$|A| = |B|$ ако постоји $A \xrightarrow[\text{на}]{1-1} B$

$|A| \leq |B|$ ако постоји $A \xrightarrow{1-1} B$

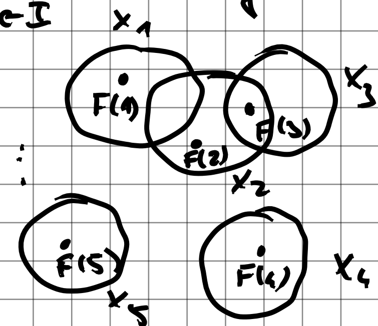
Кантор-Бернштајнова т: $|A| \leq |B|$ и $|B| \leq |A|$, онда $|A| = |B|$.

АКСИОМА ИЗБОРА

Дефиниција: Нека је $\mathcal{F}$ непразна фамилија непразних скупова. Ф-ја избора за $\mathcal{F}$ је било која ф-ја $F: \mathcal{F} \to \bigcup \mathcal{F}$ тд $(\forall X \in \mathcal{F})\ F(X) \in X$.

Нека је $\mathcal{F} = \{X_i \mid i \in I\}$ индексирана фам, тада ф-ја избора за $\mathcal{F}$ може да буде $F: I \to \bigcup_{i \in I} X_i$ тд $(\forall i \in I)\ F(i) \in X_i$.

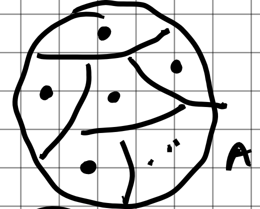
$I = \{1, 2, 3, 4, 5, \dots\} \xrightarrow{F}$



Аксиома избора: Нека је $\mathcal{F}$ непразна фам. непразних скупова. Тада постоји бар једна ф-ја избора за $\mathcal{F}$.

Теорема: Нека је P партиција непразног скупа A. Тада постоји бар једна трансверзала за P. (Свака екв. има трансверзалу.)

Доказ: Нека је $F: P \to \bigcup P = A$ ф-ја избора за P. Тада је $T = Im(F)$ је трансверзала. ☒



Задатак: Претходна т. еквивалентна је аксиоми избора, тј. доказати аксиому избора користећи претходну теорему. (Хинт. Ако је $\mathcal{F}$ непразна фам. непразних скупова, посматрати партицију $P = \{X \times \{X\} \mid X \in \mathcal{F}\}$ скупа $\bigcup P$.)

Теорема (Цорнова лема): Нека је X непразан скуп и $\preccurlyeq$ поредак на скупу X. Претпоставимо да важи: Сваки непразан ланац има горње ограничење. Тада постоји бар један максималан ел. у X.

Интуитиван доказ: (ппс) X нема максималне елем.
Нека је $a_0 \in X$; a_0 није максималан, па постоји $a_1 > a_0$; a_1 није максималан, па постоји $a_2 > a_1 \dots$

$$a_0 < a_1 < a_2 < a_3 < \dots$$

Овај ланац има горње огр. b_0, тј.

$$a_0 < a_1 < a_2 < \dots\dots < b_0.$$ Настављамо

$$b_0 < b_1 < b_2 < b_3 < \dots$$

Интуитивно, у неком тренутку ћемо искористити све ел. из X и добићемо ланац који нема горње ограничење. ↯ ∎

Коментар: Цорнова лема еквивалентна је аксиоми избора.

Парадокс Банаха и Тарског: Нека је S лопта полупр. 1.
S се може поделити на $S = K_1 \cup K_2 \cup \dots \cup K_m \cup K_{m+1} \cup \dots \cup K_n$, где $K_i \cap K_j = \emptyset$ за $1 \le i < j \le n$. Сваки део K_i може се ротирати и транслирати до дела K_i'. тако да добијемо:
$S_1 = K_1' \cup K_2' \cup \dots \cup K_m'$ и $S_2 = K_{m+1}' \cup \dots \cup K_n'$
где су S_1 и S_2 лопте полупр. 1.

Теорема: Ако су A и B непразни скупови, онда $|A| \le |B|$ или $|B| \le |A|$, тј. постоји $A \xrightarrow{1-1} B$ или $B \xrightarrow{1-1} A$.

Доказ: ПП $|B| \not\le |A|$ тј. НЕ ПОСТОЈИ $B \xrightarrow{1-1} A$.
Циљ: $|A| \le |B|$, тј. постоји $A \xrightarrow{1-1} B$.

Користићемо Цорнову лему.

Нека је $\mathcal{F} = \{ (A_0, F_0) \mid \emptyset \neq A_0 \subseteq A$ и $F_0 : A_0 \xrightarrow{1-1} B \}$

- $\underline{\mathcal{F} \neq \emptyset}$: Нека је $a_0 \in A$ и $b_0 \in B$ и $F_0 : \{a_0\} \xrightarrow{1-1} B$

$F_0(a_0) = b_0$.

па $(\{a_0\}, F_0) \in \mathcal{F}$.

- Дефинишемо $\preccurlyeq$ на $\mathcal{F}$:

$(A_0, F_0) \preccurlyeq (A_1, F_1) \quad :\equiv \quad A_0 \subseteq A_1 \quad \land \quad (\forall x \in A_0)\ F_0(x) = F_1(x).$

- $\underline{\preccurlyeq \text{ је поредак}}$:

(Р) $\quad (A_0, F_0) \preccurlyeq (A_0, F_0) \equiv A_0 \subseteq A_0 \land (\forall x \in A_0)\ F_0(x) = F_0(x)$

(АнС) $\quad (A_0, F_0) \preccurlyeq (A_1, F_1)$ и $(A_1, F_1) \preccurlyeq (A_0, F_0)$

$$\boxed{\begin{matrix} A_0 \subseteq A_1 \\ A_1 \subseteq A_0 \end{matrix}} \begin{matrix} \land\ (\forall x \in A_0)\ F_0(x) = F_1(x) \\ \land\ (\forall x \in A_1)\ F_1(x) = F_0(x) \end{matrix}$$

$\underline{A_0 = A_1} \quad \land \quad F_0(x) = F_1(x)$ за све $x \in A_0 = A_1$

$F_0, F_1 : A_0 = A_1 \to B$, па $\underline{F_0 = F_1}$

Дакле, $(A_0, F_0) = (A_1, F_1)$.

(Т) $\quad (A_0, F_0) \preccurlyeq (A_1, F_1)$ и $(A_1, F_1) \preccurlyeq (A_2, F_2)$

$\underline{A_0 \subseteq A_1} \land (\forall x \in A_0)\ F_0(x) = F_1(x)$ и $\underline{A_1 \subseteq A_2} \land (\forall x \in A_1)\ F_1(x) = F_2(x)$

тада $A_0 \subseteq A_2 \land (\forall x \in A_0)\ F_0(x) = F_1(x) = F_2(x)$

па $(A_0, F_0) \preccurlyeq (A_2, F_2)$.

Дакле, $\preccurlyeq$ јесте поредак на $\mathcal{F}$.

- Нека је $\mathcal{L}$ непразан ланац.

$\underline{\text{циљ}}$: $\mathcal{L}$ има горње ог. у $\mathcal{F}$.

запишимо $\mathcal{L} = \{ (A_i, F_i) \mid i \in I \}$. $[A_i \subseteq A, \ F_i : A_i \xrightarrow{1-1} B]$

„$\mathcal{L}$ је ланац" значи: $(\forall i, j \in I) [(A_i, F_i) \preccurlyeq (A_j, F_j) \lor (A_j, F_j) \preccurlyeq (A_i, F_i)]$

Дефинишимо $A_* := \bigcup_{i \in I} A_i$; очигледно $\boxed{A_* \subseteq A}$

Дефинишимо $F_* : A_* \xrightarrow{1-1} B$:

$F_*(x) := F_i(x)$, где је $i \in I$ било које тд. $x \in A_i$.

• F_* је коректно дефинисана у следећем смислу: Ако $x \in A_i, A_j$, онда $F_i(x) = F_j(x)$.

Како је $\mathcal{L}$ ланац, нпр. $(A_i, F_i) \preceq (A_j, F_j)$, тј. $(\forall x \in A_i)\ F_i(x) = F_j(x)$, па даље заиста $F_i(x) = F_j(x)$.

• $\boxed{F_* \text{ јесте „1-1"}}$: Нека $x_1, x_2 \in A_*$, $x_1 \neq x_2$.

Тада постоје i, j тд. $\underline{x_1 \in A_i}$ и $\underline{x_2 \in A_j}$.

Како је $\mathcal{L}$ ланац, нпр. $(A_i, F_i) \preceq (A_j, F_j)$, тј. $\underline{\underline{A_i \subseteq A_j}} \wedge (\forall x \in A_i)\ F_i(x) = F_j(x)$.

Тада $x_1, x_2 \in A_j$ и
$$F_*(x_1) = F_j(x_1) \neq F_j(x_2) = F_*(x_2) \leftarrow F_j \text{ је „1-1"}$$

Даље, $(A_*, F_*) \in \mathcal{F}$.

• (A_*, F_*) јесте горње ог. за $\mathcal{L}$, тј. $(\forall i \in I)\ (A_i, F_i) \preceq (A_*, F_*)$

$\underline{A_i \subseteq A_*}$: ✓ јер $A_* = \bigcup_{i \in I} A_i$

$\underline{(\forall x \in A_i)\ F_i(x) = F_*(x)}$: ✓ по деф. F_*

Даље, (A_*, F_*) заиста јесте горње ог. за $\mathcal{L}$.

Цорнова лема се може применити, тј. постоји максимални елемент $(M, F) \in \mathcal{F}$. Тада

$$M \subseteq A \quad \text{и} \quad F : M \xrightarrow{1-1} B.$$

1° Ако $M = A$, онда $F : A \xrightarrow{1-1} B$ и завршили смо.

2° Пп. $M \subsetneq A$. Доказаћемо да ово није могуће.

• Тада постоји $a \in A \setminus M$.

2.1° Ако је F „НА", тј. $F : M \xrightarrow[\text{НА}]{1-1} B$, тада имамо $F^{-1} : B \xrightarrow[\text{НА}]{1-1} M$, па како $M \subseteq A$ имамо

$$B \xrightarrow[\text{биј}]{F^{-1}} M \xrightarrow[1-1]{i} A \quad ; \quad i(m) = m \text{ за } m \in M$$

тј. $F^{-1}: B \xrightarrow{1-1} A$ $\lightning$

2.2° Даље, F не може бити „НА", тј. $Im(F) \subsetneq B$.

- Тада постоји $b \in B \setminus Im(F)$
- Нека $M_1 := M \cup \{a\}$; $\boxed{M \subsetneq M_1}$

  нека $F_1 : M_1 \to B$

$$F_1(x) := \begin{cases} F(x) & x \in M \\ b & x = a \end{cases} \qquad \boxed{(\forall x \in M)\ F(x) = F_1(x)}$$

очигледно $\boxed{F_1 : M_1 \xrightarrow{1-1} B}$ (јер $b \notin Im(F)$)

Даље, $(M_1, F_1) \in \mathcal{F}$ и $\underline{\underline{(M,F) < (M_1, F_1)}}$ $\lightning$

јер је (M, F) био максималан. ///

ДЕФИНИЦИЈА ПРИРОДНИХ БРОЈЕВА

Дефиниција: Следбеник скупа X је скуп

$$S(X) := X \cup \{X\}.$$

Коментар: $X = Y \quad \equiv \quad S(X) = S(Y)$

фон Нојманова дефиниција:

$0 := \emptyset.$ $\qquad |0| = 0$

$1 := S(0) = 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\}$ $\qquad |1| = 1$

$2 := S(1) = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0,1\}$ $\qquad |2| = 2$

$3 := S(2) = 2 \cup \{2\} = \{0,1,2\}$ $\qquad |3| = 3$

$4 := S(3) = \{0,1,2,3\}$

$\underline{n+1 := S(n)} = \{0,1,2,\dots,n\}$ $\qquad |n| = n$

Природан број n је скуп свих природних бројева мањих од n.

запажање: $m < n :\equiv m \in n \equiv m \subsetneq n.$

Дефиниција: (1) Скуп A је **индуктиван** ако:
- $0 \in A$;
- $(\forall x \in A)\ S(x) \in A$.

(2) $\mathbb{N}$ је најмањи индуктиван скуп.

Запажање: $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$

Теорема (Принцип мат. индукције): Нека је $P(x)$ неки предикат, где x пролази $\mathbb{N}$ (унив. домен је $\mathbb{N}$). Претпоставимо да важи:
- $P(0)$; (база индукције)
- $(\forall n)\,(P(n) \to P(n+1))$. (индукцијски корак)

Тада $(\forall n)\, P(n)$.

Доказ: Нека је $A := \{n \in \mathbb{N} \mid P(n)\} \subseteq \mathbb{N}$.
- $0 \in A$ (јер $P(0)$ према бази индукције)
- $(\forall n \in A)\ \underbrace{S(n)}_{n+1} \in A$ $\big(\equiv (\forall n)\,(n \in A \to S(n) \in A)\big)$ ← индукцијски корак.

Дакле, $A \subseteq \mathbb{N}$ је индуктиван скуп, па $A = \mathbb{N}$ јер је $\mathbb{N}$ најмањи индуктиван скуп □

пример: (Гаусова ф-ла) $0 + 1 + 2 + \dots + n = \dfrac{n(n+1)}{2}$.

Означимо $P(n)$: $0+1+2+\dots+n = \dfrac{n(n+1)}{2}$.

Тврдимо $(\forall n)\, P(n)$, доказ индукцијом

- $\underline{P(0)}$: $0 = \dfrac{0\,(0+1)}{2}$ ✓

- $\underline{(\forall n)\,(P(n) \to P(n+1))}$: Нека је n произвољно

  <u>циљ</u>: $P(n) \to P(n+1)$

(ПП) $P(n)$: $0+1+\dots+n = \dfrac{n(n+1)}{2}$ (индукцијска хипотеза)

доказујемо $P(n+1)$: $0+1+\dots+n+(n+1) = \dfrac{(n+1)(n+2)}{2}$.

$$\underbrace{0+1+\dots+n}+(n+1) \overset{\text{ИХ}}{=} \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2}+1\right)$$

$$= (n+1)\,\frac{n+2}{2} \quad \checkmark \quad \boxed{D}$$

<u>Напомена:</u> Код доказа индукцијом не смемо заборавити ни базу ни корак.

- <u>пример:</u> $(\forall n)\ 2 \mid 2n+1$ $\leftarrow$ нетачно

  <u>корак је тачан:</u> $(\forall n)(2 \mid 2n+1 \rightarrow 2 \mid 2n+3)$

  ако ИХ $2 \mid 2n+1$, тада

  $2n+3 = (2n+1)+2$, па $2 \mid 2n+1$ по ИХ

  $2 \mid 2$ ✓

  па $2 \mid 2n+3$.

  Нисмо смели да заборавимо базу ($P(0)$: $2 \mid 1$ нет.)

<u>пример:</u> $(\forall n \geq 5)\ 2^n > n^2 \equiv (\forall n)\ 2^{n+5} > (n+5)^2$

<u>Теорема</u> (Принцип потпуне индукције): Нека је $Q(n)$ предикат где $n \in \mathbb{N}$. Ако:

- $(\forall n)\left[(\forall m<n)Q(m) \rightarrow Q(n)\right]$ $(*)$

онда $(\forall n)\ Q(n)$.

<u>Доказ:</u> „обичном" индукцијом.

Означимо $P(n) : (\forall m<n)\ Q(m)$

Докажимо $(\forall n)\ P(n)$ индукцијом.

- <u>$P(0)$:</u> $(\forall m<0)\ Q(m) \equiv (\forall m \in \emptyset)\ Q(m) \equiv \top$
- <u>$(\forall n)(P(n) \rightarrow P(n+1))$</u>: Нека је n произвољно

  ИХ $P(n)$: $(\forall m<n)\ Q(m)$,

  циљ: $P(n+1)$: $(\forall m<n+1)\ Q(m) \equiv \underbrace{(\forall m<n)\ Q(m)}_{\text{тачно по ИХ}} \wedge \underbrace{Q(n)}_{(\#)}$.

<u>$(\#)$:</u> из $(*)$ $\underbrace{(\forall m<n)\ Q(m)}_{\text{тачно по ИХ}} \rightarrow Q(n)$, па $Q(n)$ тачно.

//

Дакле, $(\forall n)\, P(n)$, тј. $(\forall n)(\forall m<n)\, Q(m)$.

Докажимо $(\forall n)\, Q(n)$.

Нека је n произвољно. Према претходном важи $P(n+1)$ тј. $(\forall m<n+1)\, Q(m)$; специјално за $m=n$, важи $Q(n)$ $\boxed{\text{Ц}}$

Пример: Сваки природан број $n\geq 2$ је прост или производ простих.

Доказ: Користимо потпуну индукцију

$Q(n)$: $n+2$ је прост или производ простих

Циљ: $(\forall n)\, Q(n)$ Довољно је да докажемо:

$(\forall n)\big((\forall m<n)\, Q(m) \to Q(n)\big)$.

Нека је n произвољно.

ПИ: $(\forall m<n)\, Q(m)$, тј. $(\forall m<n)$ $m+2$ је прост или производ простих

Циљ: $Q(n)$, тј. $n+2$ је прост или производ простих

1° $n+2$ је прост: нема шта

2° $n+2$ није прост: тј. $n+2$ је сложен

тада $n+2 = a\cdot b$, $\quad 1<a,b<n+2$.

Како $a,b>1$, можемо записати $a=m_1+2$, $b=m_2+2$

Како $a,b<n+2$, тада $m_1,m_2<n$

према ПИ m_1+2 и m_2+2 су прости или производи простих.

Тада $n+2 = a\cdot b = \underline{(m_1+2)}\,\underline{(m_2+2)}$ = производ простих. $\boxed{\text{Ц}}$

Теорема: (Принцип минимума) Нека је $\emptyset\neq A\subseteq \mathbb{N}$. Тада A има минимум.

Доказ: (ПНС) $A\neq\emptyset$, $A\subseteq\mathbb{N}$, A нема минимум.

Нека је $Q(n)$: $n\notin A$

Потпуном инд. доказујемо $(\forall n)\ Q(n)$, тј. довољно је да докажемо:

$$(\forall n)\left[(\forall m<n)\ Q(m) \rightarrow Q(n)\right].$$

Нека је n произвољно.

(пп) $(\forall m<n)\ Q(m)$, тј. $(\forall m<n)\ m\notin A$

дм: $Q(n)$, тј. $n\notin A$.

(пс) $n\in A$, како $(\forall m<n)\ m\notin A$, то је n минимум скупа A ↯ јер A нема мин.

Дакле, $(\forall n)\ Q(n)$, тј. $(\forall n)\ n\notin A$.

$A\subseteq\mathbb{N}$ и $(\forall n\in\mathbb{N})\ n\notin A$, па $A=\emptyset$ ↯ јер $A\neq\emptyset$ $\boxed{\text{II}}$

Дефиниција: Нека је $\preceq$ поредак на скуп A. Поредак $\preceq$ је добар ако:

- $\preceq$ је линеаран,
- сваки непразан подскуп од A има минимум

пример: • $\leq$ на $\mathbb{N}$ је добро (принцип минимума)

• $\leq$ на $\mathbb{Z}$ није добро (нпр. $\mathbb{Z}$ нема минимум)

Цермелов принцип: На сваком скупу A постоји добар поредак.

коментар: Цермелов принцип еквивалентан је аксиоми избора.

задатак: Доказати Цорнову лему користећи Цермелов принцип.