I. SKUPOVI. FUNKCIJE. BROJEVI

§ 1. Izjave. Simboli matematičke logike

U matematici se, kao i u svakidašnjem životu, misli, tvrdnje, pitanja izriču rečenicama. **Izjava** ili **sud** je smislena rečenica koja može biti **istinita** ili **lažna** (neistinita). Upitne rečenice nisu izjave. "Broj 5 je veći od broja 3." primjer je izjave, i to istinite izjave. "Postoje dva različita pravca u ravnini koji se sijeku u barem dvije različite točke te ravnine." primjer je izjave, i to lažne izjave euklidske geometrije. Od izjava možemo tvoriti nove **složene izjave** povezujući polazne izjave veznicima, odnosno negirajući ih. Složene izjave proučava **račun izjava**, koji je dio **matematičke logike**. Navedimo sada neke standardne oznake matematičke logike kojima ćemo se služiti u ovoj knjizi, a služit će nam samo kao simboličke pokrate.

Konjunkcija $A\&B$ dvaju izjava A i B je složena izjava nastala povezivanjem izjava A, B veznikom **i** za koji se upotrebljava simbol &. $A\&B$ čita se "A i B" (ili "A et B"). Izjava $A\&B$ je po definiciji točna ako su izjave A, B istinite. Često se koristi oznaka $A \wedge B$.

Na primjer, ako je A izjava: "Broj 5 je veći od broja 3.", a izjava B: "Postoje dva različita pravca u ravnini koji se sijeku u barem dvije različite točke te ravnine.", onda je A istinita, a B lažna, pa je $A\&B$ lažna.

Disjunkcija $A \vee B$ dviju izjava A, B je složena izjava koja je lažna točno onda ako su obje izjave A, B lažne. $A \vee B$ se čita "A ili B" (ili "A vel B"; vel latinski znači ili, pri čemu se mogućnosti o kojima je riječ ne isključuju, tj. može nastupiti ili A ili B ili oba A, B, tj. bar jedan od A, B). Na primjer, za A, B odabrane kao gore je $A \vee B$ istinita izjava.

Implikacija $A \Rightarrow B$ dviju izjava A, B je složena izjava koja je lažna točno onda ako je A istinita i B lažna. $A \Rightarrow B$ se čita "A povlači B" (ili "A implicira B" ili "iz A slijedi B"). Na primjer, za A, B odabrane kao gore, izjava $A \Rightarrow B$ je lažna, dok je $B \Rightarrow A$ istinita. Za izjavu $B \Rightarrow A$ kažemo da je **obrat izjave** $A \Rightarrow B$.

Ekvivalencija $A \Leftrightarrow B$ dviju izjava A, B je složena izjava koja je istinita točno onda kada su obje izjave A, B istinite, ili kada su obje lažne. $A \Leftrightarrow B$ se čita "A je ekvivalentno sa B" (ili "A je ako i samo ako je B" ili "A je onda i samo onda kada je B"). Na primjer, "broj 1 je veći od broja 0" $\Leftrightarrow$ "broj 2 je veći od broja 1", ili npr. ako je x realni broj za koji vrijedi da je $x^2 - 5x + 6 = 0$, onda možemo pisati $(x^2 - 5x + 6 = 0) \Leftrightarrow (x = 2) \vee (x = 3)$.

Negacija $\neg A$ izjave A je izjava koja je istinita točno onda kada je izjava A

lažna. $\neg A$ se čita "nije A" (ili "non A").

Označimo li istinitost neke izjave s 1, a lažnost s 0, možemo vrijednost 1 ili 0 složene izjave s $(A, B, \dots)$ u ovisnosti o vrijednostima izjava $A, B, \dots$ iz kojih je ona sastavljena, prikazati **semantičkom tablicom** ili **tablicom istinitosti**. Tablice istinitosti za konjunkciju, disjunkciju, implikaciju, ekvivalenciju i negaciju izgledaju (ovim redom) ovako:

A	B	$A\&B$	$A \vee B$	$A \Rightarrow B$	$A \iff B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

,

A	$\neg A$
0	1
1	0

.

Kažemo da su dvije složene izjave X, Y **semantički jednake** (ili, kratko, jednake) ako im se pripadne semantičke tablice podudaraju; to se zapisuje kao $X \equiv Y$. Tako su na primjer izjave $\neg(A \Rightarrow B)$ i $(A\&\neg B)$ semantički jednake, jer im tablice istinitosti izgledaju ovako:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$
0	0	1	0
0	1	1	0
1	0	0	1
1	1	1	0

,

A	B	$\neg B$	$A\&\neg B$
0	0	1	0
0	1	0	0
1	0	1	1
1	1	0	0

.

Ovo se onda zapisuje kao $\neg(A \Rightarrow B) \equiv A\&\neg B$.

Često se u matematici implikacije $A \Rightarrow B$ dokazuju **metodom suprotnog** (ili "kontrapozicijom" ili "kontradikcijom"), tj. pretpostavi se da je istinito $\neg B$, pa se na neki način dokaže da je $\neg A$ istinito što je u kontradikciji s pretpostavkom da je A istinito. Latinski naziv za ovo je "*reductio ad absurdum*". Tablicom istinitosti se lako provjeri da je $(A \Rightarrow B) \equiv (\neg B \Rightarrow \neg A)$, pa ako smo uspjeli dokazati da $\neg B \Rightarrow \neg A$, time smo onda dokazali da $A \Rightarrow B$.

Tipična tvrdnja u matematici je oblika $A \Rightarrow B$, gdje je A pretpostavka, a B zaključak. **Dokaz** takve tvrdnje se sastoji u konstrukciji lanca implikacija $A \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \cdots \Rightarrow C_n \Rightarrow B$, pri čemu je svaka implikacija istinita ili kao aksiom ili vrijedi po definiciji ili je, pak, već otprije dokazana tvrdnja. Pri tome imamo u vidu da nam zapis $A \Rightarrow B \Rightarrow C$ znači kraći zapis izjave $(A \Rightarrow B)\&(B \Rightarrow C)$.

Isto tako kod dokazivanja metodom suprotnog često koristimo princip "isključivanja trećeg" (lat. *tertium non datur*, tj. nema treće mogućnosti), što znači da je $A \wedge (\neg A)$ istinita bez obzira kakva je izjava A. Drugim riječima, izjava $\neg(\neg A) \iff A$ je istinita za sve izjave A; još se kaže da je negacija negacije izjave njena afirmacija. Osnovni zakoni računa izjava (ili **algebre sudova**) su sljedeći:

(RI1) $\neg(\neg A) \equiv A$,

(RI2) $\neg(A\&B) \equiv (\neg A) \vee (\neg B)$,

(RI3) $\neg(A \vee B) \equiv (\neg A)\&(\neg B)$.

Promotrimo rečenicu "prirodni broj x je djeljiv prirodnim brojem y". U toj rečenici ne znamo x i y, pa se ne može utvrditi niti da je ona istinita niti da je lažna. Stoga to i nije izjava. Međutim, ako uvrstimo za x i y određene brojeve, dobit ćemo izjavu; npr. ako uvrstimo za x broj 6, a za y broj 2, dobit ćemo istinitu tvrdnju.

Za ovakve rečenice kažemo da su **izjavne funkcije**, a za x i y da su (predmetne) **varijable**, a za odnos među njima kojeg izjavna funkcija izriče da je **predikat**. Označimo li u prethodnom primjeru "... je djeljiv s ..." slovom P, onda se navedena izjavna funkcija može zapisati kao $P(x, y)$. Ovdje je riječ o **dvomjesnom predikatu**, jer izražava odnos varijabli x i y. Općenito se može razmatrati n-mjesni predikat.

Primjena neodređenih zamjenica **svaki**, u oznaci $\forall$, i **neki** u oznaci $\exists$, na sve varijable izjavne funkcije prevodi izjavnu funkciju u izjavu; $\forall$ je tzv. **univerzalni kvantifikator**, dok je $\exists$ tzv. **egzistencijalni kvantifikator**. $\forall x$ se čita "za svako x", dok se $\exists x$ čita "postoji x". U gornjem primjeru, od izjavne funkcije $P(x, y)$ možemo, npr. formirati **izjave** $(\forall x)(\exists y)P(x, y)$, što znači: "za svaki prirodni broj x postoji prirodan broj y takav da je broj x djeljiv brojem y"; ta je izjava istinita (jer u primjeru možemo uzeti da je $y = 1$ ili $y = x$). Često se koriste **kvantifikatori ograničenog djelovanja:** $(\forall x \in X)$, odnosno $(\exists y \in Y)$. Po definiciji $(\forall x \in X)P(x)$ znači $(\forall x)(x \in X \Rightarrow P(x))$, a $(\exists y \in Y)Q(y)$ znači $(\exists y)(y \in Y \& Q(y))$ (znak $\in$ je objašnjen u §2.) Simbol $\exists!$ se čita "postoji jedinstveni".

Kada ne prijeti opasnost od zabune, ponekad se kvantifikator $\forall$ izostavlja, ali se podrazumijeva. Tako se, npr., osim zapisa $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x \cdot y = y \cdot x$ upotrebljava i kraći zapis $x \cdot y = y \cdot x, x \in \mathbb{R}, y \in \mathbb{R}$.

Jedan od najučestalijih simbola u matematici je svakako simbol $=$ (čita se "jednako"). Ako se ništa posebno ne kaže, onda $a = b$ znači da su objekti čija su imena a i b, jedan te isti objekt. Kada se, međutim, u nekoj matematičkoj teoriji jednakost objekata definira svođenjem na druge pojmove, tada $=$ ne znači da se radi o istom objektu, već ima značenje koje se tom objektu pripisuje u dotičnoj situaciji (npr. jednakost skupova, funkcija, jednadžba $x^2 + 5x + 6 = 0$ itd.) Umjesto $\neg(a = b)$, obično se piše $a \neq b$. Zagradama i zarezima služimo se u matematici kako bismo isključili mogućnost da čitatelj pročita i shvati neke izjave, formule itd. drukčije nego što ih je autor zamislio.

Kad god se u ovoj knjizi pojave rečenice kao $A \Rightarrow B$, znamo da $A \Rightarrow B$, vrijedi $A \Rightarrow B$ itd. značit će to da je izjava $A \Rightarrow B$ istinita.

Ako su izjave A, $A \Rightarrow B$ istinite, onda je istinita i izjava B. To se pravilo u matematičkoj logici zove **pravilo otkidanja** ili **modus ponens**. Ako je izjava $A \Rightarrow B$ istinita, katkad još kažemo da je A **dovoljan uvjet** za B, odnosno da je B nužan uvjet za A. Ako je izjava $A \Rightarrow B \& B \Rightarrow A$ istinita, kaže se često još i da je uvjet A **ekvivalentan** uvjetu B, ili da je A **nužan i dovoljan uvjet** za B. Izjavu $A :\Leftrightarrow B$ čitamo ovako: *Definiramo* da je A istinito ako i samo ako je B istinito.

Na kraju navedimo i ovo pravilo zaključivanja: ako je $P(x)$ izjavna funkcija, pa ako je $P(a)$ istinita za bilo koji odabrani a koji dolazi u obzir, onda je istinita i izjava $(\forall x)P(x)$. To se zove **pravilo generalizacije**. Često ga zapisujemo kao

$P(x), \forall x$.

§ 2. Skupovi, relacije, funkcije

Pojam **skupa** je osnovni pojam matematike, te se ne definira, tj. ne svodi se na još jednostavnije pojmove. Svaki skup sačinjavaju njegovi **elementi** i skup je njima posve određen. Izjavu "x je element skupa S" bilježimo simbolički $x \in S$, a negaciju te izjave bilježimo $x \notin S$. Među skupove ubrajamo i tzv. **prazan skup** $\emptyset$, koji je bez elemenata. Skup S najčešće se opisuje pomoću nekog svojstva P predikata, tako da elementima iz S smatramo sve objekte x koji u danim okolnostima dolaze u obzir, a imaju svojstvo P. Tako pišemo $S = \{x|x \text{ ima svojstvo } P\}$ ili $S = \{x|P(x)\}$ i čitamo: "S je skup svih elemenata x sa svojstvom P". Ako je skup S sastavljen, npr., od elemenata a, b, c, d onda se piše $S = \{a, b, c, d\}$. Oznaka $S := \{x|P(x)\}$ znači da *definiramo* skup S kao skup svih elemenata sa svojstvom P. Elementi skupova mogu biti najrazličitiji, npr. stanovnici nekog grada, svi pravci neke ravnine, svi realni brojevi čiji je kvadrat veći od 2, pa konačno i neki skupovi mogu biti elementi nekog novog skupa. Kažemo da je skup S **podskup** ili **dio** skupa T (a skup T **nadskup** skupa S) i pišemo $S \subseteq T$ (čita se: "S je sadržan u T") ili $T \supseteq S$ (čita se: "T sadrži S") ako je svaki element $x \in S$ element od T, tj. $x \in T$. Prazan skup $\emptyset$ je podskup svakog skupa. Dva skupa S i T su **jednaki** i piše se $S = T$, ako je $S \subseteq T$ i $T \subseteq S$, tj. ako je svaki element od S element od T i svaki element od T ujedno element od S. Ako je $S \subseteq T$ i $S \neq T$, onda kažemo da je S **pravi podskup** od T; pišemo $S \subset T$. Na primjer, $\{1, 2, 3\} = \{2, 1, 3\}$, ali $\{1, 2, 3\} \neq \{1, 2\}$ i $\{1, 2\} \subset \{1, 2, 3, 4\}$. Uočite da je poredak elemenata unutar vitičastih zagrada nebitan.

Sa skupom S posve je određen **partitivni skup** od S, čiji su elementi svi podskupovi skupa S. Taj se skup obično označava sa $\mathcal{P}(S)$ ili sa 2^S. Očito je $\emptyset$, $S \in \mathcal{P}(S)$. Podskup od $\mathcal{P}(S)$ se katkad zove **familija podskupova** od S.

Neka su A, B podskupovi nekog skupa U. Tada je posve određen podskup od U

$$\{x \in U | x \in A \vee x \in B\},$$

koji se zove **unija** skupova A i B i označava sa $A \cup B$. Isto tako posve je određen podskup od U

$$\{x \in U | x \in A \,\&\, x \in B\},$$

koji se zove **presjek** skupova A i B i označava sa $A \cap B$. Nadalje, posve je određen podskup od U

$$\{x \in U | \, x \in A \,\&\, x \notin B\},$$

koji se zove **diferencija** (ili **razlika**) skupova A i B i označava se sa $A \setminus B$. Razlika $U \setminus A$ zove se **komplement** podskupa A u skupu U. Kad je jasno (iz konteksta ili drukčije) o kojem skupu U je riječ, često se za komplement od A koristi i oznaka $\overline{A}$.

Kažemo da su skupovi A i B **disjunktni** ako je $A \cap B = \emptyset$, a da se sijeku ako je $A \cap B \neq \emptyset$. **Simetrična diferencija** je $A \triangle B := (A \setminus B) \cup (B \setminus A)$.

Iz definicije unije, presjeka i komplementa može se lako dokazati da za bilo koje skupove $A, B, C, \ldots$ iz U vrijede formule:

$$(A \cup B) \cup C = A \cup (B \cup C) \qquad (A \cap B) \cap C = A \cap (B \cap C) \tag{1}$$

$$A \cup B = B \cup A \qquad A \cap B = B \cap A \tag{2}$$

$$A \cup (A \cap B) = A \qquad A \cap (A \cup B) = A \tag{3}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{4}$$

$$A \cup \overline{A} = U \qquad A \cap \overline{A} = \emptyset \tag{5}$$

$$A \cup \emptyset = A \qquad A \cap U = A \tag{6}$$

$$A \cup U = U \qquad A \cap \emptyset = \emptyset \tag{7}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \qquad \overline{A \cap B} = \overline{A} \cup \overline{B} \tag{8}$$

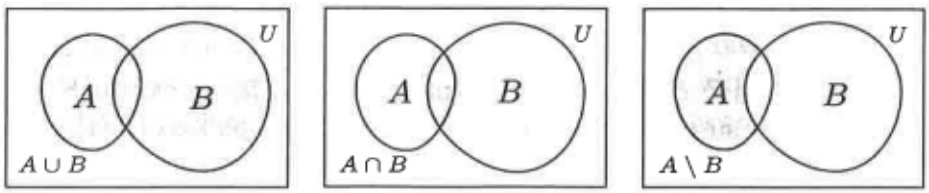
$$\overline{U} = \emptyset \qquad \overline{\emptyset} = U \tag{9}$$

$$A \cup A = A \qquad A \cap A = A \tag{10}$$

$$\overline{\overline{A}} = A \tag{11}$$

Primijetimo da su formule u lijevom i desnom stupcu međusobno dualne u smislu da zamjenom znakova $\cup$ i $\cap$, te U i $\emptyset$, one prelaze jedne u druge. Formule (8) su tzv. **De Morganove**[1] formule.

Shematski je zgodno skupove predstavljati kao dijelove omeđene zatvorenim krivuljama. To su tzv. **Vennovi**[2] **dijagrami** (za skup U se obično tada uzima čitava ravnina ili neki pravokutnik (v. sl. 1)). Partitivni skup $\mathcal{P}(U)$ zajedno s operacijama $\cup$, $\cap$, za koje vrijede formule (1)–(11), zove se **Booleova**[3] **algebra skupova** na U. Više o skupovima vidi u knjizi [15].



Slika 1.

Koristit ćemo se standardnim oznakama za osnovne skupove brojeva, i to:

$\mathbb{N}$ = skup prirodnih brojeva $= \{1, 2, 3, \ldots, n, n+1, \ldots\}$,

$\mathbb{Z}$ = skup cijelih brojeva $= \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$,

$\mathbb{Q}$ = skup racionalnih brojeva $= \{\frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{N}\}$,

$\mathbb{R}$ = skup realnih brojeva,

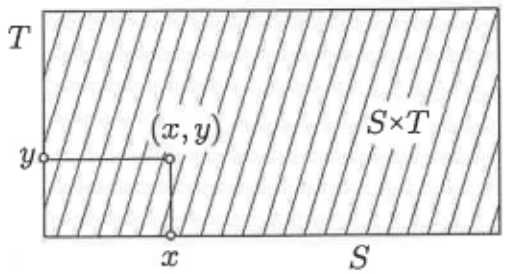
$\mathbb{C}$ = skup kompleksnih brojeva $= \{x + iy | x, y \in \mathbb{R}\}$, $i = \sqrt{-1}$,

$\mathbb{Z}^+ = \mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$,

[1] Augustus de Morgan, (1806. – 1871.), engleski matematičar i logičar.
[2] John Venn (1834. – 1923.), engleski logičar.
[3] George Boole (1815. – 1864.), engleski logičar i matematičar.

$\mathbb{N}_n = \{1, 2, 3, \ldots, n\} = [n]$.

Direktni (ili **Kartezijev**) **produkt** dvaju skupova S i T je skup $S \times T$ svih **uređenih parova** (x, y) elemenata $x \in S$, $y \in T$, tj. $S \times T = \{(x, y) | x \in S, y \in T\}$. Za uređene parove je $(x, y) = (x', y')$ ako i samo ako je $x = x'$ i $y = y'$. Napomenimo da se uređeni par (x, y) općenito razlikuje od uređenoga para (y, x). Nadalje, uređen par (x, y) se može definirati i kao skup $\{\{x\}, \{x, y\}\}$. Smatramo da je uvijek $\emptyset \times S = S \times \emptyset = \emptyset$.



Slika 2.

Direktni produkt triju skupova R, S, T definira se kao skup svih uređenih trojki (x, y, z) elemenata $x \in R$, $y \in S$, $z \in T$, tj. $R \times S \times T = (R \times S) \times T = \{(x, y, z) | x \in R, y \in S, z \in T\}$. Opet su uređene trojke (x, y, z) i (x', y', z') jednake, ako i samo ako je $x = x'$, $y = y'$, $z = z'$. Netko bi mogao pomisliti da uređenu trojku možemo definirati kao skup $\{\{x\}, \{x, y\}, \{x, y, z\}\}$, no to nije dobro (dokažite to!), nego je uređena trojka uređen par $(x, (y, z))$, a to je skup $\{\{x\}, \{\{x\}, \{\{y\}, \{y, z\}\}\}\}$. Općenito, ako imamo n skupova ($n \in \mathbb{N}$), $S_1, S_2, \ldots, S_n$, onda se njihov direktni produkt $S_1 \times S_2 \times \cdots \times S_n$ definira kao skup svih uređenih n-torki $(x_1, x_2, \ldots, x_n)$, $x_1 \in S_1, \ldots, x_n \in S_n$. Ako je $S_1 = S_2 = \cdots = S_n$, onda se n-struki produkt zapisuje još i kao S^n.

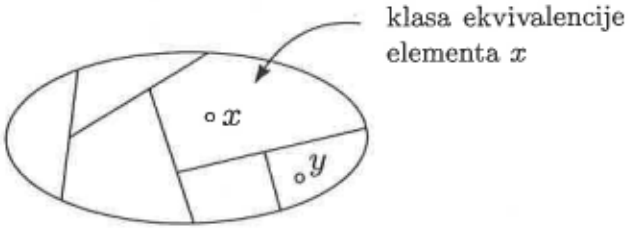
Svaki podskup $\rho \subseteq S \times S$ zove se **binarna relacija** na skupu S. Za elemente $x, y \in S$ kažemo da su u relaciji ρ, i piše se $\rho(x, y)$ ili $x \rho y$ ako je $(x, y) \in \rho$.

Relacija ρ je **refleksivna**, ako je $x \rho x$, za svako $x \in S$; relacija ρ je **simetrična** ako za svako $x, y \in S$, $x \rho y$ povlači $y \rho x$; relacija ρ je **tranzitivna** ako za svako $x, y, z \in S$, $(x \rho y) \& (y \rho z)$ povlači $x \rho z$. **Relacija ekvivalencije** (ili **klasifikacije**) je binarna relacija koja je istodobno refleksivna, simetrična i tranzitivna. Obično se relacija ekvivalencije bilježi sa $\sim$. Na primjer, jednakost elemenata "$=$" nekog skupa S je relacija ekvivalencije na S. Nadalje, za $n \in \mathbb{N}$, definirajmo za dva cijela broja $a, b \in \mathbb{Z}$ da su **kongruentni modulo** n, u zapisu $a \equiv b (\mathrm{mod}\ n)$, ako je $a - b$ djeljivo sa n. Tada je očito $a \equiv a (\mathrm{mod}\ n), \forall a \in \mathbb{Z}$, $a \equiv b (\mathrm{mod}\ n) \Rightarrow b \equiv a (\mathrm{mod}\ n)$, te $a \equiv b (\mathrm{mod}\ n)$ & $b \equiv c (\mathrm{mod}\ n) \Rightarrow a \equiv c (\mathrm{mod}\ n)$ (dokažite to!), pa je $\equiv (\mathrm{mod}\ n)$ relacija ekvivalencije na $\mathbb{Z}$. Kao daljnji primjer, označimo sa $\mathcal{P}$ skup svih pravaca u ravnini $\mathbb{R}^2$. Relacija "biti paralelan" $\parallel$ je relacija ekvivalencije na skupu $\mathcal{P}$.

Ako je $\sim$ relacija ekvivalencije na nekom skupu S, onda se S može prikazati na jedinstven način kao unija disjunktnih podskupova, tzv. **klasa ekvivalencije** s obzirom na relaciju $\sim$.

U istu klasu, po definiciji, ulaze svi međusobno ekvivalentni elementi od S. Za

$x \in S$ označimo sa $[x] = \{y \in S | y \sim x\}$ klasu ekvivalencije od x. Tada je očito $x \sim y \Leftrightarrow [x] = [y]$, te za svake dvije klase $[x], [y]$ vrijedi da se ili podudaraju ili su disjunktne. Simbolički to možemo ovako zapisati: $[x] = [y]$ ili $[x] \cap [y] = \emptyset, \forall x, y \in S$. (Dokažite sami ovu tvrdnju.) Unija svih klasa ekvivalencije je očito čitav skup S, pa relacija ekvivalencije $\sim$ na S definira jednu **"particiju"** skupa S na klase ekvivalencije.



Slika 3.

Skup svih klasa ekvivalencije s obzirom na relaciju ekvivalencije $\sim$ na S zove se **kvocijentni skup** i označava se sa $S/\sim$.

Kvocijentni skup u gornjem primjeru jednakosti elemenata na S jednak je skupu čiji su elementi jednočlani skupovi $\{x\}$, $x \in S$, tj. $S/_= = \{\{x\} \,|\, x \in S\}$, pa ga možemo identificirati sa skupom S. U drugom se primjeru, kvocijentni skup $\mathbb{Z}/\equiv (\mathrm{mod}\ n)$ često zapisuje kao $\mathbb{Z}_n$ i zove **skup ostataka modulo** n. U trećem primjeru relacije paralelnosti $\parallel$ na skupu $\mathcal{P}$ svih pravaca skup $\mathcal{P}/\parallel$ je skup svih smjerova u ravnini.

Drugi osnovni tip binarne relacije je relacija **parcijalnog uređaja** $\leq$ (manje ili jednako) na skupu S. To je binarna relacija na S koja je refleksivna, tranzitivna i **antisimetrična**, tj. ima svojstvo da za svako $x, y \in S$ $(x \leq y) \& (y \leq x)$ povlači $x = y$. Ako je osim toga, za svaki $x, y \in S$ $(x \leq y) \vee (y \leq x)$, onda se govori o **relaciji uređaja** (ili **totalnog uređaja**). Ako je $\leq$ totalni uređaj na S, onda se S zajedno s $\leq$ (tj. uređen par $(S, \leq)$) zove **totalno uređen skup** ili **uređen skup**. Tako je npr. obična nejednakost na skupu $\mathbb{R}$ realnih brojeva totalni uređaj (katkad se još zove i **linearni uređaj**). Umjesto $x \leq y$ ponekad se piše $y \geq x$ (y veće ili jednako x). Ako je $x \leq y$ i $x \neq y$, piše se $x < y$ (x manje od y), ili $y > x$ (y veće od x).

Neka je $(S, \leq)$ parcijalno (ili totalno) uređen skup, a $X \subseteq S$ neprazan podskup od S. Kažemo da je $m \in S$ **donja međa** od X ako je $m \leq x, \forall x \in X$. Skup X je **odozdo omeđen** ako postoji bar jedna donja međa od X.

Najveća donja međa ili **infimum** odozdo omeđenog skupa $X \subseteq S$ je $\inf X \in S$, ako vrijedi:

(1) $\inf X$ je donja međa skupa X,

(2) za svaku donju među m skupa X vrijedi $m \leq \inf X$.

Ako $\inf X$ postoji, onda je jedinstven. Naime, pretpostavimo da imamo dva elementa $m_1, m_2 \in S$ sa svojstvima (1), (2). Tada bi vrijedilo $(m_1 \leq m_2) \& (m_2 \leq m_1)$, a odatle izlazi $m_1 = m_2$.

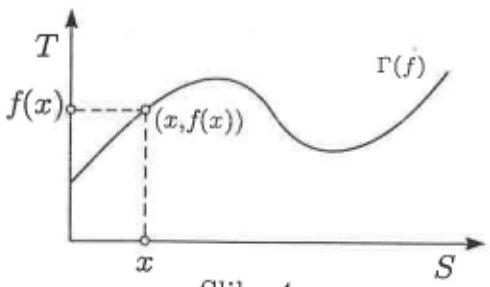
Najmanji element ili **minimum** skupa $X \subseteq S$ je element $\min X \in X$, koji je ujedno donja međa za X, tj. $\min X \leq x$, za svako $x \in X$. Ako minimum skupa X postoji, onda je jedinstven, te je očito $\inf X = \min X$.

Kažemo da je totalno uređen skup $(S, \leq)$ **dobro uređen** ako svaki njegov neprazan podskup ima minimalni element. Tako je npr. skup $\mathbb{N}$ s obzirom na obični uređaj brojeva dobro uređen, dok skup $\mathbb{R}$ s običnim uređajem to nije, jer npr. za skup $X = \{x \in \mathbb{Q} \,|\, x^2 > 2\}$, $\inf X = \sqrt{2}$ nije najmanji element od X (to ćemo kasnije pokazati).

Posve analogno definiraju se pojmovi: **gornja međa**, **odozgo omeđen skup**, **najmanja gornja međa** ili **supremum** $\sup X$ i **najveći element** ili **maksimum** $\max X$ nepraznog skupa $X \subseteq S$. Učinite to sami. Ako je $X \subseteq S$ omeđen odozdo i odozgo, kažemo da je **omeđen**. Ako je $(S, \leq)$ parcijalno uređen skup, $a, b \in S$, $a \leq b$, onda se skup $[a, b] := \{x \in S \,|\, a \leq x \leq b\}$ zove **segment** u S, a ako je $a < b$, skup $\langle a, b\rangle := \{x \in S \,|\, a < x < b\}$ **interval** u S. Često se promatraju i skupovi $[a, \cdot\rangle$, $\langle a, \cdot\rangle$, $\langle \cdot, b]$, $\langle \cdot, b\rangle$, gdje je, npr., $\langle \cdot, b] := \{x \in S \,|\, x \leq b\} \subseteq S$.

Neka su sada S i T dva skupa. **Preslikavanje** ili **funkcija**[4] sa skupa S u skup T je uređena trojka (S, T, f), koja se sastoji od skupa S, koji se zove **područje definicije** ili **domena**, skupa T, koji se zove **područje vrijednosti** ili **kodomena**, te nekog pravila f, pomoću kojeg svakom elementu $x \in S$ pridružujemo neki element $y \in T$ (koji ovisi o x). Pridruženi element y zove se **vrijednost preslikavanja** na elementu x i označava se sa $f(x)$ ili fx. Katkad je zgodna i oznaka $x \mapsto f(x)$, $x \in S$, $f(x) \in T$ ili jednostavno $x \mapsto f(x)$, kojom se označava funkcija koja prevodi element x u $f(x)$. Npr. kvadriranje je funkcija $x \mapsto x^2$, $x \in \mathbb{R}$, $x^2 \in \mathbb{R}$. Katkad se naprosto zapisuje da je funkcija kvadriranja zadana sa $y = x^2$.

Graf preslikavanja (S, T, f) je skup $\Gamma(f) = \{(x, f(x)) | x \in S\} \subseteq S \times T$:

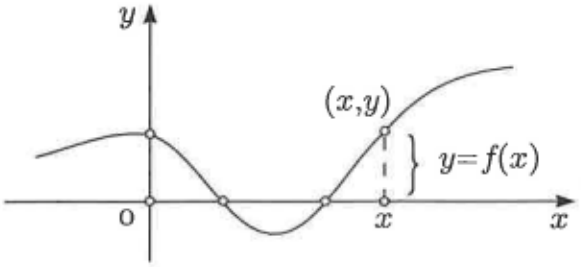


Slika 4.

Uobičajena oznaka za preslikavanje ili funkciju je $f : S \to T$. Često se još o elementima $x \in S$ govori kao o **nezavisnoj varijabli** ili **argumentu**, a o elementima $y \in T$ kao o **zavisnoj varijabli** funkcije. Pojam funkcije se može alternativno definirati ovako. $f : S \to T$ je podskup $\Gamma \subseteq S \times T$, koji ima svojstvo da za svaki $x \in S$ postoji jedan i samo jedan $y \in T$, tako da je $(x, y) \in \Gamma$. Tu smo, dakle, poistovjetili pojam funkcije s pojmom grafa, i taj je pristup s logičke strane u prednosti jer se ne služi (s nedefiniranim) pojmom "pravilo", ali je prvi pristup intuitivno bliži, a ne uzrokuje teškoće, jer se u njemu može gledati samo način govora, dok je matematički smisao iz ovoga drugog pristupa.

[4] Riječ funkcija dolazi od *lat.* fungi – obavljati, vršiti, djelovati.

Grafove funkcija $f : \mathbb{R} \to \mathbb{R}$ (ili $f : S \to \mathbb{R}$, gdje je $S \subseteq \mathbb{R}$) zadanih formulom $y = f(x)$ ili nekim propisom $x \overset{f}{\mapsto} y$ obično prikazujemo u koordinatnom sustavu kao na sl. 5, pri čemu se os x zove **apscisa**, a os y **ordinata**. Poučno je nacrtati



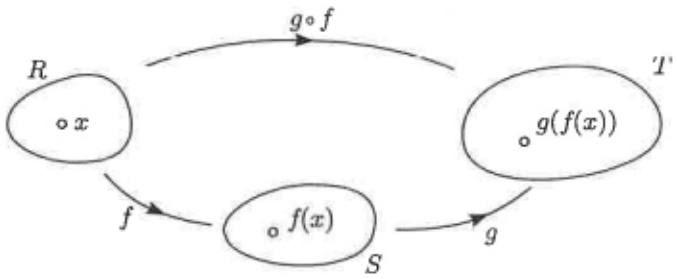
Slika 5.

grafove funkcija $\lfloor\ \rfloor, \lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$, gdje je $\lfloor x \rfloor$ = **najveći cijeli broj** $\leq x$ ("pod" od x), $\lceil x \rceil$ = **najmanji cijeli broj** $\geq x$("strop" od x). Uočite da je $\lceil x \rceil = -\lfloor -x \rfloor$. Za vježbu nacrtajte i graf funkcije $f : \mathbb{R} \to \mathbb{R}$, $f(x) = ((x)) := x - \lfloor x \rfloor - \frac{1}{2}$ (tzv. prva Bernoullijeva periodička funkcija).

Preslikavanja (S, T, f) i (S', T', f') su **jednaka** ako je $S = S'$, $T = T'$, i za svako $x \in S = S'$ je $f(x) = f(x')$. Vrlo je važno uočiti da za jednakost preslikavanja zahtijevamo da su im domene jednaki skupovi i kodomene jednaki skupovi. Npr. neka je $S \subseteq T$. Preslikavanje $i : S \to T$, definirano formulom $i(x) = x, x \in S$, zove se **inkluzija** (ili **ulaganje**). Ako je S pravi podskup od T, onda je inkluzija $i : S \to T$ različita od preslikavanja $1_S : S \to S$, koje definiramo formulom $1_S(x) = x, x \in S$, a zove se **identiteta** ili **identičko preslikavanje**. Naime, tada i, 1_S imaju različite kodomene. Još neki važniji primjeri preslikavanja su ovi: neka su S i T skupovi. Tada definiramo **projekcije** $\pi_S : S \times T \to S$ i $\pi_T : S \times T \to T$, sa $\pi_S(x, y) = x$, $\pi_T(x, y) = y$ (zapravo bi trebalo pisati $\pi_S((x, y))$, ali te dvostruke zagrade izostavljamo); projekciju π_S obično zovemo prvom, π_T drugom projekcijom. Nadalje, ako je $\sim$ relacija ekvivalencije na skupu S, onda definiramo **prirodnu projekciju** ili **kvocijentno preslikavanje** $q : S \to S/\sim$, formulom $q(x) = [x]$. Daljnji važni primjeri preslikavanja su binarne operacije. **Binarna operacija** na skupu S je svako preslikavanje skupa $S \times S$ u S. Npr. zbrajanje prirodnih brojeva je binarna operacija $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, +(k, l) \in \mathbb{N}$. Ili, $\cup$, $\cap$, $\setminus$ su binarne operacije na partitivnom skupu $S = \mathcal{P}(U)$ nekog skupa U, jer svakom paru $(A, B) \in \mathcal{P}(U) \times \mathcal{P}(U)$ pridružuju novi element $A \cup B \in \mathcal{P}(U)$, $A \cap B \in \mathcal{P}(U)$, $A \setminus B \in \mathcal{P}(U)$. **Kompozicija preslikavanja** $f : R \to S$ i $g : S \to T$ je preslikavanje $h : R \to T$, takvo da je za svako $x \in R$, $h(x) = g(f(x))$. Oznaka za kompoziciju od f i g je $g \circ f$, tj. $h = g \circ f$ ili naprosto $h = gf$ (v. sl. 6). Ako su $f : P \to R$, $g : R \to S$, $h : S \to T$ preslikavanja, onda je $h \circ (g \circ f) = (h \circ g) \circ f$, tj. za kompoziciju preslikavanja vrijedi **zakon asocijacije** (dokažite to!). Nadalje, ako su $1_S : S \to S$ i $1_T : T \to T$ identička preslikavanja, a $f : S \to T$, onda je $f \circ 1_S = 1_T \circ T = f$.

Neka je $S' \subseteq S$, a $f : S \to T$ i $f' : S' \to T$ sa svojstvom da je za svako $x \in S'$, $f(x) = f'(x)$. Tada kažemo da je f' **restrikcija** (ili **suženje**) od f na podskup S' i pišemo $f' = f|_{S'}$. Kažemo još da je f **proširenje** (ili **ekstenzija**) od f' na S.

Vrlo korisna funkcija za ispitivanje da li element nekog ("velikog") skupa U



Slika 6.

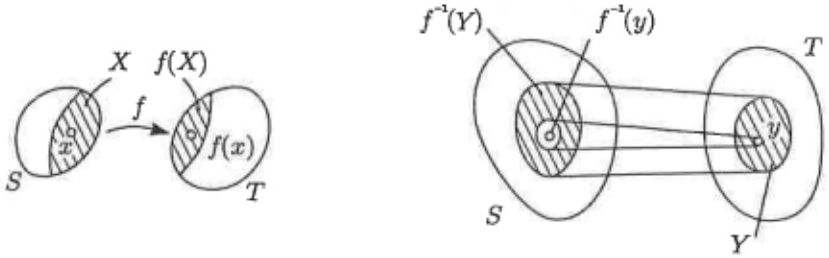
pripada nekom podskupu od U je tzv. **karakteristična funkcija** χ_S podskupa $S \subseteq U$. To je funkcija $\chi_S : U \to \{0,1\}$ definirana sa:

$$\chi_S(x) = \begin{cases} 1, & \text{ako } x \in S \\ 0, & \text{ako } x \notin S. \end{cases}$$

Umjesto skupa $\{0,1\}$ može se uzeti bilo koji dvočlani skup, npr. {istinito, lažno} itd.

Slika skupa $X \subseteq S$ pri preslikavanju $f : S \to T$ je skup $f(X) := \{y \in T | \exists x \in X \ \& \ y = f(x)\} \subseteq T$, ili kraće $f(X) = \{f(x) | x \in X\} \subseteq T$, a **slika** od f, $Imf := f(S)$.

Inverzna slika (ili **original**) skupa $Y \subseteq T$ pri preslikavanju $f : S \to T$ je skup $f^{-1}(Y) := \{x \in S | y \in Y \& y = f(x)\} \subseteq S$ ili kraće $f^{-1}(Y) = \{x \in S | f(x) \in Y\}$. Ako je $Y = \{y\}$ jednočlani skup, onda stavljamo $f^{-1}(y) := f^{-1}(\{y\}) = \{x \in S | f(x) = y\}$ i zovemo ga **originalom točke** y po f ili **vlakno** od y. Shematski možemo sliku, inverznu sliku i original točke prikazati kao na sl. 7.



Slika 7.

Neka je $f : S \to T$ preslikavanje, A, $B \subseteq S$, te C, $D \subseteq T$. Tada vrijede formule (dokažite ih sami):

$$f(A \cup B) = f(A) \cup f(B) \qquad f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D) \tag{12}$$

$$f(A \cap B) \subseteq f(A) \cap f(B) \qquad f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D) \tag{13}$$

$$f(A \setminus B) \supseteq f(A) \setminus f(B) \qquad f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D) \tag{14}$$

$$A \subseteq f^{-1}(f(A)) \tag{15}$$

$$f(f^{-1}(C)) = C \cap f(S) \subseteq C \tag{16}$$

Ako je dano i preslikavanje $g : T \to U$ i $E \subseteq U$, onda je

$$(gf)^{-1}(E) = f^{-1}g^{-1}(E). \tag{17}$$

Oznaka za skup svih preslikavanja sa skupa S u skup T je T^S.

Za preslikavanje $f : S \to T$ kažemo da je **injekcija** (ili **1-1-preslikavanje**) ako $f(x) = f(x')$povlači $x = x'$, a kažemo da je **surjekcija** (ili **preslikavanje!na**) ako je $f(S) = T$ (tj. $(\forall y \in T)(\exists x \in S)$, $f(x) = y$). f je **bijekcija** (ili **obostrano jednoznačno preslikavanje**) ako je f injekcija i surjekcija.

Kažemo da su skupovi S i T **ekvipotentni** ili **bijektivni** ako postoji bijekcija $f : S \to T$. Relacija ekvipotencije je relacija ekvivalencije, pa se skupovi svrstavaju u disjunktne klase; klasa kojoj pripada skup S zove se **kardinalni broj** skupa S i označava sa $|S|$ ili $\operatorname{card} S$.

Neka je $f : S \to T$. Kažemo da je $g : T \to S$ **inverzno preslikavanje** ili **inverz** od f ako je $gf = 1_S$ i $fg = 1_T$. Odmah se vidi da za dano preslikavanje f može postojati najviše jedno inverzno preslikavanje. Dalje, ako za $f : S \to T$ postoji inverz, onda je f bijekcija, i obratno, svaka bijekcija f dopušta inverzno preslikavanje koje se obično označava sa f^{-1}. Pojam "funkcija" uveo je Gottfried Leibniz 1692.[5]

Kažemo da je skup S **konačan skup** ako S nije ekvipotentan niti s jednim svojim pravim podskupom. Kažemo da je skup S **beskonačan** ako nije konačan, tj. ako postoji pravi podskup $S' \subset S$ i bijekcija $f : S \to S'$. Prazan skup $\emptyset$ je konačan skup i stavljamo $|\emptyset| = 0$. Kardinalan broj konačnog skupa S se još zove i **broj elemenata** od S ili **brojnost** od S. Naravno, mnoštvo je primjera konačnih skupova: skup svih studenata nekog fakulteta, skup svih stanovnika Zemlje, skup svih atoma u danas vidljivom svemiru (njegova je brojnost $\approx 10^{100}$), $\{1, 2, 3, 4, 5\}$ itd. Za razliku od tih skup $\mathbb{N}$ je beskonačan jer postoji bijekcija sa $\mathbb{N}$ na njegov pravi podskup, npr. skup svih parnih brojeva $2\mathbb{N} = \{2n | n \in \mathbb{N}\} \subset \mathbb{N}$. Funkcija $f : \mathbb{N} \to 2\mathbb{N}$, $f(n) = 2n$ je bijekcija, pa je $\mathbb{N}$ beskonačan skup. Svaki nadskup od $\mathbb{N}$ je tada također beskonačan, kao i $\mathbb{N} \times S$, gdje je $S \neq \emptyset$. Iako postoji (očita) injekcija $\mathbb{N} \to \mathbb{R}$, ne postoji injekcija $\mathbb{R} \to \mathbb{N}$ (to ćemo kasnije pokazati; v. Teorem 4). Za $n \in \mathbb{N}$ je $\operatorname{card}\{1, 2, \ldots, n\} = |[n]| = n$. Kako smo rekli, ekvipotentni skupovi S i T imaju isti kardinalni broj, tj. $\operatorname{card} S = \operatorname{card} T$ (ili $|S| = |T|$). Stoga skup S za koji postoji bijekcija $\{1, 2, \ldots, n\} \to S$ zovemo **n-člani skup**. Skup koji je ekvipotentan skupu prirodnih brojeva $\mathbb{N}$ zovemo **prebrojiv skup**. Kardinalni broj prebrojivog skupa bilježi se sa $\aleph_0$ (alef nula, prema prvom hebrejskom slovu alef). Nadalje, kažemo da kardinalni broj skupa S *nije veći* od kardinalnog broja skupa T i pišemo $\operatorname{card} S \leq \operatorname{card} T$, ako je S ekvipotentan nekom podskupu od T, tj.

$$\operatorname{card} S \leq \operatorname{card} T :\Leftrightarrow (\exists P \subseteq T)(\operatorname{card} S = \operatorname{card} T).$$

Jasno je da za $S \subseteq T$ vrijedi $\operatorname{card} S \leq \operatorname{card} T$. Kako smo vidjeli, pravi podskup parnih brojeva $2\mathbb{N} \subset \mathbb{N}$ je ekvipotentan s čitavim $\mathbb{N}$; drugi je primjer interval

[5] Gottfried Wilhelm Leibniz (1646. – 1716.), njemački matematičar i filozof. Bavio se još biologijom, geologijom, jezikoslovljem, teologijom i pravom. Smatraju ga posljednjim enciklopedistom.

realnih brojeva $\langle -1, 1\rangle \subsetneq \mathbb{R}$, jer je funkcija $x \mapsto \frac{x}{1-|x|}$ bijekcija na čitav skup realnih brojeva. Stoga možemo reći da interval $\langle -1, 1\rangle$ i čitava os realnih brojeva imaju "jednako mnogo točaka". Ako je $\operatorname{card} S \leq \operatorname{card} T$ i $\operatorname{card} S \neq \operatorname{card} T$, pišemo $\operatorname{card} S < \operatorname{card} T$. Svaki skup S za koji je $\operatorname{card} S > \operatorname{card} \mathbb{N} = \aleph_0$ zove se **neprebrojiv skup**. Sljedeći teorem pokazuje da nema "najvećeg kardinalnog broja".

TEOREM 1 (G. Cantor[6]). *Za svaki skup S vrijedi* $\operatorname{card} S < \operatorname{card} \mathcal{P}(S)$, *gdje je $\mathcal{P}(S)$ partitivni skup od S.*

Dokaz. Ako je $S = \emptyset$, tvrdnja je jasna, pa pretpostavimo da je $S \neq \emptyset$. Kako $\mathcal{P}(S)$ sadrži sve jednočlane podskupove od S, slijedi da je $\operatorname{card} S \leq \operatorname{card} \mathcal{P}(S)$. Stoga treba još pokazati da je $\operatorname{card} S \neq \operatorname{card} \mathcal{P}(S)$ za $S \neq \emptyset$.

Pretpostavimo suprotno da postoji bijekcija $f : S \to \mathcal{P}(S)$. Promotrimo podskup $A = \{x \in S | x \notin f(x)\} \subseteq S$ svih elemenata $x \in S$ koji nisu elementi pridruženog podskupa $f(x) \in \mathcal{P}(S)$. Kako je $A \in \mathcal{P}(S)$, onda postoji $a \in S$ takav da je $f(a) = A$. No za element $a \in S$ nemoguće je da je $a \in A$ (zbog definicije skupa A), ali ni $a \notin A$ (opet po definiciji od A). Time smo došli u kontradikciju s principom isključenja trećeg. □

Kardinalni broj skupa realnih brojeva se zove **kontinuum** i piše se $\operatorname{card} \mathbb{R} = \mathfrak{c}$. Kasnije ćemo pokazati da je $\operatorname{card} \mathbb{N} < \operatorname{card} \mathbb{R}$, tj. $\aleph_0 < \mathfrak{c}$, tj. da je skup realnih brojeva neprebrojiv.

Već na početku izgradnje teorije brojeva (krajem 19. st. i početkom 20. st.) postavljeno je prirodno pitanje o postojanju skupa A sa svojstvom $\aleph_0 < \operatorname{card} A < \mathfrak{c}$. Raznim ispitivanjima iskristalizirala se slutnja da takav skup ne postoji. Tako je nastala čuvena **hipoteza kontinuuma**. Pokazalo se da to pitanje zadire u same osnove izgradnje teorije skupova, pa tako i čitave matematike. Problem je konačno riješio američki matematičar Paul Cohen[7] 1963. Cohen je dokazao nerazrješivost hipoteze kontinuuma, pokazavši da niti nju niti njenu negaciju nije moguće dokazati u okviru općeprihvaćene aksiomatske teorije skupova.

U nekom smislu je to analogna situacija nezavisnosti Euklidova petog postulata o paralelama od ostalih aksioma geometrije ravnine (o čemu će biti riječi u III. poglavlju).

Spomenimo na kraju i ovaj teorem.

TEOREM 2 (Cantor-Bernstein[8]). Ako su S i T skupovi, onda vrijedi

$$\operatorname{card} S \leq \operatorname{card} T \ \&\ \operatorname{card} T \leq \operatorname{card} S \Rightarrow \operatorname{card} S = \operatorname{card} T.$$

[6] Georg Ferdinand Cantor (1845. – 1918.), njemački matematičar, jedan od osnivača teorije skupova.

[7] Paul Cohen (r. 1934.), američki matematičar, profesor univerziteta u Stanfordu. Godine 1966. na međunarodnom kongresu matematičara u Moskvi dobio je za rješenje hipoteze kontinuuma Fieldsovu medalju, što je jednako visoko priznanje kao Nobelova nagrada za druge discipline.

[8] Felix Bernstein (1878. – 1956.), njemački matematičar.