Matemática Discreta

Dirk Hofmann

Departamento de Matemática, Universidade de Aveiro
dirk@ua.pt, http://sweet.ua.pt/dirk/aulas/

Gabinete: 11.3.10

OT: Quinta, 14:00 – 15:00, Sala 11.2.24
Atendimento de dúvidas: Segunda, 13:30 – 14:30

Estratégias de Demonstração

Índice

Regras de dedução

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,
- utilizar o conhecimento que uma certa fórmula é válida.

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,
- utilizar o conhecimento que uma certa fórmula é válida.

Portanto:

De acordo, para cada símbolo lógico ($\wedge, \ldots, \Rightarrow, \ldots, \forall, \exists$), especificamos regras para

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,
- utilizar o conhecimento que uma certa fórmula é válida.

Portanto:

De acordo, para cada símbolo lógico ($\wedge, \ldots, \Rightarrow, \ldots, \forall, \exists$), especificamos regras para

- provar fórmulas com este símbolo (regras de *introdução*),

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,
- utilizar o conhecimento que uma certa fórmula é válida.

Portanto:

De acordo, para cada símbolo lógico ($\wedge$, ..., $\Rightarrow$, ..., $\forall$, $\exists$), especificamos regras para

- provar fórmulas com este símbolo (regras de *introdução*),
- utilizar a validade de fórmulas com este símbolo (regras de *eliminação*).

Considerações iniciais

O que precisamos?

Numa argumentação (= demonstração), temos que

- justificar a validade de fórmulas,
- utilizar o conhecimento que uma certa fórmula é válida.

Portanto:

De acordo, para cada símbolo lógico ($\wedge$, ..., $\Rightarrow$, ..., $\forall$, $\exists$), especificamos regras para

- provar fórmulas com este símbolo (regras de *introdução*),
- utilizar a validade de fórmulas com este símbolo (regras de *eliminação*).

Exemplo (Regras para "e")

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_\wedge \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_\wedge \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_\wedge$$

O caso de $\wedge$ ("e")

Regras para "e":

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_{\wedge} \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^{1}_{\wedge} \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^{2}_{\wedge}$$

Estas regras especificam o seguinte

O caso de $\wedge$ ("e")

Regras para "e":

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_\wedge \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_\wedge \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_\wedge$$

Estas regras especificam o seguinte

- Para provar a fórmula $\varphi \wedge \psi$, temos de provar a fórmula φ e a fórmula ψ.

O caso de $\wedge$ (“e”)

Regras para “e”:

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_\wedge \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_\wedge \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_\wedge$$

Estas regras especificam o seguinte

- Para provar a fórmula $\varphi \wedge \psi$, temos de provar a fórmula φ e a fórmula ψ.
- Se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula φ.

O caso de $\wedge$ ("e")

Regras para "e":

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_\wedge \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_\wedge \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_\wedge$$

Estas regras especificam o seguinte

- Para provar a fórmula $\varphi \wedge \psi$, temos de provar a fórmula φ e a fórmula ψ.
- Se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula φ.
- Igualmente, se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula ψ.

O caso de $\wedge$ (“e”)

Regras para “e”:

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_{\wedge} \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_{\wedge} \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_{\wedge}$$

Estas regras especificam o seguinte

- Para provar a fórmula $\varphi \wedge \psi$, temos de provar a fórmula φ e a fórmula ψ.
- Se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula φ.
- Igualmente, se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula ψ.

Nada surpreendente até aqui: “e” significa “e”.

O caso de $\wedge$ ("e")

Regras para "e":

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\,\mathsf{I}_{\wedge} \qquad \frac{\varphi \wedge \psi}{\varphi}\,\mathsf{E}^1_{\wedge} \qquad \frac{\varphi \wedge \psi}{\psi}\,\mathsf{E}^2_{\wedge}$$

Estas regras especificam o seguinte

- Para provar a fórmula $\varphi \wedge \psi$, temos de provar a fórmula φ e a fórmula ψ.
- Se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula φ.
- Igualmente, se sabemos que a fórmula $\varphi \wedge \psi$ é válida, podemos concluir a fórmula ψ.

Nada surpreendente até aqui: "e" significa "e". Mais interessantes são os casos dos quantificadores e em particular o caso da implicação.

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Mas como justificar uma implicação?

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Mas como justificar uma implicação? E como utilizar?

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Mas como justificar uma implicação? E como utilizar?

Utilizar é mais fácil ...

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Mas como justificar uma implicação? E como utilizar?

Utilizar é mais fácil ...

Formulês

$$\frac{\psi \Rightarrow \varphi \quad \psi}{\varphi}$$

Português

Sabemos que, se ψ então φ e sabemos ψ. Logo φ.

Sobre a implicação

A implicação

A implicação $\psi \Rightarrow \varphi$ expressa "Se ψ então φ".

Mas como justificar uma implicação? E como utilizar?

Utilizar é mais fácil ...

Formulês

$$\frac{\psi \Rightarrow \varphi \quad \psi}{\varphi}$$

Português

Sabemos que, se ψ então φ e sabemos ψ. Logo φ.

Exemplo

Sabemos

$$\mathsf{gato}(\mathsf{Tom}) \Rightarrow \mathsf{garra}(\mathsf{Tom}) \quad \text{e} \quad \mathsf{gato}(\mathsf{Tom}).$$

Logo garra(Tom).

A prova direta da implicação

A prova direta da implicação

Fórmulês

$$\dfrac{\boxed{\begin{matrix}\psi\\ \vdots\\ \varphi\end{matrix}}}{\psi \Rightarrow \varphi}$$

Português

Suponha[a] ψ. Então, ...(algo mais ou menos esperto) .... Logo, φ.

Portanto, $\psi \Rightarrow \varphi$ está provada. (E já não suponhamos ψ.)

[a] Notam o conjuntivo!!

A prova direta da implicação

Fórmulês

$$\dfrac{\boxed{\begin{array}{c}\psi\\ \vdots\\ \vdots\\ \varphi\end{array}}}{\psi \Rightarrow \varphi}$$

Português

Suponha[a] ψ. Então, ... (algo mais ou menos esperto) .... Logo, φ.

Portanto, $\psi \Rightarrow \varphi$ está provada. (E já não suponhamos ψ.)

[a] Notam o conjuntivo!!

A prova direta de $\psi \Rightarrow \varphi$ é um argumento hipotético: suponhamos (temporariamente) ψ até conseguimos deduzir φ, não afirmamos que ψ é válida (nem que é "razoável").

A prova direta da implicação

Fórmulês

$$\dfrac{\boxed{\begin{array}{c}\psi\\ \vdots\\ \varphi\end{array}}}{\psi \Rightarrow \varphi}$$

Português

$\boxed{\text{Suponha}^a\ \psi.\ \text{Então, \ldots (algo mais ou menos esperto) \ldots. Logo, } \varphi.}$

Portanto, $\psi \Rightarrow \varphi$ está provada. (E já não suponhamos ψ.)

[a] Notam o conjuntivo!!

A prova direta de $\psi \Rightarrow \varphi$ é um argumento hipotético: suponhamos (temporariamente) ψ até conseguimos deduzir φ, não afirmamos que ψ é válida (nem que é “razoável”).

Exemplo

Teorema. *Se o Porto ganha todos os jogos, então o Porto é campeão.*

Demonstração. Suponha que o Porto ganha todos os jogos. . . . □

Intermezzo: o quantificador $\exists$ (“existe”)

Intermezzo: o quantificador $\exists$ ("existe")

Como provar uma fórmula da forma $\exists x \ldots$?

Formulês

$$\frac{\begin{array}{c}\vdots \\ \psi\{t/x\}\end{array}}{\exists x\, \psi}$$

Português

... concluímos ψ com o termo t (tipicamente sem variáveis) em lugar da variável x.

Portanto, $\exists x\, \psi$ está provada.

Intermezzo: o quantificador $\exists$ (“existe”)

Como provar uma fórmula da forma $\exists x \ldots$?

Formulês

$$\dfrac{\begin{array}{c}\vdots\\ \psi\{t/x\}\end{array}}{\exists x\, \psi}$$

Português

... concluímos ψ com o termo t (tipicamente sem variáveis) em lugar da variável x.

Portanto, $\exists x\, \psi$ está provada.

Como utilizar uma fórmula da forma $\exists x \ldots$?

Formulês

$$\dfrac{\exists x\, \psi \qquad \boxed{\begin{array}{c}\psi\{x_0/x\}\\ \vdots\\ \varphi\end{array}}}{\varphi}$$

Português

Sabemos que $\exists x\, \psi$.

Seja x_0 um elemento tal que $\psi\{x_0/x\}$. ...(algo esperto) .... Logo, φ.

Portanto, φ está provada.

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n \; c = 2n.$$

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n \; c = 2n.$$

Teorema

Sejam a e b números inteiros: se a é par, então ab é par.

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n \; c = 2n.$$

Teorema

Sejam a e b números inteiros: se a é par, então ab é par.

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists n \; a = 2n$.

Portanto, a fórmula $\exists n \; ba = 2n$ está provada. $\square$

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n\; c = 2n.$$

Teorema

Sejam a e b números inteiros: se a é par, então ab é par.

$$(\exists n\; a = 2n) \implies (\exists n\; ba = 2n)$$

Demonstração.

Suponha que $\exists n\; a = 2n$. Seja k um número inteiro com $a = 2k$.

Portanto, a fórmula $\exists n\; ba = 2n$ está provada. $\square$

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n \; c = 2n.$$

Teorema

Sejam a e b números inteiros: se a é par, então ab é par.

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists n \; a = 2n$. Seja k um número inteiro com $a = 2k$. Portanto,

$$ba = b(2k) = 2(bk);$$

Portanto, a fórmula $\exists n \; ba = 2n$ está provada. $\square$

Um exemplo simples

Definição

Um número inteiro c é par quando é divisível por 2, ou seja,

$$\exists n \; c = 2n.$$

Teorema

Sejam a e b números inteiros: se a é par, então ab é par.

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists n \; a = 2n$. Seja k um número inteiro com $a = 2k$. Portanto,

$$ba = b(2k) = 2(bk);$$

ou seja $ba = 2n$ com $n = bk$. Portanto, a fórmula $\exists n \; ba = 2n$ está provada. $\square$

Ainda sobre a notação

Teorema

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists n \; a = 2n$. Seja k um número inteiro com $a = 2k$.

...

$\square$

Ainda sobre a notação

Teorema

$$(\exists n \; a = 2n) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists n \; a = 2n$. Seja k um número inteiro com $a = 2k$.

... $\square$

Nota

- As duas ocorrências de n são independentes (como são ligadas a quantificadores diferentes).

Ainda sobre a notação

Teorema

$$(\exists k \; a = 2k) \implies (\exists n \; ba = 2n)$$

Demonstração.

Suponha que $\exists k \; a = 2k$. Seja k um número inteiro com $a = 2k$.

. . . $\square$

Nota

- As duas ocorrências de n são independentes (como são ligadas a quantificadores diferentes).
- Por exemplo, podemos escrever k em lugar de n na primeira fórmula.

Ainda sobre a notação

Teorema

$$(\exists k\ a = 2k) \implies (\exists n\ ba = 2n)$$

Demonstração.

Suponha que existe um número inteiro k com $a = 2k$.

$\ldots$ $\square$

Nota

- As duas ocorrências de n são independentes (como são ligadas a quantificadores diferentes).
- Por exemplo, podemos escrever k em lugar de n na primeira fórmula.
- Portanto, podemos escrever a primeira linha da demonstração numa forma mais simples.

Intermezzo 2: o quantificador $\forall$ ("para todo")

Como provar uma fórmula da forma $\forall x \ldots$?

Formulês

$$\dfrac{\boxed{\begin{matrix} x \\ \vdots \\ \psi \end{matrix}}}{\forall x\, \psi}$$

Português

Seja[a] x. ...(algo esperto) .... Logo, ψ.

Portanto, $\forall x\, \psi$ está provada.

[a] Notam outra vez conjuntivo!!

Intermezzo 2: o quantificador $\forall$ ("para todo")

Como provar uma fórmula da forma $\forall x \ldots$?

Formulês

$$\frac{\boxed{\begin{array}{c} x \\ \vdots \\ \psi \end{array}}}{\forall x\, \psi}$$

Português

Seja[a] x. ...(algo esperto) .... Logo, ψ.

Portanto, $\forall x\, \psi$ está provada.

[a]Notam outra vez conjuntivo!!

Como utilizar uma fórmula da forma $\forall x \ldots$?

Formulês

$$\frac{\forall x\, \psi \qquad t \text{ um termo}}{\psi\{t/x\}}$$

Português

Sabemos que $\forall x\, \psi$. Em particular, $\psi\{t/x\}$.

Voltando ao exemplo

Teorema

Para todos os números inteiros a e b: se a é par, então ab é par.

$$\forall a, b\,((\exists n\ a = 2n) \implies (\exists n\ ba = 2n))$$

Voltando ao exemplo

Teorema

Para todos os números inteiros a e b: se a é par, então ab é par.

$$\forall a, b\,((\exists n\ a = 2n) \implies (\exists n\ ba = 2n))$$

Demonstração.

Sejam a, b números inteiros.

$\square$

Voltando ao exemplo

Teorema

Para todos os números inteiros a e b: se a é par, então ab é par.

$$\forall a, b\,((\exists n\ a = 2n) \implies (\exists n\ ba = 2n))$$

Demonstração.

Sejam a, b números inteiros.

Agora temos de provar a fórmula

$$(\exists n\ a = 2n) \implies (\exists n\ ba = 2n),$$

tratando a e b como *símbolos de constante* (tal como 2).

$\square$

Voltando ao exemplo

Teorema

Para todos os números inteiros a e b: se a é par, então ab é par.

$$\forall a, b\,((\exists n\; a = 2n) \implies (\exists n\; ba = 2n))$$

Demonstração.

Sejam a, b números inteiros.
Suponha que $\exists n\; a = 2n$. Seja k um número inteiro com $a = 2k$.
Portanto,

$$ba = b(2k) = 2(bk);$$

ou seja $b = 2n$ com $n = bk$. Portanto, a fórmula $\exists n\; ba = 2n$ está provada.

$\square$

Mais um exemplo

Recordamos

$(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$.

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\,((x\,R\,y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\,R\,z\} = \{z \in X \mid z\,R\,x\}$.

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\,((x\,R\,y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\,R\,z\} = \{z \in X \mid z\,R\,x\}$.

Demonstração.

Sejam $x, y \in X$.

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\, ((x \, R \, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x \, R \, z\} = \{z \in X \mid z \, R \, x\}$.

Demonstração.

Sejam $x, y \in X$.
Agora temos de provar:

$$((x \, R \, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\,((x\,R\,y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\,R\,z\} = \{z \in X \mid z\,R\,x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x\,R\,y$.

logo $[x] \cap [y] \neq \varnothing$.

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\, ((x\, R\, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\, R\, z\} = \{z \in X \mid z\, R\, x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x\, R\, y$. Então, $x \in [x]$ e $x \in [y]$, logo $[x] \cap [y] \neq \varnothing$.

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\, ((x \, R \, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x \, R \, z\} = \{z \in X \mid z \, R \, x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x \, R \, y$. Então, $x \in [x]$ e $x \in [y]$, portanto $x \in [x] \cap [y]$, logo $[x] \cap [y] \neq \varnothing$.

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\, ((x\, R\, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\, R\, z\} = \{z \in X \mid z\, R\, x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x\, R\, y$. Então, $x \in [x]$ e $x \in [y]$, portanto $x \in [x] \cap [y]$, logo $[x] \cap [y] \neq \varnothing$.

"$\Leftarrow$": Suponha que $[x] \cap [y] \neq \varnothing$;

$$x\, R\, y.$$

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y\,((x\,R\,y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x\,R\,z\} = \{z \in X \mid z\,R\,x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x\,R\,y$. Então, $x \in [x]$ e $x \in [y]$, portanto $x \in [x] \cap [y]$, logo $[x] \cap [y] \neq \varnothing$.

"$\Leftarrow$": Suponha que $[x] \cap [y] \neq \varnothing$; isto é, existe $z \in [x] \cap [y]$.

$$x\,R\,y.$$

$\square$

Mais um exemplo

Teorema

Seja R uma relação de equivalência num conjunto X. Então,

$$\forall x, y \, ((x \, R \, y) \Leftrightarrow [x] \cap [y] \neq \varnothing).$$

Recordamos: $[x] = \{z \in X \mid x \, R \, z\} = \{z \in X \mid z \, R \, x\}$.

Demonstração.

Sejam $x, y \in X$.

"$\Rightarrow$": Suponha que $x \, R \, y$. Então, $x \in [x]$ e $x \in [y]$, portanto $x \in [x] \cap [y]$, logo $[x] \cap [y] \neq \varnothing$.

"$\Leftarrow$": Suponha que $[x] \cap [y] \neq \varnothing$; isto é, existe $z \in [x] \cap [y]$. Portanto, $x \, R \, z$ e $z \, R \, y$, e, como R é transitiva, $x \, R \, y$.

$\square$

Ainda mais um exemplo "tolo"

Recordamos

$(\bot \Rightarrow p) \equiv \top$, ou seja, $\bot \Rightarrow p$ é verdadeira qualquer que seja p.

Ainda mais um exemplo "tolo"

Recordamos

$(\perp \Rightarrow p) \equiv \top$, ou seja, $\perp \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Ainda mais um exemplo "tolo"

Recordamos

$(\bot \Rightarrow p) \equiv \top$, ou seja, $\bot \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Ainda mais um exemplo "tolo"

Recordamos

$(\bot \Rightarrow p) \equiv \top$, ou seja, $\bot \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Teorema

Todos os unicórnios são brancos.

$$\forall x\,(\mathit{unicórnio}(x) \Rightarrow \mathit{branco}(x))$$

Ainda mais um exemplo “tolo”

Recordamos

$(\perp \Rightarrow p) \equiv \top$, ou seja, $\perp \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Teorema

Todos os unicórnios são brancos.

$$\forall x\,(\mathit{unicórnio}(x) \Rightarrow \mathit{branco}(x))$$

Demonstração.

Seja x .

$\square$

Ainda mais um exemplo "tolo"

Recordamos

$(\perp \Rightarrow p) \equiv \top$, ou seja, $\perp \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Teorema

Todos os unicórnios são brancos.

$$\forall x\,(\mathit{unicórnio}(x) \Rightarrow \mathit{branco}(x))$$

Demonstração.

Seja x um unicórnio.

$\square$

Ainda mais um exemplo “tolo”

Recordamos

$(\perp \Rightarrow p) \equiv \top$, ou seja, $\perp \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Teorema

Todos os unicórnios são brancos.

$$\forall x\, (\mathit{unic\acute{o}rnio}(x) \Rightarrow \mathit{branco}(x))$$

Demonstração.

Seja x um unicórnio. Mas não há unicórnios, temos uma contradição!! $\square$

Ainda mais um exemplo "tolo"

Recordamos

$(\perp \Rightarrow p) \equiv \top$, ou seja, $\perp \Rightarrow p$ é verdadeira qualquer que seja p. Portanto, se conseguimos deduzir uma contradição, podemos concluir qualquer afirmação.

Axioma

Não há unicórnios.

Teorema

Todos os unicórnios são brancos.

$$\forall x\,(\mathit{unicórnio}(x) \Rightarrow \mathit{branco}(x))$$

Demonstração.

Seja x um unicórnio. Mas não há unicórnios, temos uma contradição!! Logo, x é branco (do Porto, esperto, rico, gordo,...) $\square$

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar ($=$ não par) e b é ímpar, então ab é ímpar".

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar (= não par) e b é ímpar, então ab é ímpar".
Portanto, provamos a fórmula:

$$\forall a, b\,(((a \text{ é ímpar}) \wedge (b \text{ é ímpar})) \implies (ab \text{ é ímpar})).$$

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar (= não par) e b é ímpar, então ab é ímpar". Portanto, provamos a fórmula:

$$\forall a, b\,(((a \text{ é ímpar}) \wedge (b \text{ é ímpar})) \implies (ab \text{ é ímpar})).$$

Demonstração. Sejam a e b números

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar (= não par) e b é ímpar, então ab é ímpar".
Portanto, provamos a fórmula:

$$\forall a, b \, (((a \text{ é ímpar}) \wedge (b \text{ é ímpar})) \implies (ab \text{ é ímpar})).$$

Demonstração. Sejam a e b números ímpares.

ab é ímpar. $\square$

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar ($=$ não par) e b é ímpar, então ab é ímpar". Portanto, provamos a fórmula:

$$\forall a, b \, (((a \text{ é ímpar}) \wedge (b \text{ é ímpar})) \implies (ab \text{ é ímpar})).$$

Demonstração. Sejam a e b números ímpares. Isto é: existem números inteiros n e m com $a = 2n + 1$ e $b = 2m + 1$.

ab é ímpar. $\square$

Prova por contraposição

Aqui utilizamos

a tautologia $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

A afirmação "se ab é par, então a é par ou b é par" é equivalente à "se a é ímpar ($=$ não par) e b é ímpar, então ab é ímpar". Portanto, provamos a fórmula:

$$\forall a, b\,(((a \text{ é ímpar}) \wedge (b \text{ é ímpar})) \implies (ab \text{ é ímpar})).$$

Demonstração. Sejam a e b números ímpares. Isto é: existem números inteiros n e m com $a = 2n+1$ e $b = 2m+1$. Logo,

$$ab = (2n+1)(2m+1) = 4nm+2n+2m+1 = 2(2nm+n+m)+1;$$

isto é, ab é ímpar. $\square$

Continuação do exemplo

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

Continuação do exemplo

Exemplo

Teorema. *Para todos os números inteiros a e b: se ab é par, então a é par ou b é par.*

Corolário. *Para todo o número inteiro a, se a^2 é par, então a é par.*

$$\forall a\,((a^2 \text{ é par}) \implies (a \text{ é par}))$$

Demonstração. Utilizar o teorema acima no caso $a = b$.

A negação

Aqui utilizamos

a tautologia $\neg p \equiv (p \Rightarrow \perp)$; ou seja, $\neg p$ significa "p implica um absurdo (uma contradição)".

A negação

Aqui utilizamos

a tautologia $\neg p \equiv (p \Rightarrow \bot)$; ou seja, $\neg p$ significa "p implica um absurdo (uma contradição)".

Formulês

$$\dfrac{\boxed{\begin{array}{c}\psi\\ \vdots\\ \bot\end{array}}}{\neg\psi}$$

Português

Suponha ψ. Então, ...(algo mais ou menos esperto) .... Logo, uma contradição.

Portanto, $\neg\psi$ está provada. (E já não suponhamos ψ.)

A negação

Aqui utilizamos

a tautologia $\neg p \equiv (p \Rightarrow \bot)$; ou seja, $\neg p$ significa "p implica um absurdo (uma contradição)".

Formulês

$$\dfrac{\boxed{\begin{array}{c}\psi\\ \vdots\\ \bot\end{array}}}{\neg\psi}$$

Português

Suponha ψ. Então, ...(algo mais ou menos esperto) .... Logo, uma contradição.

Portanto, $\neg\psi$ está provada. (E já não suponhamos ψ.)

Nota

As vezes refere-se a este princípio também como *redução ao absurdo*. (Vamos revisitar a "redução ao absurdo" em breve.)

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Um exemplo

Teorema

O número real $\sqrt{2}$ *é irracional (= não racional). (Ou seja, não existem números inteiros* n, m *com* $\left(\frac{n}{m}\right)^2 = 2$.*)*

Demonstração.

Suponha que $\sqrt{2}$ é racional;

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Agora vamos deduzir uma contradição.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.
Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par. Isto é, existe um número k com $n = 2k$.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par. Isto é, existe um número k com $n = 2k$. Consequentemente,

$$2m^2 = n^2 = 4k^2$$

o que implica $m^2 = 2k^2$.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par. Isto é, existe um número k com $n = 2k$. Consequentemente,

$$2m^2 = n^2 = 4k^2$$

o que implica $m^2 = 2k^2$. Logo, m^2 é par e por isso m é par,

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par. Isto é, existe um número k com $n = 2k$. Consequentemente,

$$2m^2 = n^2 = 4k^2$$

o que implica $m^2 = 2k^2$. Logo, m^2 é par e por isso m é par, o que contradiz o facto que n e m não têm divisores comuns.

$\square$

Um exemplo

Teorema

O número real $\sqrt{2}$ é irracional (= não racional). (Ou seja, não existem números inteiros n, m com $\left(\frac{n}{m}\right)^2 = 2$.)

Demonstração.

Suponha que $\sqrt{2}$ é racional; ou seja, existem números inteiros n, m com $(\frac{n}{m})^2 = 2$. Aqui podemos supor que n e m não têm divisores comuns.

Como $(\frac{n}{m})^2 = 2$, então $n^2 = 2m^2$. Portanto, n^2 é par e, pelo corolário anterior, n é par. Isto é, existe um número k com $n = 2k$. Consequentemente,

$$2m^2 = n^2 = 4k^2$$

o que implica $m^2 = 2k^2$. Logo, m^2 é par e por isso m é par, o que contradiz o facto que n e m não têm divisores comuns.

Portanto, está provado que $\sqrt{2}$ não é racional. $\square$

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \bot)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Este princípio já foi utilizado no último capítulo (dedução automática).

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \bot)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo).

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \bot)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo). Suponhamos que não, portanto,

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \bot)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo). Suponhamos que não, portanto, x^y é irracional para todos os números reais irracionais x e y.

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \perp)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo). Suponhamos que não, portanto, x^y é irracional para todos os números reais irracionais x e y. Em particular, $\sqrt{2}^{\sqrt{2}}$ é irracional.

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \bot)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo). Suponhamos que não, portanto, x^y é irracional para todos os números reais irracionais x e y. Em particular, $\sqrt{2}^{\sqrt{2}}$ é irracional. Logo, $x = \sqrt{2}^{\sqrt{2}}$ é irracional e $y = \sqrt{2}$ é irracional,

$\square$

Redução ao absurdo

Aqui utilizamos

a tautologia $p \equiv \neg\neg p \equiv (\neg p \Rightarrow \perp)$; ou seja, em lugar de p mostramos que "$\neg p$ implica um absurdo (uma contradição)".

Exemplo

Teorema. Existem números reais irracionais x e y tal que x^y é racional.

Demonstração (via redução ao absurdo). Suponhamos que não, portanto, x^y é irracional para todos os números reais irracionais x e y. Em particular, $\sqrt{2}^{\sqrt{2}}$ é irracional. Logo, $x = \sqrt{2}^{\sqrt{2}}$ é irracional e $y = \sqrt{2}$ é irracional, mas

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2$$

é racional; uma contradição. $\square$

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Verificamos: $\log_2(9)$ é irracional ($=$ não racional).

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Verificamos: $\log_2(9)$ é irracional ($=$ não racional).

Suponha que $\log_2(9)$ é racional,

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Verificamos: $\log_2(9)$ é irracional (= não racional).

Suponha que $\log_2(9)$ é racional, ou seja existem números inteiros não nulos a e b com $2^{\frac{a}{b}} = 9$.

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Verificamos: $\log_2(9)$ é irracional ($=$ não racional).

Suponha que $\log_2(9)$ é racional, ou seja existem números inteiros não nulos a e b com $2^{\frac{a}{b}} = 9$. Logo,

$$2^a = 9^b = 3^{3b};$$

uma contradição porque 2^a é par e 3^{3b} é ímpar.

Continuação do exemplo

Devemos acreditar?

Conhecemos realmente números irracionais x e y com x^y racional?

Prova direta

Recordamos: $\sqrt{2}$ é irracional.

Verificamos: $\log_2(9)$ é irracional (= não racional).

Suponha que $\log_2(9)$ é racional, ou seja existem números inteiros não nulos a e b com $2^{\frac{a}{b}} = 9$. Logo,

$$2^a = 9^b = 3^{3b};$$

uma contradição porque 2^a é par e 3^{3b} é ímpar.

Finalmente: Calculamos

$$\sqrt{2}^{(\log_2 9)} = \sqrt{2^{(\log_2 9)}} = \sqrt{9} = 3.$$

Resumo

Utilizar $\psi \Rightarrow \varphi$

Sabemos que, se ψ então φ e sabemos ψ. Logo φ.

Prova direta de $\psi \Rightarrow \varphi$

Suponha ψ. .... Logo, φ.

Contraposição

$(\psi \Rightarrow \varphi) \equiv (\neg\varphi \Rightarrow \neg\psi)$.

Suponha $\neg\psi$. .... Logo, $\neg\varphi$.

Negação

$\neg\psi \equiv (\psi \Rightarrow \perp)$:

Suponha ψ. .... Contradição.

Redução ao absurdo

$\psi \equiv \neg\neg\psi \equiv (\neg\psi \Rightarrow \perp)$.

Suponha $\neg\psi$. .... Contradição.

Utilizar $\forall x\, \psi$

$\ldots \forall x\, \psi$. Em particular, $\psi\{t/x\}$.

Provar $\forall x\, \psi$

Seja x .... Logo, ψ.

Utilizar $\exists x\, \psi$

$\ldots \exists x\, \psi$. Seja x_0 com $\psi\{x_0/x\}$.

Provar $\exists x\, \psi$

$\ldots \psi\{t/x\}$. Logo, $\exists x\, \psi$.

O princípio de indução

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n \; P(n)$$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,

Nestas circunstâncias:

- $P(0)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0)$

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0) \qquad$ e $\quad P(0) \Rightarrow P(1)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0) \qquad \text{e} \quad P(0) \Rightarrow P(1)$
- $P(1)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n \, P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0) \quad \text{e} \quad P(0) \Rightarrow P(1)$
- $P(1) \quad \text{e} \quad P(1) \Rightarrow P(2)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n\ P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0)$ e $P(0) \Rightarrow P(1)$
- $P(1)$ e $P(1) \Rightarrow P(2)$
- $P(2)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n \; P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0) \quad$ e $\quad P(0) \Rightarrow P(1)$
- $P(1) \quad$ e $\quad P(1) \Rightarrow P(2)$
- $P(2) \quad$ e $\quad P(2) \Rightarrow P(3)$

A intuição

(No caso da indução em $\mathbb{N}$)

Temos como objetivo provar que todos os números naturais têm uma certa propriedade P.

$$\forall n \; P(n)$$

Suponhamos que podemos provar que

1. 0 tem a propriedade P,
2. um número $n > 0$ tem a propriedade P sempre que o número anterior a tem.

Nestas circunstâncias:

- $P(0)$ e $P(0) \Rightarrow P(1)$
- $P(1)$ e $P(1) \Rightarrow P(2)$
- $P(2)$ e $P(2) \Rightarrow P(3)$
- $P(3)$ ...

O princípio de indução (“simples” ou “fraca”)

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos $X = \{n \in \mathbb{Z} \mid n \geq n_0\}$ e P uma propriedade “aplicável” aos elementos de X.

$$\frac{P(n_0) \quad \forall n \geq n_0 \, (P(n) \Rightarrow P(n+1))}{\forall n \geq n_0 \; P(n)}$$

O princípio de indução (“simples” ou “fraca”)

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos $X = \{n \in \mathbb{Z} \mid n \geq n_0\}$ e P uma propriedade “aplicável” aos elementos de X.

$$\frac{P(n_0) \quad \forall n \geq n_0\ (P(n) \Rightarrow P(n+1))}{\forall n \geq n_0\ P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0\ P(n)$, temos duas tarefas:

O princípio de indução (“simples” ou “fraca”)

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos $X = \{n \in \mathbb{Z} \mid n \geq n_0\}$ e P uma propriedade “aplicável” aos elementos de X.

$$\frac{P(n_0) \quad \forall n \geq n_0\ (P(n) \Rightarrow P(n+1))}{\forall n \geq n_0\ P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0\ P(n)$, temos duas tarefas:

1. Condição inicial: verificar que a afirmação $P(n_0)$ é verdadeira, e

O princípio de indução ("simples" ou "fraca")

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos $X = \{n \in \mathbb{Z} \mid n \geq n_0\}$ e P uma propriedade "aplicável" aos elementos de X.

$$\frac{P(n_0) \quad \forall n \geq n_0 \; (P(n) \Rightarrow P(n+1))}{\forall n \geq n_0 \; P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0 \; P(n)$, temos duas tarefas:

1. Condição inicial: verificar que a afirmação $P(n_0)$ é verdadeira, e
2. Passo de indução: para cada $n \geq n_0$, provar a implicação

$$P(n) \Rightarrow P(n+1).$$

O princípio de indução ("simples" ou "fraca")

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos $X = \{n \in \mathbb{Z} \mid n \geq n_0\}$ e P uma propriedade "aplicável" aos elementos de X.

$$\frac{P(n_0) \quad \forall n \geq n_0\ (P(n) \Rightarrow P(n+1))}{\forall n \geq n_0\ P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0\ P(n)$, temos duas tarefas:

1. Condição inicial: verificar que a afirmação $P(n_0)$ é verdadeira, e
2. Passo de indução: para cada $n \geq n_0$, provar a implicação

   $$P(n) \Rightarrow P(n+1).$$

   Seja $n \geq n_0$ e suponha $P(n)$. ... Então, $P(n+1)$.

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$*. Para todo o* $n \in \mathbb{N}$, $(1+x)^n \geq 1+nx$*.*

Demonstração.

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$*. Para todo o* $n \in \mathbb{N}$, $(1 + x)^n \geq 1 + nx$*.*

Demonstração.

1. Para $n = 0$:

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ com $x \geq -1$. Para todo o $n \in \mathbb{N}$, $(1+x)^n \geq 1+nx$.

Demonstração.

1. Para $n = 0$: $\qquad (1+x)^0 = 1 \geq 1.$

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$. *Para todo o* $n \in \mathbb{N}$, $(1+x)^n \geq 1 + nx$.

Demonstração.

1. Para $n = 0$: $\qquad (1+x)^0 = 1 \geq 1.$
2. Seja $n \in \mathbb{N}$ e suponhamos que $(1+x)^n \geq 1 + nx$.

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$. *Para todo o* $n \in \mathbb{N}$, $(1+x)^n \geq 1 + nx$.

Demonstração.

1. Para $n = 0$: $\quad (1+x)^0 = 1 \geq 1.$
2. Seja $n \in \mathbb{N}$ e suponhamos que $(1+x)^n \geq 1 + nx$. Então,

$$(1+x)^{n+1}$$

$$1 + (n+1)x.$$

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$*. Para todo o* $n \in \mathbb{N}$, $(1+x)^n \geq 1+nx$.

Demonstração.

1. Para $n = 0$: $\quad (1+x)^0 = 1 \geq 1.$
2. Seja $n \in \mathbb{N}$ e suponhamos que $(1+x)^n \geq 1+nx$. Então,

$$(1+x)^{n+1} = (1+x)(1+x)^n$$

$$1+(n+1)x.$$

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ *com* $x \geq -1$. *Para todo o* $n \in \mathbb{N}$, $(1+x)^n \geq 1 + nx$.

Demonstração.

1. Para $n = 0$: $\quad (1+x)^0 = 1 \geq 1.$
2. Seja $n \in \mathbb{N}$ e suponhamos que $(1+x)^n \geq 1 + nx$. Então,

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geq (1+x)(1+nx) \\ &\qquad \text{[por hipótese da indução e porque } 1+x \geq 0] \\ &\qquad\qquad 1 + (n+1)x.\end{aligned}$$

$\square$

Um exemplo

Teorema

Seja $x \in \mathbb{R}$ com $x \geq -1$. Para todo o $n \in \mathbb{N}$, $(1+x)^n \geq 1 + nx$.

Demonstração.

1. Para $n = 0$: $\quad (1+x)^0 = 1 \geq 1.$
2. Seja $n \in \mathbb{N}$ e suponhamos que $(1+x)^n \geq 1 + nx$. Então,

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)(1+x)^n \\
&\geq (1+x)(1+nx) \\
&\quad \text{[por hipótese da indução e porque } 1+x \geq 0\text{]} \\
&= 1 + (n+1)x + nx^2 \geq 1 + (n+1)x.
\end{aligned}$$

$\square$

Ainda um exemplo “tolo”

Exemplo

Teorema. *Para todo o $n \geq 1$, quaisquer n números reais são iguais.*

Demonstração.

Ainda um exemplo “tolo”

Exemplo

Teorema. *Para todo o* $n \geq 1$*, quaisquer* n *números reais são iguais.*

Demonstração. Para $n = 1$, a afirmação é verdadeira.

Ainda um exemplo "tolo"

Exemplo

Teorema. *Para todo o* $n \geq 1$*, quaisquer* n *números reais são iguais.*

Demonstração. Para $n = 1$, a afirmação é verdadeira.
Seja $n \geq 1$ e consideramos os números reais $x_1, \dots, x_{n+1}$. Por hipótese da indução,

Ainda um exemplo “tolo”

Exemplo

Teorema. *Para todo o $n \geq 1$, quaisquer n números reais são iguais.*

Demonstração. Para $n = 1$, a afirmação é verdadeira.
Seja $n \geq 1$ e consideramos os números reais $x_1, \ldots, x_{n+1}$. Por hipótese da indução,

$$x_1 = \cdots = x_n$$

e

$$x_2 = \cdots = x_{n+1}.$$

Ainda um exemplo "tolo"

Exemplo

Teorema. *Para todo o $n \geq 1$, quaisquer n números reais são iguais.*

Demonstração. Para $n = 1$, a afirmação é verdadeira.
Seja $n \geq 1$ e consideramos os números reais $x_1, \ldots, x_{n+1}$. Por hipótese da indução,

$$x_1 = \cdots = x_n$$

e

$$x_2 = \cdots = x_{n+1}.$$

Logo, $x_1 = x_2 = \cdots = x_n = x_{n+1}$. $\square$

Ainda um exemplo “tolo”

Exemplo

Teorema. *Para todo o* $n \geq 1$*, quaisquer* n *números reais são iguais.*

Demonstração. Para $n = 1$, a afirmação é verdadeira.
Seja $n \geq 1$ e consideramos os números reais $x_1, \dots, x_{n+1}$. Por hipótese da indução,

$$x_1 = \cdots = x_n$$

e

$$x_2 = \cdots = x_{n+1}.$$

Logo, $x_1 = x_2 = \cdots = x_n = x_{n+1}$. $\square$

TPC: Onde está o erro???

O princípio de indução ("completa" ou "forte")

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos o conjunto $\{n \in \mathbb{Z} \mid n \geq n_0\}$.

$$\frac{\forall n \geq n_0 \ ((\forall k < n \ P(k)) \Rightarrow P(n))}{\forall n \geq n_0 \ P(n)}$$

O princípio de indução ("completa" ou "forte")

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos o conjunto $\{n \in \mathbb{Z} \mid n \geq n_0\}$.

$$\frac{\forall n \geq n_0 \ ((\forall k < n \ P(k)) \Rightarrow P(n))}{\forall n \geq n_0 \ P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0 \ P(n)$, temos a seguinte tarefa:

- para cada $n \geq n_0$, provar $P(n)$ supondo que, para todo o $k < n$ (e $k \geq n_0$), $P(k)$ é válida.

O princípio de indução (“completa” ou “forte”)

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos o conjunto $\{n \in \mathbb{Z} \mid n \geq n_0\}$.

$$\frac{\forall n \geq n_0 \; ((\forall k < n \; P(k)) \Rightarrow P(n))}{\forall n \geq n_0 \; P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0 \; P(n)$, temos a seguinte tarefa:

- para cada $n \geq n_0$, provar $P(n)$ supondo que, para todo o $k < n$ (e $k \geq n_0$), $P(k)$ é válida.

Nota

O princípio de indução ("completa" ou "forte")

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos o conjunto $\{n \in \mathbb{Z} \mid n \geq n_0\}$.

$$\frac{\forall n \geq n_0\ ((\forall k < n\ P(k)) \Rightarrow P(n))}{\forall n \geq n_0\ P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0\ P(n)$, temos a seguinte tarefa:

- para cada $n \geq n_0$, provar $P(n)$ supondo que, para todo o $k < n$ (e $k \geq n_0$), $P(k)$ é válida.

Nota

- O caso $n = n_0$ acima significa "provar $P(n_0)$" porque "para todo o $k < n_0$, $P(k)$" é trivialmente válida.

O princípio de indução (“completa” ou “forte”)

O princípio

Aqui fixamos $n_0 \in \mathbb{Z}$ e consideramos o conjunto $\{n \in \mathbb{Z} \mid n \geq n_0\}$.

$$\frac{\forall n \geq n_0 \; ((\forall k < n \; P(k)) \Rightarrow P(n))}{\forall n \geq n_0 \; P(n)}$$

Mais em detalhe:

Portanto, para provar $\forall n \geq n_0 \; P(n)$, temos a seguinte tarefa:

- para cada $n \geq n_0$, provar $P(n)$ supondo que, para todo o $k < n$ (e $k \geq n_0$), $P(k)$ é válida.

Nota

- O caso $n = n_0$ acima significa “provar $P(n_0)$” porque “para todo o $k < n_0$, $P(k)$” é trivialmente válida.
- Dependente do contexto, as vezes é necessário verificar primeiro os casos iniciais $P(n_0)$, $P(n_0 + 1)$, $\ldots$, $P(n_0 + k)$.

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

Agora:

Sabemos que

$$\forall m \geq n_0 \; ((\forall k < m \; P(k)) \Rightarrow P(m))$$

e suponhamos que

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

Agora:

Sabemos que

$$\forall m \geq n_0 \; ((\forall k < m \; P(k)) \Rightarrow P(m))$$

e suponhamos que $A = \{n \in \mathbb{N} \mid \neg P(n)\} \neq \varnothing$.

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

Agora:

Sabemos que

$$\forall m \geq n_0 \ ((\forall k < m \ P(k)) \Rightarrow P(m))$$

e suponhamos que $A = \{n \in \mathbb{N} \mid \neg P(n)\} \neq \varnothing$. Então, A tem um menor elemento, digamos m.

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

Agora:

Sabemos que

$$\forall m \geq n_0 \; ((\forall k < m \; P(k)) \Rightarrow P(m))$$

e suponhamos que $A = \{n \in \mathbb{N} \mid \neg P(n)\} \neq \varnothing$. Então, A tem um menor elemento, digamos m. Logo, para todo o $k < m$, $P(k)$.

A intuição

Recordamos que

cada subconjunto $A \subseteq \mathbb{N}$ não-vazio tem um menor elemento.

Agora:

Sabemos que

$$\forall m \geq n_0 \; ((\forall k < m \; P(k)) \Rightarrow P(m))$$

e suponhamos que $A = \{n \in \mathbb{N} \mid \neg P(n)\} \neq \varnothing$. Então, A tem um menor elemento, digamos m. Logo, para todo o $k < m$, $P(k)$. Portanto, $P(m)$; uma contradição.

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \ldots, p_k$ com $n = p_1 \cdot \cdots \cdot p_k$.

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \ldots, p_k$ com $n = p_1 \cdot \cdots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

$\square$

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \ldots, p_k$ com $n = p_1 \cdot \cdots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

Caso 1: n é primo. Portanto, $n = n$ (produto com um fator) e a afirmação é verdadeira.

$\square$

Um exemplo

Teorema

Cada número natural $n \geq 2$ *é um produto de números primos, isto é, existem números primos* $p_1, \dots, p_k$ *com* $n = p_1 \cdot \dots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

Caso 1: n é primo. Portanto, $n = n$ (produto com um fator) e a afirmação é verdadeira.

Caso 2: n não é primo.

□

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \ldots, p_k$ com $n = p_1 \cdot \cdots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

Caso 1: n é primo. Portanto, $n = n$ (produto com um fator) e a afirmação é verdadeira.

Caso 2: n não é primo. Portanto, $n = ab$ com números naturais $a, b < n$.

$\square$

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \ldots, p_k$ com $n = p_1 \cdot \cdots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

Caso 1: n é primo. Portanto, $n = n$ (produto com um fator) e a afirmação é verdadeira.

Caso 2: n não é primo. Portanto, $n = ab$ com números naturais $a, b < n$. Por hipótese de indução,

$$a = p_1 \cdot \cdots \cdot p_r \quad \text{e} \quad b = q_1 \cdot \cdots \cdot q_s,$$

com números primos $p_1, \ldots, p_r, q_1, \ldots, q_s$.

$\square$

Um exemplo

Teorema

Cada número natural $n \geq 2$ é um produto de números primos, isto é, existem números primos $p_1, \dots, p_k$ com $n = p_1 \cdot \dots \cdot p_k$.

Demonstração.

Seja $n \geq 2$ e suponha que cada número natural k com $2 \leq k < n$ é um produto de números primos.

Caso 1: n é primo. Portanto, $n = n$ (produto com um fator) e a afirmação é verdadeira.

Caso 2: n não é primo. Portanto, $n = ab$ com números naturais $a, b < n$. Por hipótese de indução,

$$a = p_1 \cdot \dots \cdot p_r \quad \text{e} \quad b = q_1 \cdot \dots \cdot q_s,$$

com números primos $p_1, \dots, p_r, q_1, \dots, q_s$. Logo.

$$n = ab = p_1 \cdot \dots \cdot p_r \cdot q_1 \cdot \dots \cdot q_s$$

é um produto de números primos.

$\square$

O princípio da gaiola de pombos

O princípio da gaiola de pombos

A ideia

n pombos devem ser postos em m casas. Se $n > m$, então pelo menos uma casa irá conter mais de um pombo.

Também conhecido como "princípio das gavetas de Dirichlet". Johann Peter Gustav Lejeune Dirichlet (1805 – 1859), matemático alemão.

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Também conhecido como "princípio das gavetas de Dirichlet".
Johann Peter Gustav Lejeune Dirichlet (1805 – 1859), matemático alemão.

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função.

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > |B|$,

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > |B|$, então f não é injetiva.

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > |B|$, então f não é injetiva.

A contraposição é mais "óbvia": Se f é injetiva, então $|A| \leq |B|$.

O princípio da gaiola de pombos

A ideia

n bolas devem ser postos em m caixas. Se $n > m$, então pelo menos uma caixa irá conter mais de uma bola.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > |B|$, então f não é injetiva.

A contraposição é mais "óbvia": Se f é injetiva, então $|A| \leq |B|$.

Formulação alternativa

Sejam A um conjunto com $|A| = n$, $m < n$ e $(A_i)_{1 \leq i \leq m}$ uma família de subconjuntos de A dois à dois disjunta com

$$A = A_1 \cup \cdots \cup A_m.$$

Então, para algum $1 \leq i \leq m$, $|A_i| \geq 2$.

Exemplo 1

Exemplo

Há duas pessoas aqui na sala que fazem anos no mesmo mês.

Exemplo 1

Exemplo

Há duas pessoas aqui na sala que fazem anos no mesmo mês.

Consideramos a função

$$\begin{aligned} f\colon \{\text{pessoas na sala}\} &\longrightarrow \{\text{janeiro}, \dots, \text{dezembro}\}, \\ p &\longmapsto \text{o mês do nascimento de } p \end{aligned}$$

com

$$|\{\text{janeiro}, \dots, \text{dezembro}\}| = 12$$

e

$$|\{\text{pessoas na sala}\}| > 12 \qquad \text{(espero)}.$$

Logo, f não é injetiva.

Exemplo 2

Exemplo

Sejam 50 *pessoas numa sala de* $7\ m \times 7\ m$. *Então, há duas pessoas entre eles com distância menor do que* $1.5\ m$.

Exemplo 2

Exemplo

Sejam 50 *pessoas numa sala de* $7\ m \times 7\ m$. *Então, há duas pessoas entre eles com distância menor do que* $1.5\ m$.

Dividimos a sala em quadrados "unitários" e consideramos a função

$$\begin{aligned} f\colon \{\text{pessoas na sala}\} &\longrightarrow \{\text{os quadrados}\} \\ p &\longmapsto \text{o quadrado onde } p \text{ está} \end{aligned}$$

Exemplo 2

Exemplo

Sejam 50 *pessoas numa sala de* $7\ m \times 7\ m$. *Então, há duas pessoas entre eles com distância menor do que* $1.5\ m$.

Dividimos a sala em quadrados "unitários" e consideramos a função

$$\begin{aligned} f\colon \{\text{pessoas na sala}\} &\longrightarrow \{\text{os quadrados}\} \\ p &\longmapsto \text{o quadrado onde } p \text{ está} \end{aligned}$$

(se p está na fronteira, escolhemos um dos quadrados).

Exemplo 2

Exemplo

Sejam 50 *pessoas numa sala de* $7\ m \times 7\ m$. *Então, há duas pessoas entre eles com distância menor do que* $1.5\ m$.

Dividimos a sala em quadrados "unitários" e consideramos a função

$$\begin{aligned} f\colon \{\text{pessoas na sala}\} &\longrightarrow \{\text{os quadrados}\} \\ p &\longmapsto \text{o quadrado onde } p \text{ está} \end{aligned}$$

(se p está na fronteira, escolhemos um dos quadrados). Como

$$|\{\text{pessoas na sala}\}| = 50 \quad \text{e} \quad |\{\text{os quadrados}\}| = 49,$$

há duas pessoas p e q no mesmo quadrado (f não é injetiva).

Exemplo 2

Exemplo

Sejam 50 *pessoas numa sala de* $7\ m \times 7\ m$. *Então, há duas pessoas entre eles com distância menor do que* $1.5\ m$.

Dividimos a sala em quadrados "unitários" e consideramos a função

$$f \colon \{\text{pessoas na sala}\} \longrightarrow \{\text{os quadrados}\}$$
$$p \longmapsto \text{o quadrado onde } p \text{ está}$$

(se p está na fronteira, escolhemos um dos quadrados). Como

$$|\{\text{pessoas na sala}\}| = 50 \quad \text{e} \quad |\{\text{os quadrados}\}| = 49,$$

há duas pessoas p e q no mesmo quadrado (f não é injetiva). Logo

"distância entre p e q" $\leq$ o comprimento do diagonal do quadrado
$$= \sqrt{2} < 1.5.$$

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \ldots n\}$ *tal que* $|q\alpha - p| < \dfrac{1}{n}$.

Nota: *Logo,* $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{qn} \leq \dfrac{1}{n^2}$.

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \ldots n\}$ *tal que* $|q\alpha - p| < \frac{1}{n}$.

Demonstração.

Para cada $k \in \{0, 1, \ldots, n\}$, consideramos $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$.

$\square$

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \ldots n\}$ *tal que* $|q\alpha - p| < \frac{1}{n}$.

Demonstração.

Para cada $k \in \{0, 1, \ldots, n\}$, consideramos $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$.

Aqui $\lfloor x \rfloor$ denota o maior número inteiro a com $a \leq x$. Logo,

$$|x - \lfloor x \rfloor| < 1.$$

Nota-se que $r_0 = 0$.

□

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \dots n\}$ *tal que* $|q\alpha - p| < \dfrac{1}{n}$.

Demonstração.

Para cada $k \in \{0, 1, \dots, n\}$, consideramos $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$. Aqui $\lfloor x \rfloor$ denota o maior número inteiro a com $a \leq x$. Logo,

$$|x - \lfloor x \rfloor| < 1.$$

Nota-se que $r_0 = 0$. Consideramos a função

$$f : \{0, 1, \dots, n\} \longrightarrow \left\{ \left[0, \frac{1}{n}\right[, \left[\frac{1}{n}, \frac{2}{n}\right[, \dots, \left[\frac{n-1}{n}, 1\right[\right\}$$

$$k \longmapsto \text{o intervalo } I \text{ com } r_k \in I$$

$\square$

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \ldots n\}$ *tal que* $|q\alpha - p| < \dfrac{1}{n}$.

Demonstração.

Para cada $k \in \{0, 1, \ldots, n\}$, consideramos $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$.

Pelo princípio da gaiola de pombos, existem números l e k (digamos $l < k$) tal que r_l e r_k tem uma distância menor do que $\frac{1}{n}$.

$\square$

O Teorema de Aproximação de Dirichlet

Teorema

Para todos os $\alpha \in \mathbb{R}$ *e* $n \in \mathbb{N}$, $n \geq 1$, *existem números inteiros* p *e* q *com* $q \in \{1, \dots n\}$ *tal que* $|q\alpha - p| < \frac{1}{n}$.

Demonstração.

Para cada $k \in \{0, 1, \dots, n\}$, consideramos $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$.

Pelo princípio da gaiola de pombos, existem números l e k (digamos $l < k$) tal que r_l e r_k tem uma distância menor do que $\frac{1}{n}$.
Portanto,

$$\frac{1}{n} > |k\alpha - \lfloor k\alpha \rfloor - l\alpha + \lfloor l\alpha \rfloor| = |(k - l)\alpha - (\lfloor k\alpha \rfloor - \lfloor l\alpha \rfloor)|$$

e escolhemos $q = k - l \in \{1, \dots n\}$ e $p = \lfloor k\alpha \rfloor - \lfloor l\alpha \rfloor$.

$\square$

Generalizando

Ideia

Suponhamos que temos m caixas. Se em cada caixa há no máximo k bolas, então temos no máximo mk bolas.

Generalizando

Ideia

Suponhamos que temos m caixas. Se em cada caixa há no máximo k bolas, então temos no máximo mk bolas.

Contraposição:

Generalizando

Ideia

Suponhamos que temos m caixas. Se em cada caixa há no máximo k bolas, então temos no máximo mk bolas.

Contraposição: Se temos mais do que mk bolas, então uma caixa tem mais do que k bolas.

Generalizando

Ideia

Suponhamos que temos m caixas. Se em cada caixa há no máximo k bolas, então temos no máximo mk bolas.

Contraposição: Se temos mais do que mk bolas, então uma caixa tem mais do que k bolas.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > k|B|$, então existe um $b \in B$ com $|f^{-1}(b)| > k$.

Generalizando

Ideia

Suponhamos que temos m caixas. Se em cada caixa há no máximo k bolas, então temos no máximo mk bolas.

Contraposição: Se temos mais do que mk bolas, então uma caixa tem mais do que k bolas.

Mais formal

Sejam A e B conjuntos finitos e $f : A \to B$ uma função. Se $|A| > k|B|$, então existe um $b \in B$ com $|f^{-1}(b)| > k$.

Formulação alternativa

Sejam A um conjunto com $|A| = n$, $mk < n$ e $(A_i)_{1 \leq i \leq m}$ uma família de subconjuntos de A dois à dois disjunta com

$$A = A_1 \cup \cdots \cup A_m.$$

Então, para algum $1 \leq i \leq m$, $|A_i| > k$.

Um exemplo

Exemplo

Na área metropolitana de Lisboa, há pelo menos 15 *pessoas com o mesmo número de fios de cabelo na cabeça.*

(Cada pessoa tem no máximo 200000 fios de cabelo na cabeça e na área metropolitana de Lisboa residem 2 821 697 pessoas[a].)

[a]fonte: Wikipédia.

Um exemplo

Exemplo

Na área metropolitana de Lisboa, há pelo menos 15 *pessoas com o mesmo número de fios de cabelo na cabeça.*

(Cada pessoa tem no máximo 200000 fios de cabelo na cabeça e na área metropolitana de Lisboa residem 2 821 697 pessoas[a].)

Agora consideramos a função "número de fios de cabelo na cabeça":

$$f : \{\text{Lisboetas}\} \longrightarrow \{0, 1, \dots, 200000\}.$$

[a] fonte: Wikipédia.

Um exemplo

Exemplo

Na área metropolitana de Lisboa, há pelo menos 15 *pessoas com o mesmo número de fios de cabelo na cabeça.*

(Cada pessoa tem no máximo 200000 fios de cabelo na cabeça e na área metropolitana de Lisboa residem 2 821 697 pessoas[a].)

Agora consideramos a função "número de fios de cabelo na cabeça":

$$f\colon \{\text{Lisboetas}\} \longrightarrow \{0, 1, \dots, 200000\}.$$

Como $14 \cdot 200001 < 2821697$, existe um $n \in \{0, 1, \dots, 200000\}$ com

$$|f^{-1}(n)| > 14; \qquad (\text{Nota: } f^{-1}(n) = \{p \mid f(p) = n\})$$

isto é, há pelo menos 15 pessoas com n fios de cabelo na cabeça.

[a] fonte: Wikipédia.