A$ (reflexividade)

(ii) $A \sim B \Rightarrow B \sim A$ (simetria)

(iii) $(A \sim B) \cap (B \sim C) \Rightarrow (A \sim C)$ (transitividade).

Segundo passo:

Existem exatamente 2 classes de equivalencia.

Exercício: verifique (i) e (ii) (feito na aula).

verifique (iii) (feito na aula).

Para provar passo 2, verifique

(i) $\exists \geq 1$ classe

(ii) $\exists \geq 2$ classes

(iii) Não existe 3 classes.

Para prova (iii), prove:

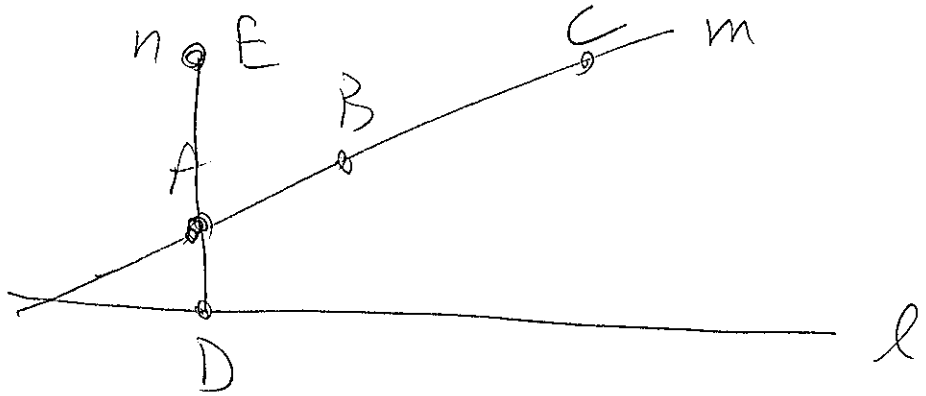
$$(A \nsim B) \wedge (B \nsim C) \Rightarrow (A \sim C).$$

Figura para transitividade:

Caso I: A, B, C não-colinear

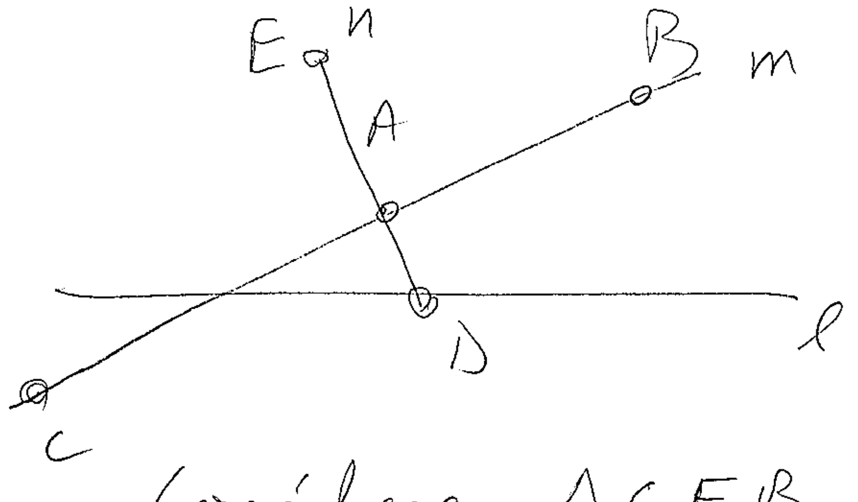
(prova direito do B4: verifique!)

Caso 2 : A, B, C ∈ m uma reta



(Considere o △AFC. Verifique primeiro que ℓ, m, n são retas distintas).

Para provar não tem 3 classes:



Considere △CEB.

Teoria dos Conjuntos: Uma Introdução. (1)

Começamos com os <u>Axiomas do CANTOR</u>. Vamos ver que isto nos leva para uma <u>contradição</u> (a sistema de axiomas é <u>inconsistente</u>), e temos que trocar para a sistema <u>Zermelo-Frankel</u>, que é consistente.

Na sistema do Cantor temos 2 ~~noções~~ basicos: <u>conjunto</u> e a relação de ser um elemento de, isto é, "$x \in A$" quer dizer que "x é um elemento do conjunto A".

<u>Def</u>: para 2 conjuntos, $A = B \iff (x \in A \iff x \in B)$. Isto é, dois conjuntos são iguais sse eles tem os mesmos elementos. Uma outra maneira a dizer isto é:

$$(A = B) \iff (\forall x,\ x \in A \text{ sse } x \in B).$$

1. Axioma de Extensão.

$(A = B) \iff (\forall x,\ x \in A \text{ sse } x \in B)$.

Depois temos a:

2. Axioma de Formação de conjuntos:

Se $S(x)$ e uma frase com x um parametro (= variavel livre) então existe um conjunto A com $(x \in A) \iff (S(x)$ e verdade.)

Escrevemos isto: $A = \{x : S(x)\}$

Variavel livre por exemplo "x e' um brasileiro" pode ser verificado, vai ser V ou F dependendo do x.

Na frase "$\forall x$, x e' brasileiro" x não e' variavel livre porque se a frase e V ou F e independente de x (e de fato falso). Neste caso a variável x é chamada ligada (em vez de livre).

<u>exemplo</u>: $x = x$ é sempre verdade (é uma tautologia). Tambem $(\forall x, x = x)$ é verdade (e tautologia) mas no primeiro x e livre, no segundo não (no primeiro, podemos testar, substituindo "$2 = 2$" ...; no segundo não faria sentido substituir e dizer "$\forall 2, 2 = 2$" pois "para todos os dois" não faz sentido...

<u>Prop.</u> Um conjunto ϕ (o conjunto vazio) existe, que não tem elementos; este conjunto é unico.

<u>Prova</u>: Definamos $\phi = \{x : x \neq x\}$. Então $(\forall x, x \notin \phi)$ é verdade. E' unico pois se A tem a mesma propriedade, eles tem os mesmos elementos (nenhum) e por <u>Ax 1</u> ~~são~~ iguais.

<u>exemplo</u>: $\{a, b\} = \{x : x = a \vee x = b\}$

<u>OBS</u>: $\{a, b\} = \{b, a\}$ por <u>Ax 1</u>.

<u>ex</u>: Dado 2 conjuntos A, B,

definamos $A \cup B = \{x : (x \in A) \vee (x \in B)\}$

$A \cap B = \{x : (x \in A) \wedge (x \in B)\}$

$A \subseteq B$ sse $(x \in A \Rightarrow x \in B)$

$A \setminus B = \{x : x \in A \wedge x \notin B\}$

(a <u>diferença</u> dos conjuntos)

Dado $A \subseteq X$, $A^c = X \setminus A$

o <u>complemento</u> de A (em X).

<u>Prop</u>: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(os dois <u>leis</u> <u>distributivos</u>.)

Para a prova,
Precisamos saber um pouco mais sobre a lógica matemática.
Dado frases P, Q, R que podem ser falsos ou verdades (F, V) creamos uma tabela de verdade:

Para uma frase só:

P	$\sim P$	$P \vee \sim P$	$P \wedge \sim P$
V	F	V	F
F	V	V	F

Para 2 frases P, Q:

P	Q	$P \Rightarrow Q$	$P \wedge Q$	$P \vee Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	F

Para 3:

P	Q	R	$P \wedge (Q \vee R)$	$(P \wedge Q) \vee (P \wedge R)$	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
V	V	V			V
V	V	F	(deve completar)		V
V	F	V			V
V	F	F			V
F	V	V			V
F	V	F			V
F	F	V			V
F	F	F			V

Isto mostra que

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R).$$

é um <u>lei distributivo</u> na lógica, e também temos:

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R),$$

São <u>tautologias</u>, frases que são verdade independente dos valores de verdade de P, Q e R individualmente.

Agora podemos provar a Proposição:

<u>Prova que</u> $A \cap (B \cup C) = (A \cap B) \cup (A \cup C)$

$$x \in A \cap (B \cup C) \iff x \in A \wedge (x \in B \cup C)$$

$$\iff \overset{P}{x \in A} \wedge (\overset{Q}{x \in B} \vee \overset{R}{x \in C})$$

$$\iff P \wedge (Q \vee R) \underset{\text{(lógica)}}{\iff} (P \wedge Q) \vee (P \wedge R)$$

$$\iff ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))$$

$$\iff (x \in (A \cap B)) \vee (x \in A \cap C)$$

$$\iff x \in ((A \cap B) \cup (A \cap C)) \quad //.$$

Exercício: Prova as leis do De Morgan: Dado $A, B \subseteq X$ então

$$(A \cup B)^c = A^c \cap B^c$$
$$(A \cap B)^c = A^c \cup B^c.$$

Prop. Dado um conjunto A,

$$\mathcal{P}(A) = \{X : X \subseteq A\}$$ existe.

Isto é a chamada conjunto potencia do A, o "conjunto de todos os conjuntos" de A,

exercício: Se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos.

O Paradoxo do Russel.

Começamos com uma pergunta: é possivel que existe um conjunto de eles mesmo?

É possível que existe um conjunto A tal que $A = \{A\}$?

No mínimo, um tal conjunto é esquisito. Vamos chamar "bons" todos os conjuntos que não ~~são~~ esquisitos neste sentido. Daí, utilizando o Axioma 2, formamo~~s~~ o conjunto

$V = \{x : x \notin x\}$, a coleção de todos os conjuntos bons.

<u>Pergunta</u>: $V \in V$ ou não? Isto é, se V mesmo é bom ou não?

<u>Resposta</u>: Se $V \in V$, então $V \notin V$. Mas, se $V \notin V$, então $V \in V$.

Daí, $V \in V \Longleftrightarrow V \notin V$, que é uma <u>contradição</u>.

Partindo dos Axiomas de Cantor, chegamos numa <u>contradição</u>. A sistema de axiomas é <u>inconsistente</u>. Temos que jogar isto fora, e começar de zero! com:

As axiomas <u>Zermelo-Frankel</u>,

(1) $\exists$ um conjunto,

(2) Dado um conjunto A, podemos forma subconjuntos:

$$\{x \in A : S(x)\}$$

(3) podemos forma uniões $A \cup B$

(4) podemos formar o conjunto potencia $\mathbb{P}(A)$.

(5) $\exists$ um conjunto infinito.

(tem mais alguns).

Para saber mais, veja por exemplo NAIVE SET THEORY do HALMOS, Observação: Se utilizamos Ax 1, 2, podemos formar $U = \{x : x = x\}$, isto é, o conjunto de todos os conjuntos, o chamado universo. Se U existe, nota que $U \in U$ (o universo não é bom!)

Também V acima pode ser formado, pois $V = \{x \in U : x \notin x\}$

De novo, nos perguntando se $V \in V$, temos

$$V \in V \Rightarrow (V \in U \wedge V \notin V)$$

$$V \notin V \Rightarrow (V \notin U \vee V \in V)$$

então $V \in V \Rightarrow (V \in U \wedge (V \notin U \vee V \in V))$

$$\Leftrightarrow \underbrace{(V \in U \wedge V \notin U)}_{\text{contradição}} \vee (V \in U \wedge V \in V)$$

$$\Leftrightarrow (V \in U) \wedge (V \in V)$$

que nos leva para $(V \in V) \Leftrightarrow (V \notin V)$ de novo //

Além do livro de Halmos, ~~veja~~ veja a referência no Wikipedia para "Tarski - Grothendieck Set Theory".