SKUPOVI

- **N, Z, Q, R, C**
- **Surjekcija, injekcija, bijekcija, inverzna funkcija**

Za funkciju $f : A \to B$ kažemo da je **surjekcija** ako je njena slika jednaka čitavoj kodomeni, tj. $f(A) = B$. Riječima: f je surjekcija ako

$$\text{za svaki } b \in B \text{ postoji } a \in A \text{ takav da je } b = f(a).$$

Svaki element kodomene B je 'pogođen' s bar jednim elementom domene A.

Za funkciju $f : A \to B$ kažemo da je **injekcija** ako različitim vrijednostima argumenta pridružuje različite vrijednosti u slici, tj.

$$\text{ako je } a_1 \neq a_2, \text{ onda je } f(a_1) \neq f(a_2).$$

Funkcija $f : A \to B$ koja je istodobno injekcija i surjekcija zove se **bijekcija**. U tom slučaju možemo definirati **inverznu funkciju** $f^{-1} : B \to A$ na sljedeći način:

$$f^{-1}(b) = a \text{ onda i samo onda ako vrijedi } f(a) = b.$$

- **Osnovni teorem aritmetike**

se jos i *Osnovnog teorema aritmetike*. On kaže da za svaki prirodan broj $a \geqslant 2$ postoje jednoznačno određeni prosti brojevi u rastućem slijedu, $p_1 < p_2 < \ldots < p_k$, takvi da je

$$a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k},$$

gdje su n_i prirodni brojevi koji su također jednoznačno određeni (n_i se zove *kratnost* prostog broja p_i u tom rastavu). Na pr. $12 = 4 \cdot 3 = 2^2 \cdot 3^1$, $9 = 3^2$, $11 = 11^1$.

- **Kartezijev produkt**

DEFINICIJA. Ako su $A_1, \ldots, A_n$ neprazni skupovi, onda definiramo **Kartezijev produkt**

$$A_1 \times A_2 \times \ldots \times A_n$$

kao skup svih poredanih n–teraca $(a_1, a_2, \ldots, a_n)$ takvih da je $a_k \in A_k$ za sve $k = 1, \ldots, n$. Taj se skup označava kraće sa $\prod_{k=1}^{n} A_k$.

- **Beskonačan skup / prebrojiv / neprebrojiv**

Za skup A kažemo da je **beskonačan** ako nije konačan. Postoje dvije osnovne vrste beskonačnih skupova:

(i) za beskonačan skup A kažemo da je **prebrojiv** ako se skup njegovih elemenata može *poredati u beskonačan slijed*: $A = \{a_1, a_2, a_3, \ldots\}$.

(ii) za beskonačan skup A kažemo da je **neprebrojiv** ako se ne može poredati u slijed.

- **Ekvipotentnost**

DEFINICIJA. Kažemo da je skup A **ekvipotentan** (jednakobrojan) sa skupom B ako postoji bijekcija $f : A \to B$.

- **Kardinalni broj / alef nula**

DEFINICIJA. Za skupove A i B kažemo da imaju isti **kardinalni broj** ako su ekvipotentni, dotično ako postoji bijekcija s jednog na drugi. Pišemo $|A| = |B|$.

DEFINICIJA. Ako je skup A prebrojiv, onda njegov kardinalni broj označavamo sa $\aleph_0$ i zovemo "**alef nula**" (prema prvom slovu $\aleph$ "alef" hebrejskoga pisma), i pišemo $|A| = \aleph_0$. Kardinalni broj skupa $\mathbf{R}$ realnih brojeva označavamo sa c i zovemo **kontinuum**. Pišemo $|\mathbf{R}| = c$.

- ***„Svaki beskonačan podskup prebrojiva skupa je prebrojiv"* + primjedba**

Teorem 3. *Svaki beskonačan podskup prebrojiva skupa je prebrojiv.*

DOKAZ. Umjesto skupa $A = \{a_1, a_2, \ldots\}$ dovoljno je tvrdnju dokazati za $\mathbf{N} = \{1, 2, \ldots\}$. Neka je dakle $A = \mathbf{N}$ i B beskonačan podskup od $\mathbf{N}$. Odaberimo najmanji prirodni broj b_1 u B. Zatim iz B izbacimo b_1 i gledamo najmanji element b_2 u preostalom skupu $B \setminus \{b_1\}$. Neka je zatim b_3 najmanji prirodni broj u $B \setminus \{b_1, b_2\}$, itd. Nije teško provjeriti da je funkcija $f : \mathbf{N} \to B$ definirana sa $f(k) = b_k$ bijekcija, pa je B prebrojiv skup. ☺

PRIMJEDBA 1. Iz prethodnog teorema vidimo da će neki skup A biti prebrojiv onda i samo onda ako postoji injektivno preslikavanje $f : A \to \mathbf{N}$ čija je slika $f(A)$ beskonačan podskup od $\mathbf{N}$. Naime ako f gledamo kao funkciju $f : A \to f(A)$, onda je f bijekcija i skup $f(A)$ je prebrojiv.

Sljedeće svojstvo imaju samo beskonačni skupovi.

- **Kodiranje (prema *Osnovnom teoremu aritmetike*)**

Teorem 1. *Skup $A = \mathbf{N} \cup \mathbf{N}^2 \cup \mathbf{N}^3 \cup \ldots$ je prebrojiv. Drugim riječima, skup svih konačnih sljedova prirodnih brojeva je prebrojiv.*

DOKAZ. Odaberimo slijed prostih brojeva $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$ itd. Skup prostih brojeva je beskonačan. Definirajmo funkciju $f : A \to \mathbf{N}$ sa

$$f(n_1, \ldots, n_k) = p_1^{n_1} \ldots p_k^{n_k}.$$

Dokažimo da je ova funkcija injekcija. Neka je $f(n_1, \ldots, n_k) = f(m_1, \ldots, m_j)$, tj. $p_1^{n_1} \ldots p_k^{n_k} = p_1^{m_1} \ldots p_j^{m_j}$. Budući da imamo jednakost brojeva koji su rastavljeni na proste faktore, prema *Osnovnom teoremu aritmetike* slijedi da je $k = j$ i $n_i = m_i$ za sve $i = 1, \ldots, k$. Time je injektivnost od f dokazana.

Slika preslikavanja f je očevidno beskonačan skup (već za "jednočlane" sljedove n je skup pripadnih vrijednosti oblika $f(n) = 2^n$, dakle beskonačan skup). Tvrdnja slijedi iz Primjedbe 1.3.1. ☺

DEFINICIJA. Funkcija $f : A \to \mathbf{N}$ iz dokaza prethodnog teorema zove se **kodiranje** skupa A. Npr. trojcu $(6, 14, 9)$ bit će pridružen kôd $2^6 3^{14} 5^9$.

BINARNE RELACIJE

- **Binarna relacija**

  DEFINICIJA. **Binarna relacija** na skupu X je bilo koji neprazan podskup $\rho \subseteq X \times X$. Kažemo da su elementi x i y *u relaciji* ρ (ili x je u relaciji s y) ako je $(x, y) \in \rho$. U tom slučaju pišemo $x \rho y$.

- **Relacija ekvivalencije (refleksivnost, simetričnost, tranzitivnost)**

  DEFINICIJA. Binarna relacija $\rho \subseteq X \times X$ zove se **relacija ekvivalencije** ako je refleksivna, simetrična i tranzitivna, tj. ako za sve x, y i z u X vrijedi:

  (a) $x \rho x$ (refleksivnost),
  (b) iz $x \rho y$ slijedi $y \rho x$ (simetričnost),
  (c) iz $x \rho y$ i $y \rho z$ slijedi $x \rho z$ (tranzitivnost).

- **Razred (klasa) ekvivalencije**

  DEFINICIJA. Neka je ρ relacija ekvivalencije na X. **Razred (klasa) ekvivalencije** $[x]$ elementa $x \in X$ je skup svih elemenata iz X koji su u relaciji s x. Dakle $[x]$ je podskup od X definiran sa

  $$[x] = \{y \in X : y \rho x\}.$$

  Zbog $x \rho x$ je uvijek $x \in [x]$. Bilo koji element y iz $[x]$ zove se *reprezentant razreda* $[x]$.

- **Kvocjentni skup**

  DEFINICIJA. Ako je ρ relacija ekvivalencije na skupu X, onda skup svih pripadnih razreda ekvivalencije zovemo **kvocjentni skup** od X s obzirom na relaciju ρ i označavamo sa $X/_\rho$:

  $$X/_\rho = \{[x]\}_{x \in X}$$

KOMBINATORIKA

- **Partitivni skup** 2^X
- **Varijacije**
  - Varijacije bez ponavljanja $\frac{n!}{(n-k)!}$
  - Permutacije
    - Permutacije bez ponavljanja $n!$
    - Permutacije s ponavljanjem
      - Multinomni teorem $\frac{n!}{n_1! \cdot \ldots \cdot n_k!}$
  - Varijacije s ponavljanjem n^k
- **Kombinacije**
  - Kombinacije bez ponavljanja $\binom{n}{k}$
    - Pascalov trokut
    - Binomna formula $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
  - Kombinacije s ponavljanjem $\binom{n+k-1}{k}$
- **Formula uključivanja i isključivanja**
  - Broj surjekcija $|Sur(A,B)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$
  - Deranžmani (permutacije u kojima niti jedan element ne stoji na svome mjestu)

    $$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$
- **Funkcije izvodnice**
  - Pravilo deriviranja i integriranja
  - $\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$
- **Dirichletovo načelo**
  - *Neka je n predmeta smješteno u m kutija i n > m. Onda postoji kutija s barem 2 predmeta.*
  - (poopćeno) *Ako je n predmeta smješteno u m kutija, onda postoji kutija koja sadrži barem* $\left\lfloor \frac{n-1}{m} \right\rfloor + 1$ *predmeta.*