1.
Skupovi

1.1. Algebra skupova

Temeljne definicije i oznake. Pod pojmom *skupa* razumijevamo bilo koju množinu elemenata. Npr.:

(a) skup svih prirodnih brojeva $\mathbf{N} = \{1, 2, 3, \ldots\}$;
(b) skup svih cijelih brojeva $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$;
(c) racionalnih brojeva $\mathbf{Q}$ (elementi su mu razlomci $\frac{a}{b}$, gdje su $a, b \in \mathbf{Z}$ i $b \neq 0$);
(d) skup svih realnih brojeva $\mathbf{R}$; on sadrži sve racionalne, kao i brojeve poput $\sqrt{2}$, $\pi = 3.14\ldots$, $e = 2.71828\ldots$, $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$, koji nisu racionalni;
(e) skup kompleksnih brojeva $\mathbf{C}$, koji sadrži sve $z = x + iy$, takve da su $x, y \in \mathbf{R}$, pri čemu je i imaginarna jedinica za koju se definira da je $i^2 = -1$.

Te vrlo važne skupove upoznali smo u osnovnoj i srednjoj školi. Povijesno, za njihovo uvođenje trebala su duga stoljeća mukotrpnog i vrlo složenog znanstvenog razvoja, osobito za nulu, negativne cijele brojeve i kompleksne brojeve. Skup realnih brojeva strogo je definiran tek u 19. stoljeću.

Neka je X bilo koji unaprijed učvršćen skup koji želimo promatrati, tzv. *univerzalni skup*. U njemu gledamo podskupove A, B, C itd. (skupove i podskupove obično označavamo velikim slovima). Činjenicu da element x pripada skupu A bilježimo sa $x \in A$ (ponekad i sa $A \ni x$, tj. skup A sadrži element x). Ako x nije u A, onda pišemo $x \notin A$. Skupove obično zadajemo na dva načina:

a) popisivanjem njegovih elemenata, ako je to moguće: npr. $A = \{1, 2, 3\}$, ili
b) opisno, s pomoću nekog svojstva. Točnije, skup A svih elemenata $x \in X$ koji imaju neku vlastitost $P(x)$ označavamo sa $A = \{x \in X : P(x)\}$. Npr. ako je $X = \mathbf{R}$ i vlastitost $P(x)$ označava da je $x = \operatorname{tg} x$, onda je $A = \{x \in \mathbf{R} : x = \operatorname{tg} x\}$ skup svih realnih rješenja jednadžbe $x = \operatorname{tg} x$. Skup racionalnih brojeva možemo opisati kao $\mathbf{Q} = \{\frac{a}{b} : a, b \in \mathbf{Z},\ b \neq 0\}$.

Skup ne ovisi o poretku elemenata u njegovu zapisu, kao niti o tome ima li ponavljanja nekog elementa: npr. $\{1,2,3\} = \{3,2,1\} = \{2,2,3,3,3,1\}$.

Sljedeća definicija je jasna: kažemo da je skup A *podskup* skupa B ako je A sadržan u B, tj. ako za svaki element $x \in X$ vrijedi da ako je $x \in A$, onda je $x \in B$. Pišemo $A \subseteq B$. Znak $\subseteq$ zovemo znakom *inkluzije* (uključivanja). Ako je $A \subseteq B$, onda kažemo da je B nadskup od A, što možemo pisati i kao $B \supseteq A$. Očevidno je $A \subseteq A$ za bilo koji skup A. Ako je $A \subseteq B$ i $A \neq B$, onda kažemo da je A *pravi podskup* od B.

Važan podskup od X je onaj koji ne sadrži niti jedan element, tzv. *prazan skup*. Označavamo ga sa $\emptyset$. Smatramo da za svaki skup A vrijedi $\emptyset \subseteq A$, tj. prazan skup je sadržan u svakom skupu. Također smatramo da postoji samo jedan prazan skup.

PRIMJEDBA 1. Mogući su i skupovi koji kao svoje elemente sadrže druge skupove. Npr. skup $A = \{\{a\}\}$ ima kao element skup $\{a\}$, tj. $\{a\} \in A$. Skup A ne sadrži element a: $a \notin A$. Isto tako skup $\emptyset$ ne sadrži niti jedan element, dok skup $\{\emptyset\}$ sadrži jedan element (element mu je prazan skup).

Radi potpunosti, čitatelja ćemo vrlo sažeto podsjetiti još i na neke temeljne pojmove u vezi s funkcijama. Neka su zadana dva neprazna skupa A i B. **Funkcijom** f iz A u B, zovemo pravilo (postupak) kojim *svakom* elementu a iz polaznog skupa A pridružujemo <u>točno jedan</u> element iz skupa B, koji označavamo sa $f(a)$, i zovemo *slikom* elementa a u skupu B. Funkciju označavamo sa $f : A \to B$. Funkcija se često zove još i **preslikavanje**. Umjesto $b = f(a)$ ponekad pišemo i $a \mapsto b$.

Kao što smo rekli, ne može nekom $a \in A$ biti pridruženo više b-ova iz B, nego samo jedan, koji zovemo $f(a)$. Ali, neki $b \in B$ može funkcijom f biti pridružen dvama ili više različitih elemenata iz A.

Za zadanu funkciju $f : A \to B$ skup A zove se **domena**, a skup B **kodomena** funkcije. Ako je $b = f(a)$, onda a zovemo argumentom funkcije, a b vrijednošću od f za argument a. Skup poredanih dvojaca $(a, f(a))$ zove se **graf** funkcije f. Kad kažemo *poredani dvojac*, onda nam to znači da je $a \in A$ prvi element, i $f(a) \in B$ drugi element u dvojcu $(a, f(a))$.

Za dvije funkcije $f : A_1 \to B_1$ i $g : A_2 \to B_2$ kažemo da su **jednake** ako imaju iste domene, tj. $A_1 = A_2$, iste kodomene, tj. $B_1 = B_2$, i za sve $a \in A$ vrijedi $f(a) = g(a)$. Npr. dvije funkcije $f : \mathbf{N} \to \mathbf{N}$ i $g : \mathbf{Z} \to \mathbf{N}$ zadane na 'isti' način: $f(x) = x^2 + 1$ i $g(x) = x^2 + 1$, smatramo različitim funkcijama jer su im domene različite.

Slijed (ili niz) u skupu A je bilo koja funkcija $f : \mathbf{N} \to A$. Vrijednosti te funkcije su $f(n) = a_n \in A$, tj. redom $a_1, a_2, a_3, \ldots$, pa slijed često označavamo i na ovaj način: (a_n).

Slika funkcije $f : A \to B$ definira se kao skup $f(A) = \{f(a) \in B : a \in A\}$, tj. kao skup svih $b \in B$ koji su 'pogođeni' s nekim $a \in A$ uz pomoć funkcije.

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.

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

To je isto što i zahtijevati da

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

Injektivna funkcija 'ne lijepi' različite elemente iz skupa A u isti element iz B. Primijetite da za *svaku* funkciju $f : A \to B$ vrijedi da iz $a_1 = a_2$ slijedi $f(a_1) = f(a_2)$.

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:

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

Inverzna funkcija je također bijekcija. Jasno je da između dva skupa A i B s konačno mnogo elemenata postoji bijekcija $f : A \to B$ onda i samo onda ako skupovi A i B imaju isti broj elemenata.

Bijekcija $f : A \to A$, tj. iz skupa A u samog sebe, često se zove **permutacija** (premjestba) skupa A. Jedna vrlo važna permutacija skupa A je **identitet** $id : A \to A$, koja sve elemente u A ostavlja nepromijenjenim: $id(a) = a$.

Za dvije funkcije $f : A \to B$ i $g : B \to C$ (primijetite da su 'ulančane' preko skupa B), definirana je nova funkcija $g \circ f : A \to C$, zadana sa $(g \circ f)(a) = g(f(a))$. Zove se **kompozicija (skladanje) funkcija** f i g. Za kompoziciju triju (ulančanih) funkcija vrijedi zakon asocijativnosti: ako je $h : C \to D$, onda imamo $h \circ (g \circ f) = (h \circ g) \circ f$.

Pretpostavimo li da je $f : A \to B$ bijekcija, očevidno vrijedi $f^{-1} \circ f = id_A$ (identitet na skupu A) i $f \circ f^{-1} = id_B$ (identitet na skupu B). Ako je zadana još jedna bijekcija, $g : B \to C$, onda je $g \circ f : A \to C$ također bijekcija. Vrijedi sljedeće važno pravilo za nalaženje inverza kompozicije dviju bijekcija:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

U ovoj knjizi često će nam se pojavljivati pojam n **faktorijela**, $n!$, koji se za $n = 0$ definira kao $0! = 1$, a za bilo koji prirodni broj n kao umnožak n uzastopnih prirodnih brojeva od 1 do n:

$$n! = n(n-1)\ldots 2 \cdot 1.$$

Npr. $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$ itd. Vrijedi $(n+1)! = (n+1) \cdot n!$. Isto tako važan će nam biti pojam **binomnog koeficijenta** $\binom{n}{k}$, koji se definira za nenegativne cijele brojeve n i k uz uvjet $k \leqslant n$ sa: $\binom{n}{0} = 1$, a za $1 \leqslant k \leqslant n$ stavljamo

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}.$$

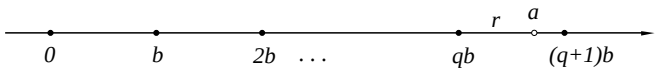
Primijetite da u brojniku imamo padajući umnožak točno k prirodnih brojeva, počevši od n. Lako se provjeri da je $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, i vrijedi svojstvo simetrije: $\binom{n}{k} = \binom{n}{n-k}$. Npr. $\binom{7}{4} = \binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35$.

Uobičajene kratke oznake za zbroj i produkt n realnih brojeva $a_1, a_2, \ldots, a_n$ su

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n, \quad \prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n.$$

Teorem o dijeljenju cijelog broja a s prirodnim brojem b kaže da postoje jednoznačno određni $q \in \mathbf{Z}$ (djelomični kvocijent) i ostatak $r \in \{0, 1, \ldots, b-1\}$ tako da je

$$a = qb + r.$$



Sl. 1.1. Algoritam dijeljenja: $a = qb + r$.

Prost ili prim broj je bilo koji prirodan broj $p \geqslant 2$ koji je djeljiv samo s 1 i sa p, tj. jedini djelitelji su mu 1 i on sam. To su redom: $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$, itd. Prostih brojeva ima beskonačno mnogo (Euklidov teorem). Podsjetimo 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. $12 = 4 \cdot 3 = 2^2 \cdot 3^1$, $9 = 3^2$, $11 = 11^1$.

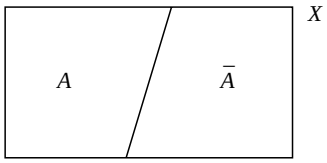
Algebra skupova. Kažemo da su skupovi A i B *jednaki* ako vrijedi $A \subseteq B$ i $B \subseteq A$. U tom slučaju pišemo $A = B$.

Unijom skupova A i B sadržanih u univerzalnom skupu X zovemo skup C svih elemenata x takvih da je $x \in A$ **ili** $x \in B$ (moguće je da je x i u oba skupa). Pišemo $C = A \cup B$. *Presjek* skupova A i B je skup D svih elemenata x takvih da je $x \in A$ **i** $x \in B$. Označavamo ga sa $D = A \cap B$ (skup zajedničkih elemenata u A i B). Ovdje smo namjerno istaknuli da je skupovna operacija $\cup$ povezana sa veznikom *ili*, a operacija $\cap$ sa veznikom *i*.

Za dva skupa A i B kažemo da su *disjunktni* ako im je presjek prazan, tj. $A \cap B = \emptyset$. Za veći broj ('familiju') skupova kažemo da čine *disjunktnu familiju skupova*, ako se niti koja dva skupa iz familije ne sijeku. Npr. tri skupa A, B i C čine disjunktnu familiju ako su $A \cap B$, $A \cap C$ i $B \cap C$ prazni skupovi.

Razlika skupova A i B je skup E svih elemenata x za koje je $x \in A$ i $x \notin B$. Oznaka je $E = A \setminus B$.

Ako je A podskup univerzalnog skupa X, onda definiramo *komplement* $\overline{A}$ skupa A sa $\overline{A} = X \setminus A$. Važno je primijetiti da komplement ovisi i o izboru univerzalnog skupa, tj. ispravnije bi bilo reći 'komplement skupa A u skupu X'. Očevidno je komplement od $\overline{A}$ jednak A, dotično $\overline{\overline{A}} = A$. Isto tako je jasno da vrijedi $A \setminus B = A \cap \overline{B}$. Komplement skupa A često se označava i sa A^c ili $\sim A$.



Sl. 1.2. Komplement skupa A.

DEFINICIJA. Za bilo koji skup X možemo definirati skup koji kao svoje elemente sadrži sve podskupove od X. Skup svih podskupova od X zovemo **partitivni skup** od

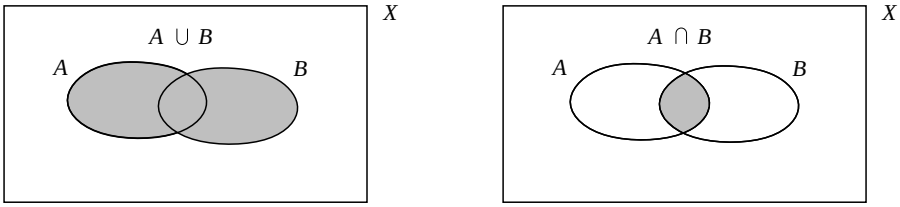
X. Označava se često sa $\mathcal{P}(X)$, ali mi ćemo radije rabiti oznaku 2^X. Razlog je sljedeći: ako skup X ima n elemenata, onda partitivni skup 2^X ima točno 2^n elemenata (vidi Teorem 3.1.5).

Npr. za skup $X = \{1,2,3\}$ je 2^X skup od sljedećih $2^3 = 8$ elemenata: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, $\{1,2,3\}$.

Kao što vidimo, elementi partitivnog skupa su podskupovi od X. Npr. $\emptyset \in 2^X$, $X \in 2^X$. Na partitivnom skupu definirane su tri osnovne operacije:

(i) dvije operacije $\cup$ (unija) i $\cap$ (presjek) koje dvama elementima $A, B \in \mathcal{P}(X)$ pridružuju treći element iz $\mathcal{P}(X)$. To su tzv. binarne operacije na X (opća definicija binarne operacije bit će dana u Poglavlju 2).

(ii) operacija komplementiranja $A \mapsto \overline{A}$, koja je unarna operacija, tj. operacija sa samo jednom varijablom $A \in \mathcal{P}(X)$.



Sl. 1.3. Unija i presjek skupova.

Nije teško dokazati da na partitivnom skupu $\mathcal{P}(X)$ vrijede neka jednostavna pravila s obzirom na tri navedene operacije: $\cup$, $\cap$ i komplementiranje u X.

Teorem 1. *Neka su $A, B, C \in 2^X$. Vrijede ova pravila algebre skupova:*

(1) idempotentnost operacija unije i presjeka: $A \cup A = A$, $A \cap A = A$;
(2) asocijativnost: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$;
(3) komutativnost: $A \cup B = B \cup A$, $A \cap B = B \cap A$;
(4) distributivnost: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
(5) **DeMorganove formule***: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$;*
(6) $A \cup \emptyset = A$, $A \cap X = A$;
(7) $A \cup X = X$, $A \cap \emptyset = \emptyset$;
(8) komplementiranost: $A \cup \overline{A} = X$, $A \cap \overline{A} = \emptyset$;
(9) involutivnost komplementiranja: $\overline{\overline{A}} = A$.

PRIMJEDBA 2. Iz teorema je vidljivo da sva navedena pravila algebre skupova imaju **svojstvo dualnosti**: ako u jednom pravilu zamijenimo svuda $\cup$ sa $\cap$ i obratno, i isto tako $\emptyset$ sa X i obratno, dobivamo također valjano pravilo algebre skupova. Na taj način se iz jednog zakona distribucije dobiva drugi – njemu dualan, iz jedne DeMorganove formule druga (i obratno).

PRIMJEDBA 3. Zbog svojstva asocijativnosti opravdano je umjesto $A \cup (B \cup C)$ pisati kraće $A \cup B \cup C$, i taj izraz računati na bilo koji od dva načina navedena u (2). Isto vrijedi i za $A \cap B \cap C$.

PRIMJEDBA 4. Ako imamo veći broj skupova $A_1, \ldots, A_n$, onda umjesto $A_1 \cup \ldots \cup A_n$ pišemo kraće $\cup_{k=1}^{n} A_k$. Slično i za presjek $\cap$. Ako imamo beskonačan slijed

(niz) skupova (A_n), $n = 1, 2, \ldots$, onda njihovu uniju označavamo sa $\cup_{k=1}^{\infty} A_k$ i slično za presjek.

PRIMJEDBA 5. U gornjem teoremu je dobro primijetiti da je $\emptyset$ najmanji, a X najveći element u sljedećem smislu: za svaki podskup A u X vrijedi $\emptyset \subseteq A \subseteq X$.

PRIMJER 1. Dokažimo za ilustraciju samo DeMorganovu formulu $\overline{A \cap B} = \overline{A} \cup \overline{B}$ u prethodnom teoremu. U tu svrhu dokažimo najprije da je skup na lijevoj strani jednakosti podskup skupa na desnoj strani. Neka je $x \in \overline{A \cap B}$, tj. $x \notin A \cap B$. Onda $x \notin A$ *ili* $x \notin B$ (jer x nije u oba skupa istodobno, vidi Sliku 1.3 desno). Dakle $x \in \overline{A}$ *ili* $x \in \overline{B}$, tj. $x \in \overline{A} \cup \overline{B}$. Time smo dokazali da je $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Obratna inkluzija dokazuje se na sličan način.

1.2. Kartezijev produkt skupova

U matematici je pojam Kartezijeva produkta skupova od iznimne važnosti, jer se susreće posvuda.

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 $\prod_{k=1}^{n} A_k$.

Kartezijev umnožak dvaju skupova dobro je gledati kao 'pravokutnik' razapet sa A_1 horizontalno i A_2 vertikalno, čiji su elementi točke oblika (a_1, a_2). Pri tom su a_1 i a_2 koordinatne vrijednosti. Vidi Sliku 3.1. Za tri skupa dobivamo 'kvadar' itd.

Korisno je znati da se Kartezijev umnožak skupova može opisati i na drugi, ravnopravan način. Ako je $(a_1, \ldots, a_n) \in \prod_{k=1}^{n} A_k$, onda taj n-terac možemo promatrati kao funkciju $f : \{1, \ldots, n\} \to \cup_{k=1}^{n} A_k$ takvu da je $f(k) = a_k$ i

$$f(k) \in A_k \qquad (*)$$

Obratno, svaka funkcija $f : \{1, \ldots, n\} \to \cup_{k=1}^{n} A_k$ sa tim svojstvom $(*)$ određuje pripadni n-terac $(a_1, \ldots, a_n)$ iz Kartezijeva produkta, gdje je $a_k = f(k)$. Drugim riječima, Kartezijev produkt skupova može se definirati i kao skup svih funkcija $f : \{1, \ldots, n\} \to \cup_{k=1}^{n} A_k$ sa svojstvom $(*)$.

PRIMJER 1. Za skupove $A_1 = \{1, 2, 3\}$ i $A_2 = \{a, b\}$ je

$$A_1 \times A_2 = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}.$$

Vidimo da za bilo koje konačne skupove A i B vrijedi da je broj elemenata u Kartezijevom produktu $A \times B$ jednak umnošku broja elemenata u A i B. Drugim riječima, vrijedi **produktno pravilo**: $|A \times B| = |A| \cdot |B|$, gdje smo s $|\cdot|$ označili broj elemenata skupa (tzv. kardinalni broj skupa).

POVIJESNA CRTICA Pojam funkcije uveo je 1694. g. *Gottfried Wilhelm Leibniz* (1646.–1716.), a u modernom smislu *Leonhard Euler* (1707.–1783.), od kojeg potječe i oznaka $f(x)$. Oznake $\subset$ i $\supset$ za relaciju podskupa i nadskupa među skupovima, kao i princip dualnosti u matematičku logiku, uveo je njemački matematičar

Ernst Schröder (1841.–1911.). Oznaku $\in$ za element skupa, zatim binarne operacije $\cup$ i $\cap$ za uniju i presjek skupova uveo je Talijan *Giuseppe Peano* (1858.–1932.). Često je korisno skupove označavati s pomoću Vennovih dijagrama, nazvanih prema engleskom matematičaru *Johnu Vennu* (1834.–1923.), vidi npr. Sliku 1.3.

1.3. Ekvipotentni skupovi, kardinalni broj

U ovom i daljnjim odjeljcima bit će nam vrlo važni pojmovi kao što su injektivna, surjektivna i bijektivna funkcija, te pojam slijeda.

DEFINICIJA. Za neprazan skup A kažemo da je **konačan** ako postoji prirodan broj n i bijekcija $f : \{1, 2, \ldots, n\} \to A$. Broj n zovemo **kardinalni broj skupa** A i označavamo ga sa $|A|$. Kažemo još da A ima n elemenata. U tom slučaju skup A je moguće zapisati kao $A = \{a_1, a_2, \ldots, a_n\}$, gdje je $a_k := f(k)$, $k = 1, \ldots, n$. I prazan skup $\emptyset$ smatramo konačnim skupom s kardinalnim brojem 0.

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.

Jasno je da je $\mathbf{N}$ prebrojiv skup. Vidjet ćemo kasnije da je čak i skup racionalnih brojeva $\mathbf{Q}$ prebrojiv, kao i to da je skup $\mathbf{R}$ neprebrojiv.

Ponekad je korisno znati ovo jednostavno svojstvo: ako je skup A *konačan* i ako je $f : A \to A$ injektivna funkcija, onda je f i surjekcija (dakle bijekcija). To slijedi odmah iz ove propozicije.

Propozicija 1. *Neka su A i B konačni skupovi koji imaju isti broj elemenata, tj. $|A| = |B|$. Funkcija $f : A \to B$ je injektivna onda i samo onda ako je surjektivna.*

DOKAZ. Neka je f injektivna funkcija. Onda skupovi A i $f(A)$ imaju isti broj elemenata, dotično $|A| = |f(A)|$. Zbog $|A| = |B|$ je onda $|f(A)| = |B|$. Odavde zajedno sa $f(A) \subseteq B$, i jer je B konačan skup, slijedi $f(A) = B$, dakle f je surjekcija.

Obratno, neka je f surjekcija. Onda je $|A| \geqslant |f(A)| = |B|$, pa zbog $|A| = |B|$ imamo $|A| = |f(A)|$. Budući da je A konačan skup, to znači da je f injekcija. ☺

Može se pokazati da beskonačni skupovi nemaju ovo svojstvo. Štoviše, skup A je beskonačan onda i samo onda ako postoji bijekcija na neki njegov pravi podskup, vidi Primjer 1 niže.

Kao što smo rekli, za beskonačan skup A kažemo da je prebrojiv ako se njegovi članovi mogu poredati u slijed: $A = \{a_1, a_2, \ldots\}$. Ekvivalentno tome, skup A je prebrojiv ako postoji *bijekcija* $f : \mathbf{N} \to A$.

Doista, ako je $A = \{a_1, a_2, \ldots, a_k, \ldots\}$ prebrojiv skup, onda možemo definirati bijekciju $f : \mathbf{N} \to A$ sa $f(k) = a_k$. Obratno, ako je $f : \mathbf{N} \to A$ bijekcija, onda skup A možemo poredati u slijed (niz) stavljajući $a_k := f(k)$. Funkcija f zove se funkcija prebrojavanja skupa A.

PRIMJER 1. Skup svih parnih brojeva $2\mathbf{N} = \{2, 4, 6, \ldots\}$ je prebrojiv, jer je $f : \mathbf{N} \to 2\mathbf{N}$, $f(k) = 2k$, bijekcija (provjerite). Općenitije, svaki beskonačan podskup

skupa prirodnih brojeva je prebrojiv, jer se očevidno može poredati u slijed brojeva po veličini, vidi Teorem 3 niže.

A što bi bio kardinalni broj skupa koji je beskonačan? Da bismo došli do tog pojma, primijetimo da skup A ima n elemenata onda i samo onda ako postoji bijekcija s A na skup $\{1,2,\ldots,n\}$. Definirajmo zato najprije pojam ekvipotentnosti među skupovima.

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

Ekvipotentnost je zapravo jedna relacija među skupovima, o kojima će više riječi biti u Poglavlju 2.

Teorem 2. *Označimo svojstvo da je skup A ekvipotentan sa skupom B oznakom $A \sim B$. Ekvipotentnost ima ova temeljna svojstva:*

(i) refleksivnost: $A \sim A$ za svaki skup A;
(ii) simetričnost: ako je $A \sim B$, onda je i $B \sim A$;
(iii) tranzitivnost: ako je $A \sim B$ i $B \sim C$, onda je $A \sim C$.

DOKAZ. (i) Identitet $\mathrm{id} : A \to A$, $\mathrm{id}(x) = x$, je bijekcija; (ii) ako je $f : A \to B$ bijekcija, onda je i inverzna funkcija $f^{-1} : B \to A$ također bijekcija; (iii) Ako su funkcije $f : A \to B$ i $g : B \to C$ bijekcije, onda je i njihova kompozicija $g \circ f : A \to C$ također bijekcija. ☺

Jasno je da za konačne skupove A i B njihova ekvipotentnost znači upravo to da imaju isti broj elemenata. Broj elemenata konačnog skupa zovemo *kardinalni broj* skupa. Razumno je na sličan način definirati i kardinalni broj za beskonačne skupove.

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

Ako je zadan konačan skup $A = \{a_1, \ldots, a_n\}$, onda je njegov kardinalni broj jednak n: $|A| = n$.

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 $|\mathbf{R}| = c$.

Kardinalne brojeve bilo koja dva skupa A i B možemo uspoređivati ovako. Kažemo da je $|A| \leqslant |B|$ (i čitamo: kardinalni broj skupa A je **manji ili jednak** od kardinalnog broja skupa B) ako postoji *injektivna* funkcija $f : A \to B$. To je isto što i reći da je skup A ekvipotentan s nekim podskupom od B (i to upravo sa $f(A)$). Ukoliko je $|A| \leqslant |B|$ i skupovi A i B nisu ekvipotentni, onda pišemo $|A| < |B|$. Ako su skupovi A i B konačni, onda $|A| \leqslant |B|$ izražava uobičajen odnos $\leqslant$ (manje ili jednako) između broja elementa skupa A i broja elemenata skupa B.

Može se pokazati da ako je $|A| \leqslant |B|$ (tj. skup A je ekvipotentan nekom podskupu od B) i $|B| \leqslant |A|$ (tj. skup B je ekvipotentan nekom podskupu A), onda postoji i bijekcija između skupova A i B, tj. $|A| = |B|$. Za beskonačne skupove ova tvrdnja zove se *Schröder–Bernsteinov teorem*, i njen dokaz nije jednostavan, vidi [Papić, str. 55]. Naravno, za konačne skupove A i B ova je tvrdnja očevidna.

Jasno je da vrijedi $\mathbf{N} \subset \mathbf{R}$, pa je dakle $\aleph_0 \leqslant c$. Kasnije ćemo pokazati da ne postoji bijekcija sa skupa $\mathbf{N}$ na $\mathbf{R}$, odakle će slijediti da su ova dva beskonačna kardinalna broja međusobno različita, tj. $\aleph_0 < c$ (vidi Teorem 1.5.1).

PRIMJER 2. Budući da postoji bijekcija sa $\mathbf{N} = \{1, 2, 3, \ldots\}$ na $2\mathbf{N}$ (skup svih parnih brojeva), onda je $|\mathbf{N}| = |2\mathbf{N}| = \aleph_0$. Dakle imamo *skup koji je ekvipotentan svom pravom podskupu*! Kod konačnih skupova se tako što ne može dogoditi. Takvu vlastitost imaju svi beskonačni skupovi, i samo oni. Evo još tri slična primjera:

(i) Skupovi $(-1, 1)$ i $\mathbf{R}$ su ekvipotentni. Dovoljno je vidjeti da je funkcija $f : \mathbf{R} \to (-1, 1)$ zadana sa $f(x) = \operatorname{th} x$ bijekcija.

(ii) Bilo koja dva otvorena intervala u $\mathbf{R}$ oblika (a, b) i (c, d) su ekvipotentna. Naime, funkcija $f : (a, b) \to (c, d)$ definirana sa $f(x) = \frac{d-c}{b-a}(x - a) + c$ je bijekcija (pravac kroz točke $A(a, c)$ i $B(b, d)$ u ravnini).

(iii) Skupovi $\mathbf{N}$ i njegov pravi podskup $\{5, 6, 7, \ldots\}$ su ekvipotentni, jer je funkcija pomaka $f(k) = k + 4$ bijekcija među njima.

U dokazu sljedećeg teorema rabit ćemo očevidnu činjenicu da svaki podskup skupa prirodnih brojeva ima minimalni element.

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.

Teorem 4. *Neka je A beskonačan skup i K njegov konačan podskup. Onda su skupovi A i $A \setminus K$ ekvipotentni, tj. $|A| = |A \setminus K|$.*

DOKAZ. Neka je $K = \{a_1, \ldots, a_k\}$. Budući da je A beskonačan skup, onda postoji prebrojiv podskup S, koji sadrži K, tj. $S = \{a_1, \ldots, a_k, a_{k+1}, \ldots\}$. Funkcija $f : A \to A \setminus K$ definirana kao identitet na $A \setminus S$ i kao pomak za k na slijedu S:

$$f(x) = \begin{cases} x, & \text{za } x \in A \setminus S, \\ a_{i+k}, & \text{za } x = a_i \in S, \end{cases}$$

je očevidno bijekcija. ☺

PRIMJER 3. Na temelju ovog stavka imamo zanimljiv zaključak: skupovi $[0, 1]$, $(0, 1]$, $(0, 1)$ su ekvipotentni.

PRIMJEDBA 2. Spomenimo da se kardinalni broj skupa A u literaturi često označava i sa $\operatorname{card} A$ ili $\sharp A$ umjesto $|A|$.

1.4. Prebrojivi skupovi i njihovo kodiranje

Rabeći Primjedbu 1.3.1 možemo lako dokazati da je npr. skup $\mathbf{N}^k = \mathbf{N} \times \ldots \times \mathbf{N}$ svih poredanih k–teraca prirodnih brojeva prebrojiv. Štoviše, vrijedi

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 $2^6 3^{14} 5^9$.

PRIMJEDBA 1. Skup svih konačnih sljedova cijelih brojeva je prebrojiv. Budući da je skup svih konačnih sljedova sastavljenih samo od 0 i 1 njegov beskonačan podskup, onda je i on prebrojiv. Čine ga sljedovi nula i jedinica oblika: 0, 101, 1101001 itd.

Pokazuje se da je skup svih *beskonačnih* sljedova nula i jedinica neprebrojiv, dotično ima kardinalni broj c (dakle ekvipotentan je sa $\mathbf{R}$; vidi sljedeći odjeljak).

Teorem 2. *Skupovi cijelih brojeva $\mathbf{Z}$ i racionalnih brojeva $\mathbf{Q}$ su prebrojivi.*

DOKAZ. (i) Najprije ćemo skup svih pozitivnih cijelih brojeva preslikati bijektivno u skup svih parnih prirodnih brojeva, a zatim negativne cijele brojeve i nulu bijektivno u neparne prirodne brojeve. To radi funkcija $f : \mathbf{Z} \to \mathbf{N}$ koja pozitivnim cijelim brojevima pridružuje parne prirodne brojeve, a nuli i negativnim cijelim brojevima pridružuje neparne prirodne brojeve:

$$f(k) = \begin{cases} 2k & \text{za } k > 0, \\ 2|k| + 1 & \text{za } k \leqslant 0, \end{cases}$$

Ona je očevidno bijekcija.

(ii) Dovoljno je pronaći injektivnu funkciju $f : \mathbf{Q} \to \mathbf{N}$, vidi Teorem 1.3.3. Možemo ju lako konstruirati kodiranjem. Svaki racionalan broj x je određen s tri podatka: predznakom p ($+1$ ili -1), brojnikom $m \in \mathbf{N}_0$ i nazivnikom $n \in \mathbf{N}$. Pretpostavit ćemo da su brojnik i nazivnik skraćeni do kraja (tj. bez zajedničkog djelitelja > 1). Funkcija $f : \mathbf{Q} \to \mathbf{N}$ definirana sa $f(p\frac{m}{n}) = 2^{p+1} 3^m 5^n$ je injektivna, što se dobiva odmah iz Osnovnog teorema aritmetike. Naime ako je $f(p_1 \frac{m_1}{n_1}) = f(p_2 \frac{m_2}{n_2})$, onda je $2^{p_1+1} 3^{m_1} 5^{n_1} = 2^{p_2+1} 3^{m_2} 5^{n_2}$, dakle $p_1 + 1 = p_2 + 1$, $m_1 = m_2$, $n_1 = n_2$, dotično $p_1 \frac{m_1}{n_1} = p_2 \frac{m_2}{n_2}$. ☺

PRIMJEDBA 2. Prebrojivost skupa $\mathbf{Z}$ cijelih brojeva može se lako dokazati i kodiranjem. Pokušajte. I prebrojivost skupa $\mathbf{Q}$ racionalnih brojeva može se dokazati izravno, tako da se poreda u slijed. Racionalne brojeve pišemo u obliku $\pm\frac{m}{n}$ i slažemo ih u slijed ovako:

(1) najprije pišemo nulu, zatim

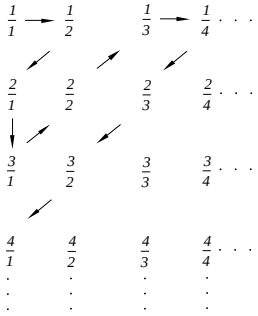
(2) poredamo sve pozitivne racionalne brojeve kojima je zbroj brojnika i nazivnika jednak 2: $\frac{1}{1}$,

(2') poredamo sve negativne racionalne brojeve kojima je zbroj brojnika i nazivnika jednak -2: $-\frac{1}{1}$,

(3) pišemo sve pozitivne racionalne brojeve kojima je zbroj brojnika i nazivnika jednak 3: $\frac{1}{2}$, $\frac{2}{1}$,

(3') poredamo sve negativne racionalne brojeve kojima je zbroj brojnika i nazivnika jednak 3: $-\frac{1}{2}$, $-\frac{2}{1}$,

itd. Dakle skup racionalnih brojeva $\mathbf{Q}$ može se poredati u slijed ovako 0, 1, -1 $\frac{1}{2}$, $\frac{2}{1}$, $-\frac{1}{2}$, $-\frac{2}{1}$, $\frac{1}{3}$, $\frac{3}{1}$, $\frac{2}{2}$, $\frac{3}{1}$, $-\frac{1}{3}$, $-\frac{2}{2}$, $-\frac{3}{1}$, itd. Pri tom se neki od racionalnih brojeva i ponavljaju. Time je dokazano da vrijedi $|\mathbf{Q}| = \aleph_0$. Sljedeća slika pokazuje kako se pozitivni racionalni brojevi mogu poredati u slijed:



Sl. 1.4.

1.5. Neprebrojivost skupa realnih brojeva

Kao što smo rekli, kardinalni broj skupa realnih brojeva $\mathbf{R}$ zovemo *kontinuum* (kažemo da realnih brojeva ima kontinuum), a kardinalni broj skupa prirodnih brojeva zovemo $\aleph_0$ (alef nula). Zbog $\mathbf{N} \subset \mathbf{R}$ je očevidno $\aleph_0 \leqslant c$. Sljedeći teorem pokazuje da je $\aleph_0 \neq c$. Skupovi realnih i racionalnih brojeva su oba beskonačni, ali ne podjednako. Pokažimo da je skup realnih brojeva 'više beskonačan' nego skup racionalnih.

Teorem 1. (Georg Cantor) *Skup* $\mathbf{R}$ *je neprebrojiv, tj. nije ekvipotentan sa skupom* $\mathbf{N}$. *Drugim riječima vrijedi* $\aleph_0 < c$, *tj. skup realnih brojeva ne može se poredati u slijed.*

DOKAZ. (Cantorov dijagonalni postupak) Pretpostavimo suprotno, tj. da je skup $\mathbf{R}$ prebrojiv. Već smo vidjeli da je $\mathbf{R}$ ekvipotentan s intervalom $(0,1]$, pa se onda i skup $(0,1]$ može poredati u slijed: $(0,1] = \{x_1, x_2, \ldots\}$. Prikažimo ove brojeve u decimalnom zapisu. Taj prikaz nije jednoznačan, jer se npr. broj s konačnim decimalnim prikazom 0.31 može pisati i u obliku beskonačnog decimalnog

prikaza $0.30999\ldots$. Za svaki broj iz $(0,1]$ rabit ćemo, radi jednoznačnosti, njegov beskonačan decimalni prikaz. Onda vrijedi

$$x_1 = 0.\boldsymbol{a}_{11}a_{12}a_{13}\ldots$$
$$x_2 = 0.a_{21}\boldsymbol{a}_{22}a_{23}\ldots$$
$$x_3 = 0.a_{31}a_{32}\boldsymbol{a}_{33}\ldots,$$

gdje su a_{ij} znamenke između 0 i 9. Pogledajmo sada slijed znamenaka a_{11}, a_{22}, a_{33} itd. na "dijagonali" u gornjem decimalnom prikazu. Odaberimo slijed znamenaka b_n iz skupa $\{1,\ldots,9\}$ na ovaj način: znamenka b_1 neka je odabrana tako da bude različita od a_{11}, b_2 različita od a_{22} itd. Onda je broj $b := 0.b_1b_2b_3\ldots$ različit od x_1 (ne podudaraju se u prvoj decimali), isto tako $b \neq x_2$ (ne podudaraju se u drugoj decimali), itd. Stoga $b \notin \{x_1, x_2, x_3\ldots\} = (0,1]$. To je kontradikcija, jer decimalni prikaz od b pokazuje da je $b \in (0,1]$. ☺

PRIMJEDBA 1. Gledajući brojeve iz intervala $[0,1]$ u binarnom zapisu, nije teško vidjeti da je na isti način i skup svih beskonačnih sljedova sastavljenih samo od nula i jedinica (npr. $010110\ldots$) neprebrojiv.

PRIMJEDBA 2. Vidjeli smo da ako je $A \subseteq \mathbf{N}$, onda je A ili konačan ili prebrojiv skup. Postavlja se pitanje vrijedi li nešto slično i za skup A za koji je

$$\mathbf{N} \subseteq A \subseteq \mathbf{R},$$

tj. slijedi li odavde da je nužno $|A| = \aleph_0$ ili $|A| = c$? Ta se hipoteza zove *Cantorova hipoteza kontinuuma*. Ili možda postoji skup A takav da je $\aleph_0 < |A| < c$, tj. postoji kardinalni broj koji je strogo između $\aleph_0$ i c?

Neočekivan odgovor na to pitanje dao je *Paul Cohen* 1964. g. Navedeni problem je *neodlučiv*. To znači da se hipoteza kontinuuma ne može niti dokazati niti opovrgnuti s pomoću preostalih aksioma teorije skupova. Drugim riječima, moguća je jedna suvisla teorija skupova u kojoj će hipoteza kontinuuma vrijediti (tj. nema kardinalnog broja između $\aleph_0$ i c), a moguća je isto tako i druga suvisla teorija skupova u kojoj hipoteza kontinuuma neće vrijediti. Hipoteza kontinuuma ne može se izvesti iz standardne aksiomatike teorije skupova, pa se ona sama može postulirati kao nezavisan aksiom teorije skupova, ili pak se može postulirati njena negacija.

Problem je sličan kao kod znamenitog petog Euklidova aksioma (aksioma o paralelama - *kroz zadanu točku u ravnini prolazi točno jedan pravac paralelan sa zadanim pravcem*): može li se peti Euklidov aksiom izvesti iz prva četiri? Pokazuje se da ne može. Pažljivo razmatranje tog pitanja dovelo je do otkrića neeuklidskih geometrija (Lobačevski, i još ranije Gauss).

PRIMJEDBA 3. Skup svih racionalnih brojeva $\mathbf{Q}$ je prebrojiv (Teorem 1.4.2), skup svih realnih je neprebrojiv (Teorem 1), dakle skup svih **iracionalnih brojeva** $\mathbf{R} \setminus \mathbf{Q}$ (tj. realnih brojeva koji nisu racionalni) je neprebrojiv, točnije, $|\mathbf{R} \setminus \mathbf{Q}| = c$. Iracionalni brojevi su točno oni čiji decimalni prikaz nije periodičan. Može se dokazati da je i $|\mathbf{C}| = c$, dotično skupovi $\mathbf{C}$ i $\mathbf{R}$ su ekvipotentni. Štoviše, za svaki prirodan broj n vrijedi $|\mathbf{R}^n| = c$, gdje je $\mathbf{R}^n$ skup svih poredanih n-teraca realnih brojeva.

Još jedan važan prebrojiv skup koji je sadržan u (neprebrojivom) skupu realnih brojeva čini skup algebarskih brojeva.

DEFINICIJA. Za realan broj a kažemo da je **algebarski broj** ako postoji polinom $P(x)$ s cjelobrojnim koeficijentima koji nisu svi 0, takav da je $P(a) = 0$.

Primjeri algebarskih brojeva su svi racionalni brojevi $\frac{b}{a}$, gdje je $a \in \mathbf{N}$, $b \in \mathbf{Z}$ (nultočka od $ax - b$), $\sqrt{2}$ (nultočka od $x^2 - 2$), $\sqrt[3]{2}$ (nultočka od $x^3 - 2$), $\sqrt[5]{2 + \sqrt{3/7}}$ (lako možete naći polinom s cjelobrojnim koeficijentima čija je ovo nultočka), itd. itd. Vrijedi ovakav iznenađujuć rezultat:

Propozicija 2. *Skup svih algebarskih brojeva je (samo) prebrojiv.*

DOKAZ. Svakom polinomu s cjelobrojnim koeficijentima možemo pridružiti konačan slijed njegovih cjelobrojnih koeficijenata. Budući da je to pridruživanje injektivno, i skup konačnih sljedova cijelih brojeva prebrojiv (po Teoremu 1.4.1), onda je i skup svih polinoma s cjelobrojnim koeficijentima prebrojiv, tj. možemo ga poredati u slijed: $P_1, P_2, P_3, \ldots$ Svakom od tih polinoma pripada konačno

mnogo kompleksnih nultočaka (najviše onoliko koliki je stupanj pripadnog polinoma; Gaussov *osnovni teorem algebre*). Prebrojivost skupa svih tih nultočaka (algebarskih brojeva) može se pokazati "nadovezivanjem". Npr. ako je P_1 polinom četvrtog stupnja s nul-točkama z_{11}, z_{12}, z_{13}, z_{14}, onda im pridružimo prirodne brojeve $1, 2, 3, 4$, ako je P_2 polinom desetog stupnja s nultočkama $z_{21}z_{22}\ldots z_{2,10}$, pridružujemo im brojeve $5, 6, \ldots 14$, itd. ☺

DEFINICIJA. Realni brojevi koji nisu algebarski zovu se **transcendentni brojevi**.

Na temelju prethodne propozicije zaključujemo da je skup transcendentnih brojeva (čak) neprebrojiv. To nije baš u skladu s činjenicom da smo do sada upoznali samo dva od njih: π i e. Ima ih međutim još, poput $2^{\sqrt{3}}$, $\ln 2$, $\sin 1$ (vidi povijesnu crticu na str. 222). Jedan neprebrojiv skup transcendentnih brojeva može se konstruirati ovako: $x = \sum_{n=1}^{\infty} \frac{a_n}{10^{n!}}$, gdje je $a_n \in \{0, 1\}$ i skup svih a_n koji su jednaki 1 je beskonačan. Da je svaki od tih brojeva transcendentan, dokazao je francuski matematičar *Joseph Liouville* (1809–1882). Njihova neprebrojivost je jasna: svakom x možemo bijektivno pridružiti slijed (a_n) nula i jedinica (taj skup sljedova je neprebrojiv).

Zadatci za vježbu

1. Ispitaj koja je od sljedećih funkcija $f : \mathbf{N} \to \mathbf{N}$ injekcija, surjekcija, ili bijekcija: (a) $f(k) = 2k + 3$ (b) $f(n) = (n-5)^2 + 3$, (c) $f(x) = x^2 + 2x + 3$ (d) $f(a) = a^3 - 3a + 5$.

2. Zadan je skup $A = \{1, 2, 3\}$. (a) Uvjeri se da ima ukupno 27 funkcija $f : A \to A$. (b) Nađi sve surjektivne funkcije $f : A \to A$. (c) Nađi sve injektivne funkcije $f : A \to A$. (d) Nađi sve bijekcije $f : A \to A$.

3. Pokaži da je skup A svih neparnih brojeva prebrojiv tako da konstruiraš bijekciju s $\mathbf{N}$ na A.

4. Konstruiraj formulom neku bijekciju sa skupa $\mathbf{N}$ na skup A svih onih prirodnih brojeva koji pri dijeljenju s 5 daju ostatak 3. Nađi njoj inverznu funkciju.

5. Konstruiraj neku bijekciju $h : A \to B$, gdje je A skup svih prirodnih brojeva koji pri dijeljenju s 5 daju ostatak 3, a B skup svih prirodnih brojeva koji pri dijeljenju s 3 daju ostatak 2.

6. Konstruiraj formulom neku injektivnu funkciju sa skupa $\mathbf{Z} \times \mathbf{Z}$ u skup $\mathbf{N}$.

7. Konstruiraj (što je moguće jednostavnijom formulom) neku surjektivnu funkciju iz skupa $\mathbf{Z} \times \mathbf{Z}$ na $\mathbf{N}$.

8. Konstruiraj neku bijekciju sa skupa $\mathbf{Z} \times \mathbf{Z}$ u skup $\mathbf{N}$.

9. (teži zadatak) Napiši računalni program koji će unosom cijelih brojeva x i y dati na izlazu redni broj n točke $T_n(x, y)$ u gore opisanom spiralnom prebrojavanju.

10. (teži zadatak) Konstruiraj bijekciju sa zatvorenog intervala $[0, 1]$ na poluotvoren interval $(0, 1]$. Nacrtaj graf te funkcije.

Naputci i rješenja

1. (a) Za injektivnost treba provjeriti da $f(k_1) = f(k_1) \Rightarrow 2k_1 + 3 = 2k_2 + 3 \Rightarrow k_1 = k_2$. (d) Ispitaj intervale monotonosti ove funkcije gledajući najprije a kao realnu varijablu.

2. (a) Sve funkcije dobijemo tako da elementima $1,2,3$ pridružujemo redom $1,1,1$ (to je prva funkcija), zatim $1,1,2$ (druga), $1,1,3$ (treća), pa

$$\begin{array}{lll} 1,2,1, & 1,2,2, & 1,2,3, \\ 1,3,1, & 1,3,2, & 1,3,3, \\ 2,1,1, & 2,1,2, & 2,1,3, \\ 2,2,1, & 2,2,2, & 2,2,3, \\ 3,1,1, & 3,1,2, & 3,1,3, \end{array}$$

i na koncu $3,2,1$, $3,2,2$, $3,3,3$ (dvadeset sedma funkcija). (b) Sve surjekcije iz konačnog skupa u samoga sebe su bijekcije, tj. kao u (d). (c) Svaka injekcija iz A u A, gdje je A konačan skup, je bijekcija. (d) Svih bijekcija iz A u A ima ukupno 6: f_1, f_2,..., $f_6 : A \to A$. Na pr. f_1 preslikava $1,2,3$ redom u $1,2,3$ (identitet), f_2 preslikava $1,2,3$ redom u $1,3,2$, f_3 redom u $2,1,3$, f_4 u $2,3,1$, f_5 u $3,1,2$, a f_6 u $3,2,1$.

3. Konstruiraj formulom neku bijekciju $f : \mathbf{N} \to 2\mathbf{N} - 1$, gdje je $2\mathbf{N} - 1$ skup svih neparnih brojeva, $2\mathbf{N} - 1 = \{1, 3, 5, \ldots\}$. Na pr. $f(k) = 2k - 1$.

4. Elementi skupa $A = \{3, 8, 13, 18, \ldots\}$ su oblika $5k + 3$, gdje je $k \in \mathbf{N} \cup \{0\}$, tj. $A = 5 \cdot (\mathbf{N} - 1) + 3$. Dakle jedna prirodna bijekcija je oblika $f(n) = 5(n-1) + 3$.

5. Neka je $f : \mathbf{N} \to A$ iz prethodnog zadatka, i na sličan način konstruiramo bijekciju $g : \mathbf{N} \to B$, $g(n) = 3(n-1)+2$. Onda je $h(x) = (g \circ f^{-1})(x) = \frac{3x+1}{5}$. Može i ovako: definiramo $h(5(n-1)+3) = 3(n-1)+2$, tj. za $x = 5(n-1)+3 = 5n-2$ je $n = \frac{1}{5}(x+2)$. Dakle, $h(x) = 3n - 1 = \frac{3}{5}(x+2) - 1 = \frac{3x+1}{5}$.

6. Za $(x,y) \in \mathbf{Z} \times \mathbf{Z}$ možemo pisati $x = (\operatorname{sgn} x) \cdot |x|$, $y = (\operatorname{sgn} y) \cdot |y|$, gdje je $\operatorname{sgn} x = 1$ za $x \geqslant 0$, a $\operatorname{sgn} x = -1$ za $x < 0$. Prema tome možemo definirati na pr. $f(x,y) = 2^{\operatorname{sgn} x + 1} 3^{|x|} 5^{\operatorname{sgn} y + 1} 7^{|y|}$. Iz osnovnog teorema aritmetike odmah slijedi da je f injektivna funkcija iz $\mathbf{Z} \times \mathbf{Z}$: $f(x_1,y_1) = f(x_2,y_2) \Rightarrow 2^{\operatorname{sgn} x_1 + 1} 3^{|x_1|} 5^{\operatorname{sgn} y_1 + 1} 7^{|y_1|} = 2^{\operatorname{sgn} x_2 + 1} 3^{|x_2|} 5^{\operatorname{sgn} y_2 + 1} 7^{|y_2|} \Rightarrow \operatorname{sgn} x_1 = \operatorname{sgn} x_2$, $|x_1| = |x_2|$, i isto za y-ne, dakle $x_1 = x_2$, $y_1 = y_2$, tj. $(x_1,y_1) = (x_2,y_2)$.

7. Na pr. $f(x,y) = |x| + 1$.

8. Skup $\mathbf{Z} \times \mathbf{Z}$ može se shvatiti kao cjelobrojna mreža u ravnini, tj. kao skup svih točaka $T(x,y)$ s cjelobrojnim koordinatama. Jedna bijekcija iz cjelobrojne mreže na skup svih prirodnih brojeva može se konstruirati tako da prebrojimo redom sve točke na mreži: prva točka neka je ishodište $T_1(0,0)$, druga neka je prva desno $T_2(0,1)$, treća neka prva sljedeća prema gore $T_3(1,1)$, i zatim nastavljamo redom spiralno oko ishodišta (u smjeru paralelno s koordinatnim osima, obrnuto od kazaljke na satu).

10. Pogledaj dokaz teorema 1.3.4.

POVIJESNA CRTICA Nijemac *Richard Dedekind* (1838.–1916.) bio je prvi koji je beskonačan skup definirao kao onaj koji je ekvipotentan sa svojim pravim podskupom. To svojstvo je znao već *Galileo Galilei* (1564.–1642.) za skup prirodnih brojeva. Opći pojam kardinalnog broja za bilo koji beskonačan skup uveo je *Georg Cantor* (1845.–1918.), kao i oznaku $\aleph_0$ za $|\mathbf{N}|$. On je dokazao da je $\aleph_0 < c$, tj. da ne postoji bijekcija između $\mathbf{N}$ i $\mathbf{R}$ (tj. skup realnih brojeva se ne može poredati u slijed), rabeći svoj znameniti dijagonalni postupak. Georg Cantor je i jedan od osnivača teorije skupova. Srednjovjekovni matematičari smatrali su paradoksom činjenicu da dva segmenta različitih duljina imaju isti broj elemenata. Nejasnoće je riješio Cantor uvođenjem relacije ekvipotentnosti među skupovima. On je pokazao da npr. skupovi $\mathbf{N} \subset \mathcal{P}(\mathbf{N}) \subset \mathcal{P}(\mathcal{P}(\mathbf{N})) \subset \ldots$ imaju kardinalne brojeve koji su ne samo svi beskonačni, nego i međusobno različiti: $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$ (vidi [Papić, Teorem 3.20]).

Dokaz da je broj π iracionalan prvi je dao *Johann Lambert* (1728.–1777.), a dokaz da je on čak transcendentan dao je tek 1882. g. njemački matematičar *Johann Lindemann* (1852.–1932.). Transcendentnost broja e dokazao je francuski matematičar *Charles Hermite* (1822.–1901.). Dokazi su vrlo složeni.

Važnu ulogu u razvoju moderne teorije skupova imali su među inim engleski matematičar *Bertrand Russel* (1872.–1970.) i austrijski matematičar *Kurt Gödel* (rođen u Brnu u današnjoj Češkoj, 1906.–1978.).

Beskonačno!
Niti koje drugo pitanje nije nikada toliko duboko dirnulo duh čovjeka.
— David HILBERT (1862.–1943.)

Prema legendi, sv. Augustin je, šečući uz obalu mora, i razmišljajući o beskonačnom, ugledao dijete koje je pokušavalo isprazniti ocean uz pomoć jedne školjke. . .

U svakoj [znanstvenoj] disciplini treba pažljivo razlučiti tri aspekta teorije:
(a) formalno logički sadržaj, (b) intuitivnu pozadinu, (c) primjene.
— William (Vilim) FELLER (1906-1970)

Nemoj samo čitati; bori se! Postavljaj svoja vlastita pitanja,
traži svoje vlastite primjere, otkrij svoje vlastite dokaze.
Je li pretpostavka nužna? Je li obrat istinit? Što se događa u specijalnom slučaju?
Što je s degeneriranim slučajevima? Gdje dokaz rabi pretpostavke?
— Paul R. HALMOS (1916.)

[Kad su ga pitali koliko ima godina.]
Imao sam x godina u godini x^2. [Izračunaj x.]
— Augustus DeMORGAN (1806.–1871.)

Cijele je brojeve stvorio dragi Bog, a sve ostalo djelo je čovjeka!
— Leopold KRONECKER (1823.–1891.)

2.
Binarne relacije

2.1. Refleksivne, simetrične, tranzitivne relacije

Svakodnevno smo okruženi mnogobrojnim relacijama na raznim skupovima, s pomoću kojih se definira "odnos" između dva elementa nekog skupa (prvog i drugog). Evo nekih "relacija" definiranih na skupu svih ljudi (zadanih na parovima od dvoje ljudi x i y): biti jednako star kao (x je jednako star kao y), biti stariji od, biti mlađi od, biti viši od, biti lakši od, biti brži od, ne biti sporiji od, imati istu boju očiju kao, biti obrazovaniji od, biti zaljubljen u, biti brat od, biti majka od, biti rođen u istom mjestu kao, biti iste nacionalnosti kao, biti u vezi putem Interneta sa, itd.itd.

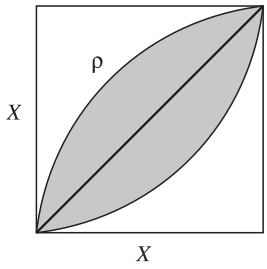
DEFINICIJA. **Binarna relacija** na skupu X je bilo koji neprazan podskup $\rho \subseteq X \times X$. Kažemo da su elementi x i y *u relaciji* ρ (ili x je u relaciji s y) ako je $(x,y) \in \rho$. U tom slučaju pišemo $x \rho y$.

PRIMJEDBA 1. Riječ *binarna* (relacija) znači da imamo "odnos" ρ između *dva* elementa, pri čemu je važno znati koji je prvi, a koji drugi. Može se naime dogoditi da bude $x \rho y$, a da ne bude $y \rho x$. Isto tako može se dogoditi da ne bude niti $x \rho y$ niti $y \rho x$. U tom slučaju kažemo da su x i y *neusporedivi* (po dotičnoj relaciji).

DEFINICIJA. Za binarnu relaciju ρ na X kažemo da je

(i) **refleksivna** ako vrijedi $(\forall x \in X)\, x \rho x$;
(ii) **simetrična** ako vrijedi $(\forall x, y \in X)(x \rho y \Rightarrow y \rho x)$;
(iii) **tranzitivna** ako vrijedi $(\forall x, y, z \in X)(x \rho y \wedge y \rho z \Rightarrow x \rho z)$.

Provjerite za vježbu koje su od relacija navedenih na skupu svih ljudi refleksivne, koje simetrične, a koje tranzitivne. Svaka refleksivna relacija sadrži "dijagonalu" u skupu $X \times X$, tj. skup $\{(x,x) : x \in X\}$. Naziv simetrične relacije jasan je sa slike.



Sl. 2.1. Simetrična relacija.

PRIMJER 1. Relacija ρ zadana na skupu X zove se *funkcija* ako za svaki $x \in X$ postoji jedincat $y \in X$ takav da je $x \rho y$ (tj. relacijom je svakom x pridružen jedincat y). Drugim riječima, iz $x \rho y_1$ i $x \rho y_2$ slijedi $y_1 = y_2$. Tu relaciju obično označavamo sa $f : X \to X$, $y = f(x)$.

Obratno, svaka funkcija $f : X \to X$ također određuje relaciju ρ. Prirodno je ρ definirati tako da je $x \rho y$ onda i samo onda ako je $y = f(x)$.

2.2. Relacija ekvivalencije

Uvedimo sada jednu osobito važnu relaciju:

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).

PRIMJER 1. Relacija $=$ (jednako) na skupu svih prirodnih brojeva je očevidno relacija ekvivalencije. Relacija $\leqslant$ nije relacija ekvivalencije, jer nije simetrična.

Pogledajmo još nekoliko primjera relacije ekvivalencije. Najprije navedimo jednu važnu definiciju.

DEFINICIJA. Kažemo da su cijeli brojevi a i b **kongruentni po modulu** n (ili modulo n), $n \in \mathbf{N}$, ako je razlika $a - b$ djeljiva sa n, tj. $n \mid a - b$. U tom slučaju pišemo

$$a \equiv b \pmod{n},$$

i čitamo "a je kongruentan b po modulu (modulo) n". To je isto što i reći da je $a - b \in n\mathbf{Z} = \{0, n, -n, 2n, -2n, \ldots\}$. Nije teško vidjeti da su a i b kongruentni po modulu n onda i samo onda ako a i b pri dijeljenju s n daju isti ostatak.

Propozicija 1. *Kongruencija po modulu n je relacija ekvivalencije na skupu svih cijelih brojeva* $\mathbf{Z}$*:*

(i) refleksivnost: $x \equiv x \pmod{n}$*;*
(ii) simetričnost: ako je $x \equiv y \pmod{n}$*, onda je* $y \equiv x \pmod{n}$*;*
(iii) tranzitivnost: ako je $x \equiv y \pmod{n}$ *i* $y \equiv z \pmod{n}$*, onda je* $x \equiv z \pmod{n}$*.*

DOKAZ. (i) Broj n dijeli $x - x = 0$; (ii) ako n dijeli $x - y$ onda n dijeli i broj $-(x-y) = y-x$; (iii) ako n dijeli $x-y$ i $y-z$, onda n dijeli i $(x-y)+(y-z) = x-z$. ☺

PRIMJER 2. Očevidno je $8 \equiv 3 \pmod{5}$, $15 \equiv 0 \pmod{5}$, $121 \equiv 1 \pmod{5}$, $17 \equiv 2 \pmod{5}$, $-11 \equiv 4 \pmod{5}$, $-8 \equiv 52 \pmod{6}$.

PRIMJER 3. Spomenimo nekoliko primjera relacija ekvivalencije koje znamo još iz osnovne škole.

1. Na skupu X svih trokuta u ravnini možemo definirati binarnu relaciju sličnosti $\sim$ među trokutima. Za dva trokuta kažemo da su *slični* (i pišemo $\triangle ABC \sim \triangle DEF$) ako su im odgovarajući kutovi jednaki. Onda su i odgovarajuće stranice proporcionalne s istim faktorom proporcionalnosti.
2. Na skupu X svih trokuta u ravnini možemo definirati binarnu relaciju sukladnosti (kongruentnosti) $\cong$ među trokutima. Za dva trokuta kažemo da su sukladna (kongruentna) ako su im odgovarajuće stranice jednake duljine. Drugim riječima, dva su trokuta sukladna ako se jedan iz drugog može dobiti gibanjem (svako gibanje trokuta u ravnini moze se realizirati s pomoću njegove translacije, rotacije i simetrije u ravnini).

PRIMJER 4. Neka je X bilo koja familija skupova (tj. skup čiji su elementi skupovi). Podsjetimo se, za skup A kažemo da je ekvipotentan (jednakobrojan) sa skupom B ako postoji bijekcija $f : A \to B$. Tu relaciju označavamo sa $\simeq$: $A \simeq B$. Relacija ekvipotentnosti skupova je relacija ekvivalencije, vidi Teorem 1.3.2.

Čitatelja možda zbunjuje zašto u ovom primjeru nismo X definirali jednostavno kao skup svih skupova. Razlog leži u poznatom paradoksu teorije skupova: pokazuje se da skup svih skupova ne postoji!

PRIMJER 5. Spomenimo još dvije jednostavne, ali korisne relacije ekvivalencije iz matematičke analize.

1. Neka je X skup svih funkcija $f : (-1,1) \to \mathbf{R}$ takvih da je $f(x) \neq 0$ za $x \neq 0$, i $\lim_{x\to 0} f(x) = 0$ (takve se funkcije zovu neizmjerno male veličine). Za $f, g \in X$ kažemo da je $f(x) \sim g(x)$ kad $x \to 0$ ako je $\lim_{x\to 0} \frac{f(x)}{g(x)} = 1$. Relacija $\sim$ je relacija ekvivalencije na X. Korisno je znati da vrijedi na pr. $x \sim \sin x \sim e^x - 1 \sim \ln(1+x)$ kad $x \to 0$. Isto tako $x \sim x + x^3$, kad $x \to 0$.
2. Neka je X skup svih redova $\sum_{n=1}^{\infty} a_n$ s pozitivnim članovima, tj. $a_n > 0$. Za dva reda iz X kažemo da su ekvivalentna, i pišemo $\sum_{n=1}^{\infty} a_n \sim \sum_{n=1}^{\infty} b_n$, ako postoji $l = \lim_{n\to\infty} \frac{a_n}{b_n}$ i $l \neq 0, \infty$. Pokazuje se da vrijedi ovaj važan teorem o uspoređivanju redova: ako su dva reda iz X ekvivalentna, onda ili oba konvergiraju, ili oba divergiraju. Na pr. $\sum_{n=1}^{\infty} \frac{n}{n^2+1} \sim \sum_{n=1}^{\infty} \frac{1}{n}$. Budući da drugi red divergira (harmonijski red), onda divergira i prvi.

PRIMJEDBA 1. Primijetimo da u relaciji ekvivalencije poredak elemenata nije važan: zbog simetričnosti je svejedno pišemo li $x \rho y$ ili $y \rho x$. U literaturi je vrlo često običaj relaciju ekvivalencije označavati i sa $\sim$ umjesto sa ρ, tako da možemo pisati $x \sim y$.

2.3. Razredi ekvivalencije, particija skupa

U ovom odjeljku ćemo pokazati sljedeću vrlo jednostavnu, ali iznimno važnu činjenicu: svakoj relaciji ekvivalencije pripada točno određen rastav skupa X na disjunktne podskupove (particija skupa X) i obratno. Ti disjunktni podskupovi zovu se razredi (klase) ekvivalencije.

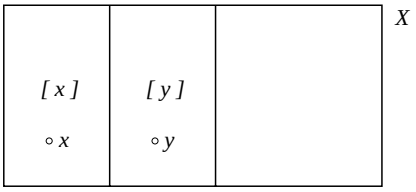
DEFINICIJA. Neka je ρ relacija ekvivalencije na X. **Razred (klasa) ekvivalencije** $[x]$ elementa $x \in X$ je skup svih elemenata iz X koji su u relaciji s x. Dakle $[x]$ je podskup od X definiran sa

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

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

Teorem 1. *Neka je ρ relacija ekvivalencije na X. Onda za sve $x, y \in X$ vrijedi ili $[x] = [y]$ ili $[x] \cap [y] = \emptyset$. Pritom je $x \rho y$ onda i samo onda ako je $[x] = [y]$.*

DOKAZ. Pretpostavimo da je $[x] \cap [y] \neq \emptyset$. Trebamo dokazati da je $[x] = [y]$. Ako postoji $z \in X$, $z \in [x] \cap [y]$, onda je $x \rho z$ i $z \rho y$. Zbog tranzitivnosti dobivamo da je $x \rho y$, tj. $x \in [y]$. Prema tome je opet zbog tranzitivnosti $[x] \subseteq [y]$. Na isti način se pokazuje i $y \in [x]$, tj. $[y] \subseteq [x]$. Dakle $[x] = [y]$. ☺



Sl. 2.2. Particija skupa određena relacijom ekivalencije.

PRIMJEDBA 1. Svi elementi u istom razredu su međusobno "ravnopravni" s obzirom na relaciju ekvivalencije. Drugim riječima, kada govorimo o razredu ekvivalencije $[x]$, onda njegov element x nije ni na koji način "glavni" reprezentant razreda, nego samo jedan od ravnopravnih predstavnika u skupu $[x]$.

U sljedećoj definiciji pojavljuje se pojam familije, koji će kod nas biti ništa drugo nego sinonim za pojam skupa. Rabi se obično kada je riječ o skupu indeksa (familija indeksa) ili o nekom skupu čiji su elementi skupovi (familija skupova). Razlog za uvođenje ovog pojma je više jezične naravi: da se izbjegne nezgrapan izraz "skup skupova", radije se govori o "familiji skupova".

DEFINICIJA. Kažemo da familija podskupova $\{A_i\}_{i \in I}$ od X čini **particiju** (disjunktni rastav) skupa X ako vrijedi

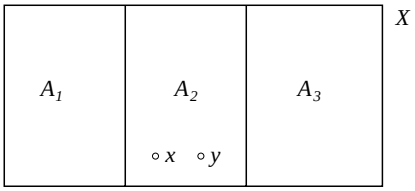
(i) $X = \cup_{i\in I} A_i$,
(ii) $A_i \cap A_j = \emptyset$ za sve $i, j \in I$, $i \neq j$, tj. familija podskupova je disjunktna.
Ponekad ćemo i sam prikaz skupa $X = \cup_{i\in I} A_i$ kao disjunktne unije podskupova A_i zvati particijom od X.

PRIMJEDBA 2. Neka je ρ relacija ekvivalencije na X. Teorem 1 kaže upravo to da je familija podskupova $\{[x]\}_{x\in X}$ particija skupa X.

Sljedeći stavak predstavlja obrat prethodnoga teorema. On pokazuje da svaka particija skupa X na prirodan način određuje relaciju ekvivalencije čiji razredi ekvivalencije se podudaraju s podskupovima iz particije.

Teorem 2. *Neka je $\{A_i\}_{i\in I}$ particija skupa X. Definirajmo relaciju ρ na skupu X tako da je $x \rho y$ onda i samo onda ako x i y pripadaju istom skupu iz particije, tj. postoji $i \in I$ tako da je $x, y \in A_i$. Onda je ρ relacija ekvivalencije. Pripadni razredi ekvivalencije podudaraju se sa skupovima A_i.*

DOKAZ. Tvrdnja je očevidna.



Sl. 2.3. Relacija ekvivalencije određena particijom: $x\rho y$.

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/ρ:

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

Prema prethodnom teoremu vidimo da je kvocjentni skup zapravo isto što i particija skupa X s obzirom na relaciju ekvivalencije ρ.

Početniku je pri prvom susretu vjerojatno teško naviknuti se da razred ekvivalencije $[x]$, koji je podskup u X, gleda kao jedan jedini element kvocjentnog skupa. Elementi u X se zapravo "grupiraju" u disjunktne skupine (razrede) prema nekom zajedničkom svojstvu. U istom razredu nalaze se samo međusobno "srodni" (ekvivalentni) elementi. Na pr. ako je X skup učenika neke škole i ρ relacija "pohađati isti razred", onda je X/ρ skup svih razreda u školi. Razred ekvivalencije $[x]$ jednak je *razredu* u kojem je učenik x.

PRIMJER 1. Neka je X skup svih ljudi na kugli zemaljskoj. Za dva čovjeka x i y reći ćemo da su u relaciji ρ ako su državljani iste države (pretpostavljamo da nitko nema dvojno državljanstvo, te da se granice ne mijenjaju s vremenom[1]). Razred $[x]$ je skup svih državljana one države kojoj pripada osoba x. Kvocjentni skup X/ρ može se poistovjetiti sa skupom D svih država u svijetu (svakom razredu $[x]$ pridružimo onu državu čiji je x državljan; pridruživanje je očevidno bijektivno): $X/\rho \simeq D$.

[1] Kada je u jednoj anketi znameniti matematičar Steinhaus iz Lavova (1887–1972, Lviv, Ukrajina) bio upitan koliko puta je putovao preko granice, odgovorio je: "Niti jednom. Ali je granica mene prešla tri puta!"

PRIMJER 2. Kvocjentni skup doista može biti i beskonačan. Uzmimo $X = \mathbf{C}$ i definirajmo relaciju ρ ovako: $z_1 \rho z_2$ ako je $\operatorname{Re} z_1 = \operatorname{Re} z_2$. Lako se vidi da je to relacija ekvivalencije, a kvocjentni skup $\mathbf{C}/_{\rho}$ jednak je familiji pravaca u kompleksnoj ravnini, koji su paralelni s imaginarnom osi.

PRIMJER 3. Promatrajmo sada iznimno važnu relaciju kongruencije $\equiv$ modulo n na skupu $\mathbf{Z}$ i odredimo kvocjentni skup $\mathbf{Z}/_{\equiv}$. Da bi odredili razred ekvivalencije $[x]$, podijelimo x sa n. Neka je kvocijent pri dijeljenju jednak q, a ostatak jednak r: $x = qn + r$. Znamo da je ostatak r sadržan u skupu $\{0, 1, \ldots, n-1\}$. Budući da je $x \equiv r \pmod{n}$, onda je $[x] = [r]$. Prema tome je

$$\mathbf{Z} = [0] \cup [1] \cup \ldots \cup [n-1].$$

Ova unija je disjunktna, jer niti koja dva različita ostatka iz skupa $\{0, 1, \ldots, n-1\}$ nisu kongruentna modulo n (razlika im je manja od n po apsolutnoj vrijednosti, pa nije djeljiva sa n). Prema tome vrijedi ovaj jednostavan, ali važan rezultat:

Propozicija 3. *Kvocjentni skup na skupu cijelih brojeva po relaciji kongruencije $\equiv$ modulo n jednak je sljedećem n-članom skupu:*

$$\mathbf{Z}/_{\equiv} = \{[0], [1], \ldots, [n-1]\}$$

Taj skup zove se **kvocjentni skup ostataka modulo** *n, ili skup razreda ostataka pri dijeljenju sa n. Razredi ekvivalencije izgledaju ovako:*

$$\begin{aligned} [0] &= \{qn : q \in \mathbf{Z}\} \\ [1] &= \{qn + 1 : q \in \mathbf{Z}\} \\ &\vdots \\ [n-1] &= \{qn + (n-1) : q \in \mathbf{Z}\}. \end{aligned}$$

Razred $[r]$, gdje je $r \in \{0, 1, \ldots, n-1\}$, sadrži skup svih onih cijelih brojeva koji dijeljenjem sa n daju ostatak jednak r, tj. brojeve oblika $qn + r$, $q \in \mathbf{Z}$. Korisno je definirati skup $n\mathbf{Z}$ svih cjelobrojnih višekratnika broja n sa $n\mathbf{Z} = \{kn : k \in \mathbf{Z}\}$. Onda particiju (rastav) skupa cijelih brojeva u Propoziciji 3 možemo pisati i ovako:

$$\mathbf{Z} = n\mathbf{Z} \cup \{n\mathbf{Z} + 1\} \cup \ldots \cup \{n\mathbf{Z} + (n-1)\}.$$

Primijetimo da su dva broja $x, y \in \mathbf{Z}$ u relaciji, tj. $[x] = [y]$, onda i samo onda ako je $x - y \in n\mathbf{Z}$. Na pr. budući da je $(-1) - (n-1) = -n \in n\mathbf{Z}$, onda je $[-1] = [n-1]$, i slično $[-2] = [n-2]$ itd.

Za $n = 2$ imamo $\mathbf{Z}/_{\equiv} = \{[0], [1]\}$, dotično $\mathbf{Z} = [0] \cup [1]$, pri čemu je $[0] = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ skup svih parnih cijelih brojeva, a $[1] = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ skup svih neparnih. Ovdje je na pr. $[-1] = [1]$.