Introdução aos Métodos de Prova

Renata de Freitas e *Petrucio Viana*
IME-UFF, Niterói/RJ

II Colóquio de Matemática da Região Sul
UEL, Londrina/PR
24 a 28 de abril 2012

Sumário

- Provas servem, principalmente, para convencer os outros.
- Enunciados.
- Métodos de prova.
- Método da Suposição.
- Método da Contraposição.
- Método da Redução ao Absurdo.
- Método da Generalização.
- Método de Indução Matemática.

- Propriedades das provas.
- Alcance e limite dos métodos de prova.

Propriedades das provas

Uma prova de um enunciado verdadeiro é uma argumentação, na linguagem matemática, que justifica a sua veracidade.

Princípio da Razão Suficiente, para Matemática:
Em Matemática, todo enunciado deve ser provado.

Fato matemático $=$ enunciado $+$ prova

As provas devem ter algumas propriedades.

Riqueza de detalhes

Uma prova deve conter riqueza de detalhes suficiente para convencer à(s) pessoa(s) a quem a prova se destina.

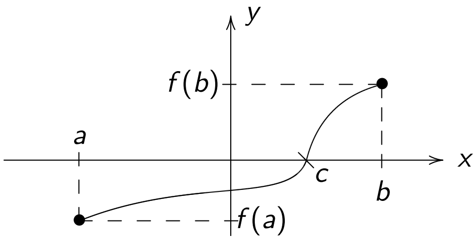
(c) **Todo espaço vetorial tem uma base.**
Prova:
Seja V um espaço vetorial.
Um conjunto B de vetores de V é uma base se, e somente se, é um linearmente independente maximal.
Seja C uma cadeia de conjuntos linearmente independentes de vetores de V.
É fácil verificar que $\bigcup C$ é linearmente independente.
Assim, pelo Lema de Zorn, V tem uma base. $\blacksquare$

Conhecimento prévio

(d) **Se** $f : [a, b] \to \mathbb{R}$ **é uma função contínua com** $f(a) < 0 < f(b)$**, então existe** $c \in [a, b]$ **tal que** $f(c) = 0$**.**

Prova:

Se for um curso de Cálculo, basta fazer uma figura.



∎

Se for um curso de Análise, não!!!

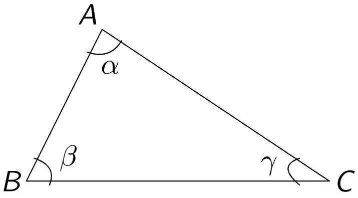
Conhecimento prévio

Riqueza de detalhes	$=$	Conhecimento prévio	$+$	Linguagem comum

Conhecimento prévio: expresso na forma de enunciados usados na elaboração da argumentação.

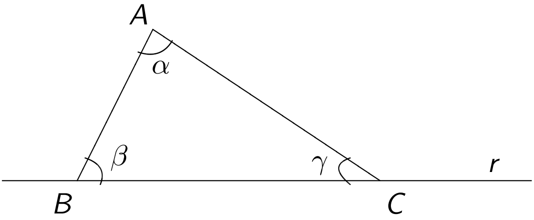
Conhecimento prévio

(e) **A soma dos ângulos internos de um triângulo é $180°$.**
Prova:
Seja um triâgulo de vértices A, B e C e ângulos internos respectivos α, β e γ.



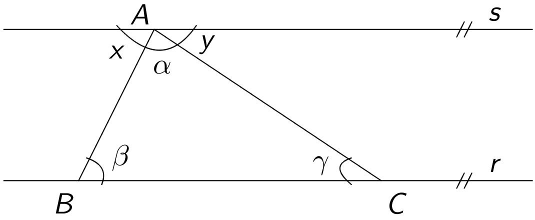
Conhecimento prévio

Seja r a reta que passa pelos vértices B e C e que contém o lado BC do triângulo.



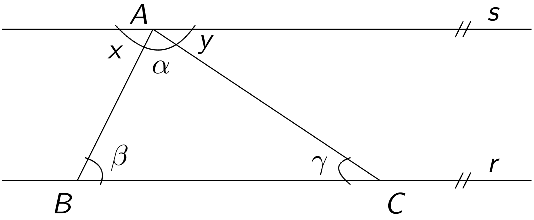
Conhecimento prévio

Traçamos pelo vértice A uma reta s paralela a r.
Sejam x e y os ângulos adjacentes a α.



Conhecimento prévio

Como os ângulos x e β são alternos internos, pelo Teorema de Tales, eles são iguais.
Analogamente, como os ângulos y e γ são alternos internos, pelo Teorema de Tales, eles são iguais.
Como $x + \alpha + y = 180°$, temos então $\alpha + \beta + \gamma = 180°$. ■



Conhecimento prévio

Principais enunciados usados:

1. **Dado um segmento de reta BC, existe uma reta que passa por B e C e que contém todos os pontos do segmento BC.**
2. AXIOMA DAS PARALELAS: **Dada uma reta r e um ponto A fora de r, existe uma única reta s que passa por A e é paralela a r.**
3. TEOREMA DE TALES: **Dadas duas retas paralelas r e s que passam, respectivamente, pelas extremidades de um segmento AB, os ângulos formados pelo segmento AB com as retas r e s e que estão em lados opostos em relação ao segmento AB são iguais.**
4. **O ângulo raso mede $180°$.**

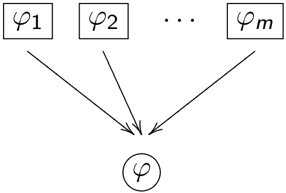
Premissas e conclusão

Os enunciados que compõem uma prova $\mathcal{P}$ são classificados em:

1. Premissas: utilizados na elaboração de $\mathcal{P}$ mas não justificados em $\mathcal{P}$.
   Axioma das paralelas.
   Teorema de Tales.
2. Intermediários: utilizados na elaboração de $\mathcal{P}$ e justificados em $\mathcal{P}$.
   Os ângulos x e β são iguais.
   $x + \alpha + \beta = 180°$.
3. Conclusão: é o enunciado que $\mathcal{P}$ justifica.
   A soma dos ângulos internos de um triângulo é $180°$.

Aplicando o PRS

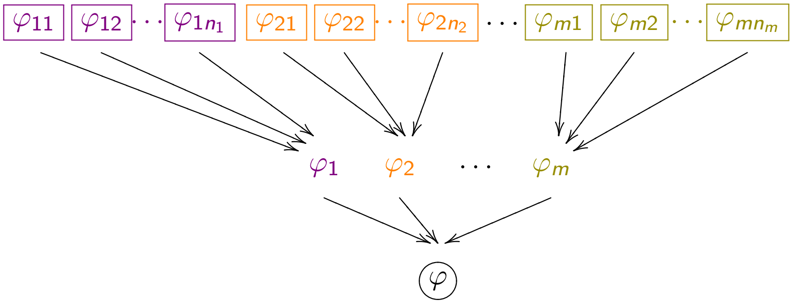
A prova de φ é baseada em premissas $\varphi_1, \ldots, \varphi_m$.



Para aceitar a verdade de $\varphi_1, \ldots, \varphi_m$ e a prova de φ, devemos ter provas de $\varphi_1, \ldots, \varphi_m$.

Aplicando o PRS

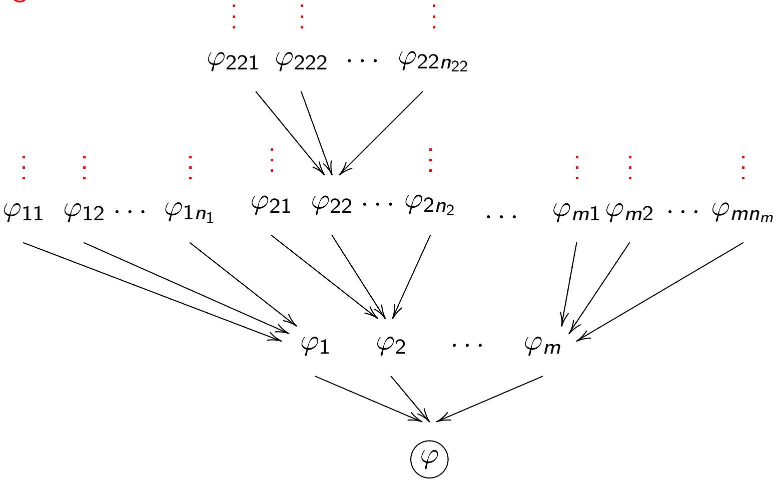
A prova de cada φ_i, $1 \leq i \leq m$, é baseada em $\varphi_{i1}, \ldots, \varphi_{in_i}$.



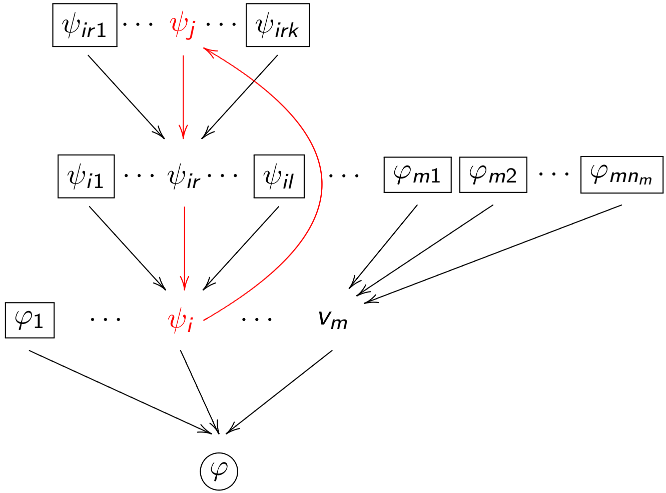
Para aceitar a verdade de $\varphi 11$, ..., $\varphi 1n_1$, $\varphi 21$, ..., $\varphi 2n_2$, ..., $\varphi m1$, ..., φ_{mn_m} e a prova de φ, devemos ter provas destas proposições, baseadas em outras premissas.

Estendendo este processo, duas coisas podem acontecer.

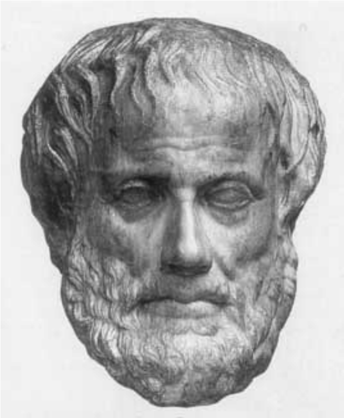
Regresso Infinito



Círculo Vicioso



Princípio básico das provas



Aristóteles (384 – 322 a.C.)

Provas não podem conter
nem regressos infinitos
nem círculos viciosos.

Evitando círculos viciosos

Nem sempre é fácil evitar círculos viciosos.

Todo natural maior ou igual a 2 **possui um fator primo.**

(Tentativa de) Prova:

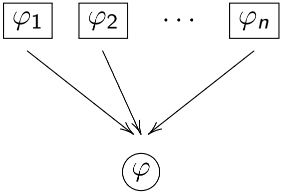
Seja m **um número natural maior ou igual a** 2**.**
Caso 1. Se m **é primo, como** m **é fator de si mesmo, ele possui um fator primo.**
Caso 2. Se m **não é primo, então** $m = ab$**, onde** a **e** b **são números naturais maiores ou iguais a** 2**. Como** a **possui um fator primo e todo fator de** a **é também fator de** m**, temos que** m **possui um fator primo.** $\blacksquare$

Identifique o círculo vicioso nesta (tentativa de) prova.

Estrutura das provas

Para evitar regressos infinitos, basta interromper o processo em algum momento.

Critério fundamental sobre estrutura de provas:
Toda prova é baseada em um certo número de enunciados aceitos sem justificativa, ou seja, aceitos sem prova.



Em resumo

- Provas são justificativas da veracidade de enunciados.
- Em Matemática, todo enunciado deve ser provado.
- Provas são baseadas em premissas, que não são provadas.
- Provas não contém círculos viciosos.

Voltando às nossas questões iniciais

- √ O que é uma prova?
- √ Por que se prova?
- ► É fácil reconhecer uma prova?
- ► É fácil fazer uma prova?
- ► Há algo que não se prova?
- √ Como fazer uma prova?

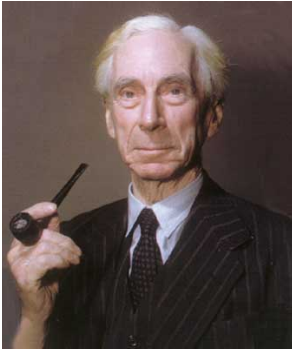
Propriedades lógicas das provas

- Provas são textos finitos.
- Provas são feitas passo a passo.

Completude

Problema 1

Existe um repertório completo de métodos de prova?



Russell

Peano

Hilbert

Whitehead, Ackermann, e outros,
propuseram um repertório, no início do século XIX.

Teorema da Completude (Gödel, 1930)

Este repertório de métodos de prova é tal que, dado qualquer conjunto de premissas, é possível provar qualquer conclusão que seja consequência destas premissas, usando os métodos de prova do repertório.

Kurt Gödel (1906 – 1978)

Regras de inferência

Este repertório é composto de uma quantidade finita de métodos da seguinte forma

$$
\begin{tikzcd}
\boxed{\varphi_1} \arrow[dr] & \boxed{\varphi_2} \arrow[d] & \cdots & \boxed{\varphi_m} \arrow[dll] \\
& \varphi & &
\end{tikzcd}
$$

Propriedades lógicas das provas

- Cada passo de uma prova é reconhecível.
- A prova, como um todo, é reconhecível.

Mas, se cada um usar os seus próprios conhecimentos prévios,
teremos dificuldades em reconhecer as provas,
mesmo se cada passo for reconhecível.

Método Axiomático

Teoria Matemática

$$=$$

Conceitos

$$+$$

Enunciados

Método Axiomático

Teoria Matemática Axiomatizada

$=$

Conceitos primitivos

$+$

Enunciados primitivos

$+$

Conceitos definidos

$+$

Enunciados provados

Método Axiomático

Axiomas

=

Lista de conhecimentos prévios
que todos reconhecem e usam.

Propriedades lógicas das provas

- Provas são feitas a partir de axiomas.
- Axiomas são reconhecíveis.
- Provas são corretas.

Incompletude

PROBLEMA 2 - megalomaníaco

Existe um conjunto de axiomas a partir do qual seja possível provar todos os enunciados (verdadeiros) da Matemática?

Incompletude

PROBLEMA 2 - pé no chão

Existe um conjunto de axiomas a partir do qual seja possível provar todos os enunciados (verdadeiros) de uma dada teoria matemática?

Incompletude

PROBLEMA 2 - pé no chão, caso particular

Existe um conjunto de axiomas a partir do qual seja possível provar todos os enunciados (verdadeiros) da Teoria dos Números?

Propriedades lógicas das provas

- Provas são textos finitos.
- Provas são feitas passo a passo.
- Provas são feitas a partir de axiomas.
- Axiomas são reconhecíveis.
- Provas são corretas.

- Provas são feitas a partir de axiomas.
- Axiomas são reconhecíveis.
- Provas são corretas.

Aritmética elementar de Peano, PA

- adição
- multiplicação
- ordem

dos naturais

Giuseppe Peano (1858 – 1932)

Aritmética elementar de Peano, PA

Os *símbolos* da *linguagem de* PA são:

- *Variáveis individuais:* $x_1, \ldots, x_n \ldots$;
- *Constante individual:* 0;
- *Símbolos para funções:* S, $+$ e $\times$;
- *Símbolos para relações:* $=$ e $<$.

Fórmulas de PA

A partir destes símbolos, podemos definir:

- *Numerais:* $0, S0, SS0, SSS0, SSSS0, \ldots$;
  O n-ésimo numeral é denotado $\mathbf{n}$.
- *Termos:* 0, x, St, $(t_1 + t_2)$, $(t_1 \times t_2)$;
- *Fórmulas atômicas:* $t_1 = t_2$ e $t_1 < t_2$;
- *Fórmulas:*

$$\begin{array}{rcl} \alpha & ::= & (t_1 = t_2) \mid (t_1 < t_2) \mid \\ & & (\neg\alpha) \mid (\alpha_1 \wedge \alpha_2) \mid (\alpha_1 \vee \alpha_2) \mid (\forall x \alpha) \mid (\exists x \alpha). \end{array}$$

Sentenças são fórmulas sem ocorrências de variáveis ou onde todas as variáveis estão quantificadas.

Exemplos

- $\exists w(x = SS0 \times w)$

  x é par

- $\exists w(x = z \times w)$

  z é fator de x

- $S0 < y \land \forall z(\exists w(y = z \times w) \rightarrow (z = S0) \lor (z = x))$

  y é primo

- $\forall x(S0 < x \rightarrow \exists y(y \text{ é fator de } x \land y \text{ é primo}))$

  Teorema Fundamental da Aritmética

Sentenças verdadeiras

- O *modelo padrão* de PA é a estrutura:

$$N = \langle \mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, S^{\mathbb{N}}, 0^{\mathbb{N}}, <^{\mathbb{N}} \rangle.$$

- Uma sentença é *verdadeira* se seu significado corresponde a uma verdade no modelo padrão.

Exemplo

(a) $0 = 0$ *é verdadeira;*

(b) $\forall x(x < Sx)$ *é verdadeira;*

(c) **Último Teorema de Fermat** *é verdadeira;*

(d) **Conjectura de Goldbach** *não sabemos se é verdadeira.*

- Há diversos *níveis* de verdade.

Axiomas de Peano

AP1. $\forall x \neg (Sx = 0)$;

AP2. $\forall x \forall y (Sx = Sy \rightarrow x = y)$;

AP3. $\forall x (x + 0 = x)$;

AP4. $\forall x \forall y (x + Sy = S(x + y))$;

AP5. $\forall x (x \times 0 = 0)$;

AP6. $\forall x \forall y (x \times Sy = (x \times y) + x)$;

AP7. $\forall x \neg (x < 0)$;

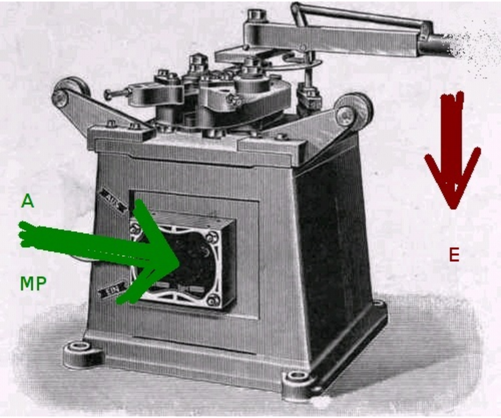
AP8. $\forall x \forall y (x < Sy \leftrightarrow (x < y) \vee (x = y))$;

AP9. Se $\alpha(x)$ é uma fórmula de PA, na qual a variável x não ocorre quantificada, então:

$$\alpha(0) \wedge (\forall x(\alpha(x) \rightarrow \alpha(Sx)) \rightarrow \forall x \alpha(x)).$$

$1^{\underline{o}}$ Teorema da Incompletude (Gödel, 1931)

Dado qualquer repertório de axiomas A e métodos de prova MP com o qual seja possível provar uma certa quantidade de aritmética, existe um enunciado verdadeiro E que não pode ser provado usando este repertório.

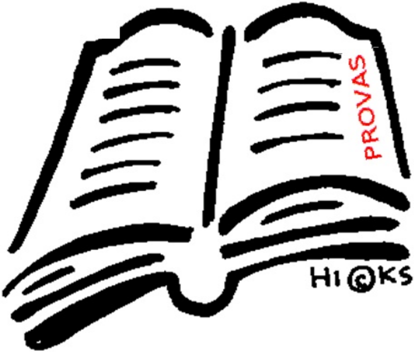


Questões

- $\surd$ O que é uma prova?
- $\surd$ Por que se prova?
- É fácil reconhecer uma prova?
- É fácil fazer uma prova?
- $\surd$ Há algo que não se prova?
- $\surd$ Como fazer uma prova?

Até a próxima!

Há muito mais sobre métodos de prova do que podemos abordar em um minicurso...



Esperamos encontrar vocês em outra oportunidade!

http://www.uff.br/grupodelogica