Uvod u matematiku

M. Klaričić Bakula, S. Braić

Split, 2011/2012

Sadržaj

Uvod **iv**

1. Građa matematike **1**
1.1. Simboli . . . 1
1.2. Apstrakcija . . . 1
1.2.1. Apstrakcija kao idealizacija . . . 2
1.2.2. Apstrakcija kao ekstrakcija . . . 2
1.3. Generalizacija . . . 2
1.4. Formalizacija . . . 3
1.5. Matematički objekti i strukture . . . 3
1.6. Oblici matematičkog mišljenja . . . 4
1.6.1. Matematički pojmovi . . . 5
1.6.2. Aksiomi . . . 6
1.6.3. Teoremi . . . 6
1.6.4. Dokazi . . . 7
1.7. Algoritamska i dijalektička matematika . . . 8

2. Osnove matematičke logike **10**
2.1. Logika sudova . . . 10
2.1.1. Uvod . . . 10
2.1.2. Jezik logike sudova . . . 11
2.1.3. Semantika . . . 12
2.1.4. Logička implikacija i logička ekvivalencija . . . 14
2.2. Logika prvog reda . . . 15
2.2.1. Uvod . . . 15
2.2.2. Jezik logike prvog reda . . . 16

3. Skupovi **20**
3.1. Osnovni pojmovi . . . 20
3.2. Zadavanje skupova . . . 21
3.3. Booleove operacije na skupovima . . . 23
3.4. Kartezijev umnožak skupova . . . 28

4. Relacije **31**
4.1. Osnovni pojmovi . . . 31
4.2. Homogene relacije . . . 34
4.2.1. Relacije ekvivalencije . . . 36
4.2.2. Relacije uređaja . . . 38

4.3. Funkcije 42

5. Skupovi brojeva **51**
5.1. Skup prirodnih brojeva 51
5.1.1. Uvod 51
5.1.2. Rekurzivna definicija niza 52
5.1.3. Zbrajanje na skupu $\mathbb{N}$ 54
5.1.4. Množenje na skupu $\mathbb{N}$ 57
5.1.5. Daljnja svojstva skupa $\mathbb{N}$ 59
5.1.6. O uređenosti skupa $\mathbb{N}$ 61
5.1.7. Djeljivost na skupu $\mathbb{N}$ 62
5.1.8. Prosti brojevi 64
5.2. Skup cijelih brojeva 66
5.2.1. Uvod 66
5.2.2. Zbrajanje i množenje na $\mathbb{Z}$ 67
5.2.3. O uređenosti skupa $\mathbb{Z}$ 68
5.2.4. Ulaganje prirodnih u cijele brojeve 70
5.2.5. Djeljivost na skupu $\mathbb{Z}$ 72
5.2.6. Kongruencije 74
5.3. Skup racionalnih brojeva 76
5.3.1. Uvod 76
5.3.2. Zbrajanje i množenje na $\mathbb{Q}$ 77
5.3.3. Ulaganje cijelih u racionalne brojeve 79
5.3.4. O uređenosti skupa $\mathbb{Q}$ 80
5.4. Skup realnih brojeva 82
5.4.1. Apsolutna vrijednost 90
5.4.2. Potencije 92
5.4.3. Binomni teorem 95
5.5. Skup kompleksnih brojeva 97
5.5.1. Uvod 97
5.5.2. Trigonometrijski oblik kompleksnog broja 101

6. Elementarne funkcije **102**
6.1. Osnovne elementarne funkcije 102
6.1.1. Konstantna funkcija 103
6.1.2. Opća potencija 103
6.1.3. Eksponencijalna funkcija 107
6.1.4. Logaritamska funkcija 107
6.1.5. Trigonometrijske funkcije 108
6.1.6. Ciklometrijske funkcije 109
6.2. Elementarne funkcije 111
6.2.1. Polinomi 112
6.2.2. Racionalne funkcije 114
6.2.3. Algebarske funkcije 115
6.2.4. Transcendentne funkcije 115
6.2.5. Hiperbolne funkcije 116
6.2.6. Area funkcije 116

Bibliografija **118**

Uvod

Najstarije poznate matematičke pločice potječu iz 2400. godine prije Krista, no uporaba matematike zasigurno se proteže na cijelu civilizaciju. Tijekom 5000 godina razvila se golema količina postupaka i pojmova poznatih kao matematika i na mnogo se načina ispreplela sa svakidašnjicom. Kakva je priroda matematike? Čime se bavi? Kako se stvara i koristi? Koliko je važna?

Nalaženje odgovora na ta teška pitanja nimalo ne olakšava činjenica da se radi o građi koja je toliko opsežna da ju je nemoguće jednoj osobi spoznati, a kamoli ukratko izložiti. No o matematici možemo razmišljati i na drugi način: matematika je ljudska djelatnost već tisućama godina i svatko je svjesno ili nesvjesno rabi. Uz golemu populaciju koja se pomalo služi matematikom, postoji i malen broj ljudi koji su profesionalni matematičari: oni rade matematiku, njeguju je, podučavaju, stvaraju i koriste se njome u mnoštvu situacija. Matematika je beskrajno složen i tajnovit svijet: istraživanje toga svijeta trebala bi biti strast svakog matematičara.

Naivna definicija matematike glasi: *matematika je znanost o količini i prostoru.* Mogli bismo također dodati da se matematika bavi i simbolizmom koji se odnosi na količinu i prostor. Ova definicija ima povijesnu osnovu i može poslužiti kao početna. Znanosti o količini i prostoru u svojemu su jednostavnijem obliku poznate kao *aritmetika* i *geometrija.* Aritmetika, kakva se poučava u osnovnoj školi, bavi se brojevima raznih vrsta i pravilima za operacije među njima. Također se bavi i svakidašnjim situacijama u kojima koristimo te operacije.
Geometrija se predaje u višim razredima i jednim se dijelom bavi pitanjima prostornih mjerenja (udaljenost, površina), no bavi se i onim aspektima prostora koji imaju estetski značaj ili element iznenađenja. Na primjer, ona nam kaže da se tri težišnice bilo kojeg trokuta sijeku u jednoj točki ili da se dijagonale u svakom paralelogramu raspolavljaju. Uči nas da se pod može popločati jednakostraničnim trokutima ili pravilnim šesterokutima, ali ne i pravilnim peterokutima.

Stoljećima se geometrija razvijala kao *induktivna znanost*, znanost u kojoj se empirijskim putem dolazilo do pojedinačnih spoznaja iz kojih su se zatim indukcijom izvodile opće tvrdnje. No, predajemo li geometriju po 2300 godina starom Euklidovom učenju, onda ona ima još jedan važan aspekt, a to je prezentacija geometrije kao *deduktivne znanosti.* Počevši od izvjesnog broja osnovnih ideja koje se uzimaju kao bjelodane same po sebi, i na osnovi nekoliko određenih pravila matematičkog i logičkog manipuliranja, euklidska geometrija gradi sustav sve složenijih dedukcija. Taj deduktivni postupak kojim se počevši od hipoteza dolazi do zaključaka nazivamo *dokazom.* Euklidska geometrija je prvi primjer formaliziranja deduktivnog sustava i postala je model za sve takve sustave. Ona je sjajno područje za vježbanje logičkog razmišljanja i pruža osnovnu poduku u tomu.

Premda su deduktivni aspekti matematike bili jasni i drevnim matematičarima,

oni nisu bili naglašavani sve do 19. stoljeća kada se mislilo da u geometriji imamo dokaz, dok ga u algebri ili aritmetici nema. S povećanim naglaskom na deduktivne aspekte u svim granama matematike definicija same matematike se mijenja: sredinom 19. stoljeća smatra se da je matematika *znanost o donošenju potrebnih zaključaka*. Time nije definiran sadržaj matematike: matematika može biti o bilo čemu, ali samo tako dugo dok se drži predloška pretpostavka-dedukcija-zaključak. No definicija matematike se stalno mijenja i svaka generacija matematičara (ili čak svaki od njih) je formulira prema svom viđenju.

Može se postaviti i pitanje koliko je matematike danas poznato? Smatra se da bi današnje matematičko znanje stalo u otprilike 60 000 svezaka prosječne veličine. Tolika količina znanja daleko nadilazi mogućnost usvajanja bilo kojeg pojedinca. Pa ipak je to mala količina usporedimo li je s drugim zbirkama koje bi sakupili za npr. medicinu, fiziku, pravo ili književnost. Još se donedavno smatralo da dobar student može savladati cjelokupnu matematiku, no danas se to ne bi moglo kazati. Sada se smatra da bi dobro obrazovani matematičar mogao imati osnovna znanja o otprilike 10% raspoloživog matematičkog saznanja. Naime, matematika je kao snažno stablo s korijenjem, deblom, granama i grančicama označenima prema pojedinim disciplinama. I to stablo stalno raste! Konstrukcije se povećavaju i popunjavaju. Stvaraju se nove teorije. Uvode se novi objekti. Pronalaze se novi međuodnosi i time se ističu nove cjeline. Traže se nove primjene. U isto vrijeme, staro i istinito se zadržava (u principu). I tako ispada da je matematika organizam koji stalno raste, a prethodna grana je preduvjet za razumijevanje iduće grane koja je njezin izdanak. Takve serijske ovisnosti uglavnom nema u drugim disciplinama.

Koliko bi matematičkih knjiga trebao proučiti budući matematičar? Ako računamo jednu knjigu po kolegiju, pa to još udvostručimo zbog dodatne i neobavezne literature, doći ćemo do broja od oko 60 knjiga. Možemo tako gledati na onih 60 000 knjiga kao na ocean znanja čija prosječna dubina iznosi 60 knjiga, iz čega slijedi da postoji oko 1 000 uskih područja u matematici, no to je samo jednostavna i gruba procjena. Američko matematičko društvo daje finiju podjelu na otprilike 3 000 kategorija matematičkih radova. U većini tih kategorija velikom se brzinom stvaraju nova znanja: ocean se povećava i u dubinu i u širinu.

Ipak, postoji granica žive matematike koju čovječanstvo može podržavati u određenom trenutku: kako nastaju nova područja, tako se neka stara moraju zanemariti. Premda se za svako pojedino područje matematike može očekivati da će postati zasićeno, i premda će se eksponencijalni porast matematičke produkcije prije ili kasnije stabilizirati, teško je predvidjeti kraj čitave matematičke produkcije, osim kao dio kraja općeg stremljenja čovječanstva za sve više znanja i moći.

Uočimo još nešto: postoji piramida znanosti, a osnovicu te piramide čini upravo matematika jer se jedino ona ne mora oslanjati ni na jednu drugu znanost!

Poglavlje 1.

Građa matematike

1.1. Simboli

Posebni znakovi koji čine dio matematičkog zapisa velik su i živopisan dodatak znakovima prirodnih jezika. Dijete će već u osnovnoj školi naučiti deset znamenki dekadskog brojevnog sustava: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, znakove za aritmetičke operacije: $+,\ -,\ \cdot, :$, znakove grupiranja: $(\ )$, $\{\}$, $[\ ]$ i znakove za relacije poput $=, <, >, \leq, \geq$. Put u matematiku vodi učenika dalje: do algebre u kojoj se obična slova javljaju u posve neobičnom kontekstu: kao nepoznanice ili varijable. Diferencijalni i integralni račun uvodi nove simbole: d, $\int$, ∞, lim, $\sum$ i tako dalje.

Trenutačno se fond posebnih matematičkih simbola koji se stalno koriste sastoji od njih nekoliko stotina, a stalno se uvode i novi. Neki se često korišteni simboli mogu pripisati poznatim autorima: npr. oznaku $n!$ dugujemo Christianu Krampu $(1760 - 1826)$, a slovo e kao oznaku za broj 2.71828... dugujemo Leonhardu Euleru $(1707 - 1783)$. Neki su simboli skraćeni oblici riječi: tako je $+$ skraćenica na slovo t latinske riječi "et" što znači veznik i, π označava početno slovo grčke riječi "perimetar" što znači opseg, oznaka za integral $\int$ predstavlja početno slovo latinske riječi "summa" i tako dalje. S druge strane, neki simboli se čine potpuno proizvoljnima.

Glavna je zadaća simbola da precizno i jasno označavaju i da skraćuju. Zapravo, bez korištenja kratica matematičko bi izražavanje jedva bilo moguće. U matematici se često koriste slova grčkog alfabeta pa ih stoga i posebno navodimo.

A	α	alfa	I	ι	iota	P	ρ	ro
B	β	beta	K	κ $(\varkappa)$	kapa	Σ	σ	sigma
Γ	γ	gama	Λ	λ	lambda	T	τ	tau
Δ	δ	delta	M	μ	mi	Υ	υ	ipsilon
E	ϵ (ε)	epsilon	N	ν	ni	Φ	ϕ (φ)	fi
Z	ζ	zeta	Ξ	ξ	ksi	X	χ	hi
H	η	eta	O	o	omikron	Ψ	ψ	psi
Θ	θ (ϑ)	theta	Π	π	pi	Ω	ω	omega

1.2. Apstrakcija

Smatra se da je matematika nastala kada je predodžba o "tri jabuke" oslobođena jabuke i postala cijeli broj "tri". To je primjer procesa apstrakcije, no kako se

pojam apstrakcije u matematici koristi u različitim kontekstima, potrebno ga je pobliže objasniti.

1.2.1. Apstrakcija kao idealizacija

Dijete olovkom, pomoću ravnala, povlači crtu po papiru. To je naslaga grafita po površini papira koja nesumnjivo ima varijabilnu širinu i debljinu, a vrh olovke ostavlja, uslijed nepravilnosti na površini i ravnalu, pomalo krivudav trag. Uz taj stvarni primjer ravne crte postoji i mentalna ideja matematičke apstrakcije idealne ravne crte, točnije pravca. Euklid kaže da je ravna crta ona crta koja jednako leži prema točkama na njoj. Ili možemo reći da je to krivulja čiji je svaki dio najkraća spojnica između dviju njezinih točaka. Pravac je zamišljen kao da se pruža u beskonačnost s obje strane.

Jednako kao što idealiziramo ravnu crtu idealiziramo i mnoge druge objekte: ravninu, kružnicu, kvadrat, sferu, kocku... Neki od tih pojmova se ne definiraju (točka, pravac, ravnina...), a drugi se, pak, definiraju pomoću jednostavnijih pojmova (kocka, kvadrat...). Razumljivo je da će svaki stvarni primjer pokazivati nesavršenosti, no um će to velikodušno previdjeti. Spomenute idealizacije prelaze tako iz prostornog iskustva u matematički svijet: Aristotel je opisao taj proces rekavši da matematičar ignorira sve što je osjetilno i ostavlja samo količinu i prostorni kontinuitet. Platonova ideja o svijetu idealiziranih objekata blisko je povezana s matematičkom intuicijom. Svi su matematički objekti apstraktni, a Platonov svijet je dom prave kružnice i pravog kvadrata.

1.2.2. Apstrakcija kao ekstrakcija

Četiri ptice kljucaju mrvice na dvorištu. Četiri su naranče na stolu. Sama uporaba riječi "četiri" podrazumijeva postojanje procesa apstrakcije u kome se izdvaja zajednička odlika ptica i naranči: za svaku pticu po jedna naranča i za svaku naranču po jedna ptica. Na taj način između ptica i naranči postoji obostrano jednoznačna korespodencija.

S jedne strane imamo stvarne objekte, to su ptice i naranče, a s druge strane apstraktni pojam "četiri" koji postoji bez obzira na ptice i naranče. Tako se dolazi do apstraktnih brojeva koji postoje bez obzira na stvarne objekte. Danas matematika uglavnom ostavlja po strani pitanje kako su nastale takve apstrakcije i usredotočuje se na skupovno-teoretski opis oblikovanja apstrakcije. Tako je na primjer apstraktni pojam "četiri" klasa svih skupova koji se mogu staviti u obostrano jednoznačnu korespodenciju s četiri ptice na dvorištu.

1.3. Generalizacija

Riječi generalizacija i apstrakcija često se rabe kao sinonimi, no riječ generalizacija ima nekoliko specifičnih značenja koja treba rasvijetliti.

Pretpostavimo da je u neko davno doba matematičar X rekao: "Ako je $\triangle ABC$ jednakostraničan trokut, onda je kut u vrhu A jednak kutu u vrhu B." Zatim je neki drugi matematičar Y primijetio da, iako je to točno, nije neophodno da trokut $\triangle ABC$ bude jednakostraničan, već je ustvrdio: "U jednakokračnom trokutu su

kutovi uz bazu jednaki." Ova druga tvrdnja je generalizacija prve: pretpostavke prve tvrdnje impliciraju pretpostavke druge tvrdnje, ali ne i obratno, dok je zaključak isti.

Jedna od prednosti generalizacije je konsolidacija (povezivanje, grupiranje) informacija: nekoliko usko povezanih činjenica ekonomično se umotaju u jedan paket. Pogledajmo primjer. Za proizvoljan prirodan broj vrijedi:

T1. Ako broj završava s 0, onda je djeljiv s 2.

T2. Ako broj završava s 2, onda je djeljiv s 2.

T3. Ako broj završava s 4, onda je djeljiv s 2.

T4. Ako broj završava s 6, onda je djeljiv s 2.

T5. Ako broj završava s 8, onda je djeljiv s 2.

K. Ako broj završava s parnim brojem, onda je taj broj djeljiv s 2.

1.4. Formalizacija

Formalizacija je proces pomoću kojega se matematika prilagođava mehaničkom procesuiranju. Npr. kompjutorski program je primjer formaliziranog teksta. Matematički tekstovi nikada nisu potpuno formalizirani: napisani su nekim jezikom da bi ih ljudi mogli čitati. Ipak, svaki se matematički tekst *može* potpuno formalizirati i to u jednom jedinom formalnom jeziku: jeziku formalne teorije skupova. Četiri simbola su posebno vezana uz teoriju skupova: $\cup$, $\subseteq$, $\in$ i $\emptyset$. Ostali simboli su simboli logike koji se upotrebljavaju u bilo kojoj formaliziranoj matematičkoj teoriji.

Formalne su jezike prvi uveli Peano i Frege krajem 19. stoljeća s namjerom da matematički dokaz učinu strožim. No ta se svrha ne može ispuniti sve dok je dokaz namjenjen ljudskom čitatelju. *Principia Mathematica* Rusella i Whiteheada bila je veličanstven pokušaj da se matematika zaista formalizira, a ostala je zapamćena kao nečitljivo remek-djelo. Ipak, pojavom računala formalni su jezici našli široku primjenu i postali jedan od nezabilaznih predmeta današnje kulture.

Formalizirani tekst je niz simbola: kada njime manipulira matematičar ili stroj, pretvara se u drugi niz simbola. Manipulacija simbolima može i sama biti predmetom matematičke teorije. Kada na manipuliranje gledamo kao na nešto što izvodi stroj, tada to računarci nazivaju *teorijom automata*, a logičari *teorijom rekurzije*. No, kada na manipuliranje gledamo kao na nešto što izvodi matematičar, tada to nazivamo *teorijom dokaza*.

1.5. Matematički objekti i strukture

Neformalno matematičko izlaganje sastoji se od imenica, glagola, pridjeva, i tako dalje. Imenicama definiramo *matematičke objekte*, npr. broj 3, skup prostih brojeva, logaritamsku funkciju... *Matematičke strukture* su nešto složenije i označavaju

matematičke objekte povezane izvjesnim relacijama, no jasna granica između matematičkih struktura i matematičkih objekata nije strogo određena. Ako se neka matematička struktura dugo koristi i ako se na njoj gradi iskustvo i intuicija, onda je možemo smatrati matematičkim objektom. Dobar primjer za to su realni brojevi: često ih smatramo matematičkim objektom, iako je riječ o matematičkoj strukturi.

Važno je shvatiti da je ponekad ono što danas smatramo jednostavnim matematičkim objektom nekad imalo psihološko značenje cijele strukture: na primjer kružnica, pravilni poliedar i slično.

Izraz "matematički objekt" podrazumijeva da objekt o kojemu se radi na neki način postoji. Mogli bismo pomisliti da je postojanja tog objekta sasvim jasno, no u stvarnosti su s tim povezane ozbiljne logičke i psihološke poteškoće. Pogledajmo jedan primjer: skup $\mathbb{N}$ ne možemo potpuno doživjeti, no matematičari svakodnevno s njim rade. Skup $\mathbb{N}$ ima svojstvo da ako sadrži neki broj, onda sadrži i njegova sljedbenika. Stoga ne može postojati najveći prirodni broj. Drugo svojstvo koje ima skup $\mathbb{N}$ jest da ga nikad ne možemo iscrpsti izostavljajući njegove članove jednog po jednog. Ta čudesna riznica sa svojstvima koja protuslove svim iskustvima iz naših konačnih života, apsolutni je temelj u matematici i smatra se da je u dosegu poimanja djece u osnovnoj školi. No, je li matematička beskonačnost prijevara? Označava li ona nešto što zapravo uopće nije beskonačno? Zašto bismo povjerovali da beskonačno postoji? U formalnoj prezentaciji taj je zahtjev usvojen aksiomatski: uveden je aksiom beskonačnosti koji kaže da induktivni (beskonačni) skup postoji.

1.6. Oblici matematičkog mišljenja

Mišljenje se u psihologiji definira kao izdvajanje u spoznaji čovjeka određenih strana i svojstava promatranog objekta i njihovo dovođenje u odgovarajuće veze s drugim objektima u cilju stjecanja novih saznanja.

Tri su osnovna oblika mišljenja: *poimanje*, *suđenje* i *zaključivanje*. Kao rezultat tih oblika mišljenja dobivaju se redom: *pojmovi*, *jednostavni sudovi* i *složeni sudovi*. Pogledajmo primjer za svaki od ovih rezultata oblika mišljenja.

1. **Pojam**: Skup svih točaka ravnine jednako udaljenih od jedne njezine čvrste točke zove se kružnica.

2. **Jednostavni sud**: Za svaki prost broj $p > 3$ broj $p^2 - 1$ je djeljiv s 24.

3. **Složeni sud**: Ako je $a \in A$ i $A \subseteq B$, onda je $a \in B$.

Oblici mišljenja imaju veliki značaj u izgradnji neke matematičke teorije. Još od starogrčke matematike većina se matematičkih disciplina nastoji u višoj fazi izgradnje strogo utemeljiti. Takav strogi pristup nekoj matematičkoj disciplini nazivamo *aksiomatskim pristupom*. Najprije kratko objasnimo što to znači aksiomatski zadati neku teoriju. Polazimo od određenog broja pojmova koji se ne definiraju, a nazivamo ih *osnovnim pojmovima*. Time smo zadali *jezik teorije*. Zatim se popišu osnovne tvrdnje o danim osnovnim pojmovima koje se smatraju istinitima. Te tvrdnje, čiju istinitost ne dokazujemo, nazivamo *aksiomima*. Pri tomu, poželjno je da izabrani aksiomi zadovoljavaju sljedeća tri principa:

1. **konzistentnost**: iz sustava aksioma ne smije se moći istodobno dokazati neka tvrdnja i njezina negacija;

2. **potpunost**: svaka tvrdnja, ili njezina negacija, je dokaziva u danom sustavu aksioma;

3. **neovisnost:** niti jedan od aksioma se ne može dobiti kao posljedica ostalih.

Svaki novi pojam aksiomatski zadane teorije uvodimo *definicijom* pomoću osnovnih ili već definiranih pojmova (to jest, unutar jezika teorije). Svaku novu *tvrdnju* dokazujemo logičkim zaključivanjem na osnovu definicija, aksioma i tvrdnji koje smo već dokazali. Dakle, možemo reći da je neko matematičko područje tvorevina osnovnih pojmova, aksioma, izvedenih pojmova i dokazanih tvrdnji. Pogledajmo podrobnije što podrazumijevamo pod tim nazivima.

1.6.1. Matematički pojmovi

Matematički pojam je oblik mišljenja u kojem se odražavaju bitna svojstva objekta koji se proučava. *Osnovni pojam* je (u pravilu) jednostavni pojam koji se smatra poznatim, pa se ne definira, tj. ne opisuje se pomoću drugih pojmova. Takvi pojmovi su npr. točka, pravac, skup... *Izvedeni pojam* je pojam koji se jasno i precizno definira, što znači da se njegovo značenje opisuje pomoću osnovnih ili ranije definiranih pojmova. *Definicija pojma* je, dakle, nabrajanje nužnih i dovoljnih obilježja toga pojma povezanih logičkom rečenicom ili simboličkim zapisom.
Prilikom definiranja nekog pojma treba paziti na sljedeće:

1. Definicija treba biti primjerena pojmu kojeg definira: ne smije biti ni preuska ni preširoka.

2. Definicija treba biti pregledna i sažeta.

3. Definicija ne smije biti izražena slikovitim ni dvosmislenim jezikom.

4. Definicija ne smije biti cirkularna. *(Skup je beskonačan ako nije konačan. Skup je konačan ako nije beskonačan.)*

5. Definicija ne smije biti negativna ako može biti pozitivna.

6. Mora postojati barem jedan objekt kojeg definicija opisuje.

Često se neki pojam može definirati na više načina. Pri tomu je važno da sve te definicije određuju isti skup objekata, tj. da su međusobno ekvivalentne.
Pogledajmo kako možemo definirati kvadrat.

D1. Pravokutnik kojemu susjedne stranice imaju jednake duljine naziva se kvadrat.

D2. Kažemo da je pravokutnik kvadrat ukoliko su mu dijagonale međusobno okomite.

D3. Kvadrat je romb kojemu je kut između susjednih stranica pravi.

Ako odaberemo jednu od tih definicija kao radnu definiciju toga pojma, onda njoj ekvivalentne definicije poprimaju značenje poučaka koji su njezine posljedice. Te poučke nazivamo *karakterizacijama* toga pojma.

1.6.2. Aksiomi

Aksiom je polazna tvrdnja o osnovnim pojmovima koja se smatra istinitom te se ne dokazuje. Pogledajmo nekoliko primjera aksioma.

A1. Cjelina je veća od dijela.

A2. Točkom izvan danog pravca može se povući jedinstveni pravac paralelan s danim pravcem.

A3. Za svaka dva pozitivna realna broja a i b postoji prirodni broj n takav da je $na > b$.

Postulat je polazna tvrdnja koja se također uzima bez dokaza. Postulat obično izražava uvjet koji mora zadovoljavati neki pojam ili izražava neki odnos među pojmovima. Evo jednog primjera postulata.

Linearni operator na V^3 je svako preslikavanje $f : V^3 \to V^3$ koje ima sljedeća svojstva:

L1. $f(\alpha \overrightarrow{a}) = \alpha f(\overrightarrow{a})$ za svaki $\alpha \in \mathbb{R}$ i svaki vektor $\overrightarrow{a} \in V^3$,

L2. $f\left(\overrightarrow{a} + \overrightarrow{b}\right) = f(\overrightarrow{a}) + f\left(\overrightarrow{b}\right)$ za sve vektore $\overrightarrow{a}, \overrightarrow{b} \in V^3$.

Tvrdnje L1. i L2. su postulati linearnog operatora.
Ipak, u modernoj matematici se najčešće ne pravi razlika između postulata i aksioma.

1.6.3. Teoremi

Teorem ili *poučak* neke matematičke teorije je sud čija se istinitost utvrđuje dokazom, tj. logičkim zaključivanjem iz aksioma i već dokazanih teorema te teorije. U izgradnji neke matematičke teorije teoremi igraju važnu ulogu: oni proširuju i produbljuju znanje o tom području matematike i o njegovim objektima. Važno je napomenuti da se pod teoremom uvijek podrazumijeva istinit sud.

U teoremu mora biti jasno istaknuto sljedeće:
(1) uz koje se uvjete razmatra određeni objekt,
(2) što se o tom objektu tvrdi.

Stoga, u formuliranju teorema razlikujemo dva dijela. Prvi dio se zove *pretpostavka* (uvjet, hipoteza, premisa) P, a drugi dio *tvrdnja* teorema (zaključak, posljedicu, konkluziju) Q. Ključne riječi su "*Ako je P, onda je Q*", odnosno "*Ako vrijedi P, onda vrijedi Q*".
Pogledajmo nekoliko primjera.

T1. Umnožak dvaju uzastopnih parnih brojeva a i b je djeljiv s 8.
P: a i b su uzastopni parni brojevi.
Q: Umnožak ab je djeljiv s 8.

T2. Dijagonale romba su okomite.
P: Dani četverokut je romb.
Q: Dijagonale toga četverokuta su okomite.

T3. Svaki obodni kut nad promjerom kružnice je pravi.
P: Dani kut je kut nad promjerom kružnice.
Q: Dani kut je pravi.

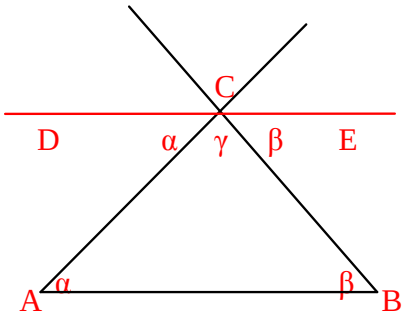
Posebno važni teoremi su prije spomenute karakterizacije pojma. Karakterizacija nekog pojma jednako određuje taj pojam kao i sama njegova definicija, tj. mogla je biti uzeta za definiciju toga pojma (u tom slučaju bi prijašnja definicija postala karakterizacija). Karakterizacije pojma su teoremi oblika "*P je ako i samo ako je Q*" ili kraće "*P je akko je Q*" i kao i sve druge teoreme dokazujemo ih. Za dokazati teoreme ovog oblika potrebno je dokazati dva teorema (nužnost i dovoljnost): "Ako je P, onda je Q" i "Ako je Q, onda je P".

U matematici se teorem za koji postoji kratki i jednostavni dokaz uobičajeno zove *propozicija*. Teorem koji sam za sebe nije od posebnog značaja, nego služe kao etapa u dokazu nekog važnijeg teorema, nazivamo *lemom*. Konačno, teorem koji je neposredna i jednostavna posljedica drugog, prethodno dokazanog teorema, nazivamo *korolarom* toga teorema. Dokaz korolara je često toliko očit da ga ni ne pišemo.

1.6.4. Dokazi

Postoje dvije osnovne vrste dokaza: *direktni dokaz* i *indirektni dokaz*.
Direktni dokaz neke tvrdnje Q sastoji se u tomu da se, polazeći od pretpostavke P, primjenom aksioma, definicija i ranije dokazanih teorema, nizom ispravnih logičkih zaključivanja dođe do tvrdnje Q. Pogledajmo jedan primjer.

Teorem. Zbroj kutova u svakom trokutu je 180^0.
Dokaz. Pretpostavka P: Neka je $\triangle ABC$ po volji odabrani trokut, te označimo $\alpha = \measuredangle CAB$, $\beta = \measuredangle ABC$ i $\gamma = \measuredangle BCA$. Tvrdnja Q: $\alpha + \beta + \gamma = 180^0$.



Vrhom C trokuta $\triangle ABC$ povucimo paralelu DE s pravcem AB. Povlačenje ove paralele omogućava nam *Aksiom o paralelama* euklidske geometrije koji kaže da se točkom izvan danog pravca može povući jedinstveni pravac paralelan s danim pravcem. Uočimo da su kutovi $\measuredangle ACD$ i $\measuredangle CAB$, odnosno $\measuredangle ECB$ i $\measuredangle ABC$ jednaki (jednakost slijedi po *Poučku o kutovima s paralelnim kracima*), pa je $\measuredangle ACD = \measuredangle CAB = \alpha$ i $\measuredangle ECB = \measuredangle ABC = \beta$. Kutovi $\measuredangle ACD$, $\measuredangle BCA$ i $\measuredangle ECB$ zajedno tvore ispruženi kut, pa je $\alpha + \beta + \gamma = \measuredangle ACD + \measuredangle BCA + \measuredangle ECB = 180^0$. ■

Od indirektnih dokaza najčešće se primjenjuju sljedeća dva:
- *dokaz obratom po kontrapoziciji*,
- *dokaz svođenjem na kontradikciju*.

Dokaz obratom po kontrapoziciji. Indirektni dokaz teorema čija je pretpostavka P, a tvrdnja Q obratom po kontrapoziciji je direktni dokaz teorema kojem je pretpostavka negacija tvrdnje $-Q$, a tvrdnja negacija pretpostavke $-P$, tj. teorem "Ako je P, onda je Q" dokazujemo dokazujući direktnim dokazom ekvivalentan mu teorem "Ako je $-Q$, onda je $-P$" (u sljedećem poglavlju ćemo se uvjeriti da su to ekvivalentni teoremi). Pogledajmo jedan primjer dokaza obratom po kontrapoziciji.

Teorem. Ako je $n \in \mathbb{N}$ i n^2 neparan broj, onda je i n neparan broj.
Dokaz. Pretpostavka P : $n \in \mathbb{N}$ i n^2 je neparan broj. Tvrdnja Q : n je neparan broj.
Dokazati ovaj teorem obratom po kontrapoziciji isto je što i dokazati direktnim dokazom teorem: *Ako je $n \in \mathbb{N}$ i n paran broj, onda je i n^2 paran broj.*
Pretpostavimo da je n paran broj. On je tada oblika $n = 2k$ za neki $k \in \mathbb{N}$. No, iz ovoga slijedi da je $n^2 = 4k^2 = 2\left(2k^2\right) = 2m$, gdja je $m = 2k^2 \in \mathbb{N}$, pa je n^2 paran broj. Sada, obratom po kontrapoziciji, zaključujemo da vrijedi polazni teorem: Ako je n^2 neparan broj, onda je i n neparan broj. ■

Dokaz svođenjem na kontradikciju. Indirektni dokaz teorema čija je pretpostavka P, a tvrdnja Q svođenjem na kontradikciju je direktni dokaz u kojem se kreće od pretpostavke P i negacije tvrdnje Q, tj. od P i $-Q$ i nizom logičkih zaključaka dođe do neke očigledne neistine. Iz toga slijedi da nešto u pretpostavci nije točno, a kako P mora biti istinita (jer je P pretpostavka polaznog teorema), slijedi da je negacija tvrdnje Q neistinita, odnosno da je tvrdnja Q istinita. Tako uz pretpostavku da vrijedi P dobivamo da vrijedi i Q, tj. vrijedi teorem "Ako je P, onda je Q". Pogledajmo primjer dokaza svođenjem na kontradikciju.

Teorem. Ako su a i b pozitivni realni brojevi, onda je $(a+b)/2 \geq \sqrt{ab}$.
Dokaz. Pretpostavka P : a i b su pozitivni realni brojevi. Tvrdnja Q : $(a+b)/2 \geq \sqrt{ab}$.
Pretpostavimo da su a i b pozitivni realni brojevi i da je $(a+b)/2 < \sqrt{ab}$. Tada je

$$a + b < 2\sqrt{ab},$$

odnosno

$$a + b - 2\sqrt{ab} < 0.$$

Ovu nejednakost možemo zapisati kao

$$\left(\sqrt{a} - \sqrt{b}\right)^2 < 0,$$

što je očigledna neistina $\Rightarrow\Leftarrow$ (kontradikcija). Dakle, vrijedi $(a+b)/2 \geq \sqrt{ab}$. ■

1.7. Algoritamska i dijalektička matematika

Da bismo razumjeli razliku između algoritamskog i dijalektičkog stajališta u matematici, dat ćemo jedan primjer. Pretpostavimo da nas zanima problem nalaženja rješenja jednadžbe $x^2 = 2$. Taj je problem mučio starogrčke matematičare: $\sqrt{2}$ postoji (kao dijagonala jediničnog kvadrata), a ipak ne postoji (kao racionalan broj).

Algoritamsko rješenje. Iz $x^2 = 2$ slijedi da je $x = 2/x$. Ako se x neznatno smanji, onda se $2/x$ neznatno uveća. Na pola puta između smanjivanja i uvećavanja biti će pravo rješenje. Jednakost $x = 2/x$ možemo zapisati u obliku $x = \frac{1}{2}\left(x + \frac{2}{x}\right)$, pa definiramo niz $(x_n)_{n\in\mathbb{N}}$ kao

$$\begin{aligned} x_1 &= 1, \\ x_{n+1} &= \frac{1}{2}\left(x_n + \frac{2}{x_n}\right),\ n = 2, 3, \ldots \end{aligned}$$

Ovaj niz konvergira prema $\sqrt{2}$ kvadratnom brzinom.

Dijalektičko rješenje. Promotrimo graf funkcije $f : \mathbb{R} \to \mathbb{R}$ definirane izrazom $f(x) = x^2 - 2$. Za $x_0 = 1$ je $f(x_0) = f(1) = -1$, a za $x_1 = 2$ je $f(x_1) = f(2) = 2$. Kako se x neprekidno mijenja od 1 do 2, tako se $f(x)$ neprekidno mijenja od negativne vrijednosti -1 prema pozitivnoj vrijednosti 2. Stoga negdje između brojeva $x_0 = 1$ i $x_1 = 2$ mora biti vrijednost od x za koju je $f(x) = 0$, tj. $x^2 = 2$.

U izvjesnom smislu, ni prvo ni drugo rješenje nije uistinu rješenje. Prvo rješenje nam daje sve bolju i bolju aproksimaciju, no kad god stali, nećemo još imati posve točno rješenje. Drugo rješenje nam samo kaže da egzaktno rješenje postoji i da se nalazi između brojeva 1 i 2, i to je sve.

Dijalektika nam daje uvid i slobodu: naše znanje o onomu što postoji može ići puno dalje od onoga što smo kadri izračunati ili čak aproksimirati. Pogledajmo jedan primjer. Uzmimo trokut s tri nejednake stranice. Pitamo se postoji li vertikalni pravac koji raspolavlja površinu trokuta, tj. koji dijeli trokut na dva lika jednakih površina? U okviru algoritamske matematike postavili bismo problem nalaženja takvog pravca. U okviru dijalektičke matematike možemo odgovoriti da takav pravac postoji bez da ga egzaktno odredimo. Treba samo primijetiti da se, pomičući vertikalni pravac s lijeva na desno, površina trokuta s lijeve strane pravca neprekidno mijenja od 0% površine polaznog trokuta do 100%, pa tako mora postojati mjesto gdje je površina tog dijela točno 50% površine polaznog trokuta. Primijetimo još da pri ovom zaključivanju uopće nisu korištena specifična svojstva trokuta, pa isti argument vrijedi za bilo kakvo područje. I tako ustvrđujemo da za svaki lik konačne površine postoji vertikalni pravac koji raspolavlja površinu tog lika, iako ga ne znamo naći, te iako možda ne znamo ni površinu područja koje raspolavljamo.

Algoritamski pristup je primjeren kada problem zahtijeva numerički odgovor, a numerička analiza, koja je istodobno grana primjenjene matematike i računarstva, je znanost dobivanja numeričkih odgovora na takve matematičke probleme. Matematika je počela kao algoritamska znanost. U vrijeme starih Grka pojavila se dijalektička, strogo logička matematika, no tek u moderna vremena nalazimo matematiku s malo ili nimalo algoritamskog konteksta.

Najveći dio ovog poglavlja preuzet je iz [2], te iz [1].

Poglavlje 2.

Osnove matematičke logike

2.1. Logika sudova

2.1.1. Uvod

U matematici, kao i u svakodnevnom životu, misli i tvrdnje izričemo rečenicama. Jedan od osnovnih problema u matematičkoj logici je ispitati istinitost neke rečenice (logičke forme) i to promatrajući samo njezin oblik, a ne i sadržaj. Logika sudova ili propozicijska logika je jedna od najjednostavnijih formalnih teorija. U njoj se rečenice promatraju kao forme sastavljene od "atomarnih" dijelova (jednostavnih sudova) koji su povezani veznicima: *ne*, *i*, *ili*, *ako...onda* i *ako i samo ako.*

Za sud se obično kaže da je to svaka suvisla izjavna rečenica koja je istinita ili lažna, ali ne i oboje. No, ovo svakako ne može biti definicija suda jer se može postaviti pitanje što je istinita rečenica ili pak što je suvisla istinita rečenica. Pogledajmo nekoliko primjera.

1. Rečenica "Dva plus dva je jednako četiri." jest sud, i to istinit.
2. Rečenica "Dva plus dva je jednako pet." jest sud, i to lažan.
3. Rečenica "x plus dva je jednako osam." nije sud jer za nju ne možemo reći je li istinita ili lažna dok ne znamo koliko je x.
4. Rečenica "Koliko je sati?" nije sud jer nije izjavna rečenica.
5. Rečenica "*Broj* 0.0001 *je mali broj*." nije sud jer nije precizirano što je mali broj.

Sudovi (1) i (2) su jednostavnog oblika, tj. atomarni su. Pomoću veznika iz jednostavnih sudova gradimo složenije sudove. Na primjer, rečenica "Ako pada kiša, onda nosim kišobran." je primjer složenog suda.

U logici sudova proučavamo i logička zaključivanja, te određujemo koja su korektna, a koja nisu. Promotrimo neke primjere.
Zaključivanje:

Ako pada kiša, onda nosim kišobran.
Pada kiša.

Nosim kišobran.

je primjer korektnog zaključivanja. Formalno zapisano, ono je oblika

$$\frac{\begin{array}{c} A \to B \\ A \end{array}}{B}$$

i nazivamo ga **modus ponens**.

No zaključivanje:

$$\frac{\begin{array}{c} \text{U nedjelju ću ići u kino.} \\ \text{Danas nije nedjelja.} \end{array}}{\text{Danas ne idem u kino.}}$$

nije korektno. Formalno ga zapisujemo kao

$$\frac{\begin{array}{c} A \to B \\ -A \end{array}}{-B} \quad .$$

Veoma je važno razlučiti koje je zaključivanje korektno, odnosno što je logička posljedica. Formalno matematičko zaključivanje može se činiti sitničavim ako ga usporedimo s dokazivanjem u svakodnevnoj praksi u kojoj je intuitivna matematička mjera strogosti najčešće dovoljna. Međutim u slučajevima sumnje ili spora valja pribjeći većoj strogosti.

2.1.2. Jezik logike sudova

Sada ćemo definirati osnovne znakove logike sudova i način na koji gradimo formule; kada je to zadano smatramo da je zadan jezik teorije. No, prije tih definicija uvest ćemo sljedeće pojmove:

Skup je osnovni matematički pojam i ne definira se, no intuitivno je jasno što pod skupom podrazumijevamo. Skup smatramo zadanim ako znamo koji su njegovi elementi. Skup koji ne sadrži nijedan element nazivamo *praznim skupom*. Unija skupova je skup čiji elementi pripadaju barem jednom od tih skupa. Skupovima ćemo se detaljno baviti u sljedećem poglavlju.

Abeceda ili *alfabet* je proizvoljan neprazan skup. Svaki element abecede je *simbol* ili *znak*. *Riječ* u nekoj abecedi je bilo koji konačan niz znakova iz dane abecede. Ako je A neka abeceda, onda s A^* označavamo skup svih riječi abecede A. Po dogovoru uzimamo da skup svih riječi proizvoljne abecede sadrži i praznu riječ; označavamo je ε. Najvažnija operacija na skupu riječi je *konkatenacija*: ako su a i b dvije riječi, onda kažemo da je riječ ab nastala konkatenacijom riječi a i b.

Primjer 1. *Neka je $A = \{\alpha, \beta\}$ i neka su $\alpha\alpha\beta\alpha, \beta\alpha\beta\beta\alpha \in A^*$ dvije riječi abecede A. Njihovom konkatenacijom dobivamo novu riječ $\alpha\alpha\beta\alpha\beta\alpha\beta\beta\alpha \in A^*$ te abecede.*

Abeceda logike sudova je unija skupova A_1, A_2 i A_3, gdje je:

1. $A_1 = \{P_0, P_1, P_2, \ldots\}$ prebrojiv skup čije elemente nazivamo *propozicijskim varijablama*,
2. $A_2 = \{-, \wedge, \vee, \to, \leftrightarrow\}$ skup *logičkih veznika*,

3. $A_3 = \{(,)\}$ skup *pomoćnih simbola* (lijeva i desna zagrada).

Logičke veznike nazivamo redom: *negacija* $(-)$, *konjukcija* $(\wedge)$, *disjunkcija* $(\vee)$, *kondicional* $(\rightarrow)$ i *bikondicional* $(\leftrightarrow)$.
Propozicijske varijable, u jednoj svojoj interpretaciji, možemo shvatiti kao jednostavne sudove. Još jedna interpretacija logike sudova su npr. elektronički logički sklopovi.

Sada ćemo definirati najvažnije riječi abecede logike sudova: formule.

Definicija 2.1.1. ***Atomarna formula*** *je svaka propozicijska varijabla.* ***Formula*** *je*

a) svaka atomarna formula,

b) ako su A i B formule, onda su i riječi $(-A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ i $(A \leftrightarrow B)$ formule,

c) riječ abecede logike sudova je formula ako i samo ako je nastala primjenom konačno mnogo puta pravila a) i b).

Primjedba 2.1.1. *Primijetimo da u prethodnoj definiciji A i B nisu formule, već samo oznake za formule. Općenito ćemo formule označavati velikim latiničnim slovima s početka abecede $(A, B, C, F, G, \ldots)$, dok ćemo za propozicijske varijable koristiti velika latinična slova s kraja abecede $(P, Q, R, S, V, \ldots)$.*

Najjednostavnija formula je, očito, sama propozicijska varijabla. Ako je A formula, te $\{P_1, ..., P_n\}$ skup propozicijskih varijabli koje se pojavljuju u formuli A, onda to kratko označavamo s $A(P_1, ..., P_n)$.

Da bismo izbjegli pisanje velikog broja zagrada uvest ćemo prioritet logičkih veznika: najveći prioritet ima negacija, zatim konjukcija i disjunkcija, a najmanji prioritet imaju kondicional i bikondicional. Na primjer, formulu $(((-P) \wedge Q) \rightarrow R)$ pišemo kao $(-P \wedge Q) \rightarrow R$ ili jednostavno $-P \wedge Q \rightarrow R$.

Ako su A i B oznake za istu formulu pišemo to na način $A \equiv B$ i govorimo da su formule A i B jednake. Znak $\equiv$ nije znak abecede logike sudova već pomoćni tzv. meta-simbol.

2.1.3. Semantika

U prethodnoj točki smo definirali sintaksu jezika logike sudova. Sada ćemo definirati semantiku: reći ćemo što znači da je neka formula istinita, odnosno neistinita.

Svako preslikavanje sa skupa propozicijskih varijabli u skup $\{0, 1\}$ nazivamo *totalnom interpretacijom* ili kratko *interpretacijom*. Ako je preslikavanje definirano sa podskupa skupa propozicijskih varijabli u skup $\{0, 1\}$, kažemo da se radi o *parcijalnoj interpretaciji*.

Kažemo da je parcijalna interpretacija I *odgovarajuća* za formulu $A(P_1, ..., P_n)$ ako je I definirana na skupu $\{P_1, ..., P_n\}$.

Po složenosti neke formule definiramo toj formuli odgovarajuće interpretacije u skladu s danom semantičkom tablicom:

P	Q	$-P$	$P \wedge Q$	$P \vee Q$	$P \to Q$	$P \leftrightarrow Q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Kažemo da je formula F *istinita za interpretaciju* I ako je vrijednost interpretacije I na formuli F jednaka 1, tj. $I(F) = 1$. Kažemo da je formula F *neistinita za interpretaciju* I ako je vrijednost interpretacije I na formuli F jednaka 0, tj. $I(F) = 0$.

Primjer 2. *Neka je* $F \equiv (-P \vee Q) \to -R$, *te* $I(P) = I(Q) = 0$ *i* $I(R) = 1$. *Odredimo* $I(F)$.

P	Q	R	$-P$	$-P \vee Q$	$-R$	$(-P \vee Q) \to -R$
0	0	1	1	1	0	0

Dakle, $I(F) = 0$. *Naravno,* $I(F)$ *ovisi o* $I(P)$, $I(Q)$ *i* $I(R)$, *pa za neke druge vrijednosti* $I(P)$, $I(Q)$ *i* $I(R)$ *može i vrijednost* $I(F)$ *biti različita. Pogledajmo sve moguće odgovarajuće interpretacije za formulu* F*:*

P	Q	R	$-P$	$-P \vee Q$	$-R$	$(-P \vee Q) \to -R$
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	1	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	1
1	0	1	0	0	0	1
1	1	0	0	1	1	1
1	1	1	0	1	0	0

Uočimo da smo gornjom tablicom formuli F pridružili funkciju sa skupa $\{0,1\}^3$ u skup $\{0,1\}$. Takvu funkciju nazivamo *istinosnom funkcijom.*

Definicija 2.1.2. *Za formulu* F *kažemo da je* ***ispunjiva*** *ako postoji interpretacija* I *za koju je* $I(F) = 1$. *Za formulu* F *kažemo da je* ***oboriva*** *ako postoji interpretacija* I *za koju je* $I(F) = 0$. *Za formulu* F *kažemo da je* ***valjana*** *ili* ***tautologija*** *ako je istinita za svaku svoju odgovarajuću interpretaciju. Za formulu* F *kažemo da je* ***antitautologija*** *ako je neistinita za svaku svoju odgovarajuću interpretaciju.*

Uočimo da su valjane formule upravo one formule koje su istinite bez obzira na istinitost svojih atomarnih dijelova.

Neke važne valjane formule (tautologije) su:.

1. $--P \leftrightarrow P$, princip dvojne negacije,
2. $P \vee -P$, princip isključenja trećeg,

3. $-(P \wedge -P)$, princip neproturječnosti,
4. $(P \to Q) \leftrightarrow (-Q \to -P)$, princip kontrapozicije,
5. $-P \to (P \to Q)$, princip negacije premise,
6. $P \wedge (P \to Q) \to Q$, princip modus ponens,
7. $-(P \vee Q) \leftrightarrow -P \wedge -Q$, De Morganov princip,
8. $-(P \wedge Q) \leftrightarrow -P \vee -Q$, De Morganov princip.

2.1.4. Logička implikacija i logička ekvivalencija

Definicija 2.1.3. *Kažemo da formula A **logički implicira** formulu B ili da formula B **logički slijedi** iz formule A, i pišemo $A \Rightarrow B$, ako za svaku interpretaciju I za koju je $I(A) = 1$ vrijedi $I(B) = 1$.*

Vrijedi sljedeća karakretizacija logičke implikacije.

Propozicija 2.1.1. *$A \Rightarrow B$ ako i samo ako je $A \to B$ valjana formula.*

Drugim riječima, implikacija se može svesti na valjanost kondicionala.

Definicija 2.1.4. *Kažemo da su formule A i B **logički ekvivalentne**, i pišemo $A \Leftrightarrow B$, ako za svaku interpretaciju I vrijedi $I(A) = I(B)$.*

Propozicija 2.1.2. *$A \Leftrightarrow B$ ako i samo ako je $A \leftrightarrow B$ valjana formula.*

Ekvivalencija se, dakle, svodi na valjanost bikondicionala.

Lako je provjeriti da vrijedi:

1. Svaka formula implicira samu sebe.
2. Ako $A \Rightarrow B$ i $B \Rightarrow C$, onda $A \Rightarrow C$ (*hipotetički silogizam*).
3. Antitautologija implicira svaku formulu, a logički slijedi samo iz antitautologije.
4. Valjana formula logički slijedi iz svake formule, a implicira samo valjane formule.
5. Logička ekvivalencija je uzajamna implikacija, tj. $A \Leftrightarrow B$ akko $A \Rightarrow B$ i $B \Rightarrow A$.
6. Svaka formula je logički ekvivalentna samoj sebi.
7. Ako je $A \Leftrightarrow B$, onda je $B \Leftrightarrow A$.
8. Ako je $A \Leftrightarrow B$ i $B \Leftrightarrow C$, onda je $A \Leftrightarrow C$.
9. Valjane formule su sve međusobno logički ekvivalentne.
10. Antitautologije su sve međusobno logički ekvivalentne.

Primjedba 2.1.2. *Vidjeli smo da je logička implikacija usko vezana uz kondicional. To je dovelo do tendencije da se "implicira" koristi za čitanje znaka " $\rightarrow$ " za kondicional, što nikako nije ispravno! Naime, kada kažemo da jedna formula implicira drugu izričemo određenu tvrdnju o tim formulama, a kada između njih stavljamo znak " $\rightarrow$ " gradimo složeniju formulu. Slično vrijedi i za logičku ekvivalenciju i znak za bikondicional " $\leftrightarrow$ ".*

Pogledajmo sada u kakvoj su vezi logička implikacija i dokaz nekog matematičkog teorema s pretpostavkom P i tvrdnjom Q. U logičkoj notaciji teorem oblika "Ako je P, onda je Q" možemo pisati kao $P \Rightarrow Q$. Uz njega su vezana sljedeća tri suda:

1. $Q \Rightarrow P$ (obrat suda),
2. $-Q \Rightarrow -P$ (obrat suda po kontrapoziciji),
3. $-P \Rightarrow -Q$ (suprotni sud).

Zanima nas kakva je veza među njima?
Znamo da $P \Rightarrow Q$ ako i samo ako je $P \rightarrow Q$ valjana formula, pa možemo ispitati njihovu vezu pomoću semantičke tablice.

P	Q	$P \rightarrow Q$	$-P \rightarrow -Q$	$Q \rightarrow P$	$-Q \rightarrow -P$
0	0	1	1	1	1
0	1	1	0	0	1
1	0	0	1	1	0
1	1	1	1	1	1

Zaključujemo:

1. P logički implicira Q ako i samo ako $-Q$ logički implicira $-P$.
2. Ako P logički implicira Q, onda ne mora Q logički implicirati P.
3. Ako P logički implicira Q, onda ne mora $-P$ logički implicirati $-Q$.

Upravo zbog (1) možemo provoditi dokaz obratom po kontrapoziciji. Isto tako, ako $P \wedge -Q$ implicira neku antitautologiju (neku očiglednu laž), onda je i $P \wedge -Q$ antitautologija (antitautologija logički slijedi samo iz antitautologije), a kako je $P \wedge -Q \equiv -(P \rightarrow Q)$, to je $P \rightarrow Q$ valjana formula, što znači da $P \Rightarrow Q$, pa možemo provoditi dokaz kontradikcijom.

2.2. Logika prvog reda

2.2.1. Uvod

U prethodnom poglavlju smo proučavali klasičnu logiku sudova. No mnoga logička zaključivanja koja koristimo u svakodnevnom životu ne možemo izraziti u logici sudova. Pogledajmo jedan primjer.

Svi ljudi su smrtni.
Grci su ljudi.

Grci su smrtni.

Lako je vidjeti da ovo jednostavno zaključivanje ne možemo opisati formulama logike sudova, već moramo u obzir uzeti i sadržaj rečenica (što ne želimo!).
Označimo redom predikate:

$$C(x) \ldots \text{“}x \text{ je čovjek”},$$
$$S(x) \ldots \text{“}x \text{ je smrtan”},$$
$$G(x) \ldots \text{“}x \text{ je Grk”}.$$

U tom slučaju gornji primjer možemo zapisati u obliku:

$$\frac{\forall x\,(C(x) \to S(x)) \quad \forall x\,(G(x) \to C(x))}{\forall x\,(G(x) \to S(x))}$$

Sljedeći primjer bio je nerješiv za srednjovjekovne logičare. Pomoću Aristotelovih silogizama nisu uspjevali zapisati ovo očito valjano zaključivanje:

$$\frac{\text{Sve elipse su krivulje.}}{\text{Svatko tko crta elipsu crta krivulju.}}$$

Uvedemo li opet oznake

$$E(x) \ldots \text{“}x \text{ je elipsa”},$$
$$K(x) \ldots \text{“}x \text{ je krivulja”},$$
$$C(x,y) \ldots \text{“}y \text{ crta } x\text{”},$$

onda gornji primjer možemo pisati kao

$$\frac{\forall x\,(E(x) \to K(x))}{\forall y\,(C(x,y) \wedge E(x) \to C(x,y) \wedge K(x))}$$

U logici sudova ne možemo formalno zapisati ni neke jednostavne matematičke pojmove kao što je npr. pojam neprekidnosti funkcije u točki. Funkcija $f : \mathbb{R} \to \mathbb{R}$ je neprekidna u točki x_0 ako je

$$\forall\varepsilon\exists\delta\forall x\,(|x - x_0| < \delta \to |f(x) - f(x_0)| < \varepsilon)$$

valjana formula.

Važno je uočiti da u prethodnim primjerima istinitost zaključka ne ovisi o istinitosti dijelova koji su dobiveni samo rastavljanjem s obzirom na logičke veznike. To znači da za opis ovakvih zaključivanja moramo prije svega usvojiti širi jezik.

Proširivanjem jezika dobivamo *logiku prvog reda* ili *predikatnu logiku*. Ona ima veću izražajnu moć, no gubi neka dobra svojstva logike sudova, a tu prije svega mislimo na odlučivost. Naime, za svaku formulu logike sudova možemo u konačno mnogo koraka provjeriti je li valjana, što nije moguće za formule logike prvog reda.

2.2.2. Jezik logike prvog reda

Abeceda $\mathcal{A}$ logike prvog reda je unija skupova $A_1, ..., A_6$, gdje je:

1. $A_1 = \{v_0, v_1, v_2, \ldots\}$ prebrojiv skup čije elemente nazivamo *individualnim varijablama*,
2. $A_2 = \{-, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists\}$ skup *logičkih veznika*,
3. $A_3 = \{R_k : k \in \mathbb{N}\}$ skup *relacijskih simbola* ili *predikata*,
4. $A_4 = \{f_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo *funkcijskim simbolima*,
5. $A_5 = \{c_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo *konstantskim simbolima*,
6. $A_6 = \{(,)\}$ skup *pomoćnih simbola* (lijeva i desna zagrada).

Veznik $\forall$ nazivamo *univerzalnim kvantifikatorom* i čitamo ga "za svaki", dok veznik $\exists$ nazivamo *egzistencijalnim kvantifikatorom* i čitamo ga "postoji (neki)". Smatramo da je za svaki od relacijskih i funkcijskih simbola poznato kolika im je mjesnost. Npr., dvomjesni funkcijski simbol interpretiramo kao funkciju s dvije varijable. Pretpostavljamo da skup A_3 sadrži barem jedan dvomjesni relacijski simbol (rezerviran je za relaciju jednakosti).

Definicija 2.2.1. *Neka je $\mathcal{A}$ abeceda logike prvog reda.* ***Term*** *je riječ abecede $\mathcal{A}$ za koju vrijedi:*

a) svaka individualna varijabla i svaki konstantski simbol iz $\mathcal{A}$ je term,

b) ako je f n-mjesni funkcijski simbol iz $\mathcal{A}$ i $t_1, \ldots, t_n$ termi, onda je i $f(t_1, \ldots, t_n)$ term,

c) riječ abecede $\mathcal{A}$ je term ako i samo ako je nastala primjenom konačno mnogo puta pravila a) i b).

Na primjer, ako je $\{\ln, \sin, \exp\} \subseteq A_4$, $\{v_1, x\} \subseteq A_1$ i $c_3 \in A_5$, onda su sljedeće riječi termi: c_3, x, $\ln x$, $\exp(\sin v_1)$, $\ln(\exp(\sin c_3))$.

Definicija 2.2.2. *Neka je $\mathcal{A}$ abeceda logike prvog reda. Ako je R n-mjesni relacijski simbol iz $\mathcal{A}$ i $t_1, \ldots, t_n$ termi, onda je $R(t_1, \ldots, t_n)$* ***atomarna formula*** *abecede $\mathcal{A}$.* ***Formula*** *u abecedi $\mathcal{A}$ je*

a) svaka atomarna formula,

b) ako su A i B formule, onda su i riječi $(-A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ i $(A \leftrightarrow B)$ formule,

c) ako je A formula i x varijabla, onda su riječi $\forall xA$ i $\exists xA$ formule,

d) riječ abecede $\mathcal{A}$ je formula ako i samo ako je nastala primjenom konačno mnogo puta pravila a), b) i c).

Slično kao i prije, poštivat ćemo prioritet logičkih veznika, s tim što sada veznici $\forall$ i $\exists$ imaju najveći i međusobno jednak prioritet.

Primjedba 2.2.1. *Uobičajeno je umjesto* $\exists x\,(x \in S \wedge P\,(x))$ *pisati* $(\exists x \in S)\,P\,(x)$, *a umjesto* $\forall x\,(x \in S \to P\,(x))$ *pisati* $(\forall x \in S)\,P\,(x)$. *No, treba uvijek voditi računa o tomu da se radi samo o uvriježenim zapisima. Također, umjesto* $\exists x P\,(x) \wedge \forall y\,(P\,(y) \to y = x)$ *uobičajeno pišemo* $\exists! x P\,(x)$ *i čitamo "postoji točno jedan* x *takav da vrijedi* $P\,(x)$*".*

Pogledajmo jedan primjer: neka je R dvomjesni relacijski simbol koji interpretiramo kao "biti jednak" na skupu realnih brojeva $\mathbb{R}$. Npr. $R\,(x, y)$ bismo čitali "x je jednak y", a $R\,(x, 2)$ bismo čitali "x je jednak 2". Također, $R\,(1, 3)$ bismo čitali "1 je jednako 3ɔ i to bi (za razliku od prethodna dva primjera) bio sud, i to lažan. Izjavna rečenica "x je jednak 2ɔ nije sud jer ne možemo utvrditi je li istinita ili lažna, a isto vrijedi i za izjavnu rečenicu "x je jednak yɔ. No uvođenjem odgovarajućeg broja kvantifikatora prilikom gradnje formule kojoj je podformula $R\,(x, y)$, dobit ćemo sudove. Na primjer,

$$(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,R\,(x, y)$$

je neistinit sud, dok su sudovi

$$(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,R\,(x, y)\,,$$

$$(\exists x \in \mathbb{R})\,R\,(x, 2)$$

istiniti sudovi. To su primjeri *zatvorenih* formula, tj. formula kod kojih su sve varijable vezane kvantifikatorima. No, definicija formule dozvoljava i formule kod kojih nisu sve varijable vezane kvantifikatorima. To su tzv. *otvorene* formule. Jedna takva bi bila

$$(\forall x \in \mathbb{R})\,R\,(x, y)\,.$$

Pogledajmo još neke primjere formula:

1. $(\forall x \in \mathbb{R})\,x \geq 0$ (ovaj sud je lažan),
2. $(\exists x \in \mathbb{N})\,x$ je paran (ovaj sud je istinit),
3. $(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,y \geq x$ (ovaj sud je istinit).

Posebnu pažnju treba posvetiti negaciji kvantifikatora. Lako se vidi da vrijedi:

1. $-\forall x A \Leftrightarrow \exists x\,(-A)$,
2. $-\exists x A \Leftrightarrow \forall x\,(-A)$.

Pogledajmo u nekoliko primjera kako se provodi negacija formula koje sadrže kvantifikatore:

1. Negacija formule

$$\forall \varepsilon \exists \delta \forall x\,(|x - x_0| < \delta \to |f\,(x) - f\,(x_0)| < \varepsilon)$$

(neprekidnost funkcije f u točki x_0) je formula

$$\exists \varepsilon \forall \delta \exists x\,(|x - x_0| < \delta \wedge |f\,(x) - f\,(x_0)| \geq \varepsilon)\,,$$

i to je formalni zapis činjenice da funkcija f ima prekid u točki x_0.

2. Negacija formule
$$\forall x \forall y \left(P\left(x, y\right) \rightarrow R\left(x, y\right) \right)$$
je formula
$$\exists x \exists y \left(P\left(x, y\right) \wedge -R\left(x, y\right) \right).$$

3. Negacija formule
$$\left(\forall x \in A\right) \left(\forall y \in A\right) \left(x \neq y \rightarrow f\left(x\right) \neq f\left(y\right)\right)$$
je formula
$$\left(\exists x \in A\right) \left(\exists y \in A\right) \left(x \neq y \wedge f\left(x\right) = f\left(y\right)\right).$$

4. Negacija formule
$$\left(\forall x \in \mathbb{R}\right) \left(\forall y \in \mathbb{R}\right) \ x^2 + y^2 \geq 0$$
je formula
$$\left(\exists x \in \mathbb{R}\right) \left(\exists y \in \mathbb{R}\right) \ x^2 + y^2 < 0.$$

Ovo je poglavlje, uz manje izmjene, preuzeto iz [8].

Poglavlje 3.

Skupovi

3.1. Osnovni pojmovi

U naivnoj teoriji skupova skup je osnovni matematički pojam koga je nemoguće definirati uz pomoć jednostavnijih pojmova, no intuitivno je jasno što podrazumijevamo pod pojmom "skup". Možemo reći da je to "množina", "mnoštvo", "kolekcija" ili slično, no time nismo rekli ništa novo, već smo samo koristili sinonime.

Matematička disciplina koja se bavi skupovima zove se *teorija skupova*. Njezin osnivač Georg Cantor (1845 – 1918) o skupu je rekao sljedeće:

Skup je mnoštvo koje shvaćamo kao jedno.

Skup, dakle, možemo smatrati cjelinom sastavljenom od osnovnih dijelova. Te osnovne dijelove koji čine neki skup (objekte koji se po nekom kriteriju ujedinjuju u cjelinu) nazivamo *elementima* ili *članovima* toga skupa.

Skupove ćemo najčešće označavati velikim latiničnim slovima $A, B, X, Y, ...$ a njihove elemente malim latiničnim slovima $a, b, x, y, ...$

Intuitivno pretpostavljamo da postoji određeni odnos između skupa i njegovih elemenata tako da za svaki objekt možemo reći pripada li nekom skupu ili ne. Pojam "*biti element*" ili "*pripadati*" skupu je također osnovni matematički pojam. Činjenicu da je x element skupa A zapisujemo kao $x \in A$ i čitamo "*x je element skupa A*" ili "*x pripada skupu A*". Slično, činjenicu da y nije element skupa A zapisujemo kao $y \notin A$ i čitamo "*y nije element skupa A*" ili "*y ne pripada skupu A*". Na primjer, ako s A označimo skup svih vrsta riba u Jadranskom moru, onda vrijedi: tunj, srdela $\in A$, pirana $\notin A$.

Smatramo također da postoji skup bez ijednog elementa. Označavamo ga $\emptyset$ i zovemo *prazan skup*.

Primjedba 3.1.1. *Na ovako nedefiniranom i vrlo nejasnom pojmu skupa Cantor je izgradio veliki dio teorije skupova. U svojim istraživanjima Cantor se nije eksplicitno pozivao na neke aksiome o skupovima. Međutim, analizom njegovih radova može se zaključiti da se gotovo svi teoremi koje je on dobio mogu izvesti iz triju aksioma:*

1. Aksiom ekstenzionalnosti: dva skupa su jednaka ako imaju iste elemente.

2. Aksiom komprehenzije: za unaprijed dano svojstvo $\varphi(x)$ postoji skup čiji su elementi baš oni objekti koji imaju to svojstvo, tj. $\{x : \varphi(x)\}$ je skup.

3. Aksiom izbora: za svaki neprazan skup postoji barem jedna funkcija čiji su originali neprazni podskupovi tog skupa, a slika su elementi originala.
Kada je teorija skupova već postala priznata u matematičkom svijetu pojavili su se paradoksi; nešto što se nikad prije nije dogodilo. Paradoks nije isto što i kontradikcija: paradoks je tvrdnja čiji je dokaz logički neupitan, ali je intuitivno sama tvrdnja vrlo upitna.

Nastali problemi se u tako postavljenoj naivnoj teoriji skupova nisu mogli prevladati, a razlozi pojave paradoksa leže upravo u klimavo postavljenim temeljima same teorije. Stoga je bilo očito da se teorija skupova mora graditi kao i svaka druga matematička teorija- zadavanjem aksioma. Tako izgrađena teorija skupova nazvana je ***aksiomatska teorija skupova****.*

Primjer 3. *Russellov paradoks: $R = \{x : x \text{ je skup i } x \notin x\}$ nije skup.*
Dokažimo da R nije skup. Pretpostavimo da je R skup. Tada možemo postaviti pitanje je li $R \in R$. Pretpostavimo prvo da vrijedi $R \in R$. To znači da R ispunjava svojstvo koje ispunjavaju svi njegovi elementi, tj. $x \notin x$, odnosno za R to znači $R \notin R$. Time smo iz pretpostavke da je $R \in R$ dobili $R \notin R$, što je kontradikcija. Pretpostavimo sada da $R \notin R$. No, tada R ispunjava definicijski uvjet da bude element skupa R, pa je $R \in R$. Dakle, opet smo dobili kontradikciju. Zaključujemo da pretpostavka da je R skup vodi u kontradikciju, pa kolekcija R nije skup.

Jedna ilustracija Russellovog paradoksa glasi: U nekom selu postoji brijač koji brije one i samo one ljude koji se ne briju sami. Pitanje: Tko brije brijača? Je li ovim svojstvom određen skup ljudi koji se briju sami, odnosno skup ljudi koje brije brijač? Ako jest, kojem od njih pripada brijač?

Pored Russellovog paradoksa postoje i drugi paradoksi naivne teorije skupova: Cantorov paradoks skupa svih skupova, Buralli-Fortijev paradoks i drugi. Više o tome možete pročitati u [6] i [7].

Što je to zapravo paradoksalno u Russellovom paradoksu? Russell je dao primjer kolekcije objekata koja nije skup pokazujući da princip komprehenzije općenito ne vrijedi. Drugim riječima, ne određuje svako svojstvo neki skup, pa Cantorov princip komprehenzije ne možemo primjenjivati prilikom izgradnje skupova. U teoriji skupova ne smijemo graditi skupove pomoću skupova koji već nisu izgrađeni. Moramo ih graditi po nivoima, a aksiomatski pristup nam omogućava takvu izgradnju skupova.

Kako svaka kolekcija objekata ne čini skup, to nas dovodi do pojma klase. Ako je $\varphi(x)$ neko svojstvo, onda kolekciju $\{x : \varphi(x)\}$ nazivamo *klasom*. Neke klase su skupovi, a neke nisu. Klase koje nisu skupovi nazivamo *pravim klasama*. Primjerice, klasa iz Russellovog paradoksa je prava klasa.

3.2. Zadavanje skupova

Skup smatramo zadanim ako je nedvosmisleno rečeno, objašnjeno ili specificirano što su elementi toga skupa. Prema tomu, zadati neki skup znači dati zakon, ograničenje, propis, specifikaciju ili svojstvo kojim se točno određuju članovi toga skupa.

Skup možemo zadati na više načina:

(1) Navođenjem potpune liste elemenata toga skupa unutar para vitičastih zagrada. Na primjer, skup samoglasnika u hrvatskom jeziku je skup $S = \{a, e, i, o, u\}$. Pri tomu poredak nije važan i ponovljene elemente ne uzimamo u obzir (osim ako se radi o *multiskupovima*). Vitičaste zagrade igraju dvostruku ulogu: one su simbol ujedinjavanja dijelova u cjelinu i klasifikator objekata na one koji pripadaju skupu i na one koji mu ne pripadaju.

(2) Isticanjem nekog karakterističnog svojstva (propisa) P koje imaju samo elementi toga skupa, a koji su ujedno elementi nekog drugog skupa A. To pišemo $\{x \in A : P(x)\}$ ili $\{x \in A \mid P(x)\}$. Na primjer, skup svih pozitivnih cijelih brojeva zapisujemo $\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\}$, a centralnu, jediničnu kružnicu $S_1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

Definirajmo sada neke jednostavne pojmove vezane uz skupove.

Definicija 3.2.1. *Neka su A i B skupovi. Kažemo da je skup A **podskup** skupa B ili da je skup A **sadržan** u skupu B, i pišemo $A \subseteq B$, ako je svaki element skupa A ujedno i element skupa B. Oznaku $\subseteq$ čitamo "inkluzija". Kažemo još i da je skup B **nadskup** skupa A ili da skup B **sadrži** skup A, i pišemo $B \supseteq A$.*

Formalno,

$$\begin{aligned} A &\subseteq B \Leftrightarrow (\forall a)\,(a \in A \to a \in B)\,, \text{ tj.} \\ A &\subseteq B \Leftrightarrow (\forall a \in A)\, a \in B. \end{aligned}$$

Ako skup A nije podskup skupa B, onda pišemo $A \nsubseteq B$. Vrijedi:

$$\begin{aligned} A &\nsubseteq B \Leftrightarrow (\exists a)\,(a \in A \wedge a \notin B)\,, \text{ tj.} \\ A &\nsubseteq B \Leftrightarrow (\exists a \in A)\, a \notin B. \end{aligned}$$

Iz definicije slijedi da je prazan skup podskup svakog skupa.

Definicija 3.2.2. *Kažemo da je skup A **jednak** skupu B, i pišemo $A = B$, ako je svaki element skupa A ujedno i element skupa B, te ako je svaki element skupa B ujedno i element skupa A.*

Očito je

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)\,,$$

pa jednakost skupova A i B provjeravamo tako da provjerimo je li $A \subseteq B$ i $B \subseteq A$. Ukoliko skupovi A i B nisu jednaki pišemo $A \neq B$. Vrijedi:

$$A \neq B \Leftrightarrow (A \nsubseteq B \vee B \nsubseteq A)\,.$$

Definicija 3.2.3. *Kažemo da je skup A **pravi podskup** skupa B, i pišemo $A \subset B$ ili $A \subsetneq B$, ako je $A \subseteq B$ i ako postoji neki $b \in B$ takav da $b \notin A$.*

Očito je

$$A \subset B \Leftrightarrow (A \subseteq B \wedge B \nsubseteq A)\,,$$

odnosno

$$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)\,.$$

Propozicija 3.2.1. *Neka su A, B i C bilo koji skupovi. Vrijedi:*

1. $A \subseteq A$,
2. $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$,
3. $(A = B \wedge B = C) \Rightarrow A = C$.

Dokaz. Direktno iz definicija. ■

Definicija 3.2.4. *Neka je A proizvoljan skup. **Partitivni skup** od A, u oznaci $\mathcal{P}(A)$, je skup svih podskupova skupa A. Često ga pišemo i kao 2^A.*

Na primjer, $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$, $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

U mnogim situacijama je potrebno promatrati samo podskupove nekog skupa U, koji tada poprima značenje *univerzalnog skupa* (skupa koji je nadskup svih promatranih skupova). Naravno, univerzalnost skupa U je relativna i varira od situacije do situacije.

Skupove i njihove međusobne odnose zorno prikazujemo *Vennovim dijagramima*. No, važno je istaknuti da takvi crteži ne predstavljaju dokaz.

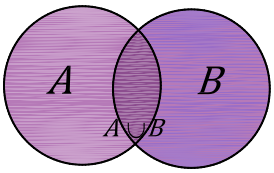
3.3. Booleove operacije na skupovima

Uvedimo sada neke operacije sa skupovima.

Definicija 3.3.1. *Neka je U dani univerzalni skup i A, B njegovi podskupovi.*

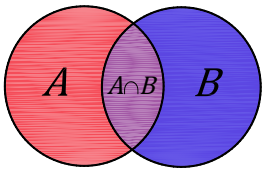
a) ***Unija*** *skupova A i B, u oznaci $A \cup B$, je skup*

$$A \cup B = \{x \in U : x \in A \vee x \in B\}.$$



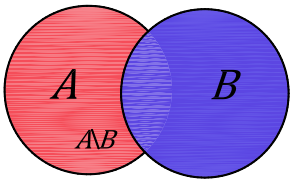
b) ***Presjek*** *skupova A i B, u oznaci $A \cap B$, je skup*

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}.$$



c) ***Razlika*** *skupova A i B, u oznaci $A \setminus B$, je skup*

$$A \setminus B = \{x \in U : x \in A \wedge x \notin B\}.$$



Operacije $\cup, \cap, \setminus$ nazivamo *Booleovim operacijama*. Uočimo da je

$$(\forall A, B \in \mathcal{P}(U))\,(A \cup B, A \cap B, A \setminus B \in \mathcal{P}(U))\,.$$

Također

$$(\forall A, B \in \mathcal{P}(U))\,(A \cap B \subseteq A \wedge B \subseteq A \cup B)\,.$$

Partitivni skup $\mathcal{P}(U)$ zajedno s operacijama $\cup, \cap, \setminus$ nazivamo *Booleovom algebrom* skupova na U.

Osim Booleovih operacija, na skupu $\mathcal{P}(U)$ možemo definirati i neke druge operacije. Jedna od njih je simetrična razlika skupova.

Definicija 3.3.2. *Neka je U dani univerzalni skup i $A, B \subseteq U$.* ***Simetrična razlika*** *skupova A i B, u oznaci $A \triangle B$, je skup*

$$A \triangle B = (A \setminus B) \cup (B \setminus A)\,.$$

Očito je $A \triangle B \subseteq U$ za svaki izbor $A, B \subseteq U$.

Zadatak 1. *Neka je U dani univerzalni skup i $A, B \subseteq U$. Dokažite da vrijedi:*

1. $A \triangle B = (A \cup B) \setminus (A \cap B)\,,$
2. $A \triangle B = B \triangle A,$
3. $(A \triangle B) \triangle C = A \triangle (B \triangle C)\,,$
4. $A \triangle \emptyset = \emptyset \triangle A = A,$
5. $A \triangle A = \emptyset.$

Definicija 3.3.3. *Neka su A i B proizvoljni neprazni skupovi. Kažemo da su skupovi A i B* ***disjunktni*** *ako je $A \cap B = \emptyset$.*

Propozicija 3.3.1. *Neka su A i B proizvoljni neprazni skupovi. Tada su $A \setminus B$ i $B \setminus A$ disjunktni skupovi, tj. $(A \setminus B) \cap (B \setminus A) = \emptyset$.*

Dokaz. Dokaz provodimo indirektno, reductio ad absurdum (svođenjem na kontradikciju). Neka su A i B proizvoljni neprazni skupovi. Pretpostavimo da vrijedi suprotno, tj. da je $(A \setminus B) \cap (B \setminus A) \neq \emptyset$. Tada postoji neki $x \in (A \setminus B) \cap (B \setminus A)$, što znači da je $x \in (A \setminus B)$ i $x \in (B \setminus A)$. Odatle je $x \in A$ i $x \notin B$, te je $x \in B$ i $x \notin A$, što je nemoguće. Budući da smo došli do kontradikcije, zaključujemo da je pretpostavka bila pogrešna. Stoga je $(A \setminus B) \cap (B \setminus A) = \emptyset$. ■

Definirajmo i jednu unarnu operaciju sa skupovima.

Definicija 3.3.4. *Neka je U dani univerzalni skup i $A \subseteq U$.* ***Komplement*** *skupa A u odnosu na skup U, u oznaci A^c, je skup*

$$A^c = U \setminus A = \{x \in U : x \notin A\}\,.$$

Na primjer, ako je $U = \{1, 2, 3, 4, 5, 6, 7\}$ i $A = \{2, 5, 6\}$, onda je $A^c = \{1, 3, 4, 7\}$. Uočimo da za svaki $A \subseteq U$ vrijedi $A^c \subseteq U$.

Primjedba 3.3.1. *Neka je U dani univerzalni skup i $A, B \subseteq U$. Vrijedi sljedeće:*

1. $U^c = \emptyset$, $\emptyset^c = U$,
2. $A \setminus B = A \cap B^c$,
3. $A = B \Leftrightarrow A^c = B^c$.

Pogledajmo koja svojstva imaju Booleove operacije sa skupovima.

Teorem 3.3.1. *Neka je U dani univerzalni skup i $A \subseteq U$. Vrijedi:*

1. $A \cup A = A$, $A \cap A = A$ *(idempotentnost),*
2. $A \cup U = U$, $A \cap U = A$,
3. $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$,
4. $A \cup A^c = U$, $A \cap A^c = \emptyset$,
5. $(A^c)^c = A$ *(involutornost).*

Dokaz. Tvrdnje $(1) - (4)$ su očite, pa ćemo dokazati samo tvrdnju (5). Dokaz ćemo provesti direktno. Neka je $A \subseteq U$. S obzirom da dokazujemo jednakost skupova, treba u stvari dokazati dvije inkluzije: $(A^c)^c \subseteq A$ i $A \subseteq (A^c)^c$.
Dokažimo najprije $A \subseteq (A^c)^c$. Ako je $A = \emptyset$, onda je očito ispunjeno $A = \emptyset \subseteq (A^c)^c$. Pretpostavimo sada da je $A \neq \emptyset$. Za bilo koji $x \in A$ vrijedi

$$x \in A \Rightarrow (x \in U \wedge x \in A) \Rightarrow (x \in U \wedge x \notin A^c) \Rightarrow x \in (A^c)^c,$$

pa je $A \subseteq (A^c)^c$.
Dokažimo da vrijedi i obratna inkluzija $(A^c)^c \subseteq A$.
Ako je $(A^c)^c = \emptyset$, onda je ispunjeno $(A^c)^c = \emptyset \subseteq A$. Pretpostavimo sada da je $(A^c)^c \neq \emptyset$. Za bilo koji $x \in (A^c)^c$ vrijedi

$$x \in (A^c)^c \Rightarrow (x \in U \wedge x \notin A^c) \Rightarrow x \in A,$$

pa je $(A^c)^c \subseteq A$, čime je dokazano da je $(A^c)^c = A$. ■

Teorem 3.3.2. *Neka je U dani univerzalni skup i $A, B \subseteq U$. Vrijedi:*

1. $A \cup B = B \cup A$, $A \cap B = B \cap A$ *(komutativnost),*
2. $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$ *(de Morganove formule).*

Dokaz. Svojstva (1) su direktne posljedice komutativnosti disjunkcije i konjukcije. Dokažimo svojstva (2). Prvo ćemo pokazati da je $(A \cup B)^c = A^c \cap B^c$, tj. da vrijede dvije odgovarajuće inkluzije. Slučajeve kada je $(A \cup B)^c$ ili $A^c \cap B^c$ prazan skup preskačemo jer tada tvrdnja trivijalno vrijedi.

Dokažimo najprije da je $(A \cup B)^c \subseteq A^c \cap B^c$. Za bilo koji $x \in (A \cup B)^c$ vrijedi

$$\begin{aligned} x \quad &\in \quad (A \cup B)^c \Rightarrow (x \in U \wedge x \notin A \cup B) \Rightarrow (x \in U \wedge x \notin A \wedge x \notin B) \\ &\Rightarrow \quad (x \in U \wedge x \notin A) \wedge (x \in U \wedge x \notin B) \Rightarrow (x \in A^c \wedge x \in B^c) \\ &\Rightarrow \quad x \in A^c \cap B^c. \end{aligned}$$

Dakle, pokazali smo da je $(A \cup B)^c \subseteq A^c \cap B^c$.
Dokažimo da vrijedi i obratna inkluzija. Za bilo koji $x \in A^c \cap B^c$ vrijedi

$$\begin{aligned} x \quad &\in \quad A^c \cap B^c \Rightarrow (x \in A^c \wedge x \in B^c) \Rightarrow (x \in U \wedge x \notin A \wedge x \notin B) \\ &\Rightarrow \quad (x \in U \wedge x \notin A \cup B) \Rightarrow x \in (A \cup B)^c. \end{aligned}$$

Dakle, $A^c \cap B^c \subseteq (A \cup B)^c$, pa smo time dokazali i jednakost tih skupova.
Drugu formulu u (2) ćemo dokazati koristeći već dokazana svojstva Booleovih operacija. Prema prvoj formuli u (2) imamo

$$(A^c)^c \cap (B^c)^c = (A^c \cup B^c)^c,$$

odakle je, po svojstvu involutornosti,

$$A \cap B = (A^c \cup B^c)^c.$$

No, prema Primjedbi 3.3.1., je

$$(A \cap B)^c = [(A^c \cup B^c)^c]^c,$$

iz čega slijedi $(A \cap B)^c = A^c \cup B^c$, što je i trebalo pokazati. ■

Analogno se mogu dokazati i sljedeća svojstva Booleovih operacija:

Teorem 3.3.3. *Neka je U dani univerzalni skup i $A, B, C \subseteq U$. Vrijedi:*

1. $(A \cup B) \cup C = A \cup (B \cup C)$ *(asocijativnost unije),*
2. $(A \cap B) \cap C = A \cap (B \cap C)$ *(asocijativnost presjeka),*
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributivnost unije prema presjeku),*
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributivnost presjeka prema uniji).*

Dokaz. Sami za vježbu. ■

Zadatak 2. *Neka je U dani univerzalni skup i $A, B, C \subseteq U$. Dokažite da vrijedi:*

1. $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$,
2. $A \cap (B \setminus C) = (A \cap B) \setminus C$,
3. $A \cap B^c$ *i* B *su disjunktni,*
4. $A \cap B$ *i* $A \cap B^c$ *su disjunktni skupovi,*
5. $A \cup B = (A \cap B^c) \cup B$ *(unija prikazana kao unija dvaju disjunktnih skupova),*

6. $A = (A \cap B) \cup (A \cap B^c)$ *(skup prikazan kao unija dvaju disjunktnih skupova).*

Primjedba 3.3.2. *Pojam unije i presjeka može se poopćiti na više skupova. Neka je $\mathcal{F}$ neka familija skupova.*

a) ***Unija skupova familije*** $\mathcal{F}$*, u oznaci* $B = \bigcup_{A \in \mathcal{F}} A$*, je skup definiran sa*

$$x \in B \Leftrightarrow (\exists A \in \mathcal{F})\, x \in A.$$

b) ***Presjek skupova familije*** $\mathcal{F}$*, u oznaci* $D = \bigcap_{A \in \mathcal{F}} A$*, je skup definiran sa*

$$x \in D \Leftrightarrow (\forall A \in \mathcal{F})\, x \in A.$$

I u ovom slučaju vrijede de Morganove formule

$$\left(\bigcup_{A \in \mathcal{F}} A\right)^c = \bigcap_{A \in \mathcal{F}} A^c,$$
$$\left(\bigcap_{A \in \mathcal{F}} A\right)^c = \bigcup_{A \in \mathcal{F}} A^c.$$

U Zadatku 2. prikazali smo skupove $A \cup B$ i A kao unije disjunktnih skupova. Općenito, svaki neprazan skup možemo prikazati kao uniju disjunktnih podskupova. Npr. skup $A = \{1, 2, 3, 4, 5\}$ možemo prikazati kao $A = \{1, 2\} \cup \{3\} \cup \{4, 5\}$. Ovakav rastav je često od velike pomoći, pa ćemo ga poopćiti u sljedećoj definiciji.

Definicija 3.3.5. *Neka je $A \neq \emptyset$ proizvoljan skup.* ***Particija*** *skupa A je svaki podskup $\mathcal{F}$ partitivnog skupa $\mathcal{P}(A)$ koji ima svojstva:*

a) $(\forall X \in \mathcal{F})\ X \neq \emptyset$,

b) $(\forall X, Y \in \mathcal{F})\ (X \cap Y = \emptyset \vee X = Y)$,

c) $\bigcup_{X \in \mathcal{F}} X = A$.

Na primjer, neka je $A = \{a, b, c, d\}$. Dvije particije skupa A su $\mathcal{F}_1 = \{\{a, b\}, \{c, d\}\}$ i $\mathcal{F}_2 = \{\{a\}, \{b, c\}, \{d\}\}$.
Vrijedi: $\mathcal{F}$ je particija skupa A ako i samo ako za svaki $x \in A$ postoji jedinstveni skup $X \in \mathcal{F}$ takav da je $x \in X$. Formalno,

$$(\forall x \in A)\, (\exists! X \in \mathcal{F})\ x \in X$$

3.4. Kartezijev umnožak skupova

U ovom ćemo se odjeljku upoznati s još jednim važnim načinom izgradnje novih skupova.

Neka su $A, B \neq \emptyset$ proizvoljni neprazni skupovi, te $a \in A$ i $b \in B$. Objekt (a, b) nazivamo *uređenim parom*, pri čemu je a prvi član (prva koordinata) uređenog para, a b drugi član (druga koordinata) uređenog para (a, b).
Stroga matematička definicija uređenog para glasi ovako:

Definicija 3.4.1. *Neka su A i B neprazni skupovi, te $a \in A$, $b \in B$. **Uređeni par** elemenata a i b, u oznaci (a, b), je skup*

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Uočimo: ako je $a = b$, onda je uređeni par $(a, b) = (a, a) = \{\{a\}\}$.
Važno je znati kada su dva uređena para jednaka. To nam govori sljedeći teorem.

Teorem 3.4.1. *Dva uređena para (a, b) i (a', b') su jednaka ako i samo ako je $a = a'$ i $b = b'$.*

Dokaz. Dokaz provodimo direktno. Trebamo dokazati istinitost dviju odgovarajućih implikacija.
Dokažimo najprije implikaciju $(a, b) = (a', b') \Rightarrow (a = a' \wedge b = b')$. Pretpostavimo da je $(a, b) = (a', b')$. Po definiciji znamo da je tada

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}. \tag{3.1}$$

Razlikujemo dva slučaja: $a = b$ i $a \neq b$.
(a) Ako je $a = b$, onda je $\{a, b\} = \{a, a\} = \{a\}$, pa iz (3.1) slijedi

$$\{\{a'\}, \{a', b'\}\} = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}.$$

Iz definicije jednakosti skupova zaključujemo da je $\{a\} = \{a'\} = \{a', b'\}$, pa je (opet po definiciji jednakosti skupova) $b' = a' = a \overset{pp}{=} b$. Dakle, $a = a'$ i $b = b'$, što je i trebalo dokazati.
(b) Ako je $a \neq b$, onda je zasigurno $\{a, b\} \neq \{a'\}$ (dvočlan skup ne može biti jednak jednočlanomu). Zbog (3.1) zaključujemo da je $\{a, b\} = \{a', b'\}$, pa je stoga i $\{a\} = \{a'\}$. Odavde je $a = a'$, a onda je i $b = b'$.
Dokažimo još implikaciju $(a = a' \wedge b = b') \Rightarrow (a, b) = (a', b')$.
Iz $a = a'$ i $b = b'$ slijedi $\{a\} = \{a'\}$ i $\{a, b\} = \{a', b'\}$. Odavde odmah slijedi

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} = (a', b'),$$

čime je dokaz završen. ■

Primjedba 3.4.1. *Uočimo da je važan poredak članova uređenog para, tj. da je $(a, b) \neq (b, a)$. Štoviše, iz $(a, b) = (b, a)$ slijedi da je $a = b$. Za razliku od toga, skupovi $\{a, b\}$ i $\{b, a\}$ su jednaki, tj. $\{a, b\} = \{b, a\}$.*

Definicija 3.4.2. *Neka su A i B neprazni skupovi.* ***Kartezijev*** *ili* ***direktni umnožak*** *skupova A i B, u oznaci $A \times B$, je skup definiran sa*

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Skupove A i B nazivamo ***faktorima*** *Kartezijeva umnoška. Ako je barem jedan od skupova A i B prazan, dogovorno uzimamo da je $A \times B = \emptyset$.*

Primjer 4. *Neka je $A = \{\alpha, \beta\}$ i $B = \{1, 2, 3\}$.*

$$\begin{aligned} A \times B &= \{(\alpha, 1), (\alpha, 2), (\alpha, 3), (\beta, 1), (\beta, 2), (\beta, 3)\}, \\ B \times A &= \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}. \end{aligned}$$

Iz gornjeg primjera je jasno da Kartezijevo množenje nije komutativna operacija. Operacija Kartezijeva množenja ima sljedeća svojstva vezana uz Booleove oparacije:

Teorem 3.4.2. *Neka su A, B, C proizvoljni skupovi. Vrijedi:*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
3. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

Dokaz. Sami za vježbu. ■

Posebno je zanimljivo Kartezijevo množenje skupa sa samim sobom.

Definicija 3.4.3. *Neka je A neprazan skup.* ***Kartezijev kvadrat*** *skupa A, u oznaci A^2, je skup definiran sa*

$$A^2 = A \times A = \{(a, b) : a, b \in A\}.$$

Primjer 5. *Dva poznata primjera Kartezijevog kvadrata su*

1. *Koordinatna ravnina: $A = B = \mathbb{R}$,*

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\},$$

2. *Jedinični kvadrat u koordinatnoj ravnini: $A = B = [0, 1]$,*

$$[0, 1]^2 = \{(x, y) : x, y \in [0, 1]\}.$$

Pojam uređenog para i Kartezijeva umnoška dvaju skupova možemo poopćiti i na više od dva faktora. Najprije induktivno definiramo uređenu n-torku na način:

$$\begin{aligned} (a_1, a_2, a_3) &= ((a_1, a_2), a_3) = \{\{(a_1, a_2)\}, \{(a_1, a_2), a_3\}\} \text{ (uređena trojka)}, \\ &\vdots \\ (a_1, \ldots, a_n) &= ((a_1, \ldots, a_{n-1}), a_n) \text{ (uređena } n\text{-torka)}, \end{aligned}$$

a potom

$$\begin{aligned} A_1 \times A_2 \times A_3 &= (A_1 \times A_2) \times A_3 = \{(a_1, a_2, a_3) : a_i \in A_i,\ i = 1, 2, 3\}, \\ &\vdots \\ A_1 \times ... \times A_{n-1} \times A_n &= (A_1 \times ... \times A_{n-1}) \times A_n = \{(a_1, ..., a_n) : a_i \in A_i,\ i = 1, ..., n\}. \end{aligned}$$

Ako je bilo koji od skupova A_i prazan, $i = 1, 2, \ldots n$, dogovorno uzimamo da je i $A_1 \times A_2 \times ... \times A_n = \emptyset$. Iz definicije Kartezijeva umnoška skupova odmah slijedi da je

$$(a_1, a_2, ..., a_n) = (a'_1, a'_2, \ldots, a'_n) \Leftrightarrow a_1 = a'_1 \wedge ... \wedge a_n = a'_n.$$

Primjedba 3.4.2. *Ne bi valjalo uređenu trojku definirati na način*

$$(a, b, c) = \{\{a\}, \{a, b\}, \{a, b, c\}\}.$$

Naime, kada bi je definirali na taj način, onda bi za trojku (b, a, b), $a \neq b$, *vrijedilo*

$$(b, a, b) = \{\{b\}, \{b, a\}, \{b, a, b\}\} = \{\{b\}, \{b, a\}\} = (b, a, a)$$

što znamo da nije istina.

Zadatak 1. *Uvjerite se da Kartezijev umnožak nije asocijativan, tj. da postoje skupovi* X, Y, Z *takvi da je* $(X \times Y) \times Z \neq X \times (Y \times Z)$.

Primjer 6. *Dva poznata primjera su:*

1. *Koordinatni prostor:* $A = B = C = \mathbb{R}$,

$$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\},$$

2. *Jedinična kocka u koordinatnom prostoru:* $A = B = C = [0, 1]$,

$$[0, 1]^3 = \{(x, y, z) : x, y, z \in [0, 1]\}.$$

Ovo poglavlje je preuzeto iz [1] i [4].

Poglavlje 4.

Relacije

4.1. Osnovni pojmovi

Pojam *relacije* je jedan od najvažnijih matematičkih pojmova matematike, a kao poseban slučaj sadrži pojam funkcije. Primjeri iz svakidašnjeg života pokazuju da je često potrebno između dvaju skupova A i B uspostaviti nekakav odnos. Neka je na primjer A skup svih dnevnih listova koji izlaze u Splitu, a B skup svih stanovnika grada Splita. Između skupova A i B postoji odnos koji povezuje dnevne listove koji izlaze u Splitu sa stanovnicima grada Splita koji ih čitaju. Tako, ako nam $s \in A$ označava *Slobodnu Dalmaciju*, onda je s u vezi upravo s onim elementima skupa B, tj. s onim stanovnicima grada Splita, koji čitaju *Slobodnu Dalmaciju*.

Pogledajmo još jedan primjer. Neka je sada $A = \{a, b, c, d\}$ društvo od četiri osobe, a $B = \{e, f, g\}$ neko drugo društvo od tri osobe. Između ta dva društva možemo uspostaviti odnos "poznavanja". Pretpostavimo da osoba a poznaje osobe e i g, osoba b poznaje osobu f, osoba c poznaje osobe e, f i g, a osoba d ne poznaje nikoga od njih. Na ovaj je način putem "poznavanja" definiran jedan odnos između skupova A i B. Prirodno je činjenicu da osoba a poznaje osobu e pisati kao uređeni par (a, e). Stoga je prirodno promatrati Kartezijev umnožak $A \times B$ jer se u njemu javljaju sve mogućnosti poznavanja.

$$\begin{aligned} A \times B &= \{(a,e), (a,f), (a,g), (b,e), (b,f), (b,g), \\ &\quad (c,e), (c,f), (c,g), (d,e), (d,f), (d,g)\}. \end{aligned}$$

Ako iz skupa $A \times B$ izdvojimo samo osobe koje se "poznaju", dobivamo skup

$$R = \{(a,e), (a,g), (b,f), (c,e), (c,f), (c,g)\}$$

koji je podskup skupa $A \times B$. To ukazuje na potrebu proučavanja proizvoljnih podskupova Kartezijeva umnoška $A \times B$.

Definicija 4.1.1. *Neka su A i B neprazni skupovi. Svaki podskup $R \subseteq A \times B$ Kartezijeva umnoška $A \times B$ nazivamo* ***binarnom relacijom*** *na skupovima A i B. Za element $a \in A$ kažemo da je* ***u relaciji*** *R s elementom $b \in B$ ako je $(a, b) \in R$. Ako je $A \neq B$ kažemo da je $R \subseteq A \times B$* ***heterogena*** *binarna relacija na skupovima A i B. Ako je $A = B$ kažemo da je $R \subseteq A \times A = A^2$* ***homogena*** *binarna relacija na skupu A.*

Za element $a \in A$ kažemo da je **u relaciji** R s elementom $b \in B$ ako je $(a,b) \in R$. Činjenicu da je $(a,b) \in R$ često pišemo u obliku aRb i čitamo "a je u relaciji R s b".

Definicija 4.1.2. *Neka je A neprazan skup. Homogenu binarnu relaciju*

$$I_A = \left\{(a,a) \in A^2 : a \in A\right\} \subseteq A^2$$

*nazivamo **dijagonalom** ili **identičnom relacijom** na skupu A. Označavamo je još Δ_A ili id_A.*

Očito je $I_A \neq A^2$ čim skup A ima više od jednog elementa.

Definiciju relacije može proširiti na podskupove Kartezijeva umnoška $A_1 \times ... \times A_n$, $n \in \mathbb{N}$, i tada govorimo o *n-arnim relacijama*. No, ovdje ćemo se baviti samo binarnim relacijama i njih ćemo u nastavku kraće zvati *relacijama*.

Uvedimo sada nekoliko pojmova vezanih uz relacije.

Definicija 4.1.3. *Neka su A i B neprazni skupovi i $R \subseteq A \times B$ neka relacija na skupovima A i B.*
***Domena relacije** R je skup*

$$D(R) = \{a \in A : (\exists b \in B)\,(a,b) \in R\} \subseteq A.$$

***Slika relacije** R je skup*

$$K(R) = \{b \in B : (\exists a \in A)\,(a,b) \in R\} \subseteq B.$$

Definicija 4.1.4. *Neka je $R \subseteq A \times B$ neprazna relacija. **Suprotna** ili **inverzna** relacija relaciji R je relacija $R^{-1} \subseteq B \times A$ definirana sa*

$$R^{-1} = \{(b,a) \in B \times A : (a,b) \in R\}.$$

Definicija 4.1.5. *Neka je $R \subseteq A \times B$ neka relacija na skupovima A i B. **Komplement** relaciji R je relacija $R^c \subseteq A \times B$ definirana sa*

$$R^c = \{(a,b) \in A \times B : (a,b) \notin R\}.$$

Definicija 4.1.6. *Neka su A, B, C neprazni skupovi, te $R \subseteq A \times B$ i $S \subseteq B \times C$. **Kompozicija** relacija R i S je relacija $S \circ R \subseteq A \times C$ definirana sa*

$$S \circ R = \{(a,c) \in A \times C : (\exists b \in B)\,(a,b) \in R \wedge (b,c) \in S\}.$$

Primjer 7. *Neka je $A = \{1,2,3\}$, $B = \{a,b\}$ i $C = \{x,y\}$. Definirajmo relacije $R \subseteq A \times B$ i $S \subseteq B \times C$ sa*

$$\begin{aligned} R &= \{(1,a),(2,b),(3,a),(3,b)\}, \\ S &= \{(a,y),(b,x)\}. \end{aligned}$$

Lako se vidi da je npr.

$$\begin{aligned} R^{-1} &= \{(a,1),(b,2),(a,3),(b,3)\}, \\ S^c &= \{(a,x),(b,y)\}, \\ S \circ R &= \{(1,y),(2,x),(3,x),(3,y)\}. \end{aligned}$$

Primjer 8. *Neka je* $A = \{1, 2, 3\}$. *Definirajmo homogene relacije* R *i* S *na skupu* A *sa*

$$\begin{aligned} R &= \{(1,1), (2,2), (3,1), (3,2)\}, \\ S &= \{(1,2), (2,3)\}. \end{aligned}$$

Vrijedi

$$\begin{aligned} S \circ R &= \{(1,2), (2,3), (3,2), (3,3)\}, \\ R \circ S &= \{(1,2), (2,1), (2,2)\}. \end{aligned}$$

Iz primjera je vidljivo da kompozicija relacija općenito nije komutativna. No, vrijedi sljedeće.

Teorem 4.1.1. *Neka su* A, B, C, D *neprazni skupovi, te* $R \subseteq A \times B$, $S \subseteq B \times C$ *i* $Z \subseteq C \times D$. *Vrijedi*

$$Z \circ (S \circ R) = (Z \circ S) \circ R.$$

Dokaz. Dokažimo da je $Z \circ (S \circ R) \subseteq (Z \circ S) \circ R$.
Za $Z \circ (S \circ R) = \emptyset$ tvrdnja trivijalno vrijedi, pa stoga pretpostavimo da je relacija $Z \circ (S \circ R) \subseteq A \times D$ neprazna.
Uzmimo proizvoljan par $(a, d) \in Z \circ (S \circ R)$, gdje je $a \in A$ i $d \in D$. Po definiciji kompozicije relacija znamo da postoji neki $c \in C$ takav da je $(a, c) \in S \circ R$ i $(c, d) \in Z$. Nadalje, jer je $(a, c) \in S \circ R$, to postoji neki $b \in B$ takav da je $(a, b) \in R$ i $(b, c) \in S$. Dakle, vrijedi

$$(\exists c \in C)\,((b, c) \in S \wedge (c, d) \in Z),$$

a po definiciji kompozicije to znači da je $(b, d) \in Z \circ S$. Sada imamo

$$(\exists b \in B)\,((a, b) \in R \wedge (b, d) \in Z \circ S),$$

pa je $(a, d) \in (Z \circ S) \circ R$, što je i trebalo dokazati.
Suprotna inkluzija se dokaže analogno. ■
Prethodni teorem nam u stvari kaže da je kompozicija relacija asocijativna. Stoga za homogenu relaciju R na skupu A ima smisla definirati potencije od R na sljedeći način:

$$\begin{aligned} R^0 &= I_A, \\ R^1 &= R, \\ R^2 &= R \circ R, \\ &\vdots \\ R^{n+1} &= R^n \circ R,\ n > 1. \end{aligned}$$

Propozicija 4.1.1. *Neka su* A *i* B *neprazni skupovi, te* $R \subseteq A \times B$. *Vrijedi:*

$$R \circ I_A = R, \quad I_B \circ R = R.$$

Dokaz. Dokazat ćemo samo identitet $R \circ I_A = R$. Drugi se dokazuje analogno.
Za $R \circ I_A = \emptyset$ tvrdnja trivijalno vrijedi, pa stoga pretpostavimo da je $R \circ I_A \subseteq A \times B$ neprazna relacija. Uzmimo proizvoljan $(a, b) \in R \circ I_A$. Po definiciji kompozicije to znači da postoji neki $a' \in A$ takav da je $(a, a') \in I_A$ i $(a', b) \in R$. No iz $(a, a') \in I_A$ slijedi da je $a = a'$, pa je $(a, b) = (a', b) \in R$. Dakle, $R \circ I_A \subseteq R$.
Obratno, uzmimo prizvoljan $(a, b) \in R$. Kako za svaki $a \in A$ vrijedi $(a, a) \in I_A$, to po definiciji kompozicije slijedi da je $(a, b) \in R \circ I_A$, pa je $R \subseteq R \circ I_A$. ■

Primjedba 4.1.1. *Neka je A neprazan skup. Partitivni skup $\mathcal{P}(A \times A)$ je skup svih homogenih relacija na skupu A. Kompozicija relacija je asocijativna, pa je $(\mathcal{P}(A \times A), \circ)$ polugrupa. Iz prethodne propozicije slijedi da za svaku homogenu relaciju R na skupu A vrijedi*

$$R \circ I_A = I_A \circ R = R. \tag{4.1}$$

Štoviše, I_A je jedina relacija na skupu A sa svojstvom da je za svaku relaciju $R \subseteq A \times A$ ispunjeno (4.1). Naime, ako bi za neku relaciju $Q \subseteq A \times A$ vrijedilo to isto, onda bismo posebno za $R = I_A$ imali

$$I_A \circ Q = Q \circ I_A = I_A. \tag{4.2}$$

No, iz (4.1) za $R = Q$ slijedi da je

$$Q \circ I_A = I_A \circ Q = Q,$$

što zajedno s (4.2) daje

$$I_A = Q.$$

Dakle, I_A je jedinični ili neutralni element u $\mathcal{P}(A \times A)$ obzirom na relaciju $\circ$, pa $(\mathcal{P}(A \times A), \circ)$ ima strukturu nekomutativnog monoida.

Lema 4.1.1. *Neka su A i B neprazni skupovi, te $R, S \subseteq A \times B$. Vrijedi:*

1. $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$,
2. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$,
3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,
4. $(R^{-1})^{-1} = R$.

Dokaz. Sami za vježbu. ■

4.2. Homogene relacije

Homogene relacije mogu imati neka posebna svojstva koja navodimo u sljedećoj definiciji.

Definicija 4.2.1. *Neka je R homogena relacija na skupu A. Kažemo da je R*

a) refleksivna ako vrijedi $(\forall x \in A)\,(x, x) \in R$,

b) irefleksivna ako vrijedi $(\forall x \in A)\,(x,x) \notin R$,

c) simetrična ako vrijedi $(\forall x \in A)\,(\forall y \in A)\,((x,y) \in R \to (y,x) \in R)$,

d) antisimetrična ako vrijedi $(\forall x \in A)\,(\forall y \in A)\,((x,y) \in R \wedge (y,x) \in R \to x = y)$,

e) tranzitivna ako vrijedi

$$(\forall x \in A)\,(\forall y \in A)\,(\forall z \in A)\,((x,y) \in R \wedge (y,z) \in R \to (x,z) \in R).$$

Ova svojstva homogenih relacija mogu se i skupovno opisati. Naime, vrijede sljedeće karakterizacije.

Propozicija 4.2.1. *Neka je R homogena relacija na skupu A. Vrijedi:*

1. *R je refleksivna ako i samo ako je $I_A \subseteq R$;*
2. *R je irefleksivna ako i samo ako je $R \cap I_A = \emptyset$;*
3. *R je simetrična ako i samo ako je $R = R^{-1}$;*
4. *R je antisimetrična ako i samo ako je $R \cap R^{-1} \subseteq I_A$;*
5. *R je tranzitivna ako i samo ako je $R \circ R \subseteq R$.*

Dokaz. Tvrdnje (1), (2) i (4) očigledno vrijede, pa ćemo dokazati samo preostale tvrdnje.
Dokažimo najprije tvrdnju 3. Pretpostavimo da je relacija R simetrična. Ako je $R = \emptyset$, onda je i $R^{-1} = \emptyset$, pa je tvrdnja trivijalno ispunjena. Pretpostavimo stoga da je R neprazna, te uzmimo proizvoljan $(x,y) \in R$. Iz simetričnosti relacije R slijedi da je $(y,x) \in R$, a iz ovoga po definiciji inverzne relacije slijedi da je $(x,y) \in R^{-1}$. Stoga je $R \subseteq R^{-1}$. Analogno se pokaže da je $R^{-1} \subseteq R$, pa je $R = R^{-1}$.
Obratno, neka je $R = R^{-1}$. Ako je $R = \emptyset$ tvrdnja trivijalno vrijedi (prazna relacija je simetrična). Pretpostavimo stoga da je $R \neq \emptyset$ i uzmimo proizvoljan par $(x,y) \in R$. Kako je $R = R^{-1}$, to je $(x,y) \in R^{-1}$, a po definiciji inverzne relacije odmah možemo zaključiti da je $(y,x) \in R$. Time smo pokazali da je R simetrična.

Dokažimo još i tvrdnju 5. Pretpostavimo da je R tranzitivna. Ako je $R \circ R = \emptyset$ tvrdnja trivijalno vrijedi, pa pretpostavimo stoga da je $R \circ R$ neprazna, te uzmimo proizvoljan par $(x,z) \in R \circ R$. Po definiciji kompozicije relacija znamo da postoji neki $y \in A$ takav da je $(x,y) \in R$ i $(y,z) \in R$. Sada iz tranzitivnosti relacije R slijedi da je i $(x,z) \in R$, pa zaključujemo da je $R \circ R \subseteq R$. Obratno, neka je $R \circ R \subseteq R$. Ako je $R = \emptyset$, onda je i $R \circ R = \emptyset$, pa tvrdnja trivijalno vrijedi (prazna relacija je tranzitivna). Pretpostavimo stoga da je R neprazna, te da je $(x,y) \in R$ i $(y,z) \in R$. Tada je $(x,z) \in R \circ R \subseteq R$, pa je $(x,z) \in R$. Dakle, R je tranzitivna, što je i trebalo pokazati. ■

Geometrijski gledano, refleksivna relacija $R \subseteq A^2$ sadrži dijagonalu I_A, irefleksivna relacija ne siječe dijagonalu I_A, a simetrična relacija je jednaka svojoj osnosimetričnoj slici s obzirom na dijagonalu I_A kao os simetrije.

Zadatak 1. *Neka je* $A = \{1, 2, 3, 4, 5\}$. *Ispitajte koja svojstva imaju sljedeće relacije:*
(a) $R_1 = \{(1, 1), (2, 1), (1, 2), (3, 5)\}$,
(b) $R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (3, 4), (4, 5)\}$,
(c) $R_3 = \{(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$,
(d) $R_4 = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (3, 4), (4, 5), (3, 5)\}$.

Zadatak 2. *Jedan od* 6 *studenata* A, B, C, D, E, F *ukrao je knjigu iz knjižnice. Svaki od njih je pitan koga je od preostalih studenata vidio u knjižnici i svi su rekli istinu osim lopova (pretpostavljamo da ako su se dvojica našla u knjižnici u isto vrijeme da su vidjeli jedan drugoga).* A *je rekao da je vidio* B *i* E, B *je rekao da je vidio* A *i* F, C *da je vidio* D *i* F, D *da je vidio* A *i* F, E *da je vidio* A *i* D, *te* F *da je vidio* C *i* B. *Tko je lopov?*

4.2.1. Relacije ekvivalencije

Definicija 4.2.2. *Homogenu binarnu relaciju koja je refleksivna, simetrična i tranzitivna nazivamo* ***relacijom ekvivalencije****.*

Ovakve relacije igraju vrlo važnu ulogu u matematici i imaju mnoga lijepa svojstva. Relaciju ekvivalencije često označavamo simbolima $\sim$ ili $\cong$. Ako je $\sim$ relacija ekvivalencije na skupu A, te $x, y \in A$ takvi da je $x \sim y$, onda kažemo da je x *ekvivalentan* s y.
Važan primjer relacije ekvivalencije je relacija $=$ "biti jednak".

Primjer 9. *Neka je* $\mathcal{T}$ *skup svih trokuta u nekoj ravnini. Relacije* $\sim$ *"biti sličan",* $\cong$ *"biti sukladan" i* ρ *"imati istu površinu" su relacije ekvivalencije na* $\mathcal{T}$ *.*

Definicija 4.2.3. *Neka je* A *neprazan skup i* $\sim$ *relacija ekvivalencije na skupu* A. *Za svaki* $a \in A$, *skup*

$$[a] = \{x \in A : x \sim a\} \subseteq A$$

svih elemenata iz A *koji su u relaciji* $\sim$ *s elementom* a *(tj. koji su s njim ekvivalentni), nazivamo* ***klasom ekvivalencije*** *relacije* $\sim$ *određenom elementom* a. *Element* a *nazivamo* ***reprezentantom*** *te klase.*

Iz refleksivnosti relacije $\sim$ slijedi da je $a \sim a$ za svaki $a \in A$, pa je $a \in [a]$, tj. klase su neprazni skupovi.

Zadatak 3. *Neka je* $\mathcal{P}$ *skup svih pravaca neke ravnine. Na skupu* $\mathcal{P}$ *definiramo relaciju* $\parallel$ *"biti paralelan". Podsjetimo se: dva pravca u ravnini su paralelna ako nemaju nijednu zajedničku točku ili ako se podudaraju. Provjerite da je* $\parallel$ *relacija ekvivalencije na skupu* $\mathcal{P}$. *Klase ekvivalencije nazivamo* ***smjerovima u ravnini.***

Pokažite da relacija $\perp$ *"biti okomit" nije relacija ekvivalencije na skupu* $\mathcal{P}$.

Pogledajmo neka važna svojstva klasa ekvivalencije.

Teorem 4.2.1. *(Teorem o klasama) Neka je* A *proizvoljan neprazan skup,* $\sim$ *relacija ekvivalencije na* A, *te* $x, y \in A$.

1. *Ako* $x \nsim y$, *onda je* $[x] \cap [y] = \emptyset$.

2. Ako je $x \sim y$, onda je $[x] = [y]$.

Dokaz. Dokažimo najprije prvu tvrdnju. Dokaz ćemo provesti kontradikcijom. Neka su $x, y \in A$ takvi da $x \nsim y$ i pretpostavimo da je $[x] \cap [y] \neq \emptyset$. To znači da postoji neki $a \in [x] \cap [y]$, pa je $a \in [x]$ i $a \in [y]$. Jer je $a \in [x]$ slijedi da je $a \sim x$, a jer je $a \in [y]$ slijedi da je $a \sim y$. Kako je $\sim$ relacija ekvivalencije na A, to je ona simetrična i tranzitivna, pa iz $a \sim x$ slijedi da je $x \sim a$, a iz $x \sim a$ i $a \sim y$ slijedi da je $x \sim y$, što je u suprotnosti s pretpostavkom da je $x \nsim y$. Dakle, mora vrijediti da je $[x] \cap [y] = \emptyset$.
Dokažimo još i drugu tvrdnju. Primijenit ćemo direktni dokaz.
Pretpostavimo da je $x \sim y$. Treba dokazati da je $[x] \subseteq [y]$ i $[y] \subseteq [x]$. Dokažimo najprije da je $[x] \subseteq [y]$. Znamo da je $[x] \neq \emptyset$ pa uzmimo bilo koji element $a \in [x]$. To znači da je $a \sim x$. Zbog tranzitivnosti relacije $\sim$, iz $a \sim x$ i $x \sim y$ slijedi da je $a \sim y$, pa je $a \in [y]$. Dakle, $[x] \subseteq [y]$. Kako je relacija $\sim$ simetrična, to iz $x \sim y$ slijedi da je $y \sim x$, pa je i $[y] \subseteq [x]$. Stoga je $[x] = [y]$. ■

Prema prethodnom teoremu zaključujemo da za proizvoljne $x, y \in A$ vrijedi: $[x] \cap [y] = \emptyset$ ili $[x] = [y]$. Odavde odmah slijedi da za svaki $x \in A$ postoji jedinstvena klasa $[a] \subseteq A$ kojoj on pripada, tj.

$$(\forall x \in A)\,(\exists!\,[a] \subseteq A)\,(x \in [a])\,.$$

Stavimo li u jedan skup sve te različite klase koje definira relacija ekvivalencije $\sim \subseteq A^2$, dobit ćemo skup čiji su elementi neprazni, po parovima disjunktni, a čija je unija jednaka čitavom skupu A, tj. dobit ćemo jednu particiju skupa A. Drugim riječima, vrijedi:

Korolar 4.2.1. *Svaka relacija ekvivalencije na skupu A definira jednu particiju skupa A. Elementi particije su klase ekvivalencije, te se u svakom pojedinom elementu particije nalaze oni i samo oni elementi skupa A koji su međusobno ekvivalentni.*

Definicija 4.2.4. *Neka je A proizvoljan neprazan skup, $\sim$ relacija ekvivalencije na skupu A. Particiju skupa A sačinjenu od klasa ekvivalencije relacije $\sim$ nazivamo* ***kvocijentnim skupom*** *skupa A po relaciji ekvivalencije $\sim$ i označavamo*

$$A \mid_{\sim} = \{[a] : a \in A\}\,.$$

Zanimljivo je da vrijedi i obrat gornjeg korolara, tj. svaka particija skupa A definira jednu relaciju ekvivalencije na skupu A čiji je kvocijentni skup jednak toj particiji. To potvrđuje sljedeći teorem.

Teorem 4.2.2. *Neka je $\mathcal{F}$ jedna particija skupa A. Tada je relacija $R_{\mathcal{F}} \subseteq A \times A$ definirana sa*

$$(x, y) \in R_{\mathcal{F}} \text{ ako i samo ako } (\exists S \in \mathcal{F})\,(x \in S \wedge y \in S)$$

relacija ekvivalencije na skupu A i $A \mid R_{\mathcal{F}} = \mathcal{F}$.

Dokaz. Neka je $x \in A$. Skup $\mathcal{F}$ je particija skupa A, pa postoji $S \in \mathcal{F}$ takav da je $x \in S$. Sada, po definicije relacije $R_{\mathcal{F}}$, slijedi da je $(x, x) \in R_{\mathcal{F}}$, pa je relacija $R_{\mathcal{F}}$ refleksivna. Neka su $x, y \in A$ i neka je $(x, y) \in R_{\mathcal{F}}$. Po definiciji relacije $R_{\mathcal{F}}$, postoji $S \in \mathcal{F}$ takav da $x, y \in S$. No, tada je i $(y, x) \in R_{\mathcal{F}}$, pa je relacija $R_{\mathcal{F}}$ simetrična. Dokažimo još i da je $R_{\mathcal{F}}$ tranzitivna. Neka su $x, y, z \in A$ i neka je $(x, y) \in R_{\mathcal{F}}$ i $(y, z) \in R_{\mathcal{F}}$. Tada postoje elementi S_1 i S_2 particije $\mathcal{F}$ takvi da su $x, y \in S_1$ i $y, z \in S_2$. No to znači da je $y \in S_1 \cap S_2$, pa je $S_1 = S_2$ zbog disjunktnosti elemenata iz $\mathcal{F}$, iz čega slijedi da su x i z u istom elementu particije $\mathcal{F}$, tj. da je $(x, z) \in R_{\mathcal{F}}$. Dakle, $R_{\mathcal{F}}$ je i tranzitivna, pa je $R_{\mathcal{F}}$ relacija ekvivalencije na skupu A. U svakom skupu $S \in \mathcal{F}$ se nalaze oni i samo oni elementi iz A koji su međusobno ekvivalentni, pa je S jedna klasa ekvivalencije. Stoga je $\mathcal{F} = A \mid R_{\mathcal{F}}$. ■

Primjer 10. *Neka je E^3 skup svih točaka u prostoru. **Orijentirana dužina** u E^3 je svaki uređeni par točaka $(A, B) \in E^3 \times E^3$. Orijentiranu dužinu (A, B) označavamo $\overrightarrow{AB}$, tj. $(A, B) = \overrightarrow{AB}$. Neka je $\mathcal{O}$ skup svih orijentiranih dužina u E^3. Dakle,*

$$\mathcal{O} = \left\{ \overrightarrow{AB} : A, B \in E^3 \right\} = E^3 \times E^3.$$

Na skupu $\mathcal{O}$ definiramo relaciju $\equiv$ "biti ekvivalentan" na sljedeći način:

$$\overrightarrow{AB} \equiv \overrightarrow{CD} \text{ ako i samo ako dužine } \overline{AD} \text{ i } \overline{BC} \text{ imaju zajedničko polovište.}$$

*Relacija $\equiv$ je relacija ekvivalencije na $\mathcal{O}$. Kvocijentni skup $V^3 = \mathcal{O} \mid \equiv$ nazivamo **prostorom vektora**, a njegove elemente (klase ekvivalencije) nazivamo **vektorima.***

4.2.2. Relacije uređaja

Osim relacije ekvivalencije s kojom smo se upoznali u prethodnoj točki, važne su nam još neke homogene relacije.

Definicija 4.2.5. *Homogenu binarnu relaciju koja je refleksivna, antisimetrična i tranzitivna nazivamo relacijom **djelomičnog** ili **parcijalnog uređaja**.*

Definicija 4.2.6. *Uređeni par (A, ρ), gdje je A neprazan skup, a ρ relacija djelomičnog uređaja na skupu A, nazivamo **djelomično** ili **parcijalno uređenim skupom**.*

Ako je ρ relacije djelomičnog uređaja, onda obično umjesto $(x, y) \in \rho$ pišemo $x \rho y$.

Primjer 11. *Definirajmo relaciju ρ na skupu $\mathbb{N}$ na sljedeći način:*

$$(x, y) \in \rho \text{ ako i samo ako } x \text{ dijeli } y.$$

Relacija ρ je refleksivna, antisimetrična i tranzitivna, pa je $(\mathbb{N}, \rho)$ djelomično uređen skup. Ipak, nisu svi elementi iz $\mathbb{N}$ "usporedivi" po ovoj relaciji, tj. postoje barem dva prirodna broja takva da prvi broj nije u relaciji s drugim niti je drugi u relaciji s prvim. Npr. $2, 5 \in \mathbb{N}$, a $(2, 5) \notin \rho$ i također $(5, 2) \notin \rho$.

Gornji primjer nas motivira za sljedeću definiciju.

Definicija 4.2.7. *Neka je ρ relacija djelomičnog uređaja na skupu A. Kažemo da je ρ relacija* ***linearnog*** *ili* ***potpunog uređaja*** *na A ako vrijedi*

$$(\forall x \in A)\,(\forall y \in A)\,((x,y) \in \rho \vee (y,x) \in \rho)\,.$$

Definicija 4.2.8. *Uređeni par (A, ρ), gdje je A neprazan skup, a ρ relacija potpunog uređaja na skupu A, nazivamo* ***potpuno uređenim skupom*** *ili jednostavno* ***uređenim skupom****.*

- Poznati uređeni skupovi su: $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$, gdje je $\leq$ uobičajena relacija "manje ili jednako" na skupovima brojeva. Analogno vrijedi i za relaciju $\geq$ ("veće ili jednako").
- Za svaki $S \neq \emptyset$, skup $(\mathcal{P}(S), \subseteq)$ je djelomično uređen skup, ali ne i uređen. Relaciju $\subseteq$ ("biti podskup") nazivamo *relacijom sadržavanja.*

Prisjetimo se da smo kod uspoređivanja brojeva često koristili relaciju $<$ ("strogo manje"). Općenito se takve relacije definiraju na sljedeći način.

Definicija 4.2.9. *Homogenu binarnu relaciju koja je irefleksivna i tranzitivna nazivamo* ***relacijom strogog djelomičnog (ili strogog parcijalnog) uređaja.***

Definicija 4.2.10. *Neka je $\prec$ relacija strogog djelomičnog uređaja na skupu A. Kažemo da je $\prec$ relacija* ***strogog linearnog*** *(ili* ***strogog potpunog****)* ***uređaja*** *na skupu A ako vrijedi*

$$(\forall x \in A)\,(\forall y \in A)\,(x \neq y \rightarrow (x \prec y \vee y \prec x))\,.$$

Definicija 4.2.11. *Uređeni par $(A, \prec)$, gdje je A neprazan skup, a $\prec$ relacija strogog potpunog uređaja na skupu A nazivamo* ***strogo uređenim skupom****.*

Uočimo: ako je na nekom skupu definirana relacija djelomičnog uređaja $\preceq$, onda na tom skupu možemo definirati i relaciju strogog djelomičnog uređaja $\prec$ na način:

$$a \prec b \Leftrightarrow a \preceq b \wedge a \neq b.$$

I obratno, ako na nekom skupu imamo definiranu relaciju strogog djelomičnog uređaja $\prec$, možemo na tom skupu definirati i relacija djelomičnog uređaja $\preceq$ na način:

$$a \preceq b \Leftrightarrow a \prec b \vee a = b.$$

Stoga, kad god je $(A, \preceq)$ djelomično uređen skup podrazumijevat ćemo da je A i strogo djelomično uređen skup, i obratno.
Ponekad ćemo $a \preceq b$ zapisivati i kao $b \succeq a$, te $a \prec b$ kao $b \succ a$, tj.

$$\begin{aligned} a &\preceq b \Leftrightarrow b \succeq a, \\ a &\prec b \Leftrightarrow b \succ a. \end{aligned}$$

Primijetimo: ako je $(A, \preceq)$ djelomično uređen skup i $X \subseteq A$, onda je i $(X, \preceq)$ djelomično uređen skup, gdje je $\preceq$ uređaj naslijeđen iz A.
Relaciju djelomičnog uređaja ćemo često označavati $\preceq$ i tu oznaku ne treba miješati s oznakom $\leq$ koju koristimo za relaciju uređaja. Uobičajeno je s $\leq$ označena relacija uređaja "manje ili jednako" na skupovima brojeva, no ponekad će nam označavati i neku drugu relaciju potpunog uređaja.

Definicija 4.2.12. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$, $X \neq \emptyset$.*

Kažemo da je $m \in X$ ***najmanji element*** *u skupu X ako vrijedi*

$$(\forall x \in X)\, m \preceq x.$$

Kažemo da je $m \in X$ ***minimalni element*** *u skupu X ako vrijedi*

$$(\forall x \in X)\, (x \preceq m \to x = m)\,.$$

Kažemo da je $n \in X$ ***najveći element*** *u skupu X ako vrijedi*

$$(\forall x \in X)\, x \preceq n.$$

Kažemo da je $n \in X$ ***maksimalni element*** *u skupu X ako vrijedi*

$$(\forall x \in X)\, (n \preceq x \to x = n)\,.$$

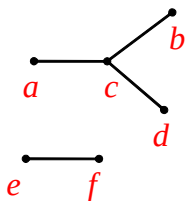
Primijetimo najprije da skup može imati najviše jedan najveći, odnosno najviše jedan najmanji element. Ako postoji najmanji (najveći) element nekog djelomično uređenog skupa, onda je taj element ujedno i minimalan (maksimalan). Obrat općenito ne vrijedi: djelomično uređen skup može imati više minimalnih ili maksimalnih elemenata, a da nema ni najmanji ni najveći element.

Primjedba 4.2.1. *Uvriježilo se najmanji element uređenog skupa označavati s* min*, a najveći s* max*. To je stoga što su u uređenom skupu pojmovi najmanji i minimalan, odnosno najveći i maksimalan ekvivalentni. Tako ćemo na primjer, za uređeni skup $(\mathbb{N}, \leq)$ reći da ima najmanji element, to je broj 1, i pisati $\min \mathbb{N} = 1$.*

Primjer 12. *Neka je $A = \{a, b, c, d, e, f\}$ i relacija $\preceq$ na skupu A dana kao*

$$\preceq = (a, a)\,, (b, b)\,, (c, c)\,, (d, d)\,, (e, e)\,, (f, f)\,, (a, c)\,, (c, b)\,, (c, d)\,, (a, b)\,, (a, d)\,, (e, f)\,.$$

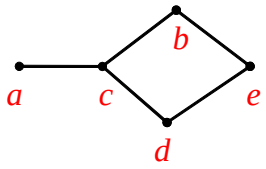
Primijetimo da je $(A, \preceq)$ djelomično uređen skup. Elementi a i e su minimalni, a elementi b, d i f su maksimalni u skupu A po relaciji $\preceq$. No, u A, po relaciji $\preceq$, nema ni najmanjeg ni najvećeg elementa.



Primjer 13. *Neka je $A = \{a, b, c, d, e\}$, te neka je relacija $\preceq$ na skupu A dana kao*

$$\begin{aligned} \preceq \; &= \{(a, a)\,, (b, b)\,, (c, c)\,, (d, d)\,, (e, e)\,, (a, c)\,, \\ &\quad (c, b)\,, (c, d)\,, (a, b)\,, (a, d)\,, (b, e)\,, (d, e)\,, (a, e)\,, (c, e)\}\,. \end{aligned}$$

Uređeni par $(A, \preceq)$ je djelomično uređen skup. Element a je minimalan i najmanji, a element e maksimalan i najveći u skupu A po relaciji $\preceq$.



Definicija 4.2.13. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$, $X \neq \emptyset$. Reći ćemo da je $d \in A$ **donja međa** ili **minoranta** skupa X u A ako vrijedi*

$$(\forall x \in X)\ \ d \preceq x.$$

*Kažemo da je X **omeđen odozdo** ako postoji barem jedna donja međa skupa X.*
*Ako je X omeđen odozdo, za donju među d kažemo da je **najveća donja međa** ili **infimum** skupa X, i označavamo $d = \inf X$, ako je $d' \preceq d$ za svaku donju među d' skupa X.*

Propozicija 4.2.2. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$ neprazan, odozdo omeđen podskup od A. Ako infimum skupa X postoji, jedinstven je.*

Dokaz. Kada bi postojala dva infimuma skupa X, recimo d_0 i d_1, moralo bi vrijediti $d_0 \preceq d_1$ i $d_1 \preceq d_0$, a kako je relacija $\preceq$ antisimetrična, to znači da je $d_0 = d_1$. ■

Primijetimo: ako donja međa $d \in A$ skupa X pripada skupu X, tj. ako je $d \in X$, onda je d najmanji element skupa X i $d = \inf X = \min X$.

Definicija 4.2.14. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$, $X \neq \emptyset$. Reći ćemo da je $g \in A$ **gornja međa** ili **majoranta** skupa X u A ako vrijedi*

$$(\forall x \in X)\ \ x \preceq g.$$

*Kažemo da je skup X **omeđen odozgo** ako postoji barem jedna gornja međa skupa X. Za skup X kažemo da je **omeđen** ako je omeđen odozgo i odozdo.*
*Ako je skup X omeđen odozgo, za gornju među g kažemo da je **najmanja gornja međa** ili **supremum** skupa X, i označavamo $g = \sup X$, ako je $g \preceq g'$ za svaku gornju među g' skupa X.*

Primijetimo: ako gornja međa $g \in A$ skupa X pripada skupu X, tj. ako je $g \in X$, onda je g najveći element skupa X i $g = \sup X = \max X$.

Primjedba 4.2.2. *Skup može imati donju među, a da nema infimum, odnosno može imati gornju među, a da nema supremum. Na primjer, neka je $A = \langle 0, 1\rangle \cup \langle 2, 3\rangle \cup \langle 5, 7\rangle$ i $\leq$ standardna uređajna relacija "manje ili jednako" na skupu A nasljeđena iz $\mathbb{R}$. Neka je $X = \langle 2, 3\rangle \subseteq A$, pa je i $(X, \leq)$ uređen skup. Skup X je omeđen jer ima i donje i gornje međe u A (svi elementi skupa $\langle 0, 1\rangle$ su donje međe skupa X, a svi elementi skupa $\langle 5, 7\rangle$ su gornje međe skupa X). No, X nema ni infimum ni supremum u A. Naime, infimum bi bio broj 2, a supremum broj 3, no $2 \notin A$ i $3 \notin A$.*

Primjer 14. *U uređenom skupu* $(\mathbb{N}, \leq)$ *je* $\inf \mathbb{N} = \min \mathbb{N} = 1$, *a* $\sup \mathbb{N}$ *ne postoji. U djelomično uređenom skupu* $(\mathcal{P}(S), \subseteq)$ *postoji i infimum i supremum:* $\inf P(S) = \min P(S) = \emptyset$, *a* $\sup P(S) = \max P(S) = S$.

Definirajmo sada neke važne podskupove djelomično uređenog skupa.

Definicija 4.2.15. *Neka je* $(A, \preceq)$ *djelomično uređen skup. Skup*

$$[a, b]_A = \{x \in A : a \preceq x \preceq b\}$$

nazivamo ***segmentom u*** A. *Skup*

$$\langle a, b\rangle_A = \{x \in A : a \prec x \prec b\}$$

nazivamo ***intervalom u*** A.
Skupove $[a, b\rangle_A = \{x \in A : a \preceq x \prec b\}$ *i* $\langle a, b]_A = \{x \in A : a \prec x \preceq b\}$ *nazivamo* ***poluzatvorenim intervalima s lijeva****, odnosno* ***s desna****.*

Označimo još: $\langle \cdot, a]_A = \{x \in A : x \preceq a\}$, $\langle \cdot, a\rangle_A = \{x \in A : x \prec a\}$,
$[a, \cdot\rangle_A = \{x \in A : x \succeq a\}$, $\langle a, \cdot\rangle_A = \{x \in A : x \succ a\}$.

4.3. Funkcije

Sada ćemo navesti neka svojstva koja može imati bilo koja binarna relacije (naravno, ta svojstva onda može imati i homogena relacija kao poseban slučaj binarne relacije).

Definicija 4.3.1. *Neka su* A *i* B *neprazni skupovi, te* $R \subseteq A \times B$. *Relacija* R *je*

a) ***injektivna*** *ako vrijedi*

$$(\forall x \in A)(\forall x' \in A)(\forall y \in B)((x, y) \in R \wedge (x', y) \in R \to x = x'),$$

b) ***funkcionalna*** *ako vrijedi*

$$(\forall x \in A)(\forall y \in B)(\forall y' \in B)((x, y) \in R \wedge (x, y') \in R \to y = y'),$$

c) ***surjektivna*** *ako vrijedi*

$$(\forall y \in B)(\exists x \in A)(x, y) \in R,$$

d) ***totalna*** *ako vrijedi*

$$(\forall x \in A)(\exists y \in B)(x, y) \in R.$$

Zadatak 1. *Dani su skupovi* $A = \{1, 2, 3, 4, 5\}$ *i* $B = \{a, b, c, d\}$. *Ispitajte koja svojstva imaju sljedeće relacije na skupovima* A *i* B*:*

a) $R_1 = \{(1, a), (1, b), (2, c), (3, d)\}$,

b) $R_2 = \{(1, a), (2, a), (3, b), (4, c), (4, d), (5, d)\}$,

c) $R_3 = \{(1,a),(2,a),(3,b),(4,a),(5,c)\}$,

d) $R_4 = \{(1,a),(2,b),(3,c),(4,d),(5,a)\}$,

e) $R_5 = \{(1,a),(2,b),(3,c),(4,d)\}$.

Definirana svojstva mogu se i skupovno opisati sljedećim karakterizacijama.

Propozicija 4.3.1. *Neka su A i B neprazni skupovi, te $R \subseteq A \times B$. Vrijedi:*

1. *R je injektivna ako i samo ako je $R^{-1} \circ R \subseteq I_A$,*
2. *R je funkcionalna ako i samo ako je $R \circ R^{-1} \subseteq I_B$,*
3. *R je surjektivna ako i samo ako je $I_B \subseteq R \circ R^{-1}$,*
4. *R je totalna ako i samo ako je $I_A \subseteq R^{-1} \circ R$.*

Dokaz. Za ilustraciju ćemo dokazati samo prvu tvrdnju. Ostale tvrdnje se dokazuju analogno. U oba smjera dokaz ćemo provesti kontradikcijom.
$\boxed{\Rightarrow}$: Pretpostavimo da je relacija R injektivna i da $R^{-1} \circ R \nsubseteq I_A$. To znači da

$$(\exists x \in A)(\exists x' \in A)\left(x \neq x' \wedge (x,x') \in R^{-1} \circ R\right),$$

pa je sigurno $R^{-1} \circ R \neq \emptyset$.
Po definiciji kompozicije relacija iz gornjega slijedi

$$(\exists x \in A)(\exists x' \in A)(\exists y \in B)\left(x \neq x' \wedge (x,y) \in R \wedge (y,x') \in R^{-1}\right),$$

a po definiciji inverzne relacije slijedi

$$(\exists x \in A)(\exists x' \in A)(\exists y \in B)(x \neq x' \wedge (x,y) \in R \wedge (x',y) \in R),$$

iz čega zaključujemo da relacija R nije injektivna što je u kontradikciji s pretpostavkom da je R injekcija. Stoga je $R^{-1} \circ R \subseteq I_A$.
$\boxed{\Leftarrow}$: Pretpostavimo da je $R^{-1} \circ R \subseteq I_A$ i da R nije injektivna. To znači da

$$(\exists x \in A)(\exists x' \in A)(\exists y \in B)(x \neq x' \wedge (x,y) \in R \wedge (x',y) \in R).$$

Iz ovoga, po definiciji inverzne relacije, slijedi

$$(\exists x \in A)(\exists x' \in A)(\exists y \in B)\left(x \neq x' \wedge (x,y) \in R \wedge (y,x') \in R^{-1}\right),$$

to jest

$$(\exists x \in A)(\exists x' \in A)\left(x \neq x' \wedge (x,x') \in R^{-1} \circ R\right),$$

pa $R^{-1} \circ R \nsubseteq I_A$, što je u kontradikciji s polaznom pretpostavkom. Dakle, relacija R mora biti injektivna. ■
Slijede još neke važne karakterizacije definiranih svojstava.

Propozicija 4.3.2. *Neka su A i B neprazni skupovi, te $R \subseteq A \times B$.*

1. *Relacija R je totalna ako i samo ako je $D(R) = A$.*

2. *Relacija R je surjektivna ako i samo ako je $K(R) = B$.*

3. *Relacija R je totalna ako i samo ako je R^{-1} surjektivna.*

4. *Relacija R je funkcionalna ako i samo ako je R^{-1} injektivna.*

Dokaz. Tvrdnje (1) i (2) slijede direktno iz definicije domene i slike relacije. Dokažimo tvrdnje (3) i (4) . Neka je $R \subseteq A \times B$.

$$\begin{aligned} R \text{ je totalna} &\Leftrightarrow (\forall x \in A)(\exists y \in B)(x,y) \in R \\ &\Leftrightarrow (\forall x \in A)(\exists y \in B)(y,x) \in R^{-1} \\ &\Leftrightarrow R^{-1} \text{ je surjektivna.} \end{aligned}$$

$$\begin{aligned} R \text{ je funkcionalna} &\Leftrightarrow (\forall x \in A)(\forall y, y' \in B)((x,y) \in R \wedge (x,y') \in R \rightarrow y = y') \\ &\Leftrightarrow (\forall y, y' \in B)(\forall x \in A)\left((y,x) \in R^{-1} \wedge (y',x) \in R^{-1} \rightarrow y = y'\right) \\ &\Leftrightarrow R^{-1} \text{ je injektivna.} \end{aligned}$$

■

Definicija 4.3.2. *Funkcionalnu relaciju nazivamo **parcijalnom funkcijom**. Relaciju $f \subseteq A \times B$ koja je funkcionalna i totalna, tj. za koju vrijedi da za svaki $x \in A$ postoji točno jedan $y \in B$ takav da je $(x,y) \in f$ nazivamo **funkcijom**.*

Formalno,

$$f \subseteq A \times B \text{ je funkcija } \Leftrightarrow (\forall x \in A)(\exists! y \in B)\, f(x) = y. \tag{4.3}$$

Kako su funkcije same po sebi važan matematički pojam posvetit ćemo im posebnu pažnju. Pogledajmo najprije jedan primjer.

Primjer 15. *Neka je H skup svih državljana Republike Hrvatske, $Z = \{0,1,\ldots,9\}$ skup znamenki dekadskog brojevnog sustava i $J = \{(a_1,\ldots,a_{13}) : a_1,\ldots,a_{13} \in Z\}$ skup svih trinaesteroznamenkastih brojeva sa znamenkama iz Z. Elemente skupa J možemo interpretirati kao $JMBG$-ove državljana RH. Definiramo relaciju $f \subseteq H \times J$ na način:*

$$(x,a) \in f \text{ ako i samo ako je broj } a \text{ } JMBG \text{ od osobe } x.$$

Znamo da svakom državljaninu RH pripada jedinstveni $JMBG$, pa je ova relacija funkcionalna i totalna. Točnije, f je funkcija.

Primjedba 4.3.1. *Često se u literaturi funkcija definira kao uređena trojka (A,B,f), gdje su A i B neprazni skupovi, a f pravilo pridruživanja po kojemu se svakom elementu $x \in A$ pridružuje jedan i samo jedan element $y \in B$, i zapisuje se kao $f : A \rightarrow B$, $f(x) = y$. No, to nije dobra definicija jer pojam "pravilo pridruživanja" nije jasan, a pobliže ga se ne opisuje. Definirajući funkciju kao relaciju koja je funkcionalna i totalna, tj. za koju vrijedi svojstvo* (4.3) *sasvim je precizno i jasno definiran taj pojam.*

Nadalje, krene li se od definicije funkcije kao uređene trojke, graf funkcije $f : A \to B$ *se definira kao skup*

$$\Gamma_f = \{(x, f(x)) : x \in A\} \subseteq A \times B.$$

No, u okviru naše definicije funkcije kao posebne relacije, graf funkcije f *i sama funkcija* f *se poklapaju, i kao što bilo koju relaciju možemo prikazati grafički, tako to možemo napraviti i kada je riječ o funkciji. Funkcije se često prikazuju dijagramima.*

Za funkciju ćemo koristiti uobičajene oznake: ako je relacija $f \subseteq A \times B$ funkcija, onda je dogovorno zapisujemo na način $f : A \to B$, a činjenicu da je uređeni par $(x, y) \in f$ zapisujemo kao $f(x) = y$. Element x nazivamo *argumentom* ili *neovisnom varijablom*, a element y *slikom*, *vrijednošću funkcije* ili *ovisnom varijablom*. Zbog totalnosti funkcije f slijedi da je $D(f) = A$, pa skup A s razlogom zovemo domenom funkcije f. Skup B nazivamo *kodomenom* od f. Općenito je $K(f) \subseteq B$.

Propozicija 4.3.3. *Neka je* $\sim$ *relacija ekvivalencije na skupu* A. *Relacija* $\tau \subseteq A \times A \mid_{\sim}$ *definirana na način*

$$(a, [x]) \in \tau \Leftrightarrow a \in [x]$$

je funkcionalna, totalna i surjektivna, tj. τ *je surjektivna funkcija.*

Dokaz. Za svaki $a \in A$ je $(a, [a]) \in \tau$, pa je relacija τ totalna. Isto tako, za svaki $[a] \in A \mid_{\sim}$ je $(a, [a]) \in \tau$, pa je τ i surjektivna. Pokažimo još i da je funkcionalna. Neka je $a \in A$, te neka su klase $[x], [y] \in A \mid_{\sim}$ takve da je $(a, [x]) \in \tau$ i $(a, [y]) \in \tau$. Iz ovoga slijedi da je $a \in [x]$ i $a \in [y]$, tj. $a \in [x] \cap [y]$. No, klase su ili jednake ili disjunktne, što znači da je $[x] = [y]$, pa je relacija τ funkcionalna. ■

Relacija τ je, dakle, funkcija $\tau : A \to A \mid_{\sim}$ definirana izrazom $\tau(a) = [a]$.

Definicija 4.3.3. *Funkciju* $\tau : A \to A \mid_{\sim}$, $\tau(a) = [a]$, *nazivamo* ***projekcijom*** *skupa* A *na kvocijentni skup* $A \mid_{\sim}$.

Projekciju ćemo često koristiti u sljedećem poglavlju kod izgradnje brojeva.
Za funkcije uvodimo još neke posebne oznake i pojmovi.

Definicija 4.3.4. *Neka je* $f : A \to B$ *funkcija,* $C \subseteq A$, *te* $D \subseteq B$.
Slika *od* C *u odnosu na funkciju* f *je skup* $f(C) = \{f(x) : x \in C\} \subseteq B$,
Praslika *od* D *u odnosu na funkciju* f *je skup* $f^{-1}(D) = \{x \in A : f(x) \in D\} \subseteq A$.
Ako se radi o jednočlanom skupu $D = \{y\} \subseteq B$, *onda umjesto* $f^{-1}(\{y\})$ *jednostavno pišemo* $f^{-1}(y) = \{x \in A : f(x) = y\}$.

Očito je $f(A) \subseteq B$, $f^{-1}(B) = A$, $f(\emptyset) = \emptyset$ i $f^{-1}(\emptyset) = \emptyset$.

Primjer 16. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f(x) = 7$ *za svaki* $x \in \mathbb{R}$. *Vrijedi:*

$$K(f) = \{7\}, \quad f^{-1}(\mathbb{R}) = f^{-1}(7) = \mathbb{R}, \quad f([1, 2]) = \{7\},$$

$$f^{-1}([1, 4]) = \emptyset, \quad f^{-1}([3, 8]) = \mathbb{R}.$$

Primjer 17. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f(x) = x^2$ *za svaki* $x \in \mathbb{R}$. *Vrijedi:*

$$K(f) = [0, \infty), \ f^{-1}(\mathbb{R}) = f^{-1}([0, \infty)) = \mathbb{R}, \ f([1, 2]) = [1, 4],$$
$$f^{-1}(4) = \{-2, 2\}, \quad f^{-1}([2, 4]) = \left[-2, \sqrt{2}\right] \cup \left[\sqrt{2}, 2\right], \quad f^{-1}(-1) = \emptyset.$$

Među funkcijama važnu ulogu igraju surjektivne i/ili injektivne funkcije. Surjektivnost i injektivnost su svojstva definirana općenito za bilo koju relaciju, a ako je relacija funkcija, onda surjektivnost funkcije $f : A \to B$ zapisujemo

$$(\forall y \in B)(\exists x \in A) f(x) = y,$$

a injektivnost

$$(\forall x, x' \in A)(f(x) = f(x') \to x = x')$$

ili ekvivalentno

$$(\forall x, x' \in A)(x \neq x' \to f(x) \neq f(x')).$$

Vidjeli smo da je funkcija $f : A \to B$ surjektivna ako i samo ako je $K(f) = B$. Za injektivnost vrijedi sljedeće:

Propozicija 4.3.4. *Neka su* A *i* B *neprazni skupovi, te* $f : A \to B$ *funkcija. Funkcija* $f : A \to B$ *je injektivna ako i samo ako vrijedi*

$$(\forall y \in K(f))(\exists x \in A) f^{-1}(y) = \{x\}.$$

Dokaz. Sami. ■

Definicija 4.3.5. *Funkciju koja je injektivna i surjektivna nazivamo* ***bijekcijom****. Homogenu bijekciju* $f : A \to A$ *na skupu* A *nazivamo* ***permutacijom*** *skupa* A.

Lako se pokaže da je identiteta

$$I_A = id_A = \left\{(x, x) \in A^2 : x \in A\right\}$$

bijektivna funkcija na A, dakle permutacija. Zapisujemo je kao i svaku drugu funkciju: $id_A : A \to A$ i definirana je izrazom $id_A(x) = x$ za svaki $x \in A$. Ta nam je funkcija od posebnog značaja.

Definirajmo još neke važne pojmove vezane uz funkcije.

Definicija 4.3.6. *Neka su* $(A, \leq_A)$ *i* $(B, \leq_B)$ *dva uređena skupa. Za funkciju* $f : A \to B$ *kažemo da je* ***rastuća*** *ako*

$$(\forall x \in A)(\forall x' \in A)(x <_A x' \to f(x) \leq_B f(x')),$$

a da je ***strogo rastuća*** *ako*

$$(\forall x \in A)(\forall x' \in A)(x <_A x' \to f(x) <_B f(x')).$$

Za funkciju $f : A \to B$ *kažemo da je* ***padajuća*** *ako*

$$(\forall x \in A)(\forall x' \in A)(x <_A x' \to f(x) \geq_B f(x')),$$

a da je ***strogo padajuća*** *ako*

$$(\forall x \in A)(\forall x' \in A)(x <_A x' \to f(x) >_B f(x')).$$

Za funkciju $f : A \to B$ *kažemo da je* ***monotona*** *ako je rastuća ili padajuća, odnosno da je* ***strogo monotona*** *ako je strogo rastuća ili strogo padajuća.*

Vrijedi:

• Svaka strogo monotona funkcija je injekcija.

• Ako je $f : A \to B$ strogo monotona na $X \subseteq A$, onda je suženje $f|_X : X \to f(X)$ bijekcija.

Zadatak 2. *Nacrtajte sljedeće funkcije, odredite im sliku, te ispitajte jesu li injektivne, surjektivne ili bijektivne:*

1. $f_1 : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f_1(x) = -2x + 1$,
2. $f_2 : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f_2(x) = -x^2 + 1$,
3. $f_3 : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f_3(x) = x^3$,
4. $f_4 : \mathbb{R} \to \mathbb{R}_0^+$ *definirana izrazom* $f_4(x) = |x|$,
5. $f_5 : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f_5(x) = e^{x+1}$,
6. $f_6 : [0,1] \to [0,1]$ *definirana izrazom* $f_6(x) = \sqrt{1-x^2}$.

Propozicija 4.3.5. *Neka je $f : A \to B$ dana funkcija, te $X, Y \subseteq A$. Vrijedi:*

1. $f(X \cup Y) = f(X) \cup f(Y)$,
2. $f(X \cap Y) \subseteq f(X) \cap f(Y)$,
3. $f(X \setminus Y) \supseteq f(X) \setminus f(Y)$.

Dokaz. Dokazat ćemo prve dvije tvrdnje. Treću dokažite sami.
Dokažimo najprije da je $f(X \cup Y) = f(X) \cup f(Y)$. Neka je $y \in f(X \cup Y)$. Tada postoji neki $x \in X \cup Y$ takav da je $y = f(x)$. Kako je $x \in X \cup Y$, to je $x \in X$ ili $x \in Y$. Stoga je $y \in f(X)$ ili je $y \in f(Y)$, pa je $y \in f(X) \cup f(Y)$. Time smo dokazali da je $f(X \cup Y) \subseteq f(X) \cup f(Y)$.
Obratno, neka je $y \in f(X) \cup f(Y)$. To znači da je $y \in f(X)$ ili je $y \in f(Y)$. Ako je $y \in f(X)$, onda postoji neki $x \in X$ takav da je $y = f(x)$, a ako je $y \in f(Y)$, onda postoji neki $x' \in Y$ takav da je $y = f(x')$. U svakom slučaju, postoji neki $x'' \in X \cup Y$ ($x'' = x$ ili $x'' = x'$) takav da je $y = f(x)$, pa je $y \in f(X \cup Y)$. Time smo dokazali da je $f(X) \cup f(Y) \subseteq f(X \cup Y)$.
Dokažimo sada drugu tvrdnju.
Uzmimo proizvoljan $y \in f(X \cap Y)$. To znači da postoji neki $x \in X \cap Y$ takav da je $y = f(x)$. Kako je $x \in X$ i $x \in Y$, to je $y \in f(X)$ i $y \in f(Y)$. Dakle, vrijedi $y \in f(X) \cap f(Y)$, pa je tvrdnja dokazana. Analogno se dokazuje i treća tvrdnja. ■

Pokažimo protuprimjerom da u tvrdnji (2) ne vrijedi jednakost, tj.

$$f(X) \cap f(Y) \not\subseteq f(X \cap Y).$$

Neka je $A = \{a, b\}$, $a \neq b$, $B = \{b\}$, te funkcija $f : A \to B$ definirana izrazom $f(a) = f(b) = b$. Neka je $X = \{a\}$ i $Y = \{b\}$. Tada je $X \cap Y = \emptyset$, pa je i $f(X \cap Y) = \emptyset$. S druge strane, $f(X) = f(Y) = \{b\}$, pa je $f(X) \cap f(Y) = \{b\} \neq \emptyset$. Dakle, $f(X) \cap f(Y) \not\subseteq f(X \cap Y)$.

Propozicija 4.3.6. *Neka je $f : A \to B$ dana funkcija, te $X, Y \subseteq B$. Vrijedi:*

1. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$,
2. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$,
3. $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$.

Dokaz. Dokazat ćemo samo prvu tvrdnju. Ostale tvrdnje dokažite sami.
Uzmimo proizvoljan $x \in f^{-1}(X \cup Y)$. Iz ovoga odmah slijedi da je $f(x) \in X \cup Y$. To dalje znači da je $f(x) \in X$ ili $f(x) \in Y$, pa je $x \in f^{-1}(X)$ ili $x \in f^{-1}(Y)$, odnosno $x \in f^{-1}(X) \cup f^{-1}(Y)$. Time smo dokazali da je $f^{-1}(X \cup Y) \subseteq f^{-1}(X) \cup f^{-1}(Y)$. Obratno, neka je $x \in f^{-1}(X) \cup f^{-1}(Y)$. Iz ovoga slijedi da je $f(x) \in X$ ili $f(x) \in Y$. Dakle, $f(x) \in X \cup Y$, pa je $x \in f^{-1}(X \cup Y)$, čime smo dokazali da je $f^{-1}(X) \cup f^{-1}(Y) \subseteq f^{-1}(X \cup Y)$, pa je $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. ■
Iz prethodne dvije propozicije vidimo da se praslike ponašaju "ljepše" nego slike.

Definicija 4.3.7. *Neka su A i B proizvoljni skupovi, te $C \subset A$. Kažemo da je funkcija $g : C \to B$ **restrikcija** ili **ograničenje** funkcije $f : A \to B$, i pišemo $g = f|_C$, ako je g poskup od f. Kažemo još da je funkcija f **ekstenzija** ili **proširenje** funkcije g.*

Primjedba 4.3.2. *Uočimo da je $g \subset f$ ako i samo ako je $D(g) \subset D(f)$ i $g(x) = f(x)$ za svaki $x \in D(g)$.*

Primjer 18. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = |x|$ za svaki $x \in \mathbb{R}$, te neka je funkcija $g : \mathbb{R}_0^+ \to \mathbb{R}$ definirana izrazom $g(x) = x$ za svaki $x \in \mathbb{R}_0^+$. Tada je $g = f|_{\mathbb{R}_0^+}$.*

Primjer 19. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = \sqrt{x^2}$ za svaki $x \in \mathbb{R}$, te neka je funkcija $g : \mathbb{R}_0^+ \to \mathbb{R}$ definirana izrazom $g(x) = x$ za svaki $x \in \mathbb{R}_0^+$. Tada je $g = f|_{\mathbb{R}_0^+}$.*

Primjer 20. *Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = \sqrt{1 - \sin^2 x} = |\cos x|$ za svaki $x \in \mathbb{R}$, te neka je funkcija $g : \left[\frac{\pi}{2}, \frac{3\pi}{2}\right] \to \mathbb{R}$ definirana izrazom $g(x) = -\cos x$ za svaki $x \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]$. Tada je $g = f|_{\left[\frac{\pi}{2}, \frac{3\pi}{2}\right]}$.*

Uočimo da je restrikcija neke funkcije na zadani skup jedinstveno određena, dok proširenje funkcije nije jedinstveno određeno. Pogledajmo jedan primjer.

Primjer 21. *Neka je funkcija $f : [0,1] \to \mathbb{R}$ definirana izrazom*

$$f(x) = \sqrt{1 - x^2} \text{ za svaki } x \in [0,1],$$

te neka je funkcija $g : [-1,1] \to \mathbb{R}$ definirana izrazom

$$g(x) = \begin{cases} x + 1, & x \in [-1, 0\rangle \\ \sqrt{1 - x^2}, & x \in [0,1], \end{cases}$$

a funkcija $h : [-1,1] \to \mathbb{R}$ definirana izrazom

$$h(x) = \begin{cases} 1, & x \in [-1, 0\rangle \\ \sqrt{1 - x^2}, & x \in [0,1]. \end{cases}$$

Tada je $f = g|_{[0,1]}$ i $f = h|_{[0,1]}$, i pri tomu je $g \neq h$, pa su funkcije g i h dva različita proširenja funkcije f.

Po definiciji kompozicije relacija znamo da je kompozicija dviju relacija opet relacija. Sada ćemo pokazati da je kompozicija dviju funkcija opet funkcija.

Teorem 4.3.1. *Neka su dane funkcije $f : A \to B$ i $g : B \to C$. Tada je i $g \circ f$ funkcija, te $g \circ f : A \to C$ i definirana je izrazom $(g \circ f)(x) = g(f(x))$ za svaki $x \in A$.*

Dokaz. Po definiciji kompozicije relacija znamo da je $g \circ f \subseteq A \times C$. Dokažimo najprije da je $D(g \circ f) = A$. Kako je $D(f) = A$ i $D(g) = B$, vrijedi

$$(\forall x \in A)(\exists y \in B)(x, y) \in f \quad \text{i} \quad (\forall y \in B)(\exists z \in C)(y, z) \in g.$$

Iz ovog, po definiciji kompozicije relacija, slijedi da je

$$(\forall x \in A)(\exists z \in C)(x, z) \in g \circ f,$$

pa je relacija $g \circ f$ totalna, tj. $D(g \circ f) = A$.
Dokažimo još da je $g \circ f$ funkcionalna.
Neka je $x \in A$ i $z, z' \in C$ takvi da je $(x, z) \in g \circ f$ i $(x, z') \in g \circ f$. Treba dokazati da je $z = z'$. Kako je $(x, z) \in g \circ f$, to postoji neki $y \in B$ takav da je $(x, y) \in f$ i $(y, z) \in g$. Kako je $(x, z') \in g \circ f$, to postoji neki $y' \in B$ takav da je $(x, y') \in f$ i $(y', z') \in g$. Sada iz $(x, y) \in f$ i $(x, y') \in f$, zbog funkcionalnosti funkcije f, slijedi da je $y = y'$. Stoga je $(y, z) \in g$ i $(y, z') \in g$ (jer je $y = y'$), pa zbog funkcionalnosti funkcije g slijedi da je $z = z'$. Dakle, $g \circ f$ je i funkcionalna, pa je $g \circ f$ funkcija i $g \circ f : A \to C$. Nadalje, za svaki $x \in A$ je

$$\begin{aligned} (g \circ f)(x) &= z \Leftrightarrow (x, z) \in g \circ f \\ &\Leftrightarrow (\exists y \in B)\, f(x) = y \wedge g(y) = z \\ &\Leftrightarrow g(f(x)) = z, \end{aligned}$$

pa je $(g \circ f)(x) = g(f(x))$ za svaki $x \in A$. ■

Primjedba 4.3.3. *Iz dokaza prethodnog teorema je vidljivo da se analogna tvrdnja može izreći i za parcijalne funkcije, tj. kompozicija dviju parcijalnih funkcija je opet parcijalna funkcija. Naime, pokazali smo da funkcionalnost kompozicije $g \circ f$ slijedi iz funkcionalnosti od f i g.*

Zadatak 3. *Dokažite:*

1. *Kompozicija dviju injekcija je injekcija,*
2. *Kompozicija dviju surjekcija je surjekcija,*
3. *Kompozicija dviju bijekcija je bijekcija.*

Sljedeći teorem će nam omogućiti da uvedemo pojam inverzne funkcije.

Teorem 4.3.2. *Neka je dana funkcija $f : A \to B$. Relacija f^{-1} je funkcija ako i samo ako je f bijekcija. Štoviše, f^{-1} je tada i sama bijekcija.*

Dokaz. Po Propoziciji 4.3.2., iz totalnosti funkcije f slijedi surjektivnost relacije f^{-1}, a iz funkcionalnosti funkcije f slijedi injektivnost relacije f^{-1}. Stoga je f^{-1} surjektivna i injektivna relacija. Ako je f bijekcija, onda injektivnost i surjektivnost od f impliciraju funkcionalnost i totalnost relacije f^{-1}, pa je f^{-1} funkcija i to bijekcija. I obratno, ako je f^{-1} funkcija, onda funkcionalnost i totalnost od f^{-1} impliciraju injektivnost i surjektivnost od f, pa je f bijekcija. ■

Iz dokaza teorema odmah slijedi da je f^{-1} parcijalna funkcija ako i samo ako je relacija f injektivna.

Teorem 4.3.3. *Neka je $f : A \to B$ bijekcija. Vrijedi*

$$\begin{aligned} f^{-1} \circ f &= id_A, \text{ tj. } \left(f^{-1} \circ f\right)(x) = x \text{ za svaki } x \in A, \\ f \circ f^{-1} &= id_B, \text{ tj. } \left(f \circ f^{-1}\right)(y) = y \text{ za svaki } y \in B, \end{aligned}$$

i f^{-1} je jedina funkcija s ovim svojstvima.

Dokaz. Po Teoremu 4.3.2. znamo da je f^{-1} bijekcija, a po Teoremu 4.3.1. i Zadatku 3. znamo da su $f^{-1} \circ f : A \to A$ i $f \circ f^{-1} : B \to B$ funkcije, i to bijekcije. Dokazat ćemo da je riječ upravo o identitetama na A, odnosno B.
Uzmimo proizvoljni $x \in A$ i $y \in B$. Vrijedi

$$\begin{aligned} \left(f^{-1} \circ f\right)(x) &= f^{-1}(f(x)) = x \,(\text{zbog injektivnosti od } f) = id_A(x), \\ \left(f \circ f^{-1}\right)(y) &= f\left(f^{-1}(y)\right) = y \,(\text{zbog funkcionalnosti od } f) = id_B(y), \end{aligned}$$

pa zaključujemo da je $f^{-1} \circ f = id_A$ i $f \circ f^{-1} = id_B$.
Dokažimo da je f^{-1} jedina funkcija s ovakvim svojstvom. Pretpostavimo suprotno, tj. da postoji neka funkcija $g : B \to A$ takva da je $g \circ f = id_A$ i $f \circ g = id_B$, a da je $g \neq f^{-1}$. Tada vrijedi

$$\begin{aligned} (g \circ f) \circ f^{-1} &= id_A \circ f^{-1} = f^{-1}, \\ g \circ \left(f \circ f^{-1}\right) &= g \circ id_B = g, \end{aligned}$$

pa zbog asocijativnosti kompozicije slijedi $g = f^{-1}$. No, ovo je u kontradikciji s pretpostavkom $g \neq f^{-1}$, pa je f^{-1} jedinstvena funkcija s ovim svojstvima. ■

Korolar 4.3.1. *Neka je $f : A \to B$ bijekcija. Vrijedi*

$$\left(f^{-1}\right)^{-1} = f.$$

Dokaz. Po prethodnom teoremu znamo da je

$$f^{-1} \circ \left(f^{-1}\right)^{-1} = id_A \text{ i } \left(f^{-1}\right)^{-1} \circ f^{-1} = id_B.$$

No, kako je već

$$f^{-1} \circ f = id_A, \text{ i } f \circ f^{-1} = id_B,$$

zbog jedinstvenosti takve funkcije slijedi $(f^{-1})^{-1} = f$. ■

Ovo poglavlje je dijelom preuzeto iz [3].

Poglavlje 5.

Skupovi brojeva

5.1. Skup prirodnih brojeva

5.1.1. Uvod

S prirodnim brojevima smo se susreli još u osnovnoj školi i svakodnevno ih koristimo, no naše znanje o njima nije podvrgnuto kritici. Jednostavno prihvaćamo da izvjesna svojstva koja imaju neki prirodni brojevi imaju i svi prirodni brojevi. Tako smo npr. uvjereni da možemo zbrojiti bilo koja dva prirodna broja. Ukoliko smo uopće došli na ideju da promatramo cijeli skup prirodnih brojeva, označimo ga s $\mathbb{N}$, ipak i dalje vjerujemo da možemo zbrojiti bilo koja dva prirodna broja i da je njihov zbroj prirodan broj. To znači da prešutno prihvaćamo postojanje funkcije "zbrajanja" sa $\mathbb{N} \times \mathbb{N}$ u $\mathbb{N}$. Ovako "eksperimentalno" izgrađen skup $\mathbb{N}$ ima sljedeća svojstva:

- $\mathbb{N}$ nije prazan.
- $\mathbb{N}$ je uređen.
- Ako je $n \in \mathbb{N}$, onda je skup svih prirodnih brojeva manjih od n konačan.
- Skup $\mathbb{N}$ ima najmanji element; to je broj 1.
- Skup $\mathbb{N}$ nema najvećeg elementa, tj. za svaki prirodan broj postoji prirodan broj veći od njega.

Posljedica ovih svojstava je postojanje injektivne funkcije $s : \mathbb{N} \to \mathbb{N}$ koja svakom $n \in \mathbb{N}$ pridružuje direktnog sljedbenika $s(n) = n+1 \in \mathbb{N}$. Pri tomu skup $\mathbb{N}$, funkcija s i broj 1 imaju jedno važno i ne posve očigledno svojstvo koje se sastoji u sljedećem:

Ako je M podskup skupa $\mathbb{N}$ i ako vrijedi:

$$1 \in M,$$

$$(\forall x \in \mathbb{N})\,(x \in M \to s(x) \in M),$$

onda je $M = \mathbb{N}$.

Ovo svojstvo je poznato pod nazivom *princip matematičke indukcije* i uzima se kao aksiom prilikom aksiomatske izgradnje skupa prirodnih brojeva. Taj aksiom ima i posebnu ulogu: koristimo ga pri dokazivanju teorema i prilikom rekurzivnog definiranja funkcija na $\mathbb{N}$.

Evo kako izgleda aksiomatska izgradnja skupa prirodnih brojeva $\mathbb{N}$.

Definicija 5.1.1. *Neprazan skup* $\mathbb{N}$ *za kojeg vrijede sljedeći aksiomi:*

*A*1) *Postoji funkcija* $s : \mathbb{N} \to \mathbb{N}$.

*A*2) *Postoji barem jedan element u* $\mathbb{N}$, *označimo ga s* 1, *takav da je* $s(n) \neq 1$ *za svaki* $n \in \mathbb{N}$.

*A*3) *Ako je* $s(m) = s(n)$ *za* $m, n \in \mathbb{N}$, *onda je* $m = n$.

*A*4) *Ako je M podskup skupa* $\mathbb{N}$ *i ako vrijedi:*

$$1 \in M,$$
$$(\forall x \in \mathbb{N})\,(x \in M \to s(x) \in M),$$

onda je $M = \mathbb{N}$,

nazivamo ***skupom prirodnih brojeva****, a njegove elemente* ***prirodnim brojevima****.*

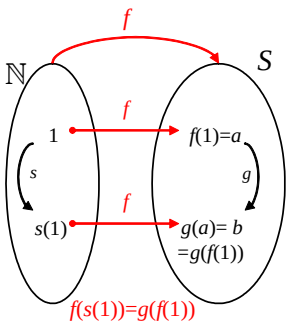
Navedene aksiome $A1) - A4)$ nazivamo *Peanovim aksiomima skupa prirodnih brojeva*, prema talijanskom matematičaru Giuseppeu Peanu $(1858 - 1931)$. Postojanje barem jednog skupa $\mathbb{N}$ koji zadovoljava navedena četiri aksioma prihvaćamo kao "iskustvenu činjenicu". Pokazat ćemo da taj skup ima sva ona svojstva za koja vjerujemo da ih ima skup prirodnih brojeva kojim se služimo u svakodnevnom životu. Time ova definicija dobiva svoje opravdanje, a sva teorija prirodnih brojeva proizlazi iz navedena četiri aksioma i opće sheme logičkog zaključivanja.

Nameće se još pitanje jedinstvenosti takvog skupa. Sljedeći teorem pokazuje da Peanovi aksiomi potpuno karakteriziraju prirodne brojeve, tj. da postoji najviše jedan skup prirodnih brojeva (određen do na izomorfizam). Dokaz toga teorema možete pronaći u [5].

Teorem 5.1.1. *Neka su* $(\mathbb{N}, s, 1)$ *i* $(\mathbb{N}', s', 1')$ *dvije uređene trojke koje zadovoljavaju Peanove aksiome. Tada postoji jedna i samo jedna bijekcija* $f : \mathbb{N} \to \mathbb{N}'$ *takva da je* $f(1) = 1'$, *a* $f(s(n)) = s'(f(n))$.

5.1.2. Rekurzivna definicija niza

Neka je S neprazan skup, $a \in S$ i $g : S \to S$. Pomoću funkcije g definirajmo funkciju $f : \mathbb{N} \to S$ na *rekurzivni* način:
Najprije broju 1 pridružimo istaknuti element $a \in S$, tj. definiramo $f(1) = a \in S$. Funkcija g elementu a pridruži element $b \in S$, a funkcija sljedbenika s broju 1 broj $s(1)$, tj. $a \overset{g}{\mapsto} g(a) = b \in S$ i $1 \overset{s}{\mapsto} s(1) \in \mathbb{N}$. Sada definiramo $f(s(1)) = b$, tj. $f(s(1)) = g(a) = g(f(1))$.



Taj postupak nastavljamo. Neka je za neko $n \in \mathbb{N}$ definirano $f(n) = x \in S$, te neka je $x \overset{g}{\mapsto} g(x) = y \in S$, a $n \overset{s}{\mapsto} s(n)$. Definiramo $f(s(n)) = y$, tj. $f(s(n)) = g(x) = g(f(n))$.

$$\begin{array}{ccc} n & \overset{f}{\longmapsto} & x = f(n) \\ \bar{\downarrow} s & & \bar{\downarrow} g \\ s(n) & \overset{f}{\longmapsto} & y = g(x) \end{array}$$

Pokazat ćemo da se ovim postupkom stvarno dobiva jedna funkcija sa $\mathbb{N}$ u S i da je ona jedinstvena. Za tako definiranu funkciju kažemo da je zadana *rekurzivno*, odnosno da je definirana *induktivno*. Prilikom ovakvog definiranja treba sagledati dvije stvari:

1. kako dobiti $f(1)$,
2. kako iz $f(n)$ dobiti $f(s(n))$.

Teorem 5.1.2. *(Rekurzivni teorem) Neka je S neprazan skup i $a \in S$. Neka je svakom elementu $n \in \mathbb{N}$ pridružena funkcija $g_n : S \to S$. Tada postoji jedna i samo jedna funkcija $f : \mathbb{N} \to S$ takva da je*

$$\begin{aligned} f(1) &= a \quad i \\ (\forall n \in \mathbb{N})\, f(s(n)) &= g_n(f(n)). \end{aligned}$$

Dokaz. Dokaz ove tvrdnje nije jednostavan, pa dajemo samo njegovu skicu. Sa $\mathcal{F}$ označimo familiju svih relacija $B \subseteq \mathbb{N} \times S$ koje imaju sljedeća svojstva:

1. $(1, a) \in B$,
2. ako je $(n, b) \in B$, onda je i $(s(n), g_n(b)) \in B$.

Budući da sam skup $\mathbb{N} \times S$ zadovoljava navedene uvjete (jer je $(1, a) \in \mathbb{N} \times S$ i za svaki $(n, b) \in \mathbb{N} \times S$ je i $(s(n), g_n(b)) \in \mathbb{N} \times S$), to je $\mathcal{F} \neq \emptyset$. Sada relaciju f definiramo kao

$$f = \bigcap_{B \in \mathcal{F}} B.$$

Korištenjem aksioma $A1) - A4)$ se dokaže da je relacija f totalna i funkcionalna, tj. da je f funkcija sa $\mathbb{N}$ u S, a iz konstrukcije relacije f je vidljivo da f ima tražena svojstva i da je jedinstvena. ■

Rekurzivni teorem ćemo često primjenjivati u posebnom slučaju kada su sve funkcije g_n jednake, tj. kada je svakom elementu $n \in \mathbb{N}$ pridružena uvijek ista funkcija $g : S \to S$. U tom slučaju vrijedi:

Korolar 5.1.1. *Za svaki neprazan skup S, svaki element $a \in S$ i svaku funkciju $g : S \to S$ postoji jedna i samo jedna funkcija $f : \mathbb{N} \to S$ takva da je*

$$\begin{aligned} f(1) &= a \quad i \\ (\forall n \in \mathbb{N})\, f(s(n)) &= g(f(n)). \end{aligned}$$

Definicija 5.1.2. *Neka je S neprazan skup. Bilo koju funkciju $f : \mathbb{N} \to S$ nazivamo **nizom** u S.*

Ako je $f(n) = a_n$, onda kažemo da je a_n n-ti član niza f.
Niz se označava s $(a_n)_{n \in \mathbb{N}}$ ili jednostavno $a_1, a_2, \ldots, a_n, \ldots$

5.1.3. Zbrajanje na skupu $\mathbb{N}$

Teorem 5.1.3. *Postoji jedna i samo jedna funkcija $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sa svojstvima:*

1. $(\forall m \in \mathbb{N})\, f(m,1) = s(m)$,
2. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, f(m, s(n)) = s(f(m,n))$.

Dokaz. Dokažimo najprije egzistenciju takve funkcije f. Jasno je da nam za dokaz naše tvrdnje treba poslužiti upravo Korolar 5.1.1., no u njemu se utvrđuje egzistencija odgovarajuće funkcije jedne varijable, dok je funkcija koju mi trebamo funkcija dviju varijabla. Zato ćemo najprije konstruirati niz funkcija f_m, $m \in \mathbb{N}$, a onda ćemo u drugom koraku konstruirati funkciju f pomoću tog niza. Pogledajmo sada kako se konstrira svaka pojedina funkcija f_m.
Neka je $m \in \mathbb{N}$ proizvoljan prirodan broj. U Korolaru 5.1.1. uzmimo da je $S = \mathbb{N}$, $g = s$ i $a = s(m)$. Prema Korolaru 5.1.1., postoji jedinstvena funkcija $f_m : \mathbb{N} \to \mathbb{N}$ takva da je

$$\begin{aligned} f_m(1) &= a = s(m), \\ (\forall n \in \mathbb{N})\, f_m(s(n)) &= g(f_m(n)) = s(f_m(n)). \end{aligned}$$

Tako je *svakom* uređenom paru $(m,n) \in \mathbb{N} \times \mathbb{N}$ pridružen *jedinstven* prirodni broj $f_m(n)$, pa je sa

$$(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; f(m,n) = f_m(n)$$

definirana jedna funkcija $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Sada, iz definicije funkcije f, slijedi

$$(\forall m \in \mathbb{N})\, f(m,1) = f_m(1) = s(m) \quad \text{i}$$

$$(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, f(m, s(n)) = f_m(s(n)) = s(f_m(n)) = s(f(m,n)),$$

pa funkcija f ima tražena dva svojstva. Time je dokazana egzistencija funkcije f.
Dokažimo još i jedinstvenost. Pretpostavimo da postoje dvije funkcije, f i g, koje zadovoljavaju uvjete teorema. Dokazat ćemo da su one jednake. Neka je

$$\begin{aligned} F_n &= \{m \in \mathbb{N} \mid f(m,n) = g(m,n)\},\ n \in \mathbb{N} \quad \text{i} \\ F &= \{n \in \mathbb{N} \mid F_n = \mathbb{N}\}. \end{aligned}$$

Primijetimo,

$$F_n = \mathbb{N} \Leftrightarrow (\forall m \in \mathbb{N})\, f(m,n) = g(m,n) \quad \text{i}$$

$$F = \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{N})\, F_n = \mathbb{N} \Leftrightarrow (\forall n, m \in \mathbb{N})\, f(m,n) = g(m,n) \Leftrightarrow f = g. \qquad (5.1)$$

Dokažimo stoga da je $F = \mathbb{N}$ i dokazat ćemo da je $f = g$. Kako je

$$(\forall m \in \mathbb{N})\, f(m,1) = s(m) = g(m,1)$$

to je $F_1 = \mathbb{N}$, tj. $1 \in F$. Nadalje, ako je $n \in F$, tj. $F_n = \mathbb{N}$, onda je $f(m,n) = g(m,n)$ za svaki $m \in \mathbb{N}$, pa je i $s(f(m,n)) = s(g(m,n))$ za svaki $m \in \mathbb{N}$. No, kako je $s(f(m,n)) = f(m, s(n))$ i $s(g(m,n)) = g(m, s(n))$, to je

$$(\forall m \in \mathbb{N})\, f(m, s(n)) = g(m, s(n)).$$

pa je $F_{s(n)} = \mathbb{N}$, tj. $s(n) \in F$. Prema tomu imamo:

$$1 \in F \quad \text{i} \quad (\forall n \in \mathbb{N})\,(n \in F \to s(n) \in F),$$

pa iz $A4$) slijedi da je $F = \mathbb{N}$, a onda je po (5.1) $f = g$. ■

Definicija 5.1.3. *Funkciju* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *za koju vrijedi*

1) $(\forall m \in \mathbb{N})\, f(m, 1) = s(m)$,

2) $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, f(m, s(n)) = s(f(m, n))$,

nazivamo ***zbrajanjem na skupu*** $\mathbb{N}$ *i umjesto* $f(m, n)$ *pišemo* $m + n$. *Brojeve* m *i* n *nazivamo* ***pribrojnicima****, a broj* $m + n$ ***zbrojem****.*

Gornje uvjete 1) i 2) možemo sada pisati u obliku:

$$(\forall m \in \mathbb{N})\, m + 1 = s(m) \quad \text{i}$$

$$(\forall m, n \in \mathbb{N})\, m + s(n) = s(m + n), \text{ tj. } m + (n + 1) = (m + n) + 1. \tag{5.2}$$

Teorem 5.1.4. *(Asocijativnost zbrajanja) Za proizvoljne brojeve* $m, n, p \in \mathbb{N}$ *vrijedi*

$$(m + n) + p = m + (n + p).$$

Dokaz. Neka su $m, n \in \mathbb{N}$ dani, ali proizvoljni prirodni brojevi. Definirajmo skup $M_{m,n} = \{p \in \mathbb{N} \mid (m + n) + p = m + (n + p)\}$. Dokažimo da je $M_{m,n} = \mathbb{N}$. Time ćemo dokazati da je $(m + n) + p = m + (n + p)$ za svaki $p \in \mathbb{N}$ i čvrste m i n.
Iz (5.2) vidimo da je $(m + n) + 1 = m + (n + 1)$, pa je $1 \in M_{m,n}$.
Uzmimo sada da je $p \in M_{m,n}$ i pokažimo da je i $s(p) \in M_{m,n}$. Vrijedi:

$$(m + n) + s(p) \overset{(5.2)}{=} s((m + n) + p) \quad \text{i}$$
$$m + (n + s(p)) \overset{(5.2)}{=} m + s(n + p) \overset{(5.2)}{=} s(m + (n + p)).$$

Budući je po pretpostavci $p \in M_{m,n}$, to je

$$(m + n) + p = m + (n + p),$$

pa je i

$$s((m + n) + p) = s(m + (n + p)).$$

Stoga je

$$(m + n) + s(p) = s((m + n) + p) = s(m + (n + p)) = m + (n + s(p)),$$

pa je $s(p) \in M_{m,n}$. Sada po aksiomu $A4$) slijedi da je $M_{m,n} = \mathbb{N}$. Time smo dokazali da vrijedi:

$$(\forall p \in \mathbb{N})\, (m + n) + p = m + (n + p)$$

za dane, a inače proizvoljne prirodne brojeve m i n. ■

Primjedba 5.1.1. *Primijetimo da gornji dokaz nije proveden do kraja. Naime, dokazali smo tek da je* $(m + n) + p = m + (n + p)$ *za svaki* $p \in \mathbb{N}$. *Za cjelovit dokaz trebali bismo još indukcijom po* m *i* n *(dvostruka indukcija) pokazati da jednakost vrijedi i za proizvoljne* $m, n \in \mathbb{N}$ *(što zbog duljine nismo napravili). Tek tada bi teorem bio u cijelosti dokazan. Inače, kada god budemo trebali dokazati da neko svojstvo vrijedi za proizvoljna tri prirodna broja, zbog složenosti, provodit ćemo ovakav necijelovit dokaz.*

Teorem 5.1.5. *(Komutativnost zbrajanja) Za proizvoljne $m, n \in \mathbb{N}$ vrijedi*

$$m + n = n + m.$$

Dokaz. Neka je $M_m = \{n \in \mathbb{N} \mid m + n = n + m\}$, $m \in \mathbb{N}$ i $M = \{m \in \mathbb{N} \mid M_m = \mathbb{N}\}$. Za dokazati tvrdnju teorema dovoljno je dokazati da je $M = \mathbb{N}$. Naime,

$$M = \mathbb{N} \Leftrightarrow (\forall m \in \mathbb{N})\, M_m = \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{N})\,(\forall m \in \mathbb{N})\, m + n = n + m$$

Pokažimo da je $1 \in M$, tj. da je $M_1 = \mathbb{N}$. Očito je $1 \in M_1$ $(1 + 1 = 1 + 1)$. Nadalje, ako je $n \in M_1$, onda je $n + 1 = 1 + n$, pa je

$$1 + s(n) = 1 + (n + 1) \overset{asoc}{=} (1 + n) + 1 \overset{pp}{=} (n + 1) + 1 = s(n) + 1,$$

iz čega slijedi da je $s(n) \in M_1$. Stoga, po $A4$) zaključujemo da je $M_1 = \mathbb{N}$, tj. $1 \in M$. Uzmimo da je $m \in M$, tj. $M_m = \mathbb{N}$. Stoga je $n + m = m + n$ za svaki $n \in \mathbb{N}$, pa je

$$s(m) + n = (m + 1) + n \overset{M_1=\mathbb{N}}{=} (1 + m) + n \overset{as}{=} 1 + (m + n) \overset{M_1=\mathbb{N}}{=} (m + n) + 1 =$$

$$\overset{pp}{=} (n + m) + 1 \overset{as}{=} n + (m + 1) = n + s(m) \text{ za svaki } n \in \mathbb{N}.$$

Stoga je $M_{s(m)} = \mathbb{N}$, tj. $s(m) \in M$. Sada, po $A4$) zaključujemo da je $M = \mathbb{N}$ čime je teorem dokazan. ■

Primjedba 5.1.2. *Pišemo* $s(1) = 1+1 = 2$, $s(2) = 2+1 = 1+2 = 3$, $s(3) = 4, \ldots$

Dokažimo sada da je zbroj prirodnih brojeva uvijek različitih od svojih pribrojnika. To ćemo svojstvo prirodnih brojeva poslije često koristiti.

Teorem 5.1.6. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, m + n \neq m.$

Dokaz. Neka je $M_m = \{n \in \mathbb{N} : m + n \neq m\}$, $m \in \mathbb{N}$ i $M = \{m \in \mathbb{N} \mid M_m = \mathbb{N}\}$. Dokazat ćemo tvrdnju dokažemo li da je $M = \mathbb{N}$. Pokažimo najprije da je $1 \in M$.

$$1 \in M \Leftrightarrow M_1 = \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{N})\, 1 + n \neq 1,$$

No, prema $A2$) je $1 + n = s(n) \neq 1$ za svaki $n \in \mathbb{N}$, pa je $1 \in M$.
Uzmimo da je $m \in M$, tj. $M_m = \mathbb{N}$. Stoga je $m + n \neq m$ za svaki $n \in \mathbb{N}$, pa je

$$s(m) + n = (1 + m) + n \overset{as}{=} 1 + (m + n) = s(m + n) \overset{A3)}{\neq} s(m) \text{ za svaki } n \in \mathbb{N}.$$

Stoga je $M_{s(m)} = \mathbb{N}$, tj. $s(m) \in M$. Sada, po $A4$) zaključujemo da je $M = \mathbb{N}$ čime je teorem dokazan. ■

Primjedba 5.1.3. *Uočimo da* $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, m + n \neq m$ *zbog komutativnosti zbrajanja na* $\mathbb{N}$ *znači isto što i* $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, m + n \neq m$.

5.1.4. Množenje na skupu $\mathbb{N}$

Sada ćemo ponoviti sličan postupak kao u prethodnoj podtočki, ali za množenje prirodnih brojeva.

Teorem 5.1.7. *Postoji jedna i samo jedna funkcija* $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *sa svojstvima:*

1. $(\forall m \in \mathbb{N})\, h(m, 1) = m$,
2. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, h(m, s(n)) = h(m, n) + m$.

Dokaz. Dokažimo najprije egzistenciju funkcije h. Za svaki $m \in \mathbb{N}$ definirajmo funkciju h_m na sljedeći način: U Korolaru 5.1.1. uzmimo da je

$$S = \mathbb{N},\ a = m \ \text{ i } \ g : \mathbb{N} \to \mathbb{N},\ g(x) = x + m \text{ za svaki } x \in \mathbb{N}.$$

Po Korolaru 5.1.1. slijedi da postoji jedinstvena funkcija $h_m : \mathbb{N} \to \mathbb{N}$ za koju je

$$\begin{aligned} h_m(1) &= a = m, \\ (\forall n \in \mathbb{N})\, h_m(s(n)) &= g(h_m(n)) = h_m(n) + m. \end{aligned}$$

Tako je *svakom* uređenom paru $(m, n) \in \mathbb{N} \times \mathbb{N}$ pridružen *jedinstven* prirodni broj $h_m(n)$, pa je sa

$$(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, h(m, n) = h_m(n)$$

definirana jedna funkcija $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Pri tomu je

$$\begin{aligned} h(m, 1) &= h_m(1) = m \quad \text{ i} \\ h(m, s(n)) &= h_m(s(n)) = h_m(n) + m = h(m, n) + m, \end{aligned}$$

pa funkcija h ima tražena dva svojstva. Time je dokazana egzistencija funkcije h. Dokažimo da je h jedina takva funkcija. Pretpostavimo da postoje dvije funkcije, h i k, s traženim svojstvima. Dokazat ćemo da su one jednake. Definirajmo skupove

$$\begin{aligned} F_n &= \{m \in \mathbb{N} \mid h(m, n) = k(m, n)\},\ n \in \mathbb{N} \ \text{ i} \\ F &= \{n \in \mathbb{N} \mid F_n = \mathbb{N}\}. \end{aligned}$$

Primijetimo,

$$F = \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{N})\, F_n = \mathbb{N} \Leftrightarrow (\forall n, m \in \mathbb{N})\, h(m, n) = k(m, n) \Leftrightarrow h = k. \tag{5.3}$$

Dokažimo stoga da je $F = \mathbb{N}$ i dokazat ćemo da je $h = k$. Kako je

$$(\forall m \in \mathbb{N})\, h(m, 1) = m = k(m, 1)$$

to je $F_1 = \mathbb{N}$, tj. $1 \in F$. Nadalje, ako je $n \in F$, tj. $F_n = \mathbb{N}$, onda je

$$(\forall m \in \mathbb{N})\, h(m, n) = k(m, n),$$

iz čega slijedi

$$(\forall m \in \mathbb{N})\, h(m, s(n)) = h(m, n) + m \overset{pp}{=} k(m, n) + m = k(m, s(n)),$$

pa je i $F_{s(n)} = \mathbb{N}$, tj. $s(n) \in F$. Prema tomu imamo:

$$1 \in F \ \text{ i } \ (\forall n \in \mathbb{N})\,(n \in F \to s(n) \in F),$$

pa iz $A4$) slijedi da je $F = \mathbb{N}$, a onda je po (5.3) $h = k$. ∎

Definicija 5.1.4. *Funkciju* $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *za koju vrijedi*

1) $(\forall m \in \mathbb{N})\, h(m, 1) = m$,

2) $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, h(m, s(n)) = h(m, n) + m$,

nazivamo ***množenjem*** *na skupu* $\mathbb{N}$ *i umjesto* $h(m, n)$ *pišemo* mn.

Uočimo da se onda umjesto $h(m, n) + p$ piše $mn + p$ i da u tom izrazu najprije treba izvršiti množenje pa tek onda zbrajanje. Zato se obično kaže da je množenje operacija višeg reda od zbrajanja.
Gornja dva uvjeta sada možemo zapisati u obliku:

$$(\forall m \in \mathbb{N})\, m1 = m \quad \text{i}$$

$$(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, ms(n) = mn + m, \text{ tj. } m(n+1) = mn + m. \tag{5.4}$$

Teorem 5.1.8. *(Teorem o distributivnosti) Za proizvoljne* $m, n, p \in \mathbb{N}$ *vrijedi*

1. $m(n + p) = mn + mp$,
2. $(m + n)p = mp + np$.

Dokaz. Dokazat ćemo samo prvu tvrdnju jer je dokaz druge tvrdnje sličan. Za dane, ali proizvoljne $m, n \in \mathbb{N}$ definiramo $M_{m,n} = \{p \in \mathbb{N} : m(n + p) = mn + mp\}$. Vrijedi: $1 \in M_{m,n}$ jer je

$$m(n+1) \overset{(5.4)}{=} mn + m \overset{(5.4)}{=} mn + m1.$$

Nadalje, ako je $p \in M_{m,n}$, tj. ako je $m(n + p) = mn + mp$, onda vrijedi

$$\begin{aligned} m[n + s(p)] &= m[n + (p + 1)] \overset{as}{=} m[(n + p) + 1] \overset{(5.4)}{=} m(n + p) + m \\ &\overset{pp}{=} (mn + mp) + m \overset{as}{=} mn + (mp + m) \overset{(5.4)}{=} mn + ms(p), \end{aligned}$$

pa je i $s(p) \in M_{m,n}$. Sada, po $A4$) zaključujemo da je $M_{m,n} = \mathbb{N}$. Time smo dokazali da je $m(n + p) = mn + mp$ za svaki $p \in \mathbb{N}$ i čvrste m i n. Matematičkom indukcijom po m i n može se pokazati da tvrdnja vrijedi i za proizvoljne $m, n \in \mathbb{N}$. ■
Zbrajanje i množenje su dvije algebarske operacije na skupu $\mathbb{N}$. Prethodnim teoremom uspostavljena je veza među njima: lijevi i desni zakon distribucije.

Teorem 5.1.9. *(Asocijativnost množenja) Za proizvoljne* $m, n, p \in \mathbb{N}$ *vrijedi*

$$m(np) = (mn)p.$$

Dokaz. Za dane, ali proizvoljne $m, n \in \mathbb{N}$ definiramo $M_{m,n} = \{p \in \mathbb{N} : m(np) = (mn)p\}$. Očito je $m(n1) = mn = (mn)1$, pa je $1 \in M_{m,n}$. Nadalje, ako je $p \in M_{m,n}$, tj. ako je $m(np) = (mn)p$, imamo

$$m(ns(p)) \overset{(5.4)}{=} m(np + n) \overset{dis}{=} m(np) + mn \overset{pp}{=} (mn)p + mn \overset{(5.4)}{=} (mn)s(p),$$

pa je $s(p) \in M_{m,n}$. Sada po $A4$) zaključujemo da je $M_{m,n} = \mathbb{N}$. Time smo dokazali da je $m(np) = (mn)p$ za svaki $p \in \mathbb{N}$ i čvrste m i n. Matematičkom indukcijom po m i n možemo pokazati da tvrdnja vrijedi i za proizvoljne $m, n \in \mathbb{N}$. ■

Teorem 5.1.10. *(Komutativnost množenja) Za proizvoljne $m, n \in \mathbb{N}$ vrijedi*

$$mn = nm.$$

Dokaz. Neka je $M_m = \{n \in \mathbb{N} \mid mn = nm\}$, $m \in \mathbb{N}$ i $M = \{m \in \mathbb{N} \mid M_m = \mathbb{N}\}$. Za dokazati tvrdnju teorema dovoljno je dokazati da je $M = \mathbb{N}$. Naime,

$$M = \mathbb{N} \Leftrightarrow (\forall m \in \mathbb{N})\, M_m = \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{N})\, (\forall m \in \mathbb{N})\, mn = nm$$

Pokažimo najprije da je $1 \in M$, tj. da je $M_1 = \mathbb{N}$. Kako je $1 \cdot 1 = 1 \cdot 1$, to je $1 \in M_1$. Nadalje, ako je $n \in M_1$, tj. ako je $1n = n1$, imamo

$$1s(n) = 1(n+1) \overset{dis}{=} 1n + 1 \overset{pp}{=} n1 + 1 = n + 1 = s(n) = s(n)\,1,$$

pa je $s(n) \in M_1$.Sada po $A4$) zaključujemo da je $M_1 = \mathbb{N}$, tj. $1 \in M$. Pretpostavimo da je $m \in M$, tj. da je $M_m = \mathbb{N}$. Stoga je $mn = nm$ za svaki $n \in \mathbb{N}$, pa je

$$s(m)\,n = (m+1)\,n \overset{dis}{=} mn + 1n \overset{pp}{=} nm + n1 \overset{dis}{=} n(m+1) = ns(m) \text{ za svaki } n \in \mathbb{N}.$$

Stoga je $M_{s(m)} = \mathbb{N}$, tj. $s(m) \in M$. Sada, po $A4$) zaključujemo da je $M = \mathbb{N}$ čime je teorem dokazan. ■

U umnošku mn brojeve m i n nazivamo **faktorima**: m je prvi faktor, a n je drugi faktor. Uočimo da se zbog simetričnosti relacije "jednako" može pisati

$$\begin{aligned} mn + mp &= m(n+p), \\ mp + np &= (m+n)\,p, \end{aligned}$$

i tada govorimo o izlučivanju zajedničkog faktora p. Tim svojstvima zbrajanja i množenja se često koristimo pri rješavanju konkretnih problema.

5.1.5. Daljnja svojstva skupa $\mathbb{N}$

Uvedimo najprije nekoliko pojmova vezanih općenito uz skupove.

Definicija 5.1.5. *Kažemo da su skupovi S i S' **ekvipotentni**, u oznaci $S \cong S'$, ako postoji barem jedna bijekcija sa S na S'.*

Lako se vidi da je relacija ekvipotencije jedna relacija ekvivalencije (na čemu?), pa se skupovi mogu svrstati u međusobno disjunktne klase ekvivalencije s obzirom na ovu relaciju. Klasu kojoj pripada neki skup S nazivamo njegovim **kardinalnim brojem** i označavamo s $\text{kard}(S)$ ili $|S|$.

Primjedba 5.1.4. *Kardinalnost je zapravo sinonim za ekvipotentnost. Relacija "biti ekvipotentan" bi očito trebala biti definirana na klasi svih skupova, ali to onda izlazi iz okvira onoga što nazivamo relacijom (relaciju smo definirali na skupu, a ne na klasi). No, pojam relacije se može na prirodan način proširiti na klase pa u tom svjetlu treba promatrati gornju relaciju.*

Kardinalni broj proizvoljnog skupa S smo definirati kao klasu ekvivalencije relacije "biti ekvipotentan", odnosno $k(S) = \{B : B \text{ je skup takav da } S \cong B\}$. No, problem je što za niti jedan neprazan skup S klasa $k(S)$ nije skup, tj. $k(S)$ je prava klasa. Da bi se to izbjeglo, u teoriji skupova se kardinalni broj skupa S definira kao točno određeni skup iz klase svih skupova koji su ekvipotentni sa skupom S.

Definicija 5.1.6. *Reći ćemo da je skup S* ***beskonačan*** *ako postoji njegov pravi podskup $S' \subset S$ takav da je $S \cong S'$. Kažemo da je skup* ***konačan*** *ako nije beskonačan.*

Definicija 5.1.7. *Neka je S konačan skup. Reći ćemo da je n broj elemenata skupa S i pisati* $\operatorname{kard}(S) = n$, *ako je $S \cong \{1, 2, \ldots, n\} \subset \mathbb{N}$.*

Sada ćemo vidjeti kakva je priroda kardinalnog broja skupa $\mathbb{N}$.

Lema 5.1.1. *Za svaki $n \in \mathbb{N} \setminus \{1\}$ postoji barem jedan $m \in \mathbb{N}$ takav da je $n = s(m)$. Drugim riječima, $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ je surjekcija.*

Dokaz. Neka je $M = s(\mathbb{N}) \cup \{1\}$. Dokažimo da je $M = \mathbb{N}$. Iz definicije skupa M slijedi da je $1 \in M$. Uzmimo neki $m \in \mathbb{N}$ i pretpostavimo da je $m \in M$. Tada je $s(m) \in s(\mathbb{N}) \subseteq M$. Po $A4$) zaključujemo da je $M = \mathbb{N}$, tj. $s(\mathbb{N}) \cup \{1\} = \mathbb{N}$. Stoga je za svaki $n \in \mathbb{N}$ ispunjeno $n = 1$ ili $n \in s(\mathbb{N})$. Ako je $n \in s(\mathbb{N}) = \mathbb{N} \setminus \{1\}$, onda postoji neki $m \in \mathbb{N}$ takav da je $s(m) = n$ pa je tvrdnja u cijelosti dokazana. ■

Korolar 5.1.2. *Skup $\mathbb{N}$ je beskonačan.*

Dokaz. Iz $A3$) slijedi da je $s : \mathbb{N} \to \mathbb{N}$ injekcija. Po prethodnoj lemi znamo da je $s : \mathbb{N} \to s(\mathbb{N}) = \mathbb{N} \setminus \{1\}$ surjekcija, pa je s bijekcija sa $\mathbb{N}$ u njegov pravi podskup $\mathbb{N} \setminus \{1\}$, tj. $\mathbb{N}$ je ekvipotentan svome pravom podskupu. Dakle, $\mathbb{N}$ je beskonačan. ■

Definicija 5.1.8. *Reći ćemo da je skup S* ***prebrojiv*** *ako je ekvipotentan skupu $\mathbb{N}$. Za beskonačan skup koji nije prebrojiv kažemo da je* ***neprebrojiv.***

Kardinalni broj skupa prirodnih brojeva, pa onda i svih prebrojivih skupova, označavamo s $\aleph_0$ i čitamo *alef-nula*.

Primjedba 5.1.5. *U nekim se knjigama prebrojiv skup definira kao skup koji je ekvipotentan nekom podskupu od $\mathbb{N}$. Po toj bi definiciji i svi konačni skupovi bili prebrojivi. Više je razloga zašto je to ponekad praktičnije, no mi ćemo se držati gornje definicije po kojoj su prebrojivi skupovi isključivo beskonačni skupovi koji su ekvipotenti skupu $\mathbb{N}$.*

Primjedba 5.1.6. *Lako se vidi da je svaki beskonačan podskup od $\mathbb{N}$ ekvipotentan skupu $\mathbb{N}$ i da je svaki podskup prebrojivog skupa konačan ili prebrojiv. No, možda je manje očigledno da je npr. prebrojiv i skup $\mathbb{N} \times \mathbb{N}$. Štoviše, takav je i skup $\mathbb{N}^k$ za proizvoljan $k \in \mathbb{N}$. Može se također pokazati da je unija konačnog broja prebrojivih ili konačnih skupova prebrojiv ili konačan skup.*

Sljedećim dvama teoremima zbog duljine preskačemo dokaz (zainteresirani ih mogu pronaći u [4]).

Teorem 5.1.11. *Za $m, n \in \mathbb{N}$ vrijedi jedna i samo jedna od sljedećih izreka:*

1. $m = n$,
2. $(\exists p \in \mathbb{N})\, m + p = n$,
3. $(\exists p \in \mathbb{N})\, n + p = m$.

Teorem 5.1.12. *(O regularnosti zbrajanja i množenja prirodnih brojeva) Ako su $m, p, q \in \mathbb{N}$, onda*

$$\begin{aligned} m + p &= m + q \Rightarrow p = q \quad i \\ mp &= mq \Rightarrow p = q. \end{aligned}$$

5.1.6. O uređenosti skupa $\mathbb{N}$

Na osnovi Teorema 5.1.11. i Teorema 5.1.12. možemo na skupu $\mathbb{N}$ uvesti strogi uređaj na sljedeći način: definiramo relaciju $<\subseteq \mathbb{N}\times\mathbb{N}$ s

$$(\forall n, m \in \mathbb{N})\, n < m \Leftrightarrow (\exists p \in \mathbb{N})\, m = n + p.$$

Lako se vidi da je relacija $<$ relacija strogog uređaja na $\mathbb{N}$, te da je $(\mathbb{N}, <)$ strogo uređen skup. Naime, relacija $<$ je irefleksivna jer ako bi za neki $n \in \mathbb{N}$ vrijedilo $n < n$, onda bi postojao $p \in \mathbb{N}$ takav da je $n = n + p$ što po Teoremu 5.1.6. nije moguće. Nadalje, ako je za neke $n, m, l \in \mathbb{N}$ ispunjeno $n < m$ i $m < l$, onda postoje p_1 i p_2 u $\mathbb{N}$ takvi da je $m = n + p_1$ i $l = m + p_2$. Iz ovoga slijedi

$$l = (n + p_1) + p_2 = n + (p_1 + p_2) = n + p_3, \quad p_3 \in \mathbb{N},$$

pa je $l < n$, čime je dokazano da je $<$ tranzitivna. I na kraju, po Teoremu 5.1.11. slijedi da su svaka dva različita elementa skupa $\mathbb{N}$ usporediva po $<$. Stoga je $(\mathbb{N}, <)$ strogo uređen skup.

Ova relacija strogog uređaja je na prirodan način povezana s operacijama zbrajanja i množenja na skupu $\mathbb{N}$:

1. Ako je $n < m$ i $n' < m'$, onda je $n + n' < m + m'$.

   Naime, $m = n + p$ i $m' = n' + p'$, pa je $m + m' = (n + n') + (p + p')$, tj. $n + n' < m + m'$;

2. Ako je $n < m$, onda je $nq < mq$ za bilo koji $q \in \mathbb{N}$.

   Naime, $m = n + p$, pa je $mq = (n + p)\, q = nq + pq,\ q \in \mathbb{N}$, te je $nq < mq$ za bilo koji $q \in \mathbb{N}$.

Ovakvo uređenje skupa $\mathbb{N}$ nazivamo *prirodnim uređenjem*. U odnosu na njega skup $\mathbb{N}$ ima najmanji element, i to je broj 1, jer za bilo koji $n \in \mathbb{N} \setminus \{1\}$ postoji $p \in \mathbb{N}$ takav da je $n = s\,(p)$, tj. $n = p + 1$, pa je $1 < n$.

Na skupu $\mathbb{N}$ možemo definirati relaciju $>\subseteq \mathbb{N}\times\mathbb{N}$ na način

$$n > m \Leftrightarrow m < n.$$

Ona je također stroga uređajna relacija. Nadalje, lako se pokaže da je relacija $\leq\subseteq \mathbb{N}\times\mathbb{N}$ definirana izrazom

$$n \leq m \Leftrightarrow n < m \vee n = m$$

relacija uređaja na skupu $\mathbb{N}$, pa je $(\mathbb{N}, \leq)$ uređen skup, kao i skup $(\mathbb{N}, \geq)$, gdje je

$$n \geq m \Leftrightarrow m \leq n.$$

Definicija 5.1.9. *Ako je S uređen skup i $f : \mathbb{N} \to S$ monotona funkcija onda f nazivamo* ***monotonim nizovima*** *elemenata skupa S.*

Definicija 5.1.10. *Neka je $(A, <)$ strogo uređen skup i neka su $x, y, z \in A$. Za elemenat y kažemo da* ***je između*** *elemenata x i z ako je $x < y < z$ ili je $z < y < x$. Strogo uređen skup $(A, <)$ je* ***diskretno uređen*** *skup ako za svaki $a \in A$ postoji $a' \in A$ takav da između a i a' nema elemenata iz A.*

Ako je skup $(A, <)$ diskretan, onda za svaki $a \in A$, $a \neq \max A$, postoji $a' \in A$ takav da je $a < a'$ i između a i a' nema elemenata iz A. Element a' se zove **neposredni sljedbenik** broja a. Također, za svaki $a \in A$, $a \neq \min A$, postoji $a'' \in A$ takav da je $a'' < a$ i između a'' i a nema elemenata iz A. Element a'' se zove **neposredni prethodnik** broja a.

Teorem 5.1.13. *Skup $(\mathbb{N}, <)$ je diskretno uređen skup. Za svaki $n \in \mathbb{N}$, broj $s(n)$ je neposredni sljedbenik broja n. Ako je $n \neq 1$, onda je neposredni prethodnik broja n broj m za koji je $s(m) = n$.*

Dokaz. Neka je $n \in \mathbb{N}$. Iz definicije relacije $<$ slijedi da je $n < n + 1 = s(n)$. Pretpostavimo da postoji neki $m \in \mathbb{N}$ takav da je $n < m < s(n)$. Iz $n < m$ slijedi da postoji neki $p \in \mathbb{N}$ takav da je $m = n + p$.
Ako je $p = 1$ onda je

$$m = n + p = n + 1 = s(n),$$

a to je u suprotnosti s pretpostavkom da je $m < s(n)$. Dakle, mora biti $p \neq 1$. No, u tom slučaju, zbog surjektivnosti funkcije $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$, postoji $q \in \mathbb{N}$ takav da je $p = s(q)$, pa je

$$m = n + p = n + s(q) = n + q + 1 = (n + 1) + q = s(n) + q,$$

što znači da je $s(n) < m$, a to nije moguće zbog pretpostavke da je $m < s(n)$. Dakle, ne postoji nijedan prirodan broj između n i $s(n)$, tj. $s(n)$ je neposredni prethodnik od n.
Neka je sada $n \in \mathbb{N}$ i $n \neq 1$. To znači da postoji neki $m \in \mathbb{N}$ takav da je $n = s(m)$. Budući da između m i $s(m)$ nema nijednog elementa iz $\mathbb{N}$ i da je $m < s(m) = n$, to je m neposredni prethodnik broja n. ■

Teorem 5.1.14. *Za svaki $n \in \mathbb{N}$ skup $L_n = \{m \in \mathbb{N} : m < n + 1\}$ je konačan.*

Dokaz. Vrijedi $L_1 = \{1\}$. Neka je $M \subseteq \mathbb{N}$ skup svih $n \in \mathbb{N}$ za koje je skup L_n konačan. Očito je $1 \in M$. Pretpostavimo da je $n \in M$. Iz prethodnog teorema slijedi da je $L_{n+1} = L_n \cup \{n + 1\}$. Kako je $n \in M$ to je L_n konačan, pa je konačan i L_{n+1}, tj. $n + 1 \in M$. Po $A4$) slijedi $M = \mathbb{N}$. ■

Teorem 5.1.15. *Skup $\mathbb{N}$ nema najvećeg elementa.*

Dokaz. Kako za svaki prirodni broj n vrijedi $n < n+1 = s(n)$, to $\mathbb{N}$ nema najvećeg elementa. ■

5.1.7. Djeljivost na skupu $\mathbb{N}$

Ovdje ćemo se detaljnije pozabaviti jednom relacijom parcijalnog uređaja vezanom uz skup prirodnih brojeva $\mathbb{N}$. To je relacija *djeljivosti*. Matematička disciplina koja, općenito govoreći, proučava svojstva prirodnih brojeva zove se *teorija brojeva*. Njezin najstariji dio je *elementarna teorija brojeva*, koja svoje začetke ima još u starohebrejskoj, starogrčkoj i starokineskoj matematici.
Temeljni pojam teorije brojeva je *djeljivost*.

Definicija 5.1.11. *Kažemo da broj $a \in \mathbb{N}$ **dijeli** broj $b \in \mathbb{N}$ ako postoji $k \in \mathbb{N}$ takav da je $b = ka$. U tom slučaju pišemo $a \mid b$. Kažemo još i da je broj b **djeljiv** brojem a, odnosno da je a **djelitelj** ili **divizor** broja b, ili pak da je b **višekratnik** broja a. Ukoliko broj $a \in \mathbb{N}$ ne dijeli broj $b \in \mathbb{N}$ pišemo $a \nmid b$.*

Prirodne brojeve koji su djeljivi s 2 zovemo *parnim* brojevima, dok sve ostale zovemo *neparnim* brojevima. Očito, skup prirodnih brojeva možemo podijeliti na dva disjunktna podskupa: skup parnih i skup neparnih brojeva.

Djeljivost je, dakle, jedna relacija na skupu $\mathbb{N}$ definirana na sljedeći način:

$$\mid = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \mid b\} \subseteq \mathbb{N} \times \mathbb{N}.$$

Pogledajmo neka važna svojstva ove relacije.

Propozicija 5.1.1. *Vrijedi:*

1. $(\forall a \in \mathbb{N})\, a \mid a$;
2. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(a \mid b \wedge b \mid a \rightarrow a = b)$;
3. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \wedge b \mid c \rightarrow a \mid c)$,

tj. relacija $\mid$ je relacija parcijalnog uređaja na skupu $\mathbb{N}$.

Dokaz. Za svaki prirodni broj a vrijedi $a = 1a$, tj. $a \mid a$, pa je relacija $\mid$ refleksivna. Neka su $a, b \in \mathbb{N}$ takvi da $a \mid b$ i $b \mid a$. Iz toga slijedi da postoje prirodni brojevi k_1 i k_2 takvi da je $b = k_1 a$ i $a = k_2 b$, pa je $b = k_1 k_2 b$. Jer je 1 jedini prirodni broj za koga vrijedi $1b = b$ (dokažite ovo sami!) zaključujemo da je $k_1 k_2 = 1$, a iz ovoga slijedi $k_1 = k_2 = 1$, tj. $a = b$. Dakle, relacija $\mid$ je antisimetrična.
I na kraju, pretpostavimo da su $a, b, c \in \mathbb{N}$ takvi da $a \mid b$ i $b \mid c$. Iz toga slijedi da postoje prirodni brojevi k_1 i k_2 takvi da je $b = k_1 a$ i $c = k_2 b$, pa je $c = k_2 k_1 a$. Označimo li $k_2 k_1 = k_3$ slijedi $c = k_3 a$, $k_3 \in \mathbb{N}$, pa $a \mid c$, tj. relacija $\mid$ je i tranzitivna. Iz svega ovoga slijedi da je relacija $\mid$ relacija parcijalnog uređaja na $\mathbb{N}$. ■

Očito je da $\mid$ nije relacija linearnog uređaja na $\mathbb{N}$, jer postoje prirodni brojevi koji nisu djeljivi međusobno ni u kojem poretku (npr. 2 i 5).

Djeljivost ima i neka dodatna lijepa svojstva.

Propozicija 5.1.2. *Vrijedi:*

1. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \wedge a \mid c \rightarrow a \mid b + c)$;
2. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \rightarrow a \mid bc)$.

Dokaz. Sami za vježbu. ■

Ako su $a, b \in \mathbb{N}$, onda skup S svih prirodnih brojeva koji dijele i a i b nije prazan (sigurno je $1 \in S$). Budući je skup S konačan, to on ima najveći element, označimo ga s $m(a, b)$. Broj $m(a, b)$ nazivamo *najvećom zajedničkom mjerom* brojeva a i b. Jasno je da vrijedi:

1. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\, m(a, b) = m(b, a)$;

2. $(\forall a \in \mathbb{N})\, m(a, a) = a$;

3. $(\forall a \in \mathbb{N})\, m(1, a) = 1$.

Definicija 5.1.12. *Kažemo da su prirodni brojevi a i b* ***relativno prosti*** *ako je $m(a, b) = 1$.*

Zadatak 1. *Dokažite da za prirodne brojeve a, b, c vrijedi:*

1. *Ako $a \mid b$, onda je $m(a, b) = a$;*

2. *Ako je $m(a, b) = 1$ i $a \mid bc$, onda $a \mid c$.*

5.1.8. Prosti brojevi

Često se postavlja pitanje koji sve brojevi dijele neki prirodni broj n. Uočimo najprije da je svaki prirodni broj n djeljiv s 1 i sa samim sobom. Iako naoko izgleda lako odrediti sve preostale djelitelje broja n, za velike brojeve n to postaje težak problem. Među svim prirodnim brojevima posebno se ističu oni koji nemaju drugih djelitelja osim jedinice i samih sebe.

Definicija 5.1.13. *Reći ćemo da je prirodni broj $p > 1$* ***prost*** *ako je djeljiv samo s 1 i sa samim sobom. Prirodne brojeve veće od 1 koji nisu prosti zovemo* ***složenim*** *brojevima.*

Dakle, skup prirodnih brojeva možemo podijeliti na tri međusobno disjunktna podskupa: $\{1\}$, skup P prostih brojeva i skup S složenih brojeva. Ti skupovi čine particiju skupa $\mathbb{N}$.

Početni dio skupa prostih brojeva P izgleda ovako:

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots\}.$$

Uočimo da je 2 najmanji prost broj i ujedno jedini paran prost broj. Svi preostali prosti brojevi su neparni.

Zanimljiv je problem odrediti sve proste brojeve manje ili jednake nekomu zadanom prirodnom broju n. Jednostavnu metodu za to je pronašao starogrčki matematičar Eratosten, pa se ona naziva *Eratostenovo sito*. Postupak je sljedeći: najprije napišemo sve prirodne brojeve manje ili jednake n.

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots, n.$$

Potom prekrižimo broj 1 jer on nije prost broj. Najmanji prosti broj je $p_1 = 2$, pa prekrižimo sve višekratnike broja 2 veće od njega. Najmanji od preostalih brojeva je 3, koji je prost, pa je $p_2 = 3$ (naravno, ako je $n > 2$). Nakon toga prekrižimo sve višekratnike broja 3 veće od 3. Ostali su

$$2, 3, 5, 7, 11, 13, 17, \ldots, n.$$

Postupak nastavljamo za $p_3 = 5$, tj. s višekratnicima broja 5 itd. Na kraju će u nizu preostati samo prosti brojevi.

Uz proste brojeve vezano je mnoštvo problema koje je lako razumjeti, ali teško riješiti. Neki od njih su postavljeni u davnoj prošlosti, a ni do danas nisu riješeni. Jedan od najpoznatijih je tzv. *Goldbachova slutnja*, koju je postavio njemački matematičar Christian Goldbach (1690 − 1764) u svom pismu Euleru 1742. Ona glasi:

Svaki paran prirodan broj veći od 2 se može prikazati kao zbroj dva prosta broja.

Npr. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7, \ldots$
Na neka pitanja vezana uz proste brojeve ipak znamo odgovoriti. Najvažniji je sljedeći teorem.

Teorem 5.1.16. *(Euklid) Prostih brojeva ima beskonačno mnogo.*

Da bismo dokazali ovaj teorem trebat će nam jedna lema.

Lema 5.1.2. *Svaki prirodni broj veći od* 1 *može se prikazati kao umnožak od jednog ili više prostih brojeva.*

Dokaz. Pretpostavimo suprotno, tj. da postoji neki prirodni broj veći od 1 koji nije umnožak prostih brojeva. Tada je skup $M \subset \mathbb{N}$ u kojemu su svi takvi brojevi neprazan, pa M ima najmanji element, označimo ga s m. On sigurno nije prost jer bi se u tom slučaju mogao prikazati kao umnožak jednog prostog broja. Kako je $m \neq 1$ zaključujemo da je m složen broj. Stoga postoje prirodni brojevi m_1 i m_2 takvi da je $m = m_1 m_2$ i $1 < m_1, m_2 < m$. No kako je m najmanji element skupa M, a m_1 i m_2 su manji od njega, to odmah slijedi da $m_1, m_2 \notin M$ pa se brojevi m_1 i m_2 mogu prikazati kao umnošci prostih brojeva, a onda se tako može prikazati i $m = m_1 m_2$, što je u kontradikciji s početnom pretpostavkom. Dakle, skup M mora biti prazan i svaki se prirodni broj veći od 1 može prikazati kao umnožak od jednog ili više prostih brojeva. ■
Sada dajemo dokaz teorema.
Dokaz. Označimo s $p_1, p_2, p_3, \ldots$ proste brojeve u rastućem poretku. Odaberimo proizvoljan prost broj, neki p_n. Dokazat ćemo da postoji prost broj veći od njega, iz čega odmah slijedi da je skup P prostih brojeva beskonačan.
Uzmimo broj $N = p_1 p_2 p_3 \cdots p_n + 1$. Očito je $N > 1, p_1, p_2, p_3, \ldots, p_n$ i N nije djeljiv ni s jednim od brojeva $p_1, p_2, p_3, \ldots, p_n$. Ako je broj N prost dokaz je gotov jer smo pronašli prost broj veći od p_n. Ako je N složen, onda je on prema prethodnoj lemi djeljiv nekim prostim brojem p, a kako N nije djeljiv ni s jednim od brojeva $p_1, p_2, p_3, \ldots, p_n$ to slijedi da je $p > p_n$, pa smo opet našli prost broj veći od p_n. Time je dokaz završen. ■

U Lemi 5.1.2. smo dokazali da se svaki prirodni broj veći od 1 može prikazati kao umnožak jednog ili više prostih brojeva, tj. može se *rastaviti na proste faktore*. Lema osigurava postojanje takvog rastava, no može se pokazati i da je takav rastav jedinstven do na poredak faktora. O tomu govori sljedeći teorem.

Teorem 5.1.17. *(Osnovni teorem aritmetike) Za svaki prirodni broj $n > 1$ postoje jedinstveni prirodni brojevi $k, \alpha_1, \ldots, \alpha_k$ i jedinstveni prosti brojevi $p_1 < \cdots < p_k$ takvi da je*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Dokaz. Jedinstvenost brojeva $k, \alpha_1, \ldots, \alpha_k$ i $p_1, \ldots, p_k$ je jednostavna posljedica činjenice da iz $m(a,b) = 1$ i $a \mid bc$ slijedi $a \mid c$ (vidi prethodni zadatak), a uzimajući u obzir da je za svaka dva različita prosta broja p i q uvijek $m(p,q) = 1$. ■
Rastav opisan u prethodnom teoremu nazivamo *kanonskim rastavom* broja n.

Primjer 22. $18 = 2^1 3^2,\ 35 = 5^1 7^1,\ 180 = 2^2 3^2 5^1$.

5.2. Skup cijelih brojeva

5.2.1. Uvod

Cijeli brojevi se uvode zbog toga što je oduzimanje općenito neizvedivo u skupu prirodnih brojeva. Svaki cijeli broj je oblika $m - n$, gdje su m i n neki prirodni brojevi. Pri tomu za cijele brojeve $m - n$ i $p - q$ vrijedi:

1. $m - n = p - q$ ako i samo ako $m + q = p + n$,
2. $(m - n) + (p - q) = (m + p) - (n + q)$,
3. $(m - n)(p - q) = (mp + nq) - (mq + np)$.

Iz ovoga je vidljivo da cijele brojeve trebamo promatrati kao uređene parove prirodnih brojeva, odnosno kao elemente skupa $\mathbb{N}\times\mathbb{N}$. Stoga ćemo definirati posebnu relaciju ekvivalencije $\sim$ na skupu $\mathbb{N} \times \mathbb{N}$ i pokazati da skup $\mathbb{N} \times \mathbb{N} \mid\sim$ ima svojstva skupa cijelih brojeva na koja smo navikli. Čitava konstrukcija se oslanja na sljedeći teorem.

Teorem 5.2.1. *Neka je relacija $\sim$ na $\mathbb{N} \times \mathbb{N}$ definirana sa*

$$(m,n) \sim (p,q) \Leftrightarrow m + q = p + n.$$

Tada vrijedi:

1. *Relacija $\sim$ je relacija ekvivalencije na $\mathbb{N} \times \mathbb{N}$;*
2. *Iz $(m,n) \sim (m',n')$ i $(p,q) \sim (p',q')$ slijedi*

$$\begin{aligned} (m+p, n+q) &\sim (m'+p', n'+q'), \\ (mp+nq, mq+np) &\sim (m'p'+n'q', m'q'+n'p'). \end{aligned}$$

Dokaz. Dokažimo najprije da je $\sim$ relacija ekvivalencije na $\mathbb{N} \times \mathbb{N}$. Očito je za sve $(m,n) \in \mathbb{N}\times\mathbb{N}$ ispunjeno $(m,n) \sim (m,n)$, jer je $m+n = m+n$, pa je $\sim$ refleksivna. Neka su $(m,n), (p,q) \in \mathbb{N}\times\mathbb{N}$ takvi da je $(m,n) \sim (p,q)$. Tada je $m+q = p+n$, no zbog svojstava zbrajanja prirodnih brojeva slijedi $p+n = m+q$, pa je $(p,q) \sim (m,n)$. Dakle, relacija $\sim$ je simetrična. I na kraju, neka su $(m,n), (p,q), (r,s) \in \mathbb{N} \times \mathbb{N}$ takvi da je$(m,n) \sim (p,q)$ i $(p,q) \sim (r,s)$. Iz ovoga slijedi

$$\left.\begin{matrix} m+q = p+n \\ p+s = r+q \end{matrix}\right\}+$$

pa je

$$(m+s)+(p+q)=(r+n)+(p+q) \overset{\text{Tm } 5.1.12.}{\Rightarrow} m+s=r+n.$$

Iz ovoga, pak, slijedi da je $(m,n)\sim(r,s)$, pa je relacija $\sim$ i tranzitivna. Time smo dokazali da je $\sim$ relacija ekvivalencije na $\mathbb{N}\times\mathbb{N}$.
Dokažimo i drugu tvrdnju. Neka je $(m,n)\sim(m',n')$ i $(p,q)\sim(p',q')$. Iz ovoga slijedi da je $m+n'=m'+n$ i $p+q'=p'+q$. Stoga je

$$\begin{aligned}(m+p)+(n'+q') &= (m+n')+(p+q')=(m'+n)+(p'+q)\\ &= (m'+p')+(n+q).\end{aligned}$$

Iz ovoga odmah slijedi da je $(m+p,n+q)\sim(m'+p',n'+q')$.
Slično se dokaže i da je $(mp+nq,mq+np)\sim(m'p'+n'q',m'q'+n'p')$. ■

Definicija 5.2.1. *Neka je $\sim$ relacija na $\mathbb{N}\times\mathbb{N}$ definirana sa*

$$(m,n)\sim(p,q)\Leftrightarrow m+q=p+n.$$

*Skup $\mathbb{Z}=\mathbb{N}\times\mathbb{N}\,|\!\sim$ nazivamo **skupom cijelih brojeva**, a njegove elemente nazivamo **cijelim brojevima**.*

5.2.2. Zbrajanje i množenje na $\mathbb{Z}$

Podsjetimo se da smo sa $\tau: A\to A\,|_{\sim}$, $\tau(a)=[a]$, definirali funkciju projekcije vezanu uz neku relaciju ekvivalencije $\sim$ na skupu A. U našem slučaju ćemo promatrati relaciju ekvivalencije $\sim$ na skupu $\mathbb{N}\times\mathbb{N}$ pomoću koje smo definirali cijele brojeve. Projekcija $\tau:\mathbb{N}\times\mathbb{N}\to\mathbb{N}\times\mathbb{N}\,|\!\sim$, $\tau(m,n)=[(m,n)]$, svakom uređenom paru prirodnih brojeva (m,n) pridružuje njemu pripadnu klasu ekvivalencije po relaciji $\sim$, tj. cijeli broj $[(m,n)]$. Može se pokazati (dokaz zbog duljine preskačemo, vidi [4]) da za proizvoljne $(m,n),(p,q)\in\mathbb{N}\times\mathbb{N}$ vrijedi:

1. $\tau(m,n)+\tau(p,q)=\tau(m+p,n+q)$;
2. $\tau(m,n)\,\tau(p,q)=\tau(mp+nq,mq+np)$.

Dakle, projekcija τ nam omogućava da operacije zbrajanja i množenja, koje smo već definirali na skupu $\mathbb{N}$, proširimo i na skup $\mathbb{Z}$, a da se pri tomu sačuvaju sva ona svojstva zbrajanja i množenja koja smo opisali u prethodnoj točki: komutativnost, asocijativnost i distributivnost.
Posebno izdvajamo cijeli broj $\tau(1,1)$. Taj se element označava s 0 i zove *nula* u $\mathbb{Z}$. Lako se vidi da je $a+0=0+a=a$ za svaki $a\in\mathbb{Z}$ i 0 je jedini element s ovim svojstvom. Elementi skupa $\mathbb{Z}$ imaju još jedno važno svojstvo koje je opisano narednim teoremom.

Teorem 5.2.2. *Za svaki $a\in\mathbb{Z}$ postoji jedinstveni $a'\in\mathbb{Z}$ takav da je*

$$a+a'=a'+a=0.$$

Dokaz. Neka je $a = \tau(m,n) \in \mathbb{Z}$. Tada za cijeli broj $a' = \tau(n,m)$ vrijedi

$$a + a' = \tau(m,n) + \tau(n,m) = \tau(m+n, n+m) = \tau(m+n, m+n).$$

Kako je $(m+n, m+n) \sim (1,1)$ (jer je $m+n+1 = 1+m+n$), to je

$$\begin{aligned} \tau(m+n, m+n) &= \tau(1,1) = 0, \text{ tj.} \\ a + a' &\overset{kom}{=} a' + a = 0. \end{aligned}$$

Dokažimo jedinstvenost elementa a'. Pretpostavimo da za neki $b \in \mathbb{Z}$ vrijedi da je $a + b = b + a = 0$. Tada je

$$b = b + 0 = b + (a + a') \overset{asoc}{=} (b + a) + a' = 0 + a' = a'.$$

■

Element a' sa svojstvom $a + a' = a' + a = 0$ nazivamo *suprotnim* ili *inverznim* elementom elementa a, a u daljnjemu ćemo ga označavati s $-a$ (minus a). Dakle, $-a \in \mathbb{Z}$ je po definiciji onaj element za koga vrijedi

$$a + (-a) = (-a) + a = 0.$$

Primijetimo da je za $a = \tau(m,n)$ njemu suprotni element $-a = \tau(n,m)$, što se vidi iz dokaza prethodnog teorema. Također, zbog jedinstvenosti suprotnog elementa lako se vidi da je $-(-a) = a$.
Zbroj $b + (-a)$ piše se kao $b - a$ i zove *razlika* elemenata b i a. Uočimo, također, da za $b = \tau(k,l)$ i $a = \tau(m,n)$ vrijedi

$$\begin{aligned} b - a &= \tau(k,l) + [-\tau(m,n)] = \tau(k,l) + \tau(n,m) = \tau(k+n, l+m) \\ &= -\tau(l+m, k+n) = -[\tau(l,k) + \tau(m,n)] = -(-b+a) = -(a-b), \end{aligned}$$

tj. izmjenimo li poredak prilikom oduzimanja dobit ćemo element suprotan onomu kojega bismo dobili u prvobitnom poretku.

5.2.3. O uređenosti skupa $\mathbb{Z}$

Strogu uređajnu relaciju na skupu $\mathbb{Z}$ uvodimo na osnovi sljedećeg teorema.

Teorem 5.2.3. *Skup $P = \{\mathbb{Z}_-, \mathbb{Z}_0, \mathbb{Z}_+\}$ je jedna particija skupa $\mathbb{Z}$, pri čemu je*

$$\begin{aligned} \mathbb{Z}_+ &= \{\tau(n+1,1) : n \in \mathbb{N}\}, \\ \mathbb{Z}_- &= \{\tau(1,n+1) : n \in \mathbb{N}\}, \\ \mathbb{Z}_0 &= \{0\}. \end{aligned}$$

Dokaz. Neka je $a = \tau(p,q) \in \mathbb{Z}$. Po Teoremu 5.1.11. znamo da za prirodne brojeve p i q postoji samo jedna od tri mogućnosti:

$$\begin{aligned} p &= q + n, \text{ za neki } n \in \mathbb{N}, \\ q &= p + n, \text{ za neki } n \in \mathbb{N}, \\ p &= q. \end{aligned}$$

Ako je $p = q + n$, onda je $(p, q) \sim (n + 1, 1)$, pa je $a = \tau(p, q) = \tau(n + 1, 1) \in \mathbb{Z}_+$.
Ako je $q = p + n$, onda je $(p, q) \sim (1, n + 1)$, pa je $a = \tau(p, q) = \tau(1, n + 1) \in \mathbb{Z}_-$.
I na kraju, ako je $p = q$, onda je $(p, p) \sim (1, 1)$, pa je $a = \tau(p, p) = \tau(1, 1) = 0 \in \mathbb{Z}_0$.
Iz ovoga slijedi da je $\mathbb{Z} \subseteq \mathbb{Z}_- \cup \mathbb{Z}_0 \cup \mathbb{Z}_+$. No, kako su $\mathbb{Z}_-, \mathbb{Z}_0, \mathbb{Z}_+ \subset \mathbb{Z}$ odmah slijedi i

$$\mathbb{Z} = \mathbb{Z}_- \cup \mathbb{Z}_0 \cup \mathbb{Z}_+.$$

Nadalje, za bilo koji $n \in \mathbb{N}$ par $(n + 1, 1) \nsim (1, 1)$ i $(n + 1, 1) \nsim (1, 1)$, pa je $\tau(n + 1, 1) \neq 0$ i $\tau(1, n + 1) \neq 0$. Stoga je $\mathbb{Z}_- \cap \mathbb{Z}_0 = \emptyset$ i $\mathbb{Z}_+ \cap \mathbb{Z}_0 = \emptyset$. Isto tako, nema prirodnih brojeva m i n takvih da je $(n + 1, 1) \sim (1, m + 1)$ (jer bi to značilo da je $(n + m) + 2 = 2$ što je po 5.1.6. nemoguće), pa je $\mathbb{Z}_- \cap \mathbb{Z}_+ = \emptyset$. ■

Elementi skupa $\mathbb{Z}_+$ zovu se *strogo pozitivni* cijeli brojevi, a elementi skupa $\mathbb{Z}_-$ *strogo negativni* cijeli brojevi.
Iz prethodnog teorema slijedi da je $\{\mathbb{Z}_-, \mathbb{Z}_0, \mathbb{Z}_+\}$ jedna particija skupa $\mathbb{Z}$. Nadalje, lako se vidi da iz $a \in \mathbb{Z}_+$ slijedi $-a \in \mathbb{Z}_-$ i obratno.

Teorem 5.2.4. *Relacija $\rho \subseteq \mathbb{Z} \times \mathbb{Z}$ definirana sa*

$$\rho = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b - a \in \mathbb{Z}_+\}$$

je relacija strogog uređaja na $\mathbb{Z}$.

Dokaz. Za proizvoljna dva $a, b \in \mathbb{Z}$, po Teoremu 5.2.3., vrijedi samo jedno od troje:

$$b - a \in \mathbb{Z}_+,\ b - a \in \mathbb{Z}_- \ \text{ ili } \ b - a \in \mathbb{Z}_0.$$

Ako je $b - a \in \mathbb{Z}_+$, onda je $(a, b) \in \rho$.
Ako je $b - a \in \mathbb{Z}_-$, onda postoji $n \in \mathbb{N}$ takav da je $b - a = \tau(1, n + 1)$. Odavde je

$$a - b = -\tau(1, n + 1) = \tau(n + 1, 1),$$

pa je $a - b \in \mathbb{Z}_+$, tj. $(b, a) \in \rho$. Dakle, svi različiti elementi iz $\mathbb{Z}$ su usporedivi.
Ako je $b - a \in \mathbb{Z}_0$, onda je $b - a = 0$, tj. $a = b$, a kako je $a - a = 0 \notin \mathbb{Z}_+$, to $(a, a) \notin \rho$ pa je ρ irefleksivna. I na kraju, relacija ρ je i tranzitivna. Naime, ako je $(a, b) \in \rho$ i $(b, c) \in \rho$, onda je

$$\left.\begin{array}{ll} b - a \in \mathbb{Z}_+, & \text{tj. } b - a = \tau(n + 1, 1),\ n \in \mathbb{N}, \\ c - b \in \mathbb{Z}_+, & \text{tj. } c - b = \tau(m + 1, 1),\ m \in \mathbb{N}. \end{array}\right\} +$$

Odatle slijedi

$$c - a = \tau(m + 1, 1) + \tau(n + 1, 1) = \tau(n + m + 1 + 1, 1 + 1) = \tau(n + m + 1, 1) \in \mathbb{Z}_+,$$

pa je $(a, c) \in \rho$. ■
Dakle, Teorem 5.2.4. nam garantira da je ρ relacija strogog uređaja na $\mathbb{Z}$. Tu relaciju označavamo s $<$ i pišemo $a < b$ kad god je (a, b) element te relacije. Zbog irefleksivnosti je $a \not< a$, a zbog tranzitivnosti iz $a < b$ i $b < c$ slijedi $a < c$. Nadalje, za svaka dva cijela broja a i b vrijedi točno jedno od troje: $a = b$, $a < b$ ili $b < a$. Pomoću relacije $<$ uvodimo relaciju $>$ sa $a > b \Leftrightarrow b < a$, koja je također relacija strogog uređaja na $\mathbb{Z}$, te preko njih relacije $\leq$ i $\geq$ koje su relacije uređaja na $\mathbb{Z}$.

Vrijedi: $a \in \mathbb{Z}_+$ ako i samo ako je $a > 0$. Naime, $a \in \mathbb{Z}_+ \Leftrightarrow a - 0 = a \in \mathbb{Z}_+ \Leftrightarrow 0 < a$.
Analogno, $a \in \mathbb{Z}_-$ ako i samo ako je $a < 0$.

Teorem 5.2.5. *Za elemente skupa $\mathbb{Z}$ vrijedi sljedeće:*

1. $(a > 0 \wedge b > 0) \Rightarrow (a + b > 0)$,
2. $(a > 0 \wedge b > 0) \Rightarrow (ab > 0)$,
3. $(a > 0 \wedge b < 0) \Rightarrow (ab < 0)$,
4. $(a < 0 \wedge b < 0) \Rightarrow (ab > 0)$,
5. $(a < b) \Rightarrow (\forall c \in \mathbb{Z})\,(a + c < b + c)$,
6. $a \neq 0 \Rightarrow a^2 = a \cdot a > 0$,
7. $ab = 0 \Rightarrow (a = 0 \vee b = 0)$,
8. $(ab = ac \wedge a \neq 0) \Rightarrow b = c$.

Dokaz. Za ilustraciju ćemo dokazati četvrtu tvrdnju. Neka su $a, b \in \mathbb{Z}$ takvi da je $a < 0$ i $b < 0$. To znači da je $a \in \mathbb{Z}_-$ i $b \in \mathbb{Z}_-$, pa postoje $n, m \in \mathbb{N}$ takvi da je

$$\begin{aligned} a &= \tau(1, n+1), \\ b &= \tau(1, m+1). \end{aligned}$$

No tada je

$$\begin{aligned} ab &= \tau(1, n+1)\,\tau(1, m+1) = \tau(1 + (n+1)(m+1), m + 1 + n + 1) \\ &= \tau(mn + 1 + (m + n + 1), 1 + (m + n + 1)) = \tau(mn + 1, 1) \in \mathbb{Z}_+. \end{aligned}$$

■

5.2.4. Ulaganje prirodnih u cijele brojeve

Vidjeli smo iz prethodnog da za svaki $a \in \mathbb{Z}_+$ postoji jedan i samo jedan $n \in \mathbb{N}$ takav da vrijedi $a = \tau(n + 1, 1)$. Na taj način je zadan jedan niz $j : \mathbb{N} \to \mathbb{Z}_+$, gdje je $j(n) = \tau(n + 1, 1)$. Lako se pokaže da niz j ima sljedeća svojstva:

1. j bijektivno preslikava $\mathbb{N}$ na $\mathbb{Z}_+$,
2. $j(m + n) = \tau(m + n + 1, 1) = \tau(m + n + 1 + 1, 1 + 1)$
   $= \tau(m + 1, 1) + \tau(n + 1, 1) = j(m) + j(n)$ (j prenosi zbrajanje iz $\mathbb{N}$ u $\mathbb{Z}_+$),
3. $j(mn) = \tau(mn + 1, 1) = \tau(mn + m + n + 1 + 1, m + n + 1 + 1)$
   $= \tau(m + 1, 1)\,\tau(n + 1, 1) = j(m)\,j(n)$ (j prenosi množenje iz $\mathbb{N}$ u $\mathbb{Z}_+$),
4. $(m < n) \Leftrightarrow (j(m) < j(n))$ (j prenosi uređaj sa $\mathbb{N}$ u uređaj u $\mathbb{Z}_+$).

Zahvaljujući svojstvima funkcije j možemo na neki način poistovijetiti skupove $\mathbb{N}$ i $\mathbb{Z}_+ = j(\mathbb{N})$. Naime, svaki teorem dokazan u $\mathbb{N}$ pomoću j prelazi u teorem u $\mathbb{Z}_+$ i obratno. Kažemo stoga da smo $\mathbb{N}$ *uložili* u $\mathbb{Z}$. Nadalje, može se pokazati da uređena trojka $(\mathbb{Z}_+, s', j(1))$, gdje je $s' : \mathbb{Z}_+ \to \mathbb{Z}_+$ definirana izrazom $s'(j(n)) = j(n + 1)$, zadovoljava Peanove aksiome $A1 - A4$. Prema tomu, $\mathbb{Z}_+$ je skup prirodnih

brojeva isto toliko koliko je i skup $\mathbb{N}$. Stoga smatramo da su elementi $n \in \mathbb{N}$ i $j(n) = \tau(n+1,1) \in \mathbb{Z}_+$ identični, pa s n označavamo cijeli broj $\tau(n+1,1)$. Tako npr. umjesto $\tau(2,1)$ pišemo 1, umjesto $\tau(3,1)$ pišemo 2 itd. No također, umjesto $\tau(1,n+1) = -\tau(n+1,1)$ pišemo $-n$ (suprotni broj broju $n \in \mathbb{N}$). Sada lako vidimo da vrijedi

$$(-1)(-1) = \tau(1,2)\tau(1,2) = \tau(1\cdot 1 + 2\cdot 2, 1\cdot 2 + 2\cdot 1) = \tau(2,1) = 1,$$

i isto tako

$$(-1)n = \tau(1,2)\tau(n+1,1) = \tau(n+1+2, 1+2n+2) = \tau(1,n+1) = -n.$$

Ovako definiran skup $\mathbb{Z}$ ima svojstva skupa cijelih brojeva na koja smo navikli, a strogo je zasnovan.

Vidjeli smo da postoji bijekcija između skupa $\mathbb{N}$ i skupa $\mathbb{Z}_+$ koji je pravi podskup skupa $\mathbb{Z}$. Iz toga slijedi da je $\mathbb{Z}_+$ prebrojiv, a onda posredno i da je $\mathbb{Z}_-$ prebrojiv jer je $\mathbb{Z}_+ \cong \mathbb{Z}_-$. Iz već spomenute činjenice da je unija konačnog broja prebrojivih skupova prebrojiva odmah slijedi da je $\mathbb{Z}$ prebrojiv. No pokazat ćemo to direktno ustanovivši jednu bijekciju između skupova $\mathbb{N}$ i $\mathbb{Z}$. Iz toga će nam slijediti da je $\operatorname{kard}(\mathbb{Z}) = \aleph_0$.

Teorem 5.2.6. *Skup $\mathbb{Z}$ je prebrojiv.*

Dokaz. Definirajmo funkciju $f : \mathbb{Z} \to \mathbb{N}$ sa

$$f(m) = \begin{cases} 2(-m)+1, & m \in \mathbb{Z}_- \\ 1, & m \in \mathbb{Z}_0 \\ 2m, & m \in \mathbb{Z}_+ \end{cases}.$$

Očito je f dobro definirana funkcija (to nam garantira Teorem 5.2.3. i činjenica da smo poistovjetili $\mathbb{N}$ i $\mathbb{Z}_+$). Pokazat ćemo da je f bijekcija.
Neka je $n \in \mathbb{N}$. Ako je $n = 1$, onda je $n = f(0)$. Ako je n paran broj, onda postoji neki $m \in \mathbb{N}$ takav da je $n = 2m$. No kako je $\mathbb{N} \cong \mathbb{Z}_+$, to je $n = 2m = f(m)$, $m \in \mathbb{Z}_+$ (uočimo da je u stvari m poistovjećen s $j(m) = \tau(m+1,1)$). I na kraju, ako je n neparan broj veći od jedan, onda postoji neki $m \in \mathbb{N}$ takav da je $n = 2m+1$, pa je $n = f(m)$, $m \in \mathbb{Z}_-$, jer je u tom slučaju $-m \in \mathbb{Z}_+$. Dakle, za svaki $n \in \mathbb{N}$ postoji neki $m \in \mathbb{Z}$ takav da je $n = f(m)$, pa je f surjekcija.

Neka su $m, m' \in \mathbb{Z}$ takvi da je $f(m) = f(m')$. S obzirom na to kako je definirana funkcija f vidimo da m i m' moraju biti oba u istom dijelu particije skupa $\mathbb{Z}$ (ili oba u $\mathbb{Z}_-$ ili oba u $\mathbb{Z}_+$ ili oba jednaka 0). U svakom slučaju, koristeći svojstva prirodnih brojeva lako dobijemo $m = m'$. Dakle, f je injekcija, pa je i bijekcija.

Stoga je $\mathbb{Z} \cong \mathbb{N}$ i $\operatorname{kard}(\mathbb{Z}) = \aleph_0$. ■

Teorem 5.2.7. *Skup $\mathbb{Z}$ nema ni najmanjeg ni najvećeg elementa.*

Dokaz. Kako $\mathbb{Z}_+$ poistovjećujemo sa skupom $\mathbb{N}$, a $\mathbb{N}$ nema najveći element, to ga nema ni $\mathbb{Z}_+$. Svi elementi skupova $\mathbb{Z}_-$ i $\mathbb{Z}_0$ su manji od svih elemenata skupa $\mathbb{Z}_+$, pa, dakle, ni sam $\mathbb{Z}$ nema najveći element. Zbog $-\mathbb{Z}_+ = \mathbb{Z}_-$ simetrično slijedi tvrdnja o najmanjem elementu. ■

5.2.5. Djeljivost na skupu $\mathbb{Z}$

Pojam djeljivosti definiran na skupu $\mathbb{N}$ možemo lako proširiti i na cijele brojeve. Naime, jednostavno kažemo da broj $a \in \mathbb{Z} \setminus \{0\}$ *dijeli* broj $b \in \mathbb{Z}$ ako postoji $k \in \mathbb{Z}$ takav da je $b = ka$.

Zadatak 1. *Dokažite da relacija djeljivosti na $\mathbb{Z}$ ima sljedeća svojstva:*

1. $(\forall a \in \mathbb{Z} \setminus \{0\})\, a \mid a$;
2. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(a \mid b \wedge b \mid a \to a = \pm b)$;
3. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \wedge b \mid c \to a \mid c)$;
4. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \wedge a \mid c \to a \mid b \pm c)$;
5. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \to a \mid bc)$.

Slično kao u slučaju prirodnih brojeva, postoje i parovi cijelih brojeva koji nisu djeljivi ni u kojem poretku. No i u tom slučaju možemo reći nešto o tim brojevima, a što, to nam govori vrlo važan rezultat elementarne teorije brojeva.

Teorem 5.2.8. *(Teorem o dijeljenju s ostatkom) Za svaki $a \in \mathbb{N}$ i svaki $b \in \mathbb{Z}$ postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je $0 \leq r < a$ i $b = qa + r$.*

Dokaz. Neka je $a \in \mathbb{N}$ i $b \in \mathbb{Z}$. Promotrimo skup

$$S = \{b - ax : x \in \mathbb{Z}\} = \{\ldots, b - 2a, b - a, b, b + a, b + 2a, \ldots\}.$$

Očito, poredamo li elemente skupa S ovako kako su gore napisani, dobit ćemo rastući niz cijelih brojeva. Kako je $S \subset \mathbb{Z}$, iz toga slijedi $S \cap \mathbb{N}_0 \neq \emptyset$. Kako je $S \cap \mathbb{N}_0 \subset \mathbb{N}_0$, to sigurno postoji jedinstveni broj $r = \min S \cap \mathbb{N}_0$. Jer je $r \in S$ i $r \in \mathbb{N}_0$, to je $0 \leq r = b - aq$ za neki jedinstveni $q \in \mathbb{Z}$. Tvrdimo da je $r < a$. Pretpostavimo suprotno, tj. da je $r = b - aq \geq a$. Tada je

$$\begin{aligned} a &\leq b - aq = r \quad |+(-a) \Rightarrow \\ 0 &\leq b - aq - a = r - a \Leftrightarrow \\ 0 &\leq b - (q+1)\,a = r - a < r, \end{aligned}$$

pa smo našli broj $b - (q + 1)\, a \in S \cap \mathbb{N}_0$ koji je manji od r, a to je u kontradikciji s minimalnošću elementa r u skupu $S \cap \mathbb{N}_0$. Dakle, pronašli smo jedinstvene brojeve $q, r \in \mathbb{Z}$ takve da je $0 \leq r < a$ i $b = qa + r$. ■

Broj q iz ovog teorema zovemo *količnik* ili *kvocijent*, a broj r *ostatak* pri dijeljenju broja b brojem a. Broj a zovemo *djelitelj* ili *divizor*, a broj b *djeljenik* ili *dividend*.

Primjer 23. $25 = 3 \cdot 7 + 4$, $-25 = (-4) \cdot 7 + 3$, *ali ne* $-25 = (-3) \cdot 7 - 4$.

Primjedba 5.2.1. *Primijetimo da $a \mid b$ ako i samo ako je ostatak r pri dijeljenju b s a jednak nuli.*

Primjedba 5.2.2. *Uočimo da je* $m(a,b) = m(r,a)$, *gdje je* r *ostatak pri dijeljenju broja* b *brojem* a. *Naime, iz* $b = qa + r$ *slijedi da kada god neki* $c \mid a$ *i* $c \mid b$, *onda i* $c \mid r$, *pa* $m(a,b) \mid r$. *Iz ovoga slijedi* $m(a,b) \mid m(r,a)$. *No analogno se dobije i da* $m(r,a) \mid m(a,b)$, *pa je* $m(a,b) = m(r,a)$.

Vrijednost funkcije najveće zajedničke mjere $m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ na uređenom paru $(a,b) \in \mathbb{N} \times \mathbb{N}$, $a < b$, dobiva se tzv. *Euklidovim algoritmom* (kako je $m(a,b) = m(b,a)$ dovoljno je uzeti da je $a < b$)

$$\begin{aligned} b &= q_1 a + r_1, \quad 0 < r_1 < a \\ a &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1}, \quad r_{n+1} = 0. \end{aligned}$$

Očito, kako je $a > r_1 > r_2 > \cdots > r_{n+1} \geq 0$ proces završava nakon konačno mnogo koraka, tj. postoji $n \in \mathbb{N}_0$ takav da je $r_{n+1} = 0$ i $r_n > 0$ (pri tomu uzimamo da je $r_0 = a$). No tada je $r_{n-1} = q_{n+1} r_n$, pa je

$$\begin{aligned} m(a,b) &= m(r_1,a) \\ &= m(r_2,r_1) \\ &\vdots \\ &= m(r_n, r_{n-1}) \\ &= r_n. \end{aligned}$$

Dakle, $m(a,b) = r_n$.
Iz gornjeg algoritma se odmah dobije

$$(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\exists c \in \mathbb{N})\,(\exists d \in \mathbb{N})\, m(a,b) = ac + bd.$$

Primjer 24. *Neka je* $a = 30$ *i* $b = 135$. *Po Euklidovom algoritmu dobijemo*

$$\begin{aligned} 135 &= 4 \cdot 30 + 15 \\ 30 &= 2 \cdot 15 + 0, \end{aligned}$$

pa je

$$m(30,135) = 15$$

i

$$15 = 1 \cdot 135 + (-4) \cdot 30.$$

Primjer 25. *Neka je* $a = 42$ *i* $b = 165$. *Po Euklidovom algoritmu dobijemo*

$$\begin{aligned} 165 &= 3 \cdot 42 + 39 \\ 42 &= 1 \cdot 39 + 3 \\ 39 &= 13 \cdot 3 + 0, \end{aligned}$$

pa je

$$m(42,165) = 3$$

i

$$\begin{aligned} 3 &= 42 - 1 \cdot 39 = 42 - 1 \cdot (165 - 3 \cdot 42) \\ &= 42 + 3 \cdot 42 - 1 \cdot 165 = 4 \cdot 42 + (-1) \cdot 165. \end{aligned}$$

5.2.6. Kongruencije

Teorem o dijeljenju s ostatkom direktno se nadovezuje na jedan važan primjer relacije ekvivalencije na skupu $\mathbb{Z}$.

Definicija 5.2.2. *Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$. Kažemo da je a **kongruentno** b **modulo** n, i pišemo $a \equiv b \pmod{n}$ ako $n \mid a - b$.*

Primjer 26. $17 \equiv 2 \pmod{5}$, $17 \equiv -3 \pmod{5}$, *ali nije* $12 \equiv 5 \pmod{4}$.

Za neki dani $n \in \mathbb{N}$ ovim je definirana jedna relacija na skupu $\mathbb{Z}$. Označavamo je s $\equiv \pmod{n}$ i zovemo "*kongruencija modulo n*". Ovaj pojam je uveo Gauss 1801. godine. Sljedeća propozicija pokazuje da je relacija $\equiv \pmod{n}$ relacija ekvivalencije na skupu $\mathbb{Z}$.

Propozicija 5.2.1. *Neka je dan neki $n \in \mathbb{N}$. Vrijedi:*

1. $(\forall a \in \mathbb{Z})\, a \equiv a \pmod{n}$;
2. $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\,(a \equiv b \pmod{n} \to b \equiv a \pmod{n})$;
3. $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\,(a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \to a \equiv c \pmod{n})$.

Dokaz. *1.* Za svaki $a \in \mathbb{Z}$ vrijedi $n \mid a - a = 0$, tj. $a \equiv a \pmod{n}$.
2. Neka su $a, b \in \mathbb{Z}$ takvi da je $a \equiv b \pmod{n}$. Iz toga slijedi da $n \mid a - b$, pa $n \mid b - a$, odakle je $b \equiv a \pmod{n}$.
3. Neka su $a, b, c \in \mathbb{Z}$ takvi da je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$. Tada vrijedi $n \mid a - b$ i $n \mid b - c$, pa zbog svojstava djeljivosti

$$n \mid (a - b) + (b - c) = a - c.$$

Dakle, $a \equiv c \pmod{n}$. ■

Budući je $\equiv \pmod{n}$ relacija ekvivalencije na skupu $\mathbb{Z}$, ona tvori jednu particiju skupa $\mathbb{Z}$. Za $a \in \mathbb{Z}$ pripadna je klasa ekvivalencije skup

$$[a] = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}.$$

Znamo da vrijedi:

$$\begin{aligned} a &\equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n} \Leftrightarrow n \mid b - a \Leftrightarrow b - a = kn,\ k \in \mathbb{Z} \Leftrightarrow \\ b &= a + kn,\ k \in \mathbb{Z}. \end{aligned}$$

Označimo li $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$, onda je

$$[a] = \{a + kn : k \in \mathbb{Z}\} \overset{\text{ozn}}{=} a + n\mathbb{Z}.$$

Taj skup nazivamo *klasom ostataka* modulo n.

Zanima nas koliko ima različitih klasa ostataka modulo n.

Propozicija 5.2.2. *Postoji točno n klasa ostataka modulo n.*

Dokaz. Dokazat ćemo da su klase $[0], [1], \ldots, [n-1]$ sve međusobno različite, te da zajedno čine cijeli $\mathbb{Z}\,|_{\equiv(\mathrm{mod}\,n)}$.
Neka su $k, l \in \mathbb{N}$ i $0 \leq k < l < n$. Dokažimo da je $[k] \neq [l]$. Pretpostavimo suprotno, tj. da je $[k] = [l]$. Tada je $k \equiv l\,(\mathrm{mod}\,n)$, tj. $n \mid k - l$. No zbog $0 < l - k < n$ to je nemoguće. Dakle, $[k] \neq [l]$.
Neka je $a \in \mathbb{Z}$ proizvoljan. Dokazat ćemo da je $[a] = [k]$ za neki $0 \leq k < n$, tj. da je $\{[0], [1], \ldots, [n-1]\} = \mathbb{Z}\,|_{\equiv(\mathrm{mod}\,n)}$.
Prema teoremu o dijeljenju s ostatkom, za a i n postoje jedinstveni $q \in \mathbb{Z}$ i $0 \leq k < n$ takvi da je $a = qn + k$. No tada je $a - k = qn$, pa $n \mid a - k$, odakle slijedi $a \equiv k\,(\mathrm{mod}\,n)$. Dakle, $[a] = [k]$.
Ovim smo pokazali da je $\mathbb{Z}\,|_{\equiv(\mathrm{mod}\,n)} = \{[0], [1], \ldots, [n-1]\}$, pa postoji točno n klasa ostataka modulo n. ■

Prema prethodnom dokazu je

$$\mathbb{Z}\,|_{\equiv(\mathrm{mod}\,n)} = \{[0], [1], \ldots, [n-1]\}.$$

No naravno, ne moramo izabrati baš ostatke $0, 1, \ldots, n-1$ za predstavnike klasa. Ako je $[a_0] = [0], [a_1] = [1], \ldots, [a_{n-1}] = [n-1]$, onda je

$$\mathbb{Z}\,|_{\equiv(\mathrm{mod}\,n)} = \{[a_0], [a_1], \ldots, [a_{n-1}]\},$$

i svaki ovakav skup $\{a_0, \ldots, a_{n-1}\}$ nazivamo *potpunim skupom ostataka modulo n*.

Kongruencije imaju još neka lijepa svojstva.

Propozicija 5.2.3. *Za dani $n \in \mathbb{N}$ ako su $a, b, c, d \in \mathbb{Z}$ takvi da je $a \equiv c\,(\mathrm{mod}\,n)$ i $b \equiv d\,(\mathrm{mod}\,n)$, onda je $a + b \equiv c + d\,(\mathrm{mod}\,n)$ i $ab \equiv cd\,(\mathrm{mod}\,n)$.*

Dokaz. Neka je $a \equiv c\,(\mathrm{mod}\,n)$ i $b \equiv d\,(\mathrm{mod}\,n)$. Tada

$$n \mid a - c \;\text{ i }\; n \mid b - d,$$

pa zbog svojstava djeljivosti $n \mid (a - c) + (b - d)$, tj. $n \mid (a + b) - (c + d)$. Odavde je

$$a + b \equiv c + d\,(\mathrm{mod}\,n).$$

Također, $cd - ab = c\,(d - b) + b\,(c - a)$, a kako $n \mid c\,(d - b)$ i $n \mid b\,(c - a)$, to $n \mid cd - ab$, iz čega odmah slijedi $ab \equiv cd\,(\mathrm{mod}\,n)$. ■

Propozicija 5.2.4. *Neka su $d, n \in \mathbb{N}$ relativno prosti brojevi. Tada za bilo koje $a, b \in \mathbb{Z}$ vrijedi*

$$ad \equiv bd\,(\mathrm{mod}\,n) \;\; \textit{ako i samo ako}\;\; a \equiv b\,(\mathrm{mod}\,n).$$

Dokaz. Sami za vježbu. ■

5.3. Skup racionalnih brojeva

5.3.1. Uvod

U ovoj ćemo točki, polazeći od skupa $\mathbb{Z}$, postupcima sličnima onima koje smo primijenili prilikom izgradnje samog skupa $\mathbb{Z}$ izgraditi skup racionalnih brojeva $\mathbb{Q}$. Svakako želimo da dobiveni skup ima svojstva na koja smo navikli. Podsjetimo se na neka od njih:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb,$$
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Upravo ovim svojstvima biti će motivirane neke od definicija koje slijede. Tako prvo svojstvo pokazuje da treba promatrati uređene parove iz $\mathbb{Z} \times \mathbb{Z}^*$ (sa $\mathbb{Z}^*$ označavamo skup $\mathbb{Z} \setminus \{0\}$) i da treba "poistovjećivati" parove (a, b) i (c, d) za koje vrijedi $ad = bc$. To nam sugerira da treba definirati odgovarajuću relaciju ekvivalencije na $\mathbb{Z} \times \mathbb{Z}^*$.

Teorem 5.3.1. *Neka je relacija $\sim$ na $\mathbb{Z} \times \mathbb{Z}^*$ definirana sa:*

$$(a, b) \sim (c, d) \quad \textit{ako i samo ako je} \quad ad = cb.$$

Tada vrijedi:

1. *Relacija $\sim$ je relacija ekvivalencije na $\mathbb{Z} \times \mathbb{Z}^*$;*
2. *Iz $(a, b) \sim (a', b')$ i $(c, d) \sim (c', d')$ slijedi*

$$\begin{aligned} (ad + cb, bd) &\sim (a'd' + c'b', b'd'), \\ (ac, bd) &\sim (a'c', b'd'). \end{aligned}$$

Dokaz. Relacija $\sim$ je očigledno refleksivna i simetrična. Dokažimo da je tranzitivna. Neka su $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$ takvi da je $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$. Tada je $ad = cb$ i $cf = ed$. Iz svojstava množenja cijelih brojeva slijedi

$$d(af) = (ad) f = (cb) f = (cf) b = (de) b = d(eb),$$

a kako je $d \neq 0$, po regularnosti množenja slijedi da je $af = eb$, tj. $(a, b) \sim (e, f)$. Dakle, $\sim$ je relacija ekvivalencije na $\mathbb{Z} \times \mathbb{Z}^*$.
Dokažimo i drugu tvrdnju. Neka je $(a, b) \sim (a', b')$ i $(c, d) \sim (c', d')$. To znači da je $ab' = a'b$ i $cd' = c'd$. Uočimo da je $bd \neq 0$ i $b'd' \neq 0$, pa su $(ad + cb, bd)$ i $(a'd' + c'b', b'd')$ elementi skupa $\mathbb{Z} \times \mathbb{Z}^*$. Dokažimo da je $(ad + cb, bd) \sim (a'd' + c'b', b'd')$, tj. da je $(ad + cb) b'd' = (a'd' + c'b') bd$. Imamo

$$\begin{aligned} (ad + cb) b'd' &= (ad)(b'd') + (cb)(b'd') = (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') = (a'd')(bd) + (c'b')(bd) \\ &= (a'd' + c'b') bd. \end{aligned}$$

Time je ova tvrdnja dokazana. Slično se dokaže i da je $(ac, bd) \sim (a'c', b'd')$. ■

Definicija 5.3.1. *Neka je $\sim$ relacija ekvivalencije na $\mathbb{Z}\times\mathbb{Z}^*$ definirana (kao gore)*

$$(a,b)\sim(c,d)\Leftrightarrow ad=cb.$$

*Skup $\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}^*\,|\sim$ nazivamo **skupom racionalnih brojeva**, a njegove elemente **racionalnim brojevima**.*

Nadalje će nam τ označavati projekciju skupa $\mathbb{Z}\times\mathbb{Z}^*$ na skup $\mathbb{Q}$. Tako je npr.

$$\tau(1,2)=[(1,2)]=\{(1,2),(-1,-2),(2,4),(-2,-4),\ldots\}.$$

5.3.2. Zbrajanje i množenje na $\mathbb{Q}$

Do relacije ekvivalencije $\sim$ došli smo zamjenivši oznaku $\frac{a}{b}$ s parom (a,b). Na sličan način, izrazi $\frac{a}{b}+\frac{c}{d}$ i $\frac{a}{b}\frac{c}{d}$ prelaze u $(ad+cb,bd)$ i (ac,bd). Time smo dobili zbrajanje i množenje na $\mathbb{Z}\times\mathbb{Z}^*$. Dobivene algebarske operacije spustimo, zatim, pomoću projekcije τ na $\mathbb{Q}$. Provode se sva razmatranja kao u točki o cijelim brojevima. Tim putem dolazimo do

$$\tau(a,b)+\tau(c,d)=\tau(ad+cb,bd), \tag{5.5}$$

$$\tau(a,b)\,\tau(c,d)=\tau(ac,bd). \tag{5.6}$$

Teorem 5.3.2. *Sa* (5.5) *i* (5.6) *definirane su funkcije sa $\mathbb{Q}\times\mathbb{Q}$ u $\mathbb{Q}$. Funkciju $+$ definiranu izrazom* (5.5) *nazivamo **zbrajanjem**, a funkciju $\cdot$ definiranu izrazom* (5.6) *nazivamo **množenjem** na $\mathbb{Q}$.*

Dokaz. Treba pokazati da su relacije $+$ i $\cdot$ funkcionalne i totalne. Totalnost je u oba slučaja očigledna (za bilo koje $\tau(a,b),\tau(c,d)\in\mathbb{Q}$ su $\tau(ad+cb,bd)$ i $\tau(ac,bd)$ elementi iz $\mathbb{Q}$). Dokažimo da je relacija $+$ funkcionalna, tj. da dva jednaka elementa iz $\mathbb{Q}\times\mathbb{Q}$ imaju i jednake zbrojeve. Neka su $(\tau(a,b),\tau(c,d))$ i $(\tau(a',b'),\tau(c',d'))$ dva jednaka elementa iz $\mathbb{Q}\times\mathbb{Q}$. Dokažimo da je

$$\begin{aligned}\tau(a,b)+\tau(c,d) &= \tau(a',b')+\tau(c',d'),\ \text{tj.}\\ \tau(ad+cb,bd) &= \tau(a'd'+c'b',b'd').\end{aligned}$$

Iz $(\tau(a,b),\tau(c,d))=(\tau(a',b'),\tau(c',d'))$ slijedi da je $\tau(a,b)=\tau(a',b')$ i $\tau(c,d)=\tau(c',d')$, odnosno $(a,b)\sim(a',b')$ i $(c,d)\sim(c',d')$. Sada, po Teoremu 5.3.1., vrijedi

$$(ad+cb,bd)\sim(a'd'+c'b',b'd'),$$

pa je $\tau(ad+cb,bd)=\tau(a'd'+c'b',b'd')$.
Analogno se dokaže i funkcionalnost za množenje. ■

Teorem 5.3.3. *Zbrajanje i množenje su komutativne i asocijativne operacije na $\mathbb{Q}$. Također je zbrajanje distributivno prema množenju na $\mathbb{Q}$.*

Dokaz. Sami. ■

Teorem 5.3.4. *Za svaki element $\tau(a,b)$ skupa $\mathbb{Q}$ vrijedi*

$$\begin{aligned}\tau(a,b)+\tau(0,1) &= \tau(0,1)+\tau(a,b)=\tau(a,b),\\ \tau(a,b)\,\tau(0,1) &= \tau(0,1)\,\tau(a,b)=\tau(0,1),\\ \tau(a,b)\,\tau(1,1) &= \tau(1,1)\,\tau(a,b)=\tau(a,b).\end{aligned}$$

Štoviše, $\tau(0,1)$ i $\tau(1,1)$ su jedinstveni elementi skupa $\mathbb{Q}$ s ovim svojstvima.

Dokaz. Za svaki $a\in\mathbb{Z}$ i za svaki $b\in\mathbb{Z}^*$ vrijedi:

$$\begin{aligned}\tau(a,b)+\tau(0,1) &= \tau(a\cdot 1+0\cdot b,b\cdot 1)=\tau(a,b)=\tau(0,1)+\tau(a,b),\\ \tau(a,b)\,\tau(0,1) &= \tau(a\cdot 0,b\cdot 1)=\tau(0,b)=\tau(0,1)=\tau(0,1)\,\tau(a,b) \quad \text{i}\\ \tau(a,b)\,\tau(1,1) &= \tau(a\cdot 1,b\cdot 1)=\tau(a,b)=\tau(1,1)\,\tau(a,b).\end{aligned}$$

Dokažimo jedinstvenost elementa $\tau(0,1)$. Pretpostavimo da postoji još neki element $\tau(x,y)$ u $\mathbb{Q}$ takav da za sve $\tau(a,b)\in\mathbb{Q}$ vrijedi

$$\tau(a,b)+\tau(x,y)=\tau(x,y)+\tau(a,b)=\tau(a,b).$$

Tada je posebno

$$\tau(x,y)=\tau(x,y)+\tau(0,1)=\tau(0,1),$$

čime je jedinstvenost dokazana.
Dokažimo jedinstvenost elementa $\tau(1,1)$. Pretpostavimo da postoji još neki element $\tau(x,y)$ u $\mathbb{Q}$ takav da za sve $\tau(a,b)\in\mathbb{Q}$ vrijedi

$$\tau(a,b)\,\tau(x,y)=\tau(x,y)\,\tau(a,b)=\tau(a,b).$$

Tada je posebno

$$\tau(x,y)=\tau(x,y)\,\tau(1,1)=\tau(1,1),$$

pa je i $\tau(1,1)$ jedinstveni element s gornjim svojstvom. ■

Zbog prethodnog teorema ima, dakle, smisla označiti

$$\tau(0,1)\equiv 0,\ \tau(1,1)\equiv 1.$$

Označimo sada $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$. Vrijedi sljedeće:

Teorem 5.3.5. *Za svaki element $\tau(a,b)\in\mathbb{Q}$ postoji jedinstveni element $x\in\mathbb{Q}$ takav da je*

$$\tau(a,b)+x=x+\tau(a,b)=\tau(0,1).$$

Za svaki element $\tau(a,b)\in\mathbb{Q}^*$ postoji jedinstveni element $y\in\mathbb{Q}^*$ takav da je

$$\tau(a,b)\cdot y=y\cdot\tau(a,b)=\tau(1,1).$$

Dokaz. Neka je $\tau(a,b)\in\mathbb{Q}$. Odaberemo li $x=\tau(-a,b)\in\mathbb{Q}$ vrijedit će

$$\tau(a,b)+\tau(-a,b)=\tau(ab-ab,bb)=\tau(0,bb)=\tau(0,1)=\tau(-a,b)+\tau(a,b).$$

Neka je sada $x'\in\mathbb{Q}$ neki element takav da je

$$\tau(a,b)+x'=x'+\tau(a,b)=\tau(0,1).$$

Jedinstvenost elementa x slijedi iz činjenice da je

$$x' = x' + 0 = x' + (\tau(a,b) + x) = (x' + \tau(a,b)) + x = \tau(0,1) + x = x.$$

Odaberemo li za $\tau(a,b) \in \mathbb{Q}^*$ element $y = \tau(b,a) \in \mathbb{Q}^*$, vrijedi

$$\tau(a,b)\,\tau(b,a) = \tau(ab,ba) = \tau(ab,ab),$$

a kako je $\tau(c,c) = \tau(1,1)$ za svaki $c \in \mathbb{Z}^*$, to je $\tau(ab,ab) = \tau(1,1)$, pa je

$$\tau(a,b)\,\tau(b,a) = \tau(b,a) \cdot \tau(a,b) = \tau(1,1).$$

Na sličan način kao kod zbrajanja dokažemo i jedinstvenost elementa y s navedenim svojstvima. ■

Dakle, za svaki $\tau(a,b) \in \mathbb{Q}$ vrijedi:

$$\tau(a,b) + \tau(-a,b) = \tau(-a,b) + \tau(a,b) = \tau(0,1),$$

tj. $\tau(-a,b)$ je inverzni element elementa $\tau(a,b)$ za zbrajanje na $\mathbb{Q}$. Označavamo ga

$$\tau(-a,b) = -\tau(a,b)$$

i zovemo *suprotni element* elementa $\tau(a,b)$. Nadalje, za svaki $\tau(a,b) \in \mathbb{Q}^*$ vrijedi:

$$\tau(a,b) \cdot \tau(b,a) = \tau(b,a) \cdot \tau(a,b) = \tau(1,1),$$

tj. $\tau(b,a)$ je inverzni element elementa $\tau(a,b)$ za množenje na $\mathbb{Q}$. Označavamo ga

$$\tau(b,a) = \tau(a,b)^{-1}$$

i zovemo *recipročni element* elementa $\tau(a,b)$.

Iz Teorema 5.3.4. i 5.3.5. slijedi da su $(\mathbb{Q},+)$ i $(\mathbb{Q}^*,\cdot)$ Abelove grupe.

Primjedba 5.3.1. *Pojam inverznog elementa s obzirom na množenje racionalnih brojeva je nešto novo u odnosu na ono što smo do sada imali. Upravo u tomu treba tražiti smisao uvođenja racionalnih brojeva.*

5.3.3. Ulaganje cijelih u racionalne brojeve

Lako se pokaže da je funkcija $j : \mathbb{Z} \to \mathbb{Q}$ definirana izrazom

$$j(m) = \tau(m,1) \text{ za svaki } m \in \mathbb{Z},$$

dobro definirana i da je injekcija. Štoviše, za sve $m, m' \in \mathbb{Z}$ je ispunjeno

$$\begin{aligned} j(m+m') &= \tau(m+m',1) = \tau(m,1) + \tau(m',1) = j(m) + j(m'), \\ j(mm') &= \tau(mm',1) = \tau(m,1)\,\tau(m',1) = j(m)\,j(m') \quad \text{i} \end{aligned}$$

$$j(1) = \tau(1,1) = 1_Q.$$

Ove činjenice nam omogućavaju da poistovijetimo cijeli broj m s racionalnim brojem $j(m) = \tau(m,1) \in \mathbb{Q}$, odnosno da uložimo skup $\mathbb{Z}$ u skup $\mathbb{Q}$.

Kako je za $n \neq 0$ ispunjeno

$$\tau(m,n)\,\tau(n,1) = \tau(mn,n) = \tau(m,1),$$

to je racionalni broj $\tau(m,n)$ rješenje jednadžbe

$$xj(n) = j(m),$$

pa je

$$x = \tau(m,n) \equiv \frac{j(m)}{j(n)} \equiv \frac{m}{n}.$$

Ovim je dan prikaz racionalnog broja kao kvocijenta dvaju cijelih brojeva, pri čemu je nazivnik n različit od nule.
Sada kada smo sve ovo dokazali možemo uvesti oznake na koje smo navikli: za $\tau(a,b) \in \mathbb{Q}$ ćemo pisati $\frac{a}{b}$. Uočimo da vrijedi

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb,$$

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+cb}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

Također je

$$-\frac{a}{b} = \frac{-a}{b} \quad \text{i} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \text{ za } a \neq 0.$$

Teorem 5.3.6. *Skup $\mathbb{Q}$ je prebrojiv.*

Dokaz. Znamo da je skup $\mathbb{Z}$ prebrojiv, pa je takav i $\mathbb{Z} \times \mathbb{Z}$. Jer je $\mathbb{Z}^* \subset \mathbb{Z}$, to je i $\mathbb{Z} \times \mathbb{Z}^* \subset \mathbb{Z} \times \mathbb{Z}$, pa je i $\mathbb{Z} \times \mathbb{Z}^*$ prebrojiv (znamo da nije konačan). Budući je $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* \,|\sim$ slika projekcije $\tau : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$, to je skup $\mathbb{Q}$ konačan ili prebrojiv. Znamo da je $\mathbb{Z} \subset \mathbb{Q}$, pa je $\mathbb{Q}$ prebrojiv. Štoviše, kako je i $\mathbb{N} \subset \mathbb{Q}$, to je $\mathbb{N} \cong \mathbb{Q}$, pa je $\operatorname{kard}\mathbb{Q} = \aleph_0$. ■

5.3.4. O uređenosti skupa $\mathbb{Q}$

Uređajnu relaciju na $\mathbb{Q}$ uvodimo na osnovi sljedećeg teorema.

Teorem 5.3.7. *$\mathcal{P} = \{\mathbb{Q}_-, \mathbb{Q}_0, \mathbb{Q}_+\}$ je particija skupa $\mathbb{Q}$, pri čemu je*

$$\mathbb{Q}_- = \left\{\frac{a}{b} \in \mathbb{Q} : ab < 0\right\}, \quad \mathbb{Q}_0 = \{0\}, \quad \mathbb{Q}_+ = \left\{\frac{a}{b} \in \mathbb{Q} : ab > 0\right\}.$$

Dokaz. Dokažimo najprije da ovakva definicija skupova $\mathbb{Q}_-, \mathbb{Q}_0$ i $\mathbb{Q}_+$ ima smisla, tj. da je suglasna s relacijom ekvivalencije $\sim$ na $\mathbb{Z} \times \mathbb{Z}^*$.
Ako je $\tau(a,b) = \tau(c,d) \in \mathbb{Q}^*$, onda je $ad = bc$, pa je $(ab)(cd) = (bc)^2 > 0$. Dakle, ab i cd moraju biti istog predznaka, pa su $\tau(a,b)$ i $\tau(c,d)$ oba istodobno u $\mathbb{Q}_+$ ili u $\mathbb{Q}_-$. Stoga definicija skupova $\mathbb{Q}_-$, $\mathbb{Q}_0$ i $\mathbb{Q}_+$ ne ovisi o predstavnicima klasa pa su ti skupovi dobro definirani.

Također se lako vidi da je $\mathbb{Q}_- \cap \mathbb{Q}_+ = \emptyset$. Posebno, ako je $\tau(a,b) = 0 \in \mathbb{Q}_0$, onda je $\tau(a,b) = \tau(0,1)$, pa je $a \cdot 1 = 0 \cdot b = 0$, iz čega slijedi $a = 0$, odnosno $ab = 0$. U tom slučaju je očito $\mathbb{Q}_0 \cap \mathbb{Q}_- = \mathbb{Q}_0 \cap \mathbb{Q}_+ = \emptyset$. To pokazuje da su skupovi $\mathbb{Q}_-$, $\mathbb{Q}_0$ i $\mathbb{Q}_+$ međusobno disjunktni. Pokažimo još da je njihova unije cijeli $\mathbb{Q}$. Neka je $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Tada je ispunjeno jedno od sljedećega:

1) $(a < 0 \wedge b < 0) \vee (a > 0 \wedge b > 0)$, iz čega slijedi $ab > 0$, pa je $\frac{a}{b} \in \mathbb{Q}_+$;

2) $(a < 0 \wedge b > 0) \vee (a > 0 \wedge b < 0)$, iz čega slijedi $ab < 0$, pa je $\frac{a}{b} \in \mathbb{Q}_-$;

3) $(a = 0 \wedge b < 0) \vee (a = 0 \wedge b > 0)$, iz čega slijedi $ab = 0$, pa je $\frac{a}{b} \in \mathbb{Q}_0$;

Dakle, $\mathbb{Q} = \mathbb{Q}_- \cup \mathbb{Q}_0 \cup \mathbb{Q}_+$ pa je $\mathcal{P}$ jedna particija skupa $\mathbb{Q}$. ■

Elemente skupa $\mathbb{Q}_+$ nazivamo *strogo pozitivnim* racionalnim brojevima, a elemente skupa $\mathbb{Q}_-$ *strogo negativnim* racionalnim brojevima.

Teorem 5.3.8. *Skup* $\rho = \{(x,y) \in \mathbb{Q} \times \mathbb{Q} : y - x \in \mathbb{Q}_+\}$ *je relacija strogog uređaja na* $\mathbb{Q}$.

Dokaz. Uočimo najprije da je za bilo koje $x, y \in \mathbb{Q}$ uvijek $y - x \in \mathbb{Q}$, pa je po prethodnom teoremu ispunjeno $y - x \in \mathbb{Q}_0$ ili $y - x \in \mathbb{Q}_+$ ili $y - x \in \mathbb{Q}_-$.
Neka je $x \neq y$. Ako je $y - x \in \mathbb{Q}_+$, onda je $(x,y) \in \rho$. Ako je, pak, $y - x \in \mathbb{Q}_-$, onda je $-(y-x) = x - y \in \mathbb{Q}_+$, pa je sada $(y,x) \in \rho$. Dakle, svi različiti elementi skupa $\mathbb{Q}$ su usporedivi.
Ostala je još mogućnost $x = y$. No tada je $y - x = 0 \in \mathbb{Q}_0$, a kako je $\mathbb{Q}_0 \cap \mathbb{Q}_+ = \emptyset$, to za svaki $x \in \mathbb{Q}$ vrijedi $(x,x) \notin \rho$. Dakle, relacija ρ je irefleksivna. Treba još pokazati da je ρ tranzitivna.
Neka su $(x,y) \in \rho$ i $(y,z) \in \rho$. Tada je $y - x \in \mathbb{Q}_+$ i $z - y \in \mathbb{Q}_+$. Trebamo dokazati da je $(x,z) \in \rho$, tj. da je $z - x \in \mathbb{Q}_+$. To ćemo dokazati dokazujući jednu jaču tvrdnju: dokazat ćemo da je skup $\mathbb{Q}_+$ zatvoren s obzirom na zbrajanje.

Neka su $x = \frac{a}{b}, y = \frac{c}{d} \in \mathbb{Q}_+$, pri čemu je $ab > 0$ i $cd > 0$. Vrijedi

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}.$$

Sada imamo

$$(ad + cb)\, bd = (ad)\,(bd) + (cb)\,(bd) = (ab)\, d^2 + (cd)\, b^2 > 0.$$

Dakle, $x + y \in \mathbb{Q}_+$, pa je skup $\mathbb{Q}_+$ zatvoren s obzirom na zbrajanje.

Sada imamo:

$$z - x = (z - y) + (y - x) \in \mathbb{Q}_+ \Rightarrow (x,z) \in \rho,$$

pa je relacija ρ tranzitivna. Ovime je dokazano da je relacija ρ relacija strogog uređaja na skupu $\mathbb{Q}$. ■

Ova relacija strogog uređaja na $\mathbb{Q}$ ima mnoga lijepa svojstva. Tako, za svaka dva cijela broja m i n vrijedi:

$$\text{ako je } m < n \text{ onda je } j(m) < j(n),$$

pa preslikavanje j čuva uređaj na $\mathbb{Z}$. Također vrijedi i sljedeće.

Teorem 5.3.9. *Zbrajanje i množenje na $\mathbb{Q}$ su kompatibilne operacije sa strogim uređajem na $\mathbb{Q}$. Točnije vrijedi:*

1. $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x < y \to x + z < y + z)$;
2. $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,((x < y \wedge 0 < z) \to xz < yz)$.

Sada ćemo ukazati na još jedno važno svojstvo skupa $\mathbb{Q}$ koje nemaju ni skup $\mathbb{N}$ ni skup $\mathbb{Z}$.

Definicija 5.3.2. *Za strogo uređeni skup $(S, <)$ kažemo da je **gust** ako između svaka dva elementa skupa S postoji još neki element skupa S, tj. ako vrijedi*

$$(\forall a \in S)\,(\forall b \in S)\,(a < b \to (\exists c \in S)\,(a < c < b)).$$

Teorem 5.3.10. *Skup $\mathbb{Q}$ je gust.*

Dokaz. Neka su a, b proizvoljni elementi skupa $\mathbb{Q}$ za koje vrijedi $a < b$. Za element $c = \frac{a+b}{2} \in \mathbb{Q}$ vrijedi da je $a < c < b$. ■

5.4. Skup realnih brojeva

Skup realnih brojeva ima temeljnu ulogu u matematici, posebice u matematičkoj analizi. Uobičajena su dva pristupa ovom skupu: *induktivni* (konstruktivni), koji polazi od Peanovih aksioma za skup prirodnih brojeva, i *aksiomatski* (deduktivni) u kojem se popišu aksiomi skupa realnih brojeva (no to pretpostavlja dobro poznavanje nekih algebarskih struktura). Mi smo krenuli od Peanovih aksioma, tj. od skupa prirodnih brojeva, pa skup realnih brojeva gradimo induktivno. Ključnu ulogu pri toj izgradnji imaju, naravno, racionalni brojevi.

Vidjeli smo da elemente skupa $\mathbb{Q}$ možemo zbrajati i množiti (i oduzimati i dijeliti- izuzev s nulom). Pri tomu zbrajanje i množenje na $\mathbb{Q}$ imaju ova svojstva:

$A1$ $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\; x + (y + z) = (x + y) + z$ (asocijat. zbrajanja);

$A2$ $(\exists 0 \in \mathbb{Q})\,(\forall x \in \mathbb{Q})\; 0 + x = x + 0 = x$ (neutralni element za zbrajanje);

$A3$ $(\forall x \in \mathbb{Q})\,(\exists -x \in \mathbb{Q})\; x+(-x) = (-x)+x = 0$ (inverzni element za zbrajanje);

$A4$ $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\; x + y = y + x$ (komutativnost zbrajanja);

$A5$ $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (asocijativnost množenja);

$A6$ $(\exists 1 \in \mathbb{Q} \setminus \{0\})\,(\forall x \in \mathbb{Q})\; 1 \cdot x = x \cdot 1 = x$ (neutralni element za množenje);

$A7$ $(\forall x \in \mathbb{Q} \setminus \{0\})\,(\exists x^{-1} \in \mathbb{Q})\; x \cdot x^{-1} = x^{-1} \cdot x = 1$ (inverzni element za množenje);

$A8$ $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\; x \cdot y = y \cdot x$ (komutativnost množenja);

$A9$ $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\; x \cdot (y + z) = x \cdot y + x \cdot z$ (distributivnost množenja prema zbrajanju).

Svaki skup koji ima barem dva različita elementa i na kojem su definirane algebarske operacije zbrajanja i množenja s navedenih devet svojstava zove se *polje*. Skup racionalnih brojeva je, dakle, polje uz standardne operacije zbrajanja i množenja.

No na skupu $\mathbb{Q}$ osim navedene strukture polja postoji i uređajna struktura. Pokazali smo da je $(\mathbb{Q}, \leq)$ uređen skup, te da relacija $\leq$ ima, između ostalih, i ova svojstva:

Aa) $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x \leq y \wedge y \leq z \rightarrow x \leq z)$ (tranzitivnost);

Ab) $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(x \leq y \wedge y \leq x \rightarrow x = y)$ (antisimetričnost);

Ac) $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(x \leq y \vee y \leq x)$ (linearnost);

Ad) $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x \leq y \rightarrow x + z \leq y + z)$ (kompatibilnost relacije $\leq$ prema zbrajanju);

Ae) $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(0 \leq x \wedge 0 \leq y \rightarrow 0 \leq xy)$ (kompatibilnost prema množenju).

Općenito, svako polje koje je uređen skup i u kome vrijede svojstva *Ad*) i *Ae*) nazivamo *uređenim poljem*. Stoga je $\mathbb{Q}$ uređeno polje.

Racionalne brojeve je pogodno prikazati pomoću točaka nekog pravca. U tu svrhu, učvrstimo proizvoljnu točku O (ishodište) odabranoga pravca i točku E_1, različitu od O, na desnoj strani od točke O. Točki O pridružimo cijeli broj 0, a točki E_1 prirodni broj 1. Sada, počevši od točke E_1, nanesimo dužinu $\overline{OE_1}$ uzastopce na "desnu" zraku pravca OE_1 i to tako da početak svake sljedeće dužine bude kraj prethodne. Tako dobivamo dužine: $\overline{E_1E_2}$, $\overline{E_2E_3}$, $\overline{E_3E_4}$, ... Pridružujući rubovima tih dužina redom (s obzirom na relaciju $\leq$) prirodne brojeve, preslikat ćemo skup prirodnih brojeva injektivno u skup svih točaka pravca OE_1 ($m \mapsto E_m$ za svaki $m \in \mathbb{N}$). Preslikavajući na isti način preostale cijele brojeve ($\mathbb{Z}_-$) na "lijevu" zraku pravca, smjestit ćemo injektivno i skup $\mathbb{Z}$ u skup svih točaka odabranoga pravca. Pri tomu se uvodi i strogi uređaj na pravcu: $m < n$ u $\mathbb{Z}$ ako i samo ako je E_m "lijevo od" E_n. Nadalje, poznatim načinom dijeljenja dužine možemo svakom racionalnom broju $q = \frac{m}{n}$ pridružiti jedinstvenu točku E_q na odabranomu pravca. Tako se i $\mathbb{Q}$ injektivno i čuvajući uređaj preslika u skup svih točaka promatranoga pravca.

Budući da je $\mathbb{Q}$ svuda gust, moglo bi se pomisliti da je na opisani način svakoj točki na odabranom pravcu pridružen neki racionalan broj, tj. da je opisana funkcija iz $\mathbb{Q}$ u skup svih točaka na tom pravcu surjektivna. Da se radi o zabludi pokazuje ovaj jednostavni primjer: Konstruirajmo kvadrat nad "osnovnom" dužinom $\overline{OE_1}$, pa zarotirajmo njegovu dijagonalu oko točke O polažući je na "desnu" zraku pravca OE_1. Njezin kraj upadne u neku točku T odabrane zrake. Kada bi točka T bila slika nekog racionalnog broja q, vrijedilo bi $q^2 = 1^2 + 1^2 = 2$, što je uobičajeno pisati kao $q = \sqrt{2}$. Pokazat ćemo da $\sqrt{2}$ nije racionalan broj, tj. da točka T nije slika racionalnog broja, pa stoga gore opisano preslikavanje nije surjektivno. U tu svrhu trebat će nam sljedeća lema:

Lema 5.4.1. *Kvadrat $n^2 = n \cdot n$ prirodnog broja n je paran (neparan) ako i samo ako je n paran (neparan).*

Dokaz. Sami. ■

Pretpostavimo da točki T odgovara racionalni broj $q = \sqrt{2}$. To znači da postoje $m, n \in \mathbb{N}$ takvi da im je najveća zajednička mjera 1 i da je $\sqrt{2} = \frac{m}{n}$. Tada je $2 = \frac{m^2}{n^2}$, tj. $m^2 = 2n^2$, pa bi po prethodnoj lemi i m bio paran broj, tj. $m = 2k$ za neki $k \in \mathbb{N}$. To bi dalje značilo da je $n^2 = 2k^2$, pa bi i n bio paran, tj. $n = 2l$ za neki $l \in \mathbb{N}$. No, to bi značilo da su brojevi m i n djeljivi sa 2 što je u kontradikciji s pretpostavkom da im je najveća zajednička mjera 1.

Vidjeli smo da točka T koja odgovara "veličini" $\sqrt{2}$ nije slika racionalnog broja po opisanom preslikavanju. Drugim riječima, tretiramo li $\sqrt{2}$ kao neki "novi broj", tada $\sqrt{2} \notin \mathbb{Q}$. Zato se kaže da u skupu $\mathbb{Q}$ postoje praznine. Posljedica je to činjenice da u skupu $\mathbb{Q}$ postoje odozgo (odozdo) omeđeni podskupovi $A \subseteq \mathbb{Q}$ koji nemaju uvijek supremum (infimum) u $\mathbb{Q}$. Takav je, na primjer, skup $A = \left\{\left(1 + \frac{1}{n}\right)^n \in \mathbb{Q} : n \in \mathbb{N}\right\} \subseteq \mathbb{Q}$ koji je omeđen odozgo, a nema supremum u $\mathbb{Q}$. Sve ovo navodi na novo proširenje (na skup realnih brojeva) u slijedu $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$, u kojem će svaki njegov odozgo omeđeni podskup imati supremum, odnosno svaki odozdo omeđeni podskup toga skupa imati će infimum u tom skupu. U tu svrhu definirajmo pojam koji ima ključnu ulogu u konstrukciji skupa realnih brojeva: prerez.

Neka je $(X, \leq)$ uređen skup. Na skupu $\mathcal{P}(X)$ definiramo relaciju $<$ na način: za sve $A, A' \subseteq X$ vrijedi

$$A < A' \Leftrightarrow (\forall x \in A)\,(\forall x' \in A')\ \ x < x'.$$

Definicija 5.4.1. *Neka je $(X, \leq)$ uređen skup.* ***Prerezom*** *u skupu X smatramo svaki podskup $B \subseteq X$ za koji je ispunjeno:*
(i) $B \neq \emptyset$ i $B \neq X$,
(ii) $X \setminus B < B$,
(iii) B nema najmanji element.

Mi ćemo promatrati uređeni skup $(\mathbb{Q}, \leq)$ i prereze u njemu.
Označimo sa $\mathbb{R}$ skup svih prereza u $\mathbb{Q}$.

Primjedba 5.4.1. *Često se prerezi u $\mathbb{Q}$, tj. elementi skupa $\mathbb{R}$, označavaju dvojako- kao elementi $r \in \mathbb{R}$ i kao odgovarajući prerezi $B \subseteq \mathbb{Q}$, što pišemo $r \equiv B$.*

Uvedimo uređaj u $\mathbb{R}$. Neka je $\leq \subseteq \mathbb{R} \times \mathbb{R}$, te $r_1, r_2 \in \mathbb{R}$, $r_1 \equiv B_1$ i $r_2 \equiv B_2$, gdje su B_1 i B_2 dva prereza u $\mathbb{Q}$. Stavljamo

$$r_1 \leq r_2 \text{ ako i samo ako je } B_2 \subseteq B_1.$$

Lako se pokaže da je $\leq$ relacija uređaja na skupu $\mathbb{R}$, pa je $(\mathbb{R}, \leq)$ uređen skup. Sada možemo dokazati sljedeći važan teorem.

Teorem 5.4.1. *Svaki neprazan i odozdo omeđen skup $A \subseteq \mathbb{R}$ ima infimum u $\mathbb{R}$.*

Dokaz. Neka je A neprazan, odozdo omeđen skup u $\mathbb{R}$ i neka je $m \in \mathbb{R}$ jedna njegova donja međa, tj. $m \leq a$ za svaki $a \in A$. Po definiciji skupa $\mathbb{R}$ i uređaja $\leq$ na njemu, znamo da je m pojednostavljena oznaka za neki prerez B_m, i da svaki $a \in A$ označava neki prerez B_a. Budući da je $m \leq a$ za svaki $a \in A$, to je $B_a \subseteq B_m$ za

svaki $a \in A$, pa je i $B = \bigcup_{a\in A} B_a \subseteq B_m$. Skup A je neprazan pa su takvi i B_a, dakle, i B. Nadalje,

$$\mathbb{Q}\backslash B = \mathbb{Q}\backslash \left(\bigcup_{a\in A} B_a \right) = \bigcap_{a\in A} (\mathbb{Q}\backslash B_a) < B_a \text{ za svaki } a \in A.$$

Skup B nema najmanji element jer bi u protivnom taj element pripadao nekom B_a pa bi on bio $\min B_a$, što je u kontradikciji s činjenicom da je B_a prerez. Dakle, skup B je prerez u $(\mathbb{Q}, \leq)$.
Kao i do sada, pojednostavnimo oznaku $B \equiv b \in \mathbb{R}$. Vrijedi: $b \leq a$ za svaki $a \in A$ jer je $B_a \subseteq B$ za svaki $a \in A$. Dakle, b je donja međa skupa A.
Neka je $b' \in \mathbb{R}$ bilo koja donja međa od A s pripadnim prerezom B'. Tada je $b' \leq a$ za svaki $a \in A$, pa je $B' \supseteq B_a$ za svaki $a \in A$. Stoga je $B' \supseteq \bigcup_{a\in A} B_a = B \Rightarrow b' \leq b$, pa je b najveća donja međa od A, tj. $b = \inf A$. ■

Primjedba 5.4.2. *U aksiomatskoj izgradnji realnih brojeva ovaj se teorem uzima kao posljednji, petnaesti aksiom uz, već prije navedenih,* 14 *aksioma uređenoga polja. On, ustvari, razlikuje skup realnih brojeva od skupa racionalnih brojeva koji je također uređeno polje.*

Pokazali smo, dakle, da u skupu $\mathbb{R}$ svaki odozdo omeđen skup $A \subseteq \mathbb{R}$ ima infimum u $\mathbb{R}$. Iz toga ćemo dobiti i da svaki odozgo omeđen skup ima supremum u $\mathbb{R}$. No, za to dokazati, definirajmo operacije zbrajanja i množenja na skupu $\mathbb{R}$.
Neka su $B_1 \equiv r_1$, $B_2 \equiv r_2 \in \mathbb{R}$. Stavljamo

$$r_1 + r_2 \equiv B_1 + B_2 = \{q_1 + q_2 \in \mathbb{Q} : q_1 \in B_1, q_2 \in B_2\} = B \equiv r.$$

Pokazuje se da je ovo zbrajanje dobro definirano, tj. da je skup B neki prerez u $\mathbb{Q}$. Primijetimo da je $0 \equiv \langle 0, \cdot \rangle_{\mathbb{Q}} = \{q \in \mathbb{Q} : q > 0\} \in \mathbb{R}$ neutralni element za zbrajanje u $\mathbb{R}$ i da svaki element iz $\mathbb{R}$ ima inverz. Naime, inverz od $r \equiv B \in \mathbb{R}$ je element $-r \equiv B' = \langle -\inf B, \cdot \rangle_{\mathbb{Q}} = \{q \in \mathbb{Q} : q > -\inf B\}$. Komutativnost i asocijativnost zbrajanja u $\mathbb{R}$ slijede iz komutativnosti i asocijativnosti zbrajanja u $\mathbb{Q}$.
Za definirati množenje u $\mathbb{R}$ razlikujemo tri slučaja:

- Ako je $r_1 > 0$ i $r_2 > 0$, onda je

$$r_1 \cdot r_2 \equiv B_1 \cdot B_2 = \{q_1 \cdot q_2 \in \mathbb{Q} : q_1 \in B_1, q_2 \in B_2\} = B \equiv r.$$

- Ako je $r_1 < 0$ i $r_2 > 0$, onda je $r_1 \cdot r_2 = -\left((-r_1) \cdot r_2\right)$.
- Ako je $r_1 > 0$ i $r_2 < 0$, onda je $r_1 \cdot r_2 = -\left(r_1 \cdot (-r_2)\right)$.

Pokazuje se da je gore definirani skup $B = B_1 \cdot B_2$ neki prerezi u $\mathbb{Q}$ (pa je množenje dobro definirano) i da je $r > 0$. Primijetimo još da je prerez $\langle 1, \cdot \rangle_{\mathbb{Q}} = \{q \in \mathbb{Q} : q > 1\}$ neutralni element za množenje u $\mathbb{R}$.

Sada možemo dokazati da vrijedi:

Korolar 5.4.1. *Svaki neprazan odozgo omeđen skup $A \subseteq \mathbb{R}$ ima supremum u $\mathbb{R}$.*

Dokaz. Neka je A neprazan, odozgo omeđen skup u $\mathbb{R}$. Promatramo skup $-A = \{-a : a \in A\} \subseteq \mathbb{R}$. Očito je $-A \neq \emptyset$ (jer je $A \neq \emptyset$). Neka je $m \in \mathbb{R}$ neka gornja međa skupa A, tj. $a \leq m$ za svaki $a \in A$. No tada je $-m \leq -a$ za svaki $-a \in (-A)$, pa je skup $-A$ omeđen odozdo. Stoga, po prethodnom teoremu, postoji $\mu = \inf(-A)$. Kako je $\mu \leq -a$ za svaki $-a \in (-A)$, to je $a \leq -\mu$ za svaki $a \in A$, pa je $-\mu$ gornja međa skupa A. Pokažimo da je $-\mu$ i najmanja gornja međa, tj. supremum.
Neka je g neka druga gornja međa skupa A. Tada je $a \leq g$ za svaki $a \in A$, pa je $-g \leq -a$ za svaki $-a \in (-A)$, tj. $-g$ je donja međa skupa $-A$. Kako je $\mu = \inf(-A)$, to je $-g \leq \mu$, tj. $-\mu \leq g$ što znači da je $-\mu = \sup A$. ■

Primjedba 5.4.3. *Može se provjeriti da skup $(\mathbb{R}, +, \cdot, \leq)$ zadovoljava svih devet aksioma polja $A1 - A9$, svojstva $Aa - Ae$, te refleksivnost za $\leq$, pa je $(\mathbb{R}, +, \cdot, \leq)$ uređeno polje. Zbog toga što vrijedi Teorem 5.4.1. kaže se da je $\mathbb{R}$* ***potpuno*** *uređeno polje.*

Definicija 5.4.2. *Skup $\mathbb{R}$ s ovako definiranim operacijama $+$ i $\cdot$, te uređajem $\leq$ nazivamo* ***potpuno uređenim poljem realnih brojeva*** *i označavamo $(\mathbb{R}, +, \cdot, \leq)$, a njegove elemente nazivamo* ***realnim brojevima.***

Kao i do sada, jednostavnosti radi, najčešće ćemo ispuštati oznake za strukturu i umjesto $(\mathbb{R}, +, \cdot, \leq)$ pisati samo $\mathbb{R}$.
Primijetimo najprije da se svaki racionalan broj smije smatrati prerezom. Naime, funkcija ulaganja $j : \mathbb{Q} \to \mathbb{R}$ definirana izrazom

$$j(q) = B_q = \langle q, \cdot \rangle_{\mathbb{Q}} = \{q' \in \mathbb{Q} : q' > q\}$$

je injektivna ($B_q = B_{q'} \Leftrightarrow q = q'$ za svaki $q \in \mathbb{Q}$, pa je zapravo $\inf B_q = q$), te čuva operacije zbrajanja i množenja, kao i uređaj $\leq$ na $\mathbb{Q}$, tj. vrijedi:

1. $(\forall q \in \mathbb{Q})(\forall p \in \mathbb{Q})\ j(q + p) = j(q) + j(p)$;
2. $(\forall q \in \mathbb{Q})(\forall p \in \mathbb{Q})\ j(q \cdot p) = j(q) \cdot j(p)$;
3. $(\forall q \in \mathbb{Q})(\forall p \in \mathbb{Q})\ (q \leq p \Rightarrow j(q) \leq j(p))$.

Ove činjenice nam omogućavaju da poistovijetimo racionalan broj q s realnim brojem $B_q = \langle q, \cdot \rangle_{\mathbb{Q}}$, odnosno da uložimo skup $\mathbb{Q}$ u skup $\mathbb{R}$. Stoga je $\mathbb{Q} \subseteq \mathbb{R}$, odnosno vrijedi: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Prikazujući skupove $\mathbb{N}, \mathbb{Z}$ i $\mathbb{Q}$ pomoću točaka na brojevnom pravcu vidjeli smo da na tom pravcu postoje točke koje ne odgovaraju ni jednom racionalnom broju, npr. dijagonala jediničnog kvadrata odgovara veličini $\sqrt{2}$, ali $\sqrt{2} \notin \mathbb{Q}$. No, $\sqrt{2}$ odgovara prerezu $B = \{q \in \mathbb{Q}_+ : q^2 > 2\}$, pa je $\sqrt{2} \in \mathbb{R}$. Stoga je $\mathbb{R} \setminus \mathbb{Q} \neq \emptyset$. Štoviše, pokazuje se da svakoj točki T brojevnog pravca odgovara točno jedan realan broj r i obratno, pa se kaže da skup $\mathbb{R}$, za razliku od $\mathbb{Q}$, nema praznina. Pri tomu je relacija $<$ u $\mathbb{R}$ isto što i "biti lijevo" na brojevnom pravcu.

Definicija 5.4.3. *Skup $\mathbb{R} \setminus \mathbb{Q} = \mathbb{J}$ nazivamo* ***skupom iracionalnih brojeva,*** *a njegove elemente* ***iracionalnim brojevima.***

Istaknimo još neke važne podskupove skupa $\mathbb{R}$.

Definicija 5.4.4. *Skup* $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\} = \langle 0, +\infty \rangle$ *nazivamo skupom* ***pozitivnih realnih brojeva****, a njegove elemente* ***pozitivnim realnim brojevima****.*

Skup $\mathbb{R}_+ \cup \{0\} = \{x \in \mathbb{R} : x \geq 0\} = [0, +\infty\rangle$ *nazivamo skupom* ***nenegativnih realnih brojeva****.*

Skup $\mathbb{R}_- = \{x \in \mathbb{R} : x < 0\} = \langle -\infty, 0\rangle$ *nazivamo skupom* ***negativnih realnih brojeva****, a njegove elemente* ***negativnim realnim brojevima****.*

Primjedba 5.4.4. *Očigledno je*

$$\begin{aligned} \mathbb{R} &= \mathbb{R}_- \cup \{0\} \cup \mathbb{R}_+, \\ \mathbb{R}_- \cap \mathbb{R}_+ &= \mathbb{R}_- \cap \{0\} = \mathbb{R}_+ \cap \{0\} = \emptyset, \end{aligned}$$

pa je $\{\mathbb{R}_-, \{0\}, \mathbb{R}_+\}$ *jedna particija skupa* $\mathbb{R}$*. Također, vrijedi*

$$(\forall x, y \in \mathbb{R})\,(x \in \mathbb{R}_- \wedge y \in \mathbb{R}_+ \to x < y)\,.$$

Teorem 5.4.2. *Neka su* $x, y, z, x_1, \ldots, x_n, y_1, \ldots, y_n$ *realni brojevi. Tada vrijedi:*

1. $(\forall i \in \{1, \ldots, n\})\,(x_i \leq y_i) \to x_1 + \cdots + x_n \leq y_1 + \cdots y_n$;
2. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq y \leftrightarrow (\exists z \in \mathbb{R})\, x + z \leq y + z)\,$;
3. $(\forall x \in \mathbb{R})\,(2x = x \to x = 0)\,$;
4. $(\forall x \in \mathbb{R})\, 0 \cdot x = 0$;
5. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\, x\,(-y) = (-x)\, y = -\,(xy)\,$;
6. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(\forall z \in \mathbb{R})\,(x \leq y \wedge 0 \leq z \to xz \leq yz)\,$;
7. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq 0 \wedge 0 \leq y \to xy \leq 0)\,$;
8. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq 0 \wedge y \leq 0 \to 0 \leq xy)\,$;
9. $(\forall x \in \mathbb{R})\,(x \neq 0 \to x^2 > 0)\,$;
10. $(\forall x \in \mathbb{R})\,(x > 0 \to x^{-1} > 0)\,$;
11. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(0 < x < y \leftrightarrow 0 < y^{-1} < x^{-1})\,.$

Dokaz. 1) Iz $x_1 \leq y_1$, $x_2 \leq y_2$ i uređenosti polja $\mathbb{R}$ (točnije svojstva Ad) slijedi

$$x_1 + x_2 \leq y_1 + x_2 \;\text{ i }\; y_1 + x_2 \leq y_1 + y_2,$$

pa po svojstvu tranzitivnosti slijedi $x_1 + x_2 \leq y_1 + y_2$. Dokaz dalje ide indukcijom po $n \in \mathbb{N}$. Provedite ga za vježbu sami.
2) Neka je $x \leq y$. Po svojstvu Ad) za svaki $z \in \mathbb{R}$ je tada $x + z \leq y + z$. Obratno, neka postoji neki $z_0 \in \mathbb{R}$ takav da je $x + z_0 \leq y + z_0$. Tada je po Ad) za svaki $z \in \mathbb{R}$

$$(x + z_0) + z \leq (y + z_0) + z,$$

pa je i $x + (z_0 + z) \leq y + (z_0 + z)\,$. Uzmemo li posebno $z = -z_0$ slijedi tvrdnja.

3) Neka je $2x = x$. Tada je

$$\begin{aligned} 0 &= x + (-x) = 2x + (-x) = (x + x) + (-x) \\ &= x + [x + (-x)] = x + 0 = x. \end{aligned}$$

4) Neka je $x \in \mathbb{R}$. Vrijedi

$$0 \cdot x = (0 + 0)\, x = 0 \cdot x + 0 \cdot x = 2\,(0 \cdot x)\,,$$

pa po 3) slijedi da je $0 \cdot x = 0$.
5) Pomnožimo li s x jednakost $y + (-y) = 0$ dobivamo

$$x\,[y + (-y)] = x \cdot 0 = 0 \cdot x = 0 = xy + x\,(-y)\,,$$

pa je xy suprotni element od $x\,(-y)$, a zbog jedinstvenosti istoga je onda $-xy = x\,(-y)$. Analogno se dobije $-xy = (-x)\,y$.
6) Iz $x \leq y$ po Ad) dobivamo $x + (-x) \leq y + (-x)$, tj. $0 \leq y + (-x)$. Za $0 \leq z$ po Ae) vrijedi $0 \leq z\,(y + (-x))$, odnosno $xz \leq yz$.
7) i 8) se dokazuje slično kao 6).
9) Po 8) imamo da je za bilo koji $x \in \mathbb{R}$ ispunjeno $x^2 \geq 0$. Pretpostavimo da je $x \neq 0$ i da je $x^2 = 0$. Znamo da takav x ima inverz s obzirom na množenje, pa je

$$0 = x^{-1} \cdot 0 = x^{-1}x^2 = \left(x^{-1}x\right) x = 1 \cdot x = x,$$

što je u kontradikciji s pretpostavkom da je $x \neq 0$. Dakle, za $x \neq 0$ je $x^2 > 0$.
10) Neka je $x > 0$. Kako je $xx^{-1} = 1 = 1^2 > 0$, zaključujemo da je i $x^{-1} > 0$.
11) Iz $0 < x < y$ po prethodnoj tvrdnji slijedi $y^{-1} > 0$, pa je

$$0 = y^{-1} \cdot 0 < y^{-1}x < y^{-1}y = 1.$$

Odavde iz $x^{-1} > 0$ slijedi

$$0 = x^{-1} \cdot 0 < x^{-1}\left(y^{-1}x\right) = y^{-1} < x^{-1} \cdot 1 = x^{-1}.$$

■

Sada ćemo se pozabaviti još nekim temeljnim svojstvima skupa realnih brojeva.

Sljedeća dva teorema donose još dva važna svojstva skupa realnih brojeva (prvi od njih vrijedi i u $\mathbb{Q}$). Može se dokazati da su oni zajedno ekvivalentni Teoremu 5.4.1., odnosno Korolaru 5.4.1..

Teorem 5.4.3. *(Arhimedov aksiom) Skup realnih brojeva $\mathbb{R}$ je Arhimedovo polje, tj. za svaka dva realna broja $a, b \in \mathbb{R}$, $a > 0$, postoji $n \in \mathbb{N}$ takav da je $na > b$.*

Dokaz. Neka su $a, b \in \mathbb{R}$, $a > 0$. Pretpostavimo suprotno, tj. da je $na \leq b$ za svaki $n \in \mathbb{N}$. Tada je skup $\mathbb{N}a = \{na : n \in \mathbb{N}\}$ omeđen odozgo brojem b pa po prethodnom korolaru ima supremum. Označimo $b_0 = \sup \mathbb{N}a$. Kako je $a > 0$, to je $b_0 + a > b_0$, tj. $b_0 - a < b_0$. Stoga broj $b_0 - a$ ne može biti gornja međa skupa $\mathbb{N}a$ (jer je manji od supremuma toga skupa), pa postoji $n_0 \in \mathbb{N}$ takav da je $n_0 a > b_0 - a$, iz čega slijedi da je $n_0 a + a > b_0$, tj $(n_0 + 1)\, a > b_0$. No, kako je $(n_0 + 1)\, a \in \mathbb{N}a$, došli smo u kontradikciju s pretpostavkom da je $b_0 = \sup \mathbb{N}a$. ■

Korolar 5.4.2. *Za svaki $r \in \mathbb{R}$ postoje prirodni brojevi n_1 i n_2 takvi da je*

$$-n_1 < r < n_2.$$

Dokaz. Kako je $1 > 0$, po prethodnom teoremu zaključujemo da postoji $n_2 \in \mathbb{N}$ takav da je $n_2 \cdot 1 > r$, tj. $r < n_2$. Analogno, postoji $n_1 \in \mathbb{N}$ takav da je $n_1 \cdot 1 > -r$, tj. $-n_1 < r$. Dakle, postoje $n_1, n_2 \in \mathbb{N}$ takvi da je $-n_1 < r < n_2$ što je i trebalo dokazati. ■

Teorem 5.4.4. *(Cantorov aksiom) Neka je za svaki $n \in \mathbb{N}$ dan segment $[a_n, b_n] \subseteq \mathbb{R}$ i neka iz $n \leq m$ slijedi da je $[a_m, b_m] \subseteq [a_n, b_n]$, tj. $a_n \leq a_m \leq b_m \leq b_n$. Tada je*

$$\bigcap_{n\in\mathbb{N}} [a_n, b_n] \neq \emptyset.$$

Dokaz. Neka je $A = \{a_n \in \mathbb{R} : n \in \mathbb{N}\}$ i $B = \{b_n \in \mathbb{R} : n \in \mathbb{N}\}$. Očito je $\emptyset \neq A \leq B \neq \emptyset$, pa je svaki element skupa B gornja međa od A, tj.A je omeđen odozgo. Stoga, po Korolaru 5.4.1., postoji $\sup A = a \in \mathbb{R}$, te je $a_n \leq a$ za svaki $n \in \mathbb{N}$. Pokažimo da je $a \leq b_n$ za svaki $n \in \mathbb{N}$. Kad ne bi bilo tako, postojao bi neki $n_0 \in \mathbb{N}$ za koji je $a > b_{n_0}$, pa $b_{n_0} \in B$ ne bi bio gornja međa skupa A, a znamo da je svaki element iz B gornja međa skupa A. Stoga mora biti $a \leq b_n$ za svaki $n \in \mathbb{N}$. Dakle, $a_n \leq a \leq b_n$ za svaki $n \in \mathbb{N}$, tj. $a \in [a_n, b_n]$ za svaki $n \in \mathbb{N}$. Time je teorem dokazan.
Može se još pokazati da je $\bigcap_{n\in\mathbb{N}} [a_n, b_n] = [a, b]$, gdje je $a = \sup A$ i $b = \inf B$. ■

Sjetimo se da skupovi $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ imaju "jednako mnogo" ($\aleph_0$) elemenata, tj. da su ekvipotentni i prebrojivo beskonačni. Dokazat ćemo da smo proširenjem skupa $\mathbb{Q}$ iracionalnim brojevima pridodali "mnogo više" elemenata, tj. da je skup realnih brojeva beskonačan i neprebrojiv. Najprije dokažimo ovaj teorem:

Teorem 5.4.5. *U svakom intervalu $\langle a, b\rangle \subseteq \mathbb{R}$, $a < b$, postoji neki racionalan broj, tj. $\langle a, b\rangle_{\mathbb{Q}} \neq \emptyset$.*

Dokaz. Primijetimo da za svaki $r > 0$ postoji neki $q \in \mathbb{Q}$ takav da je $0 < q \leq r$. Zaista, budući da je $r > 0$, to za pripadne prereze vrijedi $B_r \subsetneq B_0$, tj. $B_0 \setminus B_r \neq \emptyset$. Postoji, dakle, neki $q \in B_0 \setminus B_r \subseteq \mathbb{Q}$ što onda povlači da je $0 < q \leq r$. Uzmimo sada da je $r' = \frac{r}{2}$, pa postoji $q \in \mathbb{Q}$ takav da je $0 < q \leq r' = \frac{r}{2} < r$. Prema tomu, za svaki $r \in \mathbb{R}$ je $\langle 0, r\rangle_{\mathbb{Q}} \neq \emptyset$. Primijetimo da ista konstrukcija vrijedi za svaki par $a, b \in \mathbb{R}$, $a < b$. ■

Teorem 5.4.6. *Svaki interval $\langle a, b\rangle \subseteq \mathbb{R}$, $a < b$, je neprebrojiv skup. Skup $\mathbb{R}$ je neprebrojiv.*

Dokaz. Dokazat ćemo da je svaki interval $\langle a, b\rangle \subseteq \mathbb{R}$ neprebrojiv dokazujući da ne postoji surjekcija iz $\mathbb{N}$ na $\langle a, b\rangle \subseteq \mathbb{R}$, $a < b$. Da bismo to dokazali, promatrajmo bilo koju funkciju $f : \mathbb{N} \to \langle a, b\rangle$. Princip definicije indukcijom dopušta, za svaki $n \in \mathbb{N}$, definiramo segment $I_n = [a_n, b_n] \subset \langle a, b\rangle$ tako da je $I_{n+1} \subseteq I_n$ i $f(n) \in \langle a, b\rangle \setminus I_n$. Opišimo induktivni korak $n \mapsto n + 1$:

Neka su segmenti $I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n$, za koje je $f(k) \in \langle a, b\rangle \setminus I_k$ za svaki $k \in [1, n]_{\mathbb{N}}$, već definirani. Uzmimo

$$I_{n+1} = \begin{cases} \left[\frac{a_n+b_n}{2}, b_n\right], & f(n+1) \leq a_n, \\ \left[a_n, \frac{a_n+f(n+1)}{2}\right] & a_n < f(n+1) < b_n, \\ \left[a_n, \frac{a_n+b_n}{2}\right] & f(n+1) \geq b_n. \end{cases}$$

Po Cantorovu aksiomu postoji neki realni broj $x \in \bigcap_{n\in\mathbb{N}} I_n \neq \emptyset$. Po konstrukciji mora biti $f(n) \neq x$ za svaki $n \in \mathbb{N}$. Naime, za svaki $n \in \mathbb{N}$ je $x \in I_n$, a $f(n) \notin I_n$. Zaključujemo da za svaku funkciju $f : \mathbb{N} \to \langle a, b\rangle$ postoji $x \in \langle a, b\rangle \setminus f(\mathbb{N})$. Dakle, f nije surjekcija. Odavde odmah slijedi da interval $\langle a, b\rangle \subseteq \mathbb{R}$ nije prebrojiv skup, pa onda naravno ni sam skup $\mathbb{R}$ kao njegov pravi nadskup. ■

Korolar 5.4.3. *Skup svih iracionalnih brojeva $\mathbb{J}$ je neprebrojiv.*

Dokaz. Iz prethodnog teorema slijedi da je svaki interval $\langle a, b\rangle \subseteq \mathbb{R}$ neprebrojiv. Budući da je $\langle a, b\rangle = \langle a, b\rangle_{\mathbb{J}} \cup \langle a, b\rangle_{\mathbb{Q}}$ disjunktna unija u kojoj je $\langle a, b\rangle_{\mathbb{Q}}$ prebrojiv skup, to $\langle a, b\rangle_{\mathbb{J}}$ mora biti neprebrojiv (unija dva prebrojiva skupa je prebrojiv skup), pa je neprebrojiv i $\mathbb{J} \supset \langle a, b\rangle_{\mathbb{J}}$. ■

Znamo da se kardinalni broj svih prebrojivih skupova označava s $\aleph_0$. Kardinalni broj skupa $\mathbb{R}$ označava se sa c (čitamo **continuum**) i po prethodnom je $\aleph_0 \neq c$.

Pokazali smo da svaki racionalan broj q može poistovjetiti s prerez $B_q = \langle q, \cdot\rangle_{\mathbb{Q}} = \{q' \in \mathbb{Q} : q' > q\}$ i da je $q = \inf B$. Pokažimo sada da se svaki realan broj r može poistovjetiti sa $B_r = \langle r, \cdot\rangle_{\mathbb{Q}} = \{q \in \mathbb{Q} : q > r\}$ i da je $r = \inf B$. Naime, vrijedi sljedeći teorem.

Teorem 5.4.7. *Ako je $r \in \mathbb{R}$, onda je $\langle r, \cdot\rangle_{\mathbb{Q}}$ prerez u skupu $\mathbb{Q}$ i za svaki prerez $B \subseteq \mathbb{Q}$ u skupu $\mathbb{Q}$ postoji jedan jedini $r \in \mathbb{R}$ takav da je $B = \langle r, \cdot\rangle_{\mathbb{Q}}$.*

Dokaz. Po Korolaru 5.4.2., za svaki $r \in \mathbb{R}$ postoje dva cijela broja q_1 i q_2 takva da je $q_1 < r < q_2$, što dokazuje da je skup $B = \langle r, \cdot\rangle_{\mathbb{Q}} \neq \emptyset$ i da je $\mathbb{Q}\backslash B \neq \emptyset$. Nadalje, ako je $a \in \mathbb{Q}\backslash B$, onda je $a \leq r < b$ za svaki $b \in B$, pa je $a < b$ za svaki $a \in \mathbb{Q}\backslash B$ i svaki $b \in B$, što dokazuje da je $\mathbb{Q}\backslash B < B$. Napokon, ne postoji $b_0 = \min B$ jer bi tada iz $b_0 \in B$ slijedilo da je $r < b_0$ pa bi, po Teoremu 5.4.5., u intervalu $\langle r, b_0\rangle$ postojao racionalan broj $q \in \langle r, b_0\rangle_{\mathbb{Q}}$. Kako je $r < q$, to bi $q \in \langle r, \cdot\rangle_{\mathbb{Q}} = B$ što je nemoguće jer je $q < b_0 = \min B$.
Obratno, ako je $B \subseteq \mathbb{Q}$ prerez u $\mathbb{Q}$, onda je svaka točka skupa $\mathbb{Q}\backslash B$ donja međa za B, pa B ima infimum (Teorem 5.4.1.). Označimo $r = \inf B \subseteq \mathbb{R}$. Sigurno je $B \subseteq \langle r, \cdot\rangle_{\mathbb{Q}}$ jer je $r < b$ za svaki $b \in B$. Neka je $q \in \langle r, \cdot\rangle_{\mathbb{Q}}$, tj. $q \in \mathbb{Q}$ i $r < q$. Tada, po definiciji infimuma, q ne može biti donja međa za skup B, već postoji neki $b \in B$ takav da je $b < q$. Kako je $\mathbb{Q}\backslash B < \{b\}$, to $q \notin \mathbb{Q}\backslash B$, tj. $q \in B$, pa je $B = \langle r, \cdot\rangle_{\mathbb{Q}}$. ■

5.4.1. Apsolutna vrijednost

Definicija 5.4.5. *Funkcija $|\ \ | : \mathbb{R} \to \mathbb{R}_+ \cup \{0\}$ zove se **apsolutna vrijednost** ili **modul** ako je*

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$$

Očito, za bilo koji $x \in \mathbb{R}$ je $|x| = \max\{-x, x\}$. Broj $|x|$ nazivamo *apsolutnom vrijednošću* broja x. Npr. $|7| = 7,\ |0| = 0$ i $|-3| = 3$.

Teorem 5.4.8. *Vrijedi:*

1. $(\forall x \in \mathbb{R})\,(\forall a \in \mathbb{R}_+)\,(-a \leq x \leq a \Leftrightarrow |x| \leq a)$;
2. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,|x+y| \leq |x| + |y|$ *i* $|x+y| = |x| + |y| \Leftrightarrow (\exists t > 0)\,x = ty$, $x, y \neq 0$
3. $(\forall x, y \in \mathbb{R})\,||x| - |y|| \leq |x - y|$;
4. $(\forall x, y \in \mathbb{R})\,|xy| = |x| \cdot |y|$.

Dokaz. 1) Neka je $-a \leq x \leq a$. Ako je $x \geq 0$, onda je $|x| = x \leq a$, a ako je $x < 0$, onda je $|x| = -x \leq -(-a) = a$.
Obratno, neka je $|x| \leq a$. Ako je $x \geq 0$, onda je $-a \leq x$ (zbog $a > 0$), a kako je $|x| = x \leq a$ dobivamo $-a \leq x \leq a$. Ako je, pak, $x < 0$, onda je sigurno $x \leq a$, a iz $-x = |x| \leq a$ množenjem s -1 slijedi $x \geq -a$, pa je opet $-a \leq x \leq a$.

2) Ako je $x \geq 0$ i $y \geq 0$, onda je i $x + y \geq 0$, pa je

$$|x+y| = x + y = |x| + |y|.$$

Ako je $x \leq 0$ i $y \leq 0$, onda je i $x + y \leq 0$, pa je

$$|x+y| = -(x+y) = (-x) + (-y) = |x| + |y|.$$

Ako je $x \leq 0$ i $y \geq 0$, onda je (zbog $x \leq 0 \leq |x|$)

$$x + y \leq y \leq y + |x| = |x| + |y|.$$

Nadalje, zbog $-|y| \leq 0 \leq y$ je

$$x + y \geq x \geq x - |y| = -|x| - |y| = -(|x| + |y|).$$

Sada imamo

$$-(|x| + |y|) \leq x + y \leq |x| + |y|,$$

pa je po prvoj tvrdnji $|x+y| \leq |x| + |y|$.

3) Iz $|x| = |y + (x-y)| \leq |y| + |x-y|$ slijedi $|x| - |y| \leq |x-y|$, a analogno i $|y| - |x| \leq |y-x| = |x-y|$, pa je

$$-|x-y| \leq |x| - |y| \leq |x-y|.$$

Sad po prvoj tvrdnji slijedi $||x| - |y|| \leq |x-y|$. ■

Teorem 5.4.9. *Funkcija* $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $d(x,y) = |x-y|$ *ima svojstva:*

1. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,d(x,y) \geq 0$;
2. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(d(x,y) = 0 \Leftrightarrow x = y)$;
3. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,d(x,y) = d(y,x)$;
4. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(\forall z \in \mathbb{R})\,d(x,z) \leq d(x,y) + d(y,z)$.

Definicija 5.4.6. *Funkcija* d *zove se* ***razdaljinska funkcija****, a broj* $d(x,y) = |x-y|$ *zove se* ***udaljenost*** *realnih brojeva* x *i* y.

5.4.2. Potencije

Asocijativnosti zbrajanja i množenja u $\mathbb{R}$ dopuštaju da se rekurzivno definiraju zbroj i umnožak od konačno realnih brojeva. Tako je za *zbroj* ili *sumu* od n realnih brojeva (pribrojnika) $x_1, ..., x_n \in \mathbb{R}$, $n \in \mathbb{N}$, u oznaci: $\sum_{i=1}^{n} x_i = x_1 + ... + x_n$, rekurzivna definicija ova:

$$\begin{aligned} \sum_{i=1}^{1} x_i &= x_1, \\ \sum_{i=1}^{k+1} x_i &= \sum_{i=1}^{k} x_i + x_{k+1},\ k \in \mathbb{N}. \end{aligned}$$

Pri tomu je $\left(\sum_{i=1}^{n} x_i\right) \cdot y = \sum_{i=1}^{n} (x_i y)$.

Posebice, za $x_1 = ... = x_n = x$, dobivamo $\sum_{i=1}^{n} x_i = nx$.

Umnožak ili *produkt* od n realnih brojeva (faktora) $x_1, ..., x_n \in \mathbb{R}$, $n \in \mathbb{N}$, u oznaci: $\prod_{i=1}^{n} x_i = x_1 \cdot ... \cdot x_n$, rekurzivno definiramo ovako:

$$\begin{aligned} \prod_{i=1}^{1} x_i &= x_1, \\ \prod_{i=1}^{k+1} x_i &= \prod_{i=1}^{k} x_i \cdot x_{k+1},\ k \in \mathbb{N}. \end{aligned}$$

Ako je pri tomu $x_1 = ... = x_n = x$, onda se umnožak $\prod_{i=1}^{n} x_i = x^n$ naziva **n-tom potencijom** broja x. Za x se kaže da je **baza**, a za n da je **eksponent** potencije x^n. Po definiciji je, dakle,

$$\begin{aligned} x^1 &= x, \\ x^{k+1} &= x^k \cdot x,\ k \in \mathbb{N}. \end{aligned}$$

Odatle indukcijom zaključujemo da za sve $x, y \in \mathbb{R}$ i $m, n \in \mathbb{N}$, vrijedi

$$\left.\begin{array}{c} x^m \cdot x^n = x^{m+n}, \\ (x^m)^n = x^{m \cdot n}, \\ (x \cdot y)^n = x^n \cdot y^n, \end{array}\right\} (*)$$

i

$$\begin{aligned} 0 &\leq x < y \Rightarrow x^n < y^n, \\ 0 &\leq x < 1 \Rightarrow 0 \leq x^n < 1, \\ x &> 1 \Rightarrow x^n > 1, \\ x &> 1 \wedge m < n \Rightarrow x^m < x^n, \\ 0 &< x < 1 \wedge m < n \Rightarrow x^m > x^n. \end{aligned}$$

Potenciranje prirodnim eksponentima proširujemo na negativne cjelobrojne eksponente $-n \in \mathbb{Z}_-$ i nulu stavljajući

$$\begin{aligned} x^{-n} &= \frac{1}{x^n} \text{ za svaki } x \in \mathbb{R}, \\ x^0 &= 1 \text{ za svaki } x \in \mathbb{R}\setminus\{0\}. \end{aligned}$$

Pokazuje se da i dalje vrijede jednakosti $(*)$.

Recimo sada nešto o decimalnom zapisu realnog broja. Brojeve $0, 1, 2, 3, 4, 5, 6, 7, 9$ nazivamo i *decimalnim znamenkama*. Decimalni zapis prirodnog (pa onda i cijelog i racionalnog) broja zasniva se na sljedećoj činjenici:

Za svaki $m \in \mathbb{N}$ postoji jedinstvena funkcija $p : \mathbb{R} \to \mathbb{R}$, $p(x) = a_n x^n + ... + a_1 x + a_0$, $a_n \neq 0$, kojoj su koeficijenti $a_0, a_1, ..., a_n$ decimalne znamenke i za koju je $p(10) = m$. Tada je pripadni decimalni zapis broja $m = p(10)$ upravo $a_n a_{n-1}...a_1 a_0$. Primjerice, prirodni broj $7 \cdot (10)^3 + 4 \cdot (10)^2 + 0 \cdot (10)^1 + 5$ ima decimalni zapis 7405. Dakle, broj 10 je "bazičan" za decimalni sustav- odatle naziv! Na isti način zapisujemo i negativne cijele brojeve $-m$ stavljajući znak $-$ ispred zapisa za m.
Napomenimo da se pored decimalnoga rabe i neki drugi sustavi za zapisivanje cijelih brojeva. Primjerice, binarni sustav u kojem ulogu "bazičnoga" broja preuzima broj 2, pa taj sustav ima samo dvije binarne znamenke: 0 i 1.

Osvrnimo se sada i na decimalno zapisivanje racionalnih brojeva. Ako je racionalan broj oblika $q = \frac{m}{10^n}$, $m \in \mathbb{Z}, n \in \mathbb{N}$, nazivamo ga *decimalnim brojem*. Neka je $m > 0$ i neka je njegov decimalni zapis $m = a_k a_{k-1}...a_1 a_0 = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0$. Tada je $q = a_k \cdot 10^{k-n} + ... + a_1 \cdot 10^{1-n} + a_0 \cdot 10^{-n}$, pa se za decimalni zapis decimalnog broja q uzima:

$$q = \begin{cases} a_k a_{k-1}...a_n, a_{n-1}...a_0, & k \geq n, \\ 0, a_k...a_0, & k = n-1, \\ 0, \underbrace{0...0}_{n-k-1 \text{ put}} a_k...a_0, & k \leq n-2 \end{cases}$$

U slučaju da je $m < 0$ postupamo kao i u slučaju $m > 0$ dodajući znak $-$ ispred zapisa. Primjerice, izraz $347,18$ je decimalni zapis decimalnog broja

$$3 \cdot 10^2 + 4 \cdot 10 + 7 + 1 \cdot 10^{-1} + 8 \cdot 10^{-2} = \frac{34718}{10^2};$$

dok je $-0,695$ decimalni zapis broja

$$-\left(6 \cdot 10^{-1} + 9 \cdot 10^{-2} + 5 \cdot 10^{-3}\right) = \frac{-695}{10^3}.$$

Postoje, međutim, i nedecimalni racionalni brojevi, npr. $\frac{1}{3}$. Može se pokazati da je svaki racionalan broj ili decimalan ili dopušta tzv. periodički decimalni zapis (neke znamenke ili neke skupine znamenaka iza decimalnog zareza se pravilno ponavljaju). Primjerice, $\frac{1}{3} = 0,33333... = 0,\dot{3}$, $\frac{1219}{990} = 1,2313131... = 1,2\dot{3}\dot{1}$.
Sada bi trebalo "otkriti" pogodna tehnička pravila (sheme) za izvođenje računskih operacija $(+, -, \cdot, :)$ u skupu racionalnih brojeva s decimalnim zapisom njegovih elemenata. No, ona su čitatelju dobro poznata iz osnovne škole, pa ćemo ih ovdje ispustiti.

Sjetimo se da smo potenciranje bili definirali samo za cjelobrojne eksponente. Sljedeći "teorem o jedinstvenosti baze" jamči mogućnost potenciranja racionalnim eksponentom, tzv. korijenovanje.

Teorem 5.4.10. *Neka su dani $a \in \mathbb{R}$, $a \geq 0$ i $n \in \mathbb{N}$. Tada postoji točno jedan $x \in \mathbb{R}$, $x \geq 0$, takav da je $x^n = a$.*

U dokazu teorema ćemo trebati neka svojstva množenja i potenciranja realnih brojeva, koja ćemo iskazati dvjema lemama.

Lema 5.4.2. *Neka su $x, y, \varepsilon \in \mathbb{R}$, $\varepsilon > 0$. Tada postoje $\delta_1, \delta_2 \in \mathbb{R}$, $\delta_1 > 0$, $\delta_2 > 0$ takvi da vrijedi:*

$$(\forall s, t \in \mathbb{R})\,(|s| < \delta_1 \wedge |t| < \delta_2) \rightarrow |(x+s)(y+t) - xy| < \varepsilon$$

Dokaz. Uzmimo $\delta_1 = \min\left\{1, \frac{\varepsilon}{2(1+|y|)}\right\}$ i $\delta_2 = \frac{\varepsilon}{2(1+|x|)}$. Stoga je $\delta_1 > 0$ i $\delta_2 > 0$ i za $s, t \in \mathbb{R}$, $|s| < \delta_1$ i $|t| < \delta_2$, vrijedi:

$$\begin{aligned} |(x+s)(y+t) - xy| &= |(x+s)t + sy| \leq |t|\,(|x| + |s| + |s|\,|y|) \\ &< |t|\,(|x|+1) + |s|\,(1+|y|) \\ &\leq \delta_2\,(|x|+1) + \delta_1\,(1+|y|) \\ &\leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

■

Lema 5.4.3. *Za svaki $x, \varepsilon \in \mathbb{R}$, $\varepsilon > 0$ i za svaki $n \in \mathbb{N}$ postoji $\delta \in \mathbb{R}_+$ takav da vrijedi:*

$$(\forall s \in \mathbb{R})\,|s| < \delta \rightarrow |(x+s)^n - x^n| < \varepsilon.$$

Dokaz. Tvrdnju dokazujemo matematičkom indukcijom. Za $n = 1$ je $\left|(x+s)^1 - x^1\right| = |s|$, pa je dovoljno uzeti neki $\delta < \varepsilon$. Pretpostavimo da je tvrdnja istinita za bilo koji $n \in \mathbb{N}$. Označimo $y = x^n$. Po prethodnoj lemi postoje brojevi $\delta_1, \delta_2 \in \mathbb{R}_+$ takvi da iz $|s| < \delta_1$ i $|t| < \delta_2$ slijedi $|(x+s)(x^n+t) - x^{n+1}| < \varepsilon$. Po induktivnoj pretpostavci, za $\delta_2 > 0$ postoji $\delta_3 > 0$ takav da iz $|s| < \delta_3$ slijedi $|(x+s)^n - x^n| < \delta_2$. Neka $\delta = \min\{\delta_1, \delta_3\}$, pa je $\delta > 0$ i, za svaki $s \in \mathbb{R}$, iz $|s| < \delta$ slijedi $|s| < \delta_1$ i $|(x+s)^n - x^n| < \delta_2$. Uzmimo $t = (x+s)^n - x^n$, pa to, skupa s prethodnim, jamči da $|s| < \delta$ povlači

$$\left|(x+s)^{n+1} - x^{n+1}\right| = \left|(x+s)(x+s)^n - x^{n+1}\right| = \left|(x+s)(x^n+t) - x^{n+1}\right| < \varepsilon.$$

■

Dokaz. (dokaz teorema) Neka je $A = \{r \in \mathbb{R} : r \geq 0 \wedge a < r^n\} \subseteq \mathbb{R}$, $n \in \mathbb{N}$. Čim je $r > \max\{a, 1\}$, već je $r^n > r > a$, što dokazuje da je $A \neq \emptyset$. Nadalje, $\{0\} \leq A$ pa je A omeđen odozdo. Sada, po Teoremu 5.4.1., postoji $\inf A = x$ i očito je $x \geq 0$. Tvrdimo: $x^n = a$.
Pretpostavimo protivno, tj. neka je $x^n \neq a$. Tada je $x^n > a$ ili je $x^n < a$, pa je $\varepsilon = |a - x^n| > 0$. Sada, po prethodnoj lemi, za taj ε postoji $\delta > 0$ takav da za svaki $s \in \mathbb{R}$ vrijedi

$$|s| < \delta \rightarrow |(x+s)^n - x^n| < \varepsilon.$$

Pretpostavimo najprije da je $x^n > a$. Onda je $x > 0$ (jer ne može biti 0) i $\varepsilon = x^n - a$. Za $s < 0$ takav da je $|s| < \delta$ i $|s| < x$, imamo da je $0 < x + s < x$ i

$$0 < x^n - (x+s)^n = |(x+s)^n - x^n| < \varepsilon = x^n - a \Rightarrow a < (x+s)^n \Rightarrow x + s \in A,$$

što je kontradikcija s činjenicom da je $x + s < x = \inf A$.
Preostaje mogućnost da je $x^n < a$. Tada je $\varepsilon = a - x^n$. Uzmimo takav $s > 0$ da je $s \leq \delta$, pa je $x < x + s$ i

$$0 < (x+s)^n - x^n = |(x+s)^n - x^n| < \varepsilon = a - x^n \Rightarrow (x+s)^n < a.$$

Budući da je $x = \inf A$ i $s > 0$, to postoji $r \in A$ takav da je $r < x + s$. No, po definiciji skupa A mora biti $a < r^n < (x+s)^n$ što je u kontradikciji s već dokazanom nejednakosti $a > (a+s)^n$. Ovim smo dokazali postojanje realnoga broja $x \geq 0$ za kojeg je $x^n = a$. Dokažimo i njegovu jedinstvenost!
Pretpostavimo da pored x postoji i broj $y \geq 0$ za kojeg je $y^n = a$. Kad bi bilo $y < x$ bilo bi i $a = y^n < x^n = a$ što je nemoguće, a isto povlači i pretpostavka $y > x$. Preostaje $x = y$. ■

Definicija 5.4.7. *Jedino rješenje $x \geq 0$ jednadžbe $x^n = a$, $n \in \mathbb{N}$, $a \geq 0$, označava se sa $a^{\frac{1}{n}}$ ili $\sqrt[n]{a}$ i zove n-**ti korijen** od a.*

Na ovaj način je uvedena potencija s eksponentom $\frac{1}{n}$. Napomenimo da se drugi korijen od a piše jednostavno $\sqrt{a}$.

Ovaj teorem jamči valjanost potenciranja realnog broja $a > 0$ bilo kojim racionalnim eksponentom $q = \frac{m}{n} \in \mathbb{Q}$ što zapisujemo

$$a^q = a^{\frac{m}{n}} = \left(a^{\frac{1}{n}}\right)^m = \left(\sqrt[n]{a}\right)^m,$$

Lako se vidi da je $\left(a^{\frac{1}{n}}\right)^m = (a^m)^{\frac{1}{n}}$. Nadalje, nije teško dokazati da sva pravila za potenciranje cjelobrojnim eksponentima ostaju valjana i pri potenciranju racionalnim eksponentima. Napokon, za $a \geq 0$ mogu se uvesti i potencije s proizvoljnim realnim eksponentom $r \in \mathbb{R}$ na način:

$$\begin{aligned} a^r &= \inf\{a^q : q \in \mathbb{Q} \wedge q > r\}, \text{ za } a \geq 1; \\ a^r &= \left(\frac{1}{a}\right)^{-r}, \text{ za } 0 < a < 1. \end{aligned}$$

Nadalje, za svaki $r \in \mathbb{R}\setminus\{0\}$ definiramo da je $0^r = 0$.
Pokazuje se da su i dalje sva pravila $(*)$ očuvana.

5.4.3. Binomni teorem

Neka je $n \in \mathbb{N}$. Označimo s $n! = 1 \cdot 2 \cdot \cdots \cdot n$. Posebno se uzima da je $0! = 1$.
Očito je za svaki prirodni broj n ispunjeno $(n+1)! = (n+1)\,n!$.
Za $n \in \mathbb{N}$ i $k \in \{0, 1, \ldots, n\}$ broj

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

nazivamo *binomnim koeficijentom*. Vrijedi:

$$\begin{aligned} \binom{n}{k} &= \binom{n}{n-k}, \\ \binom{n}{0} &= \binom{n}{n} = 1, \\ \binom{n}{k} + \binom{n}{k+1} &= \binom{n+1}{k+1}. \end{aligned}$$

Teorem 5.4.11. *Za bilo koji $n \in \mathbb{N}$ i za sve $a, b \in \mathbb{R}$ vrijedi*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Dokaz. Označimo sa M skup svih prirodnih brojeva n za koje vrijedi binomni teorem za bilo koji izbor $a, b \in \mathbb{R}$. Očigledno je $1 \in M$. Pretpostavimo da je $n \in M$. Tada vrijedi

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \overset{pp}{=} (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\
&= (a+b)\left[\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n\right] \\
&= \binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{n-1}a^2 b^{n-1} + \binom{n}{n}ab^n + \\
&\quad \binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n-1}ab^n + \binom{n}{n}b^{n+1} \\
&= \binom{n+1}{0}a^{n+1} + \left(\binom{n}{1} + \binom{n}{0}\right)a^n b + \cdots \\
&\quad \cdots + \left(\binom{n}{n} + \binom{n}{n-1}\right)ab^n + \binom{n+1}{0}b^{n+1} \\
&= \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.
\end{aligned}$$

Dakle, $n+1 = s(n) \in M$, pa je $M = \mathbb{N}$. ■

Primjer 27. *Vrijedi:*

1. $(a+b)^2 = a^2 + 2ab + b^2$;
2. $(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$;
3. $(a+b)^4 = a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4$.

Očito, binomni koeficijenti su dobili takvo ime jer se pojavljuju kao koeficijenti u binomnom razvoju. Oni se mogu poredati u tzv. *Pascalov trokut.*

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & \vdots & & & &
\end{array}$$

Primjedba 5.4.5. *Binomni je teorem važan kod dokazivanja egzistencije supremuma niza* $a : \mathbb{N} \to \mathbb{R}$ *definiranog izrazom*

$$a(n) = a_n = \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k}.$$

Pomoću binomnog teorema se pokaže da je za svaki $n \in \mathbb{N}$ *ispunjeno* $2 \leq a_n < 3$, *a kako je ovaj niz realnih brojeva očigledno rastući, to on u skupu* $\mathbb{R}$ *ima supremum. Označimo sa*

$$\begin{aligned} e &= \sup\{a_n : n \in \mathbb{N}\} \\ &= \sup\left\{\left(2 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right) : n \in \mathbb{N}\right\} = 2,718281828459045\cdots. \end{aligned}$$

Iracionalni broj e zovemo ***bazom prirodnih*** *ili* ***Neperovih logaritama.***

5.5. Skup kompleksnih brojeva

5.5.1. Uvod

Skup kompleksnih brojeva ćemo izgraditi pomoću skupa realnih brojeva. Osnova za to nam je sljedeći teorem.

Teorem 5.5.1. *Skup* $\mathbb{R}\times\mathbb{R} = \mathbb{R}^2 = \{(a,b) : a,b \in \mathbb{R}\}$ *je polje u odnosu na operacije zbrajanja i množenja definirane za sve* $(a_1,b_1),(a_2,b_2) \in \mathbb{R}^2$ *sa:*

1. $(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$;
2. $(a_1,b_1) \cdot (a_2,b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.

Dokaz. Dokazat ćemo korak po korak da je $\mathbb{R}^2$ polje s obzirom na ovako definirane operacije zbrajanja i množenja. Istaknimo najprije da je očito za sve $(a_1,b_1),(a_2,b_2) \in \mathbb{R}^2$ ispunjeno

$$(a_1 + a_2, b_1 + b_2), (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \in \mathbb{R}^2,$$

pa su ove operacije dobro definirane.

1) Za sve $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned} (a_1,b_1) + [(a_2,b_2) + (a_3,b_3)] &= (a_1,b_1) + (a_2 + a_3, b_2 + b_3) \\ &= (a_1 + a_2 + a_3, b_1 + b_2 + b_3) \\ &= (a_1 + a_2, b_1 + b_2) + (a_3,b_3) \\ &= [(a_1,b_1) + (a_2,b_2)] + (a_3,b_3), \end{aligned}$$

tj. zbrajanje je asocijativno.

2) Za element $(0,0) \in \mathbb{R}^2$ i za sve $(a,b) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned} (0,0) + (a,b) &= (0 + a, 0 + b) = (a,b) \\ &= (a + 0, b + 0) = (a,b) + (0,0), \end{aligned}$$

tj. $(0,0) \in \mathbb{R}^2$ je neutralni element za zbrajanje.

3) Za sve $(a_1, b_1), (a_2, b_2) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) \\ &= (a_2 + a_1, b_2 + b_1) \\ &= (a_2, b_2) + (a_1, b_1),\end{aligned}$$

tj. zbrajanje je komutativno.

4) Za svaki $(a, b) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned}(a, b) + (-a, -b) &= (a + (-a), b + (-b)) = (0, 0) \\ &= ((-a) + a, (-b) + b) = (-a, -b) + (a, b),\end{aligned}$$

pa svaki $(a, b) \in \mathbb{R}^2$ ima inverzni element

$$(-a, -b) \equiv -(a, b) \in \mathbb{R}^2$$

s obzirom na zbrajanje.

5) Za sve $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{R}^2$ vrijedi (račun provedite sami!)

$$(a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] = [(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3),$$

tj. množenje je asocijativno.

6) Za element $(1, 0) \in \mathbb{R}^2$ i za sve $(a, b) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned}(1, 0) \cdot (a, b) &= (1 \cdot a - 0 \cdot b, 1 \cdot b + a \cdot 0) = (a, b) \\ &= (a \cdot 1 - b \cdot 0, a \cdot 0 + 1 \cdot b) = (a, b) \cdot (1, 0),\end{aligned}$$

tj. $(1, 0) \in \mathbb{R}^2$ je neutralni element za množenje.

7) Za sve $(a_1, b_1), (a_2, b_2) \in \mathbb{R}^2$ vrijedi

$$\begin{aligned}&(a_1, b_1) \cdot (a_2, b_2) \\ = \;&(a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1) \\ = \;&(a_2 a_1 - b_2 b_1, a_2 b_1 + a_1 b_2) \\ = \;&(a_2, b_2) \cdot (a_1, b_1),\end{aligned}$$

tj. množenje je komutativno.

8) Za svaki $(a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ vrijedi

$$\begin{aligned}(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) &= \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \cdot (a, b), \\ &= \left(\frac{a^2}{a^2 + b^2} - \frac{-b^2}{a^2 + b^2}, \frac{-ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2} \right) \\ &= (1, 0)\end{aligned}$$

pa svaki $(a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ ima inverzni element

$$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \equiv (a, b)^{-1} \in \mathbb{R}^2 \setminus \{(0, 0)\}$$

s obzirom na množenje.

9) Za sve $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{R}^2$ vrijedi (račun provedite sami!)

$$(a_1, b_1) \cdot [(a_2, b_2) + (a_3, b_3)] = (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1)(a_3, b_3),$$

tj. množenje je distributivno s obzirom na zbrajanje. ■

Definicija 5.5.1. *Polje $\mathbb{R} \times \mathbb{R}$, u oznaci $\mathbb{C}$, nazivamo **poljem kompleksnih brojeva**, a njegove elemente **kompleksnim brojevima**.*

Kompleksne brojeve najčešće označavamo slovima $z, w, \ldots$

Uočimo da skup

$$\mathbb{R}' = \{(a, 0) : a \in \mathbb{R}\}$$

ima svojstva skupa realnih brojeva. Naime, preslikavanje $j : \mathbb{R} \to \mathbb{R}'$ definirano izrazom $j(a) = (a, 0)$ za svaki $a \in \mathbb{R}$, ima svojstvo da je za sve $a, b \in \mathbb{R}$ ispunjeno

1. $j(a + b) = (a + b, 0) = (a, 0) + (b, 0) = j(a) + j(b)$;
2. $j(ab) = (ab, 0) = (a, 0)(b, 0) = j(a)\, j(b)$;

pa se operacije zbrajanja i množenja na $\mathbb{R}$ prenose na $\mathbb{R}'$. Također se lako vidi da je j bijekcija. Zbog svega toga smijemo poistovijetiti skupove $\mathbb{R}$ i $\mathbb{R}'$ i za $a \in \mathbb{R}$ pisati

$$(a, 0) \equiv a.$$

Skup $\mathbb{R}'$ nazivamo skupom *realnih kompleksnih brojeva*. Upravo nam ova činjenica omogućava da dođemo do dobro poznatog *standardnog zapisa* kompleksnog broja. Naime, za svaki $z = (a, b) \in \mathbb{R}$ vrijedi:

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) \equiv a + b(0, 1).$$

Uvedemo li oznaku

$$i \equiv (0, 1)$$

dobivamo

$$z = a + bi = \mathrm{Re}(z) + \mathrm{Im}(z)\, i.$$

Realni broj $\mathrm{Re}(z)$ nazivamo *realnim dijelom* kompleksnog broja z, realni broj $\mathrm{Im}(z)$ nazivamo *imaginarnim dijelom* kompleksnog broja z, a i nazivamo *imaginarnom jedinicom*. Uočimo da sam i nije dio imaginarnog dijela broja z.

Stavimo li da je $i^0 \equiv 1$, lako se provjeri da vrijedi

$$i^0 = 1,\ i^1 = 1,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1.$$

Stoga je za svaki cijeli broj k ispunjeno

$$i^k = i^n, \quad k \equiv n \pmod 4,\ n \in \{0, 1, 2, 3\}$$

pa se vrlo lako mogu računati potencije imaginarne jedinice ako im je eksponent cijeli broj. Npr.

$$i^{243} = i^3 = -i, \quad i^{-563} = i^1 = i.$$

Postavlja se pitanje: je li skup $\mathbb{C}$ uređeno polje, tj. možemo li definirati relaciju uređaja na skupu $\mathbb{C}$? Naredni teorem to opovrgava.

Teorem 5.5.2. *Na skupu $\mathbb{C}$ ne postoji relacija uređaja $\leq$ takva da je $\mathbb{C}$ uređeno polje.*

Dokaz. Pretpostavimo da je $\mathbb{C}$ uređeno polje u odnosu na neku relaciju uređaja $\leq$. Označimo

$$\mathbb{C}_+ = \{z \in \mathbb{C} : z > 0\},$$

gdje je $0 = (0,0)$. Svakako je $i \in \mathbb{C}_+$ ili $-i \in \mathbb{C}_+$.
Ako je $i = (0,1) \in \mathbb{C}_+$, onda je po aksiomu Ae) i $i^2 = -1 \in \mathbb{C}_+$, te $i^4 = 1 \in \mathbb{C}_+$, pa je $\{-1, 1\} \subset \mathbb{C}_+$. No tada po Ad) iz $0 < -1$ slijedi $0 + 1 < -1 + 1$, tj. $1 < 0$. Ovo bi značilo da je $1 \in \mathbb{C}_-$, pa je $\mathbb{C}_- \cap \mathbb{C}_+ \neq \emptyset$. Analogno se dobije krene li se od pretpostavke $-i \in \mathbb{C}_+$.
Dakle, nije moguće postići particiju $\{\mathbb{C}_-, \mathbb{C}_0, \mathbb{C}_+\}$, pa $\mathbb{C}$ ne može biti uređeno polje. ■

Ovaj teorem nam ukazuje na to da je struktura skupa $\mathbb{C}$ bitno različita od strukture skupa $\mathbb{R}$, iako je skup $\mathbb{C}$ izgrađen pomoću skupa $\mathbb{R}$.

Definicija 5.5.2. *Neka je $z = a + bi \in \mathbb{C}$. Tada broj*

$$\overline{z} = a - bi \in \mathbb{C}$$

nazivamo ***konjugirano kompleksnim brojem*** *broja z.*

Sada možemo definirati preslikavanje $conj : \mathbb{C} \to \mathbb{C}$ sa

$$z \mapsto \overline{z}.$$

Lako se provjeri da za sve $z_1, z_2 \in \mathbb{C}$ vrijedi:

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$;
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$;
3. $\overline{\overline{z_1}} = z_1$.

Također je za sve $z = a + bi \in \mathbb{C}$ ispunjeno

$$z\overline{z} = a^2 + b^2 \in \mathbb{R},$$

pa je izrazom

$$|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2},$$

dobro definirano preslikavanje "apsolutna vrijednost" $|\ | : \mathbb{C} \to \mathbb{R}_+ \cup \{0\}$. Broj $r(z) = |z|$ nazivamo *radiusom* kompleksnog broja z.

Kompleksne brojeve prikazujemo u tzv. Gaussovoj ravnini. Koristeći apsolutnu vrijednost kompleksnog broja možemo definirati i udaljenost među kompleksnim brojevima. Razdaljinsku funkciju $d : \mathbb{C} \times \mathbb{C} \to \mathbb{R}_+ \cup \{0\}$ za sve $(z_1, z_2) \in \mathbb{C} \times \mathbb{C}$ definiramo izrazom:

$$d(z_1, z_2) = |z_2 - z_1|,$$

i ona ima ista svojstva kao i kod realnih brojeva (ta svojstva smo naveli u Teoremu 5.4.9.).

5.5.2. Trigonometrijski oblik kompleksnog broja

Podsjetimo se da smo u svakom novom skupu brojeva mogli uvesti neku novu operaciju. Tako smo u skupu $\mathbb{Z}$ mogli oduzimati (tj. dobili smo inverzne elemente u odnosu na zbrajanje), u skupu $\mathbb{Q}$ smo mogli dijeliti (tj. dobili smo inverzne elemente u odnosu na množenje), a u skupu $\mathbb{R}$ smo mogli računati potencije pozitivnih brojeva i kada je eksponent racionalan broj, tj. mogli smo vaditi korjene iz pozitivnih brojeva. U skupu $\mathbb{C}$ je pak moguće vaditi korjene iz svih komplesnih brojeva. Također, u skupu $\mathbb{R}$ je za $n \in \mathbb{N}$ i $a \in \mathbb{R}$ jednadžba $x^n = a$ imala najviše dva rješenja (ovisno o predznaku broja a i parnosti broja n), no u skupu $\mathbb{C}$ ona će uvijek imati točno n rješenja.

Da bismo na jednostavan način vadili korjene iz kompleksnih brojeva uvest ćemo novi način zapisivanja kompleksnih brojeva.
Nacrtamo li broj $z = a + bi \in \mathbb{C}$ u Gaussovoj ravnini lako se vidi da vrijedi

$$b = r \sin \varphi, \quad a = r \cos \varphi,$$

gdje je $r = r(z)$, a $\varphi = \arg(z) \in [0, 2\pi\rangle$ kut koji spojnica ishodišta $(0,0)$ i točke (a,b) zatvara s pozitivnim dijelom realne osi. Taj kut nazivamo *argumentom* kompleksnog broja.
Sada smo dobili

$$z = a + bi = r(\cos \varphi + i \sin \varphi),$$

i ovakav zapis nazivamo *trigonometrijskim oblikom* kompleksnog broja.
Sada se za bilo koje $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$,$z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2) \in \mathbb{C}$ aritmetičke operacije provode u skladu sa sljedećim formulama:

$$\begin{aligned}
z_1 z_2 &= r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)), \\
\frac{z_1}{z_2} &= \frac{r_1}{r_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)), \\
z_1^n &= r_1^n (\cos n\varphi_1 + i \sin n\varphi_1), \\
\sqrt[n]{z_1} &= \sqrt[n]{r_1} \left(\cos \frac{\varphi_1 + 2k\pi}{n} + i \sin \frac{\varphi_1 + 2k\pi}{n} \right), \ k = 0, 1, \ldots, n-1.
\end{aligned}$$

Uočimo da u ovakvom zapisu nije lako zbrajati kompleksne brojeve.

Primjer 28. *Neka je* $z = i = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$. *Tada je npr.*

$$z^3 = \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2} = 0 + i(-1) = -i.$$

Također je npr.

$$\begin{aligned}
\sqrt{z} &= \cos \frac{\frac{\pi}{2} + 2k\pi}{2} + i \sin \frac{\frac{\pi}{2} + 2k\pi}{2} \\
&= \cos \frac{(1+4k)\pi}{4} + i \sin \frac{(1+4k)\pi}{4}, \ k = 0, 1,
\end{aligned}$$

pa su rješenja $w_1 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$ *i* $w_2 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$.

Napomenimo još da n-ti korjeni iz nekog kompleksnog broja z leže u vrhovima pravilnog n-terokuta upisanog središnjoj kružnici radiusa $\sqrt[n]{r(z)}$, pri čemu je kut među susjednim vrhovima upravo $\arg(z)/n$.

Ovo poglavlje je većim dijelom preuzeto iz [4].

Poglavlje 6.

Elementarne funkcije

6.1. Osnovne elementarne funkcije

Definicija 6.1.1. *Neka je S neprazan skup. Bilo koju funkciju $f : S \to \mathbb{R}$ nazivamo* ***realnom funkcijom****. Ako je još i $S \subseteq \mathbb{R}$, onda kažemo da je f* ***realna funkcija realne varijable****.*

U ovom poglavlju ćemo se baviti realnim funkcijama realne varijable.
Pokazali smo da vrijedi:

- Svaka strogo monotona funkcija je injekcija.
- Za svaku funkciju $f : A \to B$, suženje $f : A \to f(A)$ je surjekcija.
- Ako je $f : A \to B$ strogo monotona na nekom $I \subseteq A$, onda je suženje $f|_I : I \to f(I)$ bijekcija.
- Ako je $f : A \to B$ bijekcija, onda postoji funkcija $g : B \to A$ takva da je $g \circ f = id_A$ i $f \circ g = id_B$. Funkcija g je jedinstvena, označavamo je sa $g = f^{-1}$ i nazivamo inverznom funkcijom funkcije f. Grafički prikaz inverzne funkcije f^{-1} je osno simetričan grafičkom prikazu funkcije f s obzirom na pravac $y = x$.

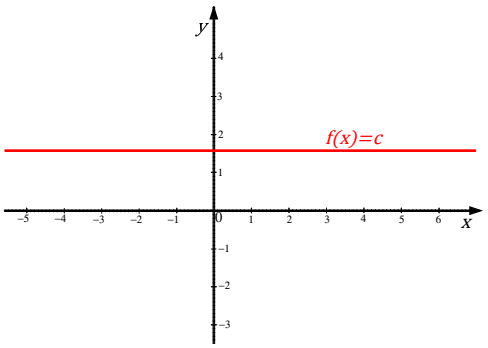
Definicija 6.1.2. *Neka je $D = \mathbb{R}$ ili $D = \langle -a, a\rangle \subseteq \mathbb{R}$. Kažemo da je funkcija $f : D \to \mathbb{R}$* ***parna*** *ako je $f(-x) = f(x)$. Funkcija f je* ***neparna*** *ako je $f(-x) = -f(x)$.*

Osnovne elementarne funkcije su:

1. Konstantna funkcija
2. Opća potencija
3. Eksponencijalna funkcija
4. Logaritamska funkcija
5. Trigonometrijske funkcije
6. Ciklometrijske funkcije

6.1.1. Konstantna funkcija

Za svaki $c \in \mathbb{R}$ definiramo funkciju $f : \mathbb{R} \to \mathbb{R}$ izrazom $f(x) = c$. Tako definiranu funkciju nazivamo **konstantnom funkcijom**. Slika funkcije f je $K(f) = \{c\}$.



Slika 1.

6.1.2. Opća potencija

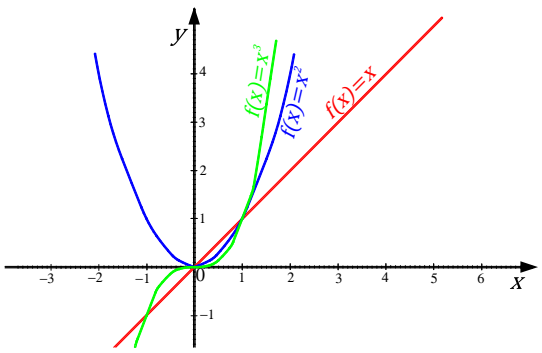
Za svaki $r \in \mathbb{R}\setminus\{0\}$ definiramo funkciju $f : D \to \mathbb{R}$, $D \subseteq \mathbb{R}$, izrazom $f(x) = x^r$. Tako definiranu funkciju nazivamo **općem potencijom**. Domenu D računamo ovisno o r, u skladu s definicijom potencije x^r, pa razlikujemo sljedeće slučajeve:

1. $r \in \mathbb{N}$,
2. $r \in \mathbb{Z}_-$,
3. $r = \frac{m}{n} \in \mathbb{Q}\setminus\mathbb{Z}$,
4. $r \in \mathbb{R}\setminus\mathbb{Q}$.

Primjedba 6.1.1. *Ne razmatramo slučaj kada je* $r = 0$ *jer je u tom slučaju funkcija* $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$, $f(x) = x^r = x^0 = 1$ *suženje konstantne funkcije.*

1. Potencije s prirodnim eksponentom

Za $r = n \in \mathbb{N}$ potencija x^r je dobro definirana za svaki $x \in \mathbb{R}$. Stoga je $D = \mathbb{R}$, tj. opća potencija je funkcija $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$. Za $n = 1, 2, 3$ opća potencija je oblika

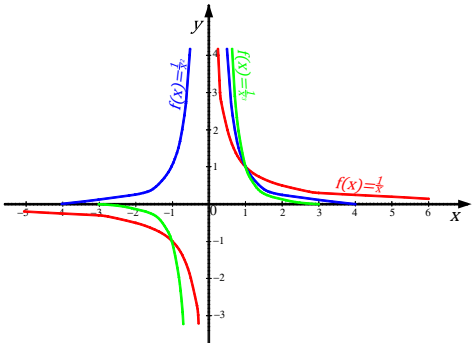


Slika 2.

Uočimo:
Ako je r paran broj, onda je $K(f) = [0, +\infty\rangle$ i f je parna funkcija.
Ako je r neparan broj, onda je $K(f) = \mathbb{R}$ i f je neparna funkcija.

2. Potencije s cijelobrojnim eksponentom

Za $r \in \mathbb{Z}_-$ potencija x^r je dobro definirana za svaki $x \in \mathbb{R}\setminus\{0\}$. Stoga je $D = \mathbb{R}\setminus\{0\}$, tj. opća potencija je $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$, $f(x) = x^r$. Za $r = -1, -2, -3$ opća potencija je oblika



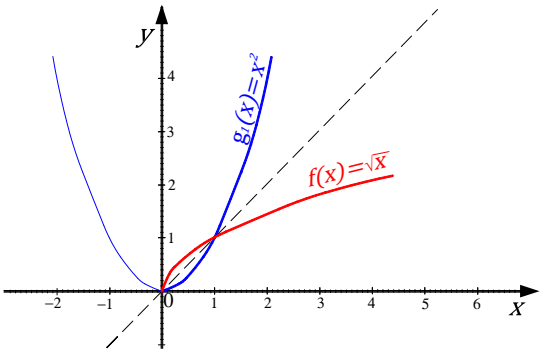
Vrijedi:
Ako je r paran broj, onda je $K(f) = \langle 0, +\infty\rangle$ i f je parna funkcija.
Ako je r neparan broj, onda je $K(f) = \mathbb{R}\setminus\{0\}$ i f je neparna funkcija.

3. Potencije s racionalnim eksponentom

(a) Za $r = \frac{1}{n}$, $n \in \mathbb{N}$, je $f(x) = x^{\frac{1}{n}} = \sqrt[n]{x}$. Razlikujemo dva slučaja:
Ako je n neparan, onda je $D = \mathbb{R}$, tj. opća potencija je $f : \mathbb{R} \to \mathbb{R}$ i $K(f) = \mathbb{R}$.
Ako je n paran, onda je $D = [0, +\infty\rangle$, tj. opća potencija je $f : [0, +\infty\rangle \to \mathbb{R}$ i $K(f) = [0, +\infty\rangle$.
Za svaki $x \in D$ vrijedi $\left(x^{\frac{1}{n}}\right)^n = x$, te za svaki $y \in K(f)$ je $(y^n)^{\frac{1}{n}} = y$.

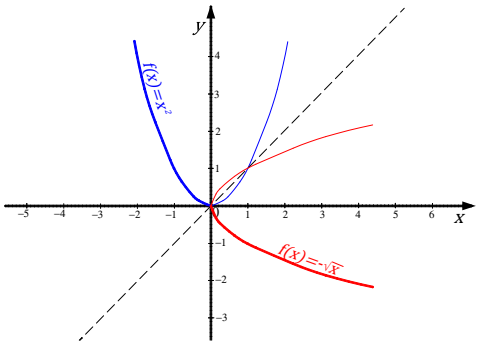
Primjer 29. *Za $r = \frac{1}{2}$ opća potencija je funkcija $f : [0, +\infty\rangle \to \mathbb{R}$, $f(x) = x^{\frac{1}{2}} = \sqrt{x}$ i $K(f) = [0, +\infty\rangle$. Kako je f strogo rastuća funkcija, to je $f : [0, +\infty\rangle \to [0, +\infty\rangle$ bijekcija. Neka je funkcija $g : \mathbb{R} \to \mathbb{R}$ zadana s $g(x) = x^2$ i $g_1 : [0, +\infty\rangle \to [0, +\infty\rangle$ njezino suženje. Funkcja g_1 je bijekcija, a njezina inverzna funkcija je upravo funkcija $f : [0, +\infty\rangle \to [0, +\infty\rangle$. Naime, za svaki $x \in [0, +\infty\rangle$ vrijedi*

$$\begin{aligned} f(g_1(x)) &= f\left(x^2\right) = \left(x^2\right)^{\frac{1}{2}} = |x| = x \quad i \\ g_1(f(x)) &= g_1\left(x^{\frac{1}{2}}\right) = \left(x^{\frac{1}{2}}\right)^2 = x. \end{aligned}$$



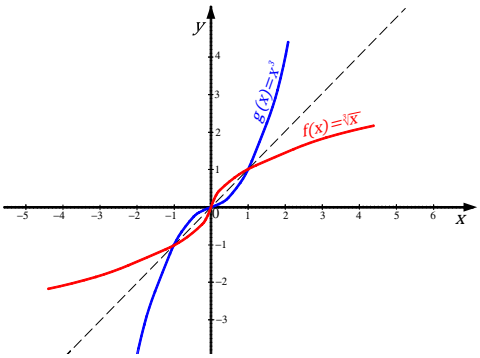
Uočimo:

Ako suženje funkcije g definiramo na način $g_2 : \langle -\infty, 0] \to [0, +\infty\rangle$, $g_2(x) = x^2$, tada je i g_2 bijekcija, a njezina inverzna funkcija je funkcija $f_2 : [0, +\infty\rangle \to \langle -\infty, 0]$ definirana sa $f_2(x) = -x^{\frac{1}{2}}$.



Primjer 30. *Za $r = \frac{1}{3}$ opća potencija je funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana s $f(x) = x^{\frac{1}{3}} = \sqrt[3]{x}$. Neka je funkcija $g : \mathbb{R} \to \mathbb{R}$ zadana s $g(x) = x^3$. Funkcja g je bijekcija, a njezina inverzna funkcija je upravo funkcija f. Naime, za svaki $x \in \mathbb{R}$ vrijedi*

$$\begin{aligned} f(g(x)) &= f\left(x^3\right) = \left(x^3\right)^{\frac{1}{3}} = x \quad i \\ g(f(x)) &= g\left(x^{\frac{1}{3}}\right) = \left(x^{\frac{1}{3}}\right)^3 = x. \end{aligned}$$

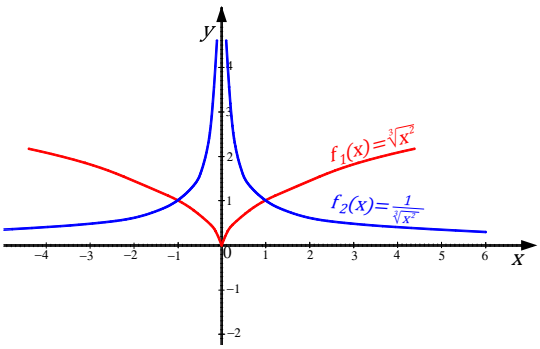


(*b*) Za ostale $r \in \mathbb{Q}\backslash\mathbb{Z}$, tj. $r = \frac{p}{n}, p \in \mathbb{Z}\backslash\{0\}, n \in \mathbb{N}\backslash\{1\}$, $m(p,n) = 1$, opća potencija je definirana sa $f(x) = x^{\frac{p}{n}} = \sqrt[n]{x^p}$. Razlikujemo četiri slučaja:

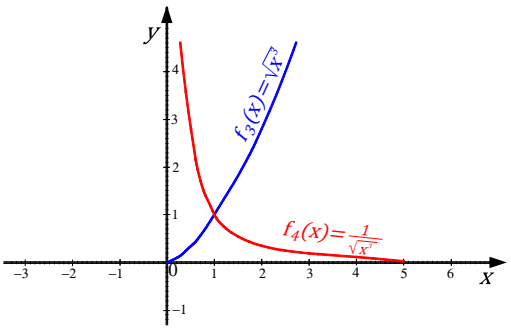
- ako je n neparan i $p > 0$, onda je $D = \mathbb{R}$,
- ako je n neparan i $p < 0$, onda je $D = \mathbb{R}\backslash\{0\}$,
- ako je n paran i $p > 0$, onda je $D = [0, +\infty\rangle$,
- ako je n paran i $p < 0$, onda je $D = \langle 0, +\infty\rangle$.

Primjer 31. *Za $r = \frac{2}{3}$ opća potencija $f_1 : \mathbb{R} \to [0, +\infty\rangle$ je definirana sa $f_1(x) = x^{\frac{2}{3}} = \sqrt[3]{x^2}$. Slika funkcije je $K(f_1) = [0, +\infty\rangle$.*

Za $r = -\frac{2}{3}$ *opća potencija* $f_2 : \mathbb{R}\setminus\{0\} \to \langle 0, +\infty\rangle$ *je definirana s* $f_2(x) = x^{-\frac{2}{3}} = \frac{1}{\sqrt[3]{x^2}}$.
Slika funkcije je $K(f_2) = \langle 0, +\infty\rangle$.

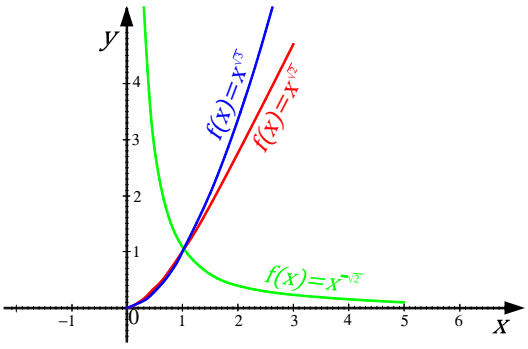


Primjer 32. *Za* $r = \frac{3}{2}$ *opća potencija* $f_3 : [0, +\infty\rangle \to \mathbb{R}$ *je definirana s* $f_3(x) = x^{\frac{3}{2}} = \sqrt{x^3}$. *Slika funkcije je* $K(f_3) = [0, +\infty\rangle$.
Za $r = -\frac{3}{2}$ *opća potencija* $f_4 : \langle 0, +\infty\rangle \to \mathbb{R}$ *je definirana s* $f_4(x) = x^{-\frac{3}{2}} = \frac{1}{\sqrt{x^3}}$.
Slika funkcije je $K(f_4) = \langle 0, +\infty\rangle$.



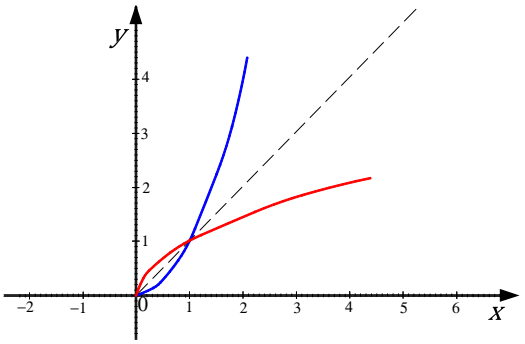
4. Potencije s realnim eksponentom

Kako je potencija x^r definirana za svaki $r \in \mathbb{R}$ kad god je $x \in \langle 0, +\infty\rangle$, to je za $r \in \mathbb{R} \setminus \mathbb{Q}$ opća potencija definirana sa $f(x) = x^r$, te
ako je $r > 0$, onda je $f : [0, +\infty\rangle \to \mathbb{R}$,
ako je $r < 0$, onda je $f : \langle 0, +\infty\rangle \to \mathbb{R}$.



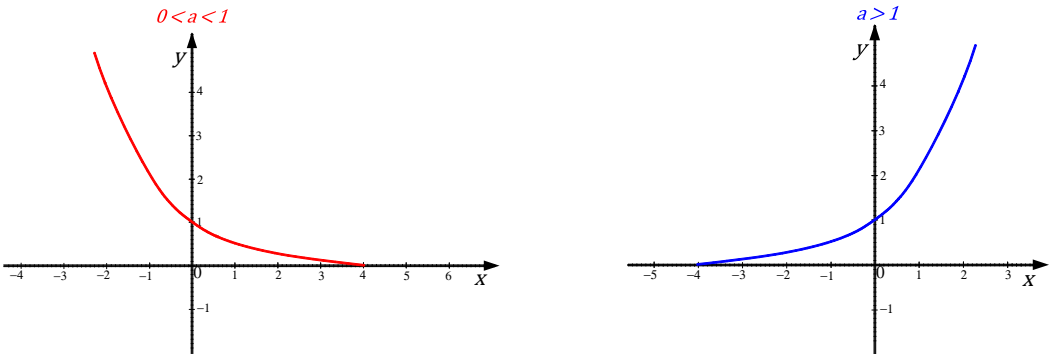
Vrijedi općenito:

Inverzna funkcija (suženja) opće potencije je opet opća potencija. Preciznije, ako je $f(x) = x^r$, onda je $f^{-1}(x) = x^{\frac{1}{r}}$, "kad god ti izrazi imaju smisla".



6.1.3. Eksponencijalna funkcija

Neka je $a \in \mathbb{R}^+ \setminus \{1\}$. Funkciju $f : \mathbb{R} \to \mathbb{R}$ definiranu s $f(x) = a^x$ nazivamo **eksponencijalnom funkcijom**. Za $0 < a < 1$ funkcija f je strogo padajuća, a za $a > 1$ strogo rastuća.



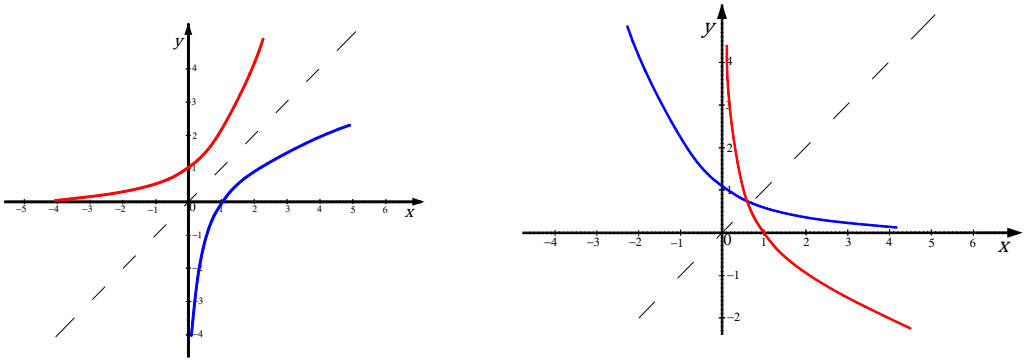
Stoga je f injekcija za svaki $a \in \mathbb{R}^+ \setminus \{1\}$ i $K(f) = \langle 0, +\infty \rangle$, pa je $f : \mathbb{R} \to \langle 0, +\infty \rangle$ bijekcija. Zbog injektivnosti vrijedi $a^x = a^y \Rightarrow x = y$,

a iz $a^x < a^y$ slijedi $\begin{cases} x < y, & a > 1 \quad \text{(rastuća)} \\ x > y, & 0 < a < 1 \quad \text{(padajuća)} \end{cases}$

6.1.4. Logaritamska funkcija

Vidjeli smo da je eksponencijalna funkcija $f : \mathbb{R} \to \langle 0, +\infty \rangle$, $f(x) = a^x$, $a \in \mathbb{R}^+ \setminus \{1\}$, bijekcija pa ima inverznu funkciju. Inverzna funkcija eksponencijalne funkcije f naziva se **logaritamska funkcija** i označava s $\log_a$. Dakle, $f^{-1} : \langle 0, +\infty \rangle \to \mathbb{R}$ je definirana s $f(x) = \log_a x$. Stoga je

$$\log_a x = y \Leftrightarrow a^y = x.$$



Nadalje, kako je $(f \circ f^{-1})(x) = x$ i $(f^{-1} \circ f)(x) = x$, to je

$$a^{\log_a x} = x \quad \text{i} \quad \log_a a^x = x.$$

Svojstva:

$$\begin{aligned} \log_a (xy) &= \log_a x + \log_a y \\ \log_a \frac{x}{y} &= \log_a x - \log_a y \\ \log_a x^k &= k \log_a x \\ \log_a x &= \frac{\log_b x}{\log_b a}. \end{aligned}$$

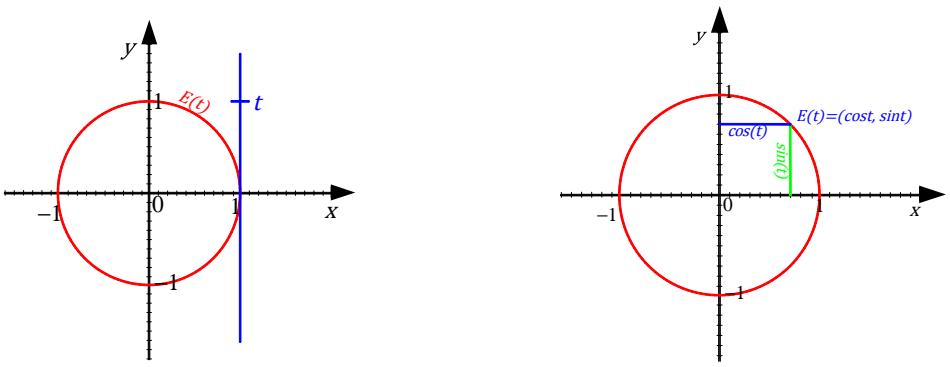
Specijalno, za $x = b$, dobivamo $\log_a b \cdot \log_b a = 1$, a za $a = b^k$ da je $\log_{b^k} x = \frac{1}{k} \log_b x$.

U primjeni važnu ulogu igraju eksponencijalne i logaritamske funkcije s bazom 10 i s bazom e, gdje je $e = 2.71828...$ transcendentan broj. Logaritam po bazi 10 nazivamo **dekadski** ili **Briggsov logaritam**, a logaritam po bazi e **prirodni logaritam**. Zbog njihove važnosti za njih koristimo posebne oznake. Tako je $\log_{10} = \log$, a $\log_e = \ln$.

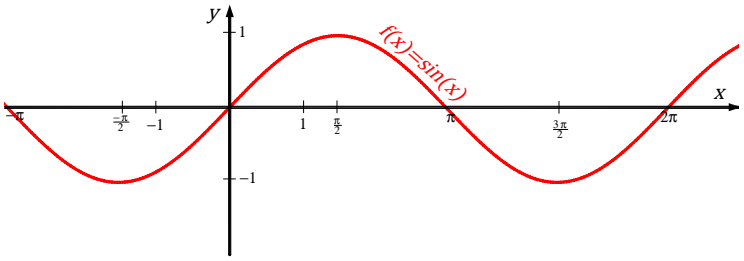
6.1.5. Trigonometrijske funkcije

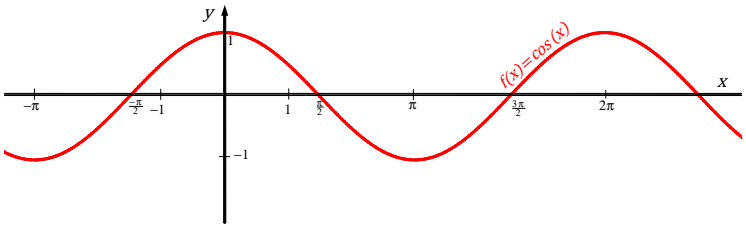
Trigonometrijske funkcije su: **sinus, kosinus, tangens i kotangens.**

Neka je dana kružnica sa središtem u točki $(0, 0)$ i polumjera $r = 1$, te pravac $x = 1$. Namatanjem pravca na kružnicu svakoj točki tog pravca pridružena je jedna točka na kružnici: $t \mapsto E(t) = (\cos t, \sin t)$- prvu koordinatu te točke označavamo sa $\cos t$, a drugu sa $\sin t$.



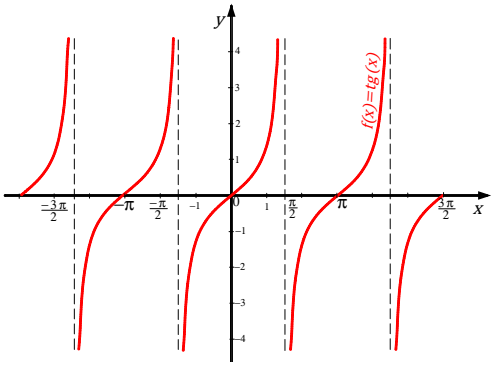
Na taj način dobili smo dva surjektivna preslikavanja $\cos, \sin : \mathbb{R} \to [-1, 1]$

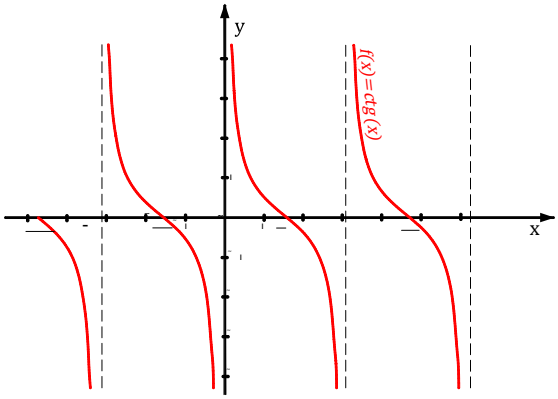




Preostale dvije trigonometrijske funkcije definirane su sa:

$\operatorname{tg} : \mathbb{R} \setminus \left\{(2k-1)\frac{\pi}{2} \mid k \in \mathbb{Z}\right\} \to \mathbb{R}$, $\operatorname{tg} x = \frac{\sin x}{\cos x}$ i $\operatorname{ctg} : \mathbb{R} \setminus \{k\pi \mid k \in \mathbb{Z}\} \to \mathbb{R}$, $\operatorname{ctg} x = \frac{\cos x}{\sin x}$



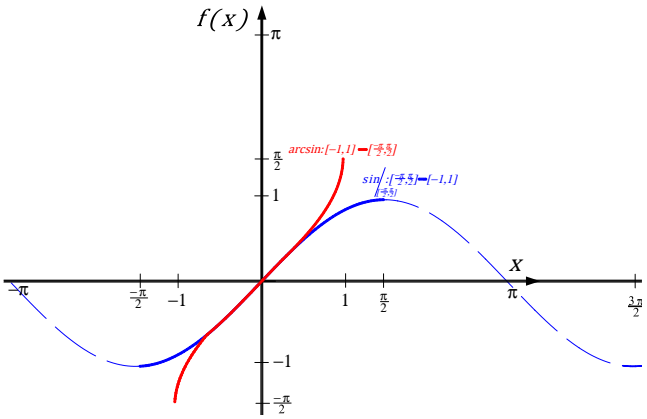


6.1.6. Ciklometrijske funkcije

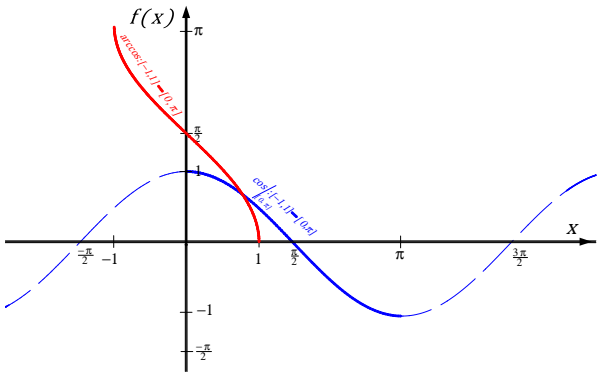
Suzimo funkciju $\sin : \mathbb{R} \to [-1, 1]$ na područje $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$.

Suženje $\sin|_{\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]} : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ je bijekcija, pa ima inverznu funkciju-

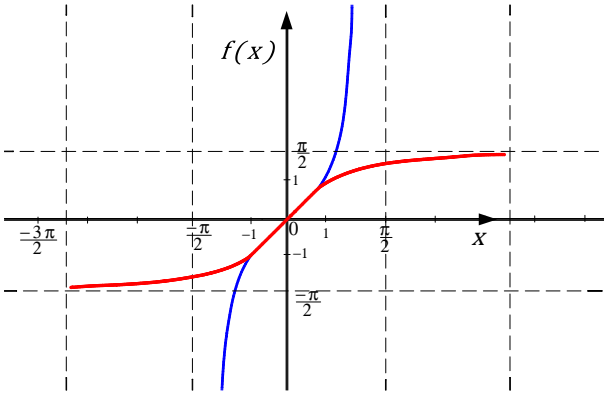
označavamo je s $\arcsin : [-1,1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$.



Suzimo funkciju $\cos : \mathbb{R} \to [-1,1]$ na područje $[0,\pi]$.
Suženje $\cos|_{[0,\pi]}: [0,\pi] \to [-1,1]$ je bijekcija pa ima inverznu funkciju-
označavamo je s $\arccos : [-1,1] \to [0,\pi]$.

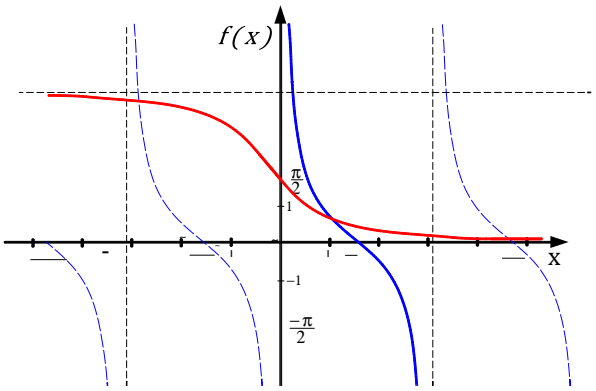


Uzmemo li jednu granu tangens funkcije, npr. na intervalu $\left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle$,
funkcija $\operatorname{tg}|_{\left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle}: \left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle \to \mathbb{R}$ je bijekcija pa ima inverznu funkciju-
označavamo je s $\operatorname{arctg} : \mathbb{R} \to \left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle$.



Uzmemo li jednu granu kotangens funkcije, npr. na intervalu $\langle 0, \pi \rangle$,
funkcija $\operatorname{ctg}|_{\langle 0,\pi \rangle}: \langle 0,\pi \rangle \to \mathbb{R}$ je bijekcija pa ima inverznu funkciju-

označavamo je s $\operatorname{arcctg} : \mathbb{R} \to \langle 0, \pi \rangle$.



6.2. Elementarne funkcije

Neka su $f, g : X \subseteq \mathbb{R} \to \mathbb{R}$ neke realne funkcije. Osnovne računske operacije definiraju se na prirodan način:

$f + g : X \to \mathbb{R}, \quad (f+g)(x) = f(x) + g(x)$;
$f - g : X \to \mathbb{R}, \quad (f-g)(x) = f(x) - g(x)$;
$f \cdot g : X \to \mathbb{R}, \quad (f \cdot g)(x) = f(x) \cdot g(x)$;
$\frac{f}{g} : X \setminus \{x \in X \mid g(x) = 0\} \to \mathbb{R}, \quad \left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)}$
$-f : X \to \mathbb{R}, \quad (-f)(x) = -f(x)$.

Definicija 6.2.1. ***Elementarnom funkcijom*** *smatramo svaku funkciju koja se može konstruirati od osnovnih elementarnih funkcija i njihovih restrikcija primjenjujući (konačno puta) zbrajanje, oduzimanje, množenje, dijeljenje i komponiranje funkcija.*

Označimo s $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ skup svih funkcija sa $\mathbb{R}$ u $\mathbb{R}$. Funkciju $o \in \mathbb{R}^{\mathbb{R}}$ definiranu s $o(x) = 0$, za svaki $x \in \mathbb{R}$, nazivamo **nul-funkcijom**.

Očito je da je zbrajanje funkcija asocijativno i komutativno (jer je takvo zbrajanje realnih brojeva). Za nul-funkciju $o \in \mathbb{R}^{\mathbb{R}}$ i za svaku funkciju $f \in \mathbb{R}^{\mathbb{R}}$ vrijedi da je $f + o = o + f = f$, pa je o neutralni element za zbrajanje. Nadalje, za svaku funkciju $f \in \mathbb{R}^{\mathbb{R}}$ postoji funkcija $-f \in \mathbb{R}^{\mathbb{R}}$ takva da je $f + (-f) = (-f) + f = o$, pa svaki $f \in \mathbb{R}^{\mathbb{R}}$ ima inverz u skupu $\mathbb{R}^{\mathbb{R}}$. Dakle, $\left(\mathbb{R}^{\mathbb{R}}, +\right)$ je Abelova grupa.

I množenje funkcija je asocijativno i komutativno, a funkcija $j \in \mathbb{R}^{\mathbb{R}} \setminus \{o\}$, gdje je $j(x) = 1$ za svaki $x \in \mathbb{R}$, je jedinični element za množenje budući da za svaku funkciju $f \in \mathbb{R}^{\mathbb{R}} \setminus \{o\}$ vrijedi da je $f \cdot j = j \cdot f = f$. Stoga je $\left(\mathbb{R}^{\mathbb{R}} \setminus \{o\}, \cdot\right)$ monoid. Nadalje, za funkciju $f \in \mathbb{R}^{\mathbb{R}} \setminus \{o\}$ vrijedi da je $f(x) \cdot \frac{1}{f(x)} = j(x)$, za svaki x za koji su obje funkcije definirane, a funkcija $\frac{1}{f} \notin \mathbb{R}^{\mathbb{R}} \setminus \{o\}$ općenito (domene im se razlikuju: $D(f) = \mathbb{R}$, a $D\left(\frac{1}{f}\right) = \mathbb{R} \setminus \{x \in \mathbb{R} \mid f(x) = 0\}$), pa $f \in \mathbb{R}^{\mathbb{R}} \setminus \{o\}$ općenito nema inverz, te $\left(\mathbb{R}^{\mathbb{R}} \setminus \{o\}, \cdot\right)$ nema strukturu grupe.

Osnovna podjela elementarnih funkcija:

1. Polinomi

2. Racionalne funkcije
3. Algebarske funkcije
4. Transcendentne funkcije

6.2.1. Polinomi

Polinomi spadaju među najjednostavnije realne funkcije.

Definicija 6.2.2. *Neka je* $n \in \mathbb{N}_0$ *i* $a_0, \ldots, a_n \in \mathbb{R}$. *Funkciju* $p_n : \mathbb{R} \to \mathbb{R}$ *definiranu s*

$$p_n(x) = a_0 + a_1 x + \cdots + a_n x^n$$

za sve $x \in \mathbb{R}$ *nazivamo* ***polinomom****. Brojevi* $a_0, \ldots, a_n$ *zovu se* ***koeficijenti*** *polinoma* p_n. *Ako je* $a_n \neq 0$, *onda kažemo da je polinom* p_n *stupnja* n *i pišemo* $\partial p_n = n$, *a broj* a_n *nazivamo* ***vodećim koeficijentom*** *polinoma* p_n. *Posebno, ako je* $a_n = 1$ *kažemo da je polinom* p_n ***normiran****.*

Očito, nul-funkcija $o \in \mathbb{R}^{\mathbb{R}}$ je polinom, nazivamo ga **nul-polinomom** i to je jedini polinom nedefiniranoga stupnja. Polinom $p_0(x) = a_0,\ a_0 \neq 0$, je polinom nultog stupnja,

$p_1(x) = a_0 + a_1 x,\ a_1 \neq 0$, polinom prvog stupnja,

$p_2(x) = a_0 + a_1 x + a_2 x^2,\ a_2 \neq 0$, polinom drugog stupnja...

S P_n označavamo skup svih polinoma stupnja $\leq n$ uključujući i nul-polinom, a s P skup svih polinoma nad $\mathbb{R}$, tj. $P = \bigcup_{n \in \mathbb{N}_0} P_n$. Skupovi $(P_n, +)$ i $(P, +)$ su Abelove grupe.

Teorem 6.2.1. *Polinom* $p_n = o$ *ako i samo ako je* $a_0 = a_1 = \cdots = a_n = 0$.

Dokaz. Smjer dovoljnosti je očigledan (iz $a_0 = a_1 = \cdots = a_n = 0$ slijedi da je $p_n = o$). Dokažimo nužnost. Neka je $p_n = o$, tj. $p_n(x) = a_0 + a_1 x + \cdots + a_n x^n = 0$ za svaki $x \in \mathbb{R}$.

Pretpostavimo da postoji $m \in \{0, 1, \ldots, n\}$ takav da je $a_0 = a_1 = \cdots = a_{m-1} = 0$ i $a_m \neq 0$.Tada je i polinom $q(x) = a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n = 0$ za svaki $x \in \mathbb{R}$, tj. $q = o$, pa za svaki $x \in \mathbb{R} \setminus \{0\}$ vrijedi

$$a_m + a_{m+1} x + \cdots + a_n x^{n-m} = 0, \quad \text{tj.} \quad a_{m+1} x + \cdots + a_n x^{n-m} = -a_m. \qquad (*)$$

Neka je $M = \max\{|a_m|, \ldots, |a_n|\} > 0$. Za $x \in \left\langle 0, \frac{1}{2} \right\rangle$ iz $(*)$ slijedi

$$\begin{aligned} |a_m| &= \left|a_{m+1} x + \cdots + a_n x^{n-m}\right| \leq |a_{m+1}|\, x + \cdots + |a_n|\, x^{n-m} \leq Mx\left(1 + x + \cdots + x^{n-m-1}\right) \\ &\leq Mx\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-m-1}}\right) = Mx\frac{1 - \frac{1}{2^{n-m}}}{1 - \frac{1}{2}} = 2Mx\frac{2^{n-m} - 1}{2^{n-m}} \leq 2Mx. \end{aligned}$$

Dakle, $\frac{|a_m|}{2M} \leq x$ za svaki $x \in \left\langle 0, \frac{1}{2} \right\rangle$.

Uzmemo li sada za x redom brojeve $\frac{1}{2^2}, \frac{1}{2^3}, \ldots, \frac{1}{2^k}, \ldots \in \left\langle 0, \frac{1}{2} \right\rangle$, dobivamo

$$\frac{|a_m|}{2M} \leq \frac{1}{2^k}, \quad \text{tj.} \quad 2^k \frac{|a_m|}{2M} \leq 1 \ \text{ za svaki } \ k \in \{2, 3, \ldots\}.$$

Kako je $\frac{|a_m|}{2M} \neq 0$, a $\mathbb{R}$ Arhimedovo polje, to za svaki $k \in \{2,3,\ldots\}$ postoji prirodni broj $n_k \in \{2,3,\ldots\}$ takav da je $n_k \frac{|a_m|}{2M} > 1$, pa je $1 < n_k \frac{|a_m|}{2M} \leq 2^{n_k} \frac{|a_m|}{2M} \leq 1$ (koristeći $i \leq 2^i$), što nije moguće $(1<1)$. Dakle, mora biti $\frac{|a_m|}{2M} = 0$, pa je $a_m = 0$, a ovo je u kontradikciji s početnom pretpostavkom. Stoga je $a_0 = a_1 = \cdots = a_n = 0$. ■

Korolar 6.2.1. *Polinomi* $p_n(x) = a_0 + a_1 x + \cdots + a_n x^n$ *i* $q_m(x) = b_0 + b_1 x + \cdots + b_m x^m$ *su jednaki ako i samo ako je* $n = m$ *i* $a_i = b_i$ *za svaki* $i \in \{1,\ldots,n\}$.

Dokaz. Smjer dovoljnosti je očigledan. Dokažimo smjer nužnosti. Neka je $p_n = q_m$. Promotrimo polinom $p_n - q_m$. Očigledno mora biti $p_n - q_m = o$, pa je po prethodnom teoremu $n = m$ i $a_i - b_i = 0$ za svaki $i \in \{1,\ldots,n\}$. ■

Teorem 6.2.2. *Neka je* g_m *polinom stupnja* m. *Za svaki polinom* p_n *stupnja* n *postoji jedinstveni uređeni par polinoma* (q,r) *takav da je*

$$p_n = q g_m + r,$$

pri čemu je $\partial r < m$ *kad god je* $r \neq o$, *a* $\partial q = n - m$ *kad god je* $n \geq m$.

Polinom q nazivamo **kvocijentom**, polinom g_m **djeliteljem** ili **divizorom**, a polinom r **ostatkom** pri djeljenju polinoma p_n polinomom g_m. Ako je $r = o$ kažemo da je polinom p_n **djeljiv** s polinomom g_m ili da je g_m njegova **mjera**.

Definicija 6.2.3. *Normirani polinom* $m(p,q)$ *nazivamo* ***najvećom zajedničkom mjerom*** *ne nul-polinoma* p *i* q *ako ima sljedeća dva svojstva:*

a) $m(p,q)$ *je mjera polinoma* p *i* q;

b) ako r *dijeli i* p *i* q, *onda* r *dijeli i* $m(p,q)$.

Egzistenciju i praktičan postupak za nalaženje najveće zajedničke mjere dvaju ne-nul polinoma dobivamo iz tzv. Euklidova algoritma za polinome koji je analogan algoritmu za prirodne brojeve.

Teorem 6.2.3. *Za svaka dva polinoma* $p, q \neq o$ *postoji najveća zajednička mjera* $m(p,q)$ *i ona je jedinstvena. Pored toga, postoje polinomi* a *i* b *takvi da je* $ap + bq = m(p,q)$ *i* $\partial a < \partial q$, $\partial b < \partial p$.

Definicija 6.2.4. *Kažemo da su polinomi* $p, q \neq o$ ***relativno prosti*** *ako je* $m(p,q) = j$.

Definicija 6.2.5. *Kažemo da je polinom* p ***ireducibilan*** *nad poljem* $\mathbb{R}$ *ako*

$$p = q \cdot g \Rightarrow \partial q = 0 \vee \partial g = 0.$$

Iz prethodnog teorema slijede sljedeće tvrdnje:

1. Ako je p relativno prost s q i g, onda je relativno prost i s $q \cdot g$;
2. Ako je q djelitelj umnoška $p \cdot g$, te p i q relativno prosti, onda q dijeli g;

3. Ako su relativno prosti polinomi q i g djelitelji polinoma p, onda je i $q \cdot g$ djelitelj od p;

4. Svaki polinom p je umnožak ireducibilnih polinoma i ta faktorizacija je jedinstvena do na permutaciju.

Pokazuje se da se svaki polinom nad $\mathbb{R}$ može faktorizirati kao

$$p_n(x) = a_n (x - x_1)^{\alpha_1} \cdot \ldots \cdot (x - x_k)^{\alpha_k} \left(x^2 + p_1 x + q_1\right)^{\lambda_1} \cdot \ldots \cdot \left(x^2 + p_s x + q_s\right)^{\lambda_s},$$

gdje su $x_1, ...x_k$ realne nule višestrukosti (kratnosti) α_i,
polinomi $x^2 + p_j x + q_j \ \ (j = 1, ..., s)$ ireducibilni nad $\mathbb{R}$, tj. nultočke su im parovi konjugirano kompleksnih brojeva,
te $(\alpha_1 + \ldots + \alpha_k) + 2(\lambda_1 + \ldots + \lambda_s) = n$.

Vidimo, dakle, da je stupanj ireducibilnih polinoma u tom rastavu manji ili jednak od 2.

Neka je p_n polinom stupnja n nad poljem $\mathbb{C}$. Tada vrijedi:

1. Ako je $z = a + bi \in \mathbb{C}$ nula polinoma, onda je i $\overline{z} = a - bi$ nula tog polinoma.

2. Ako je x_0 nul-točka (nula) polinoma p_n, onda je $p_n(x) = (x - x_0) \cdot p_{n-1}(x)$.

3. Polinom $n-$tog stupnja ima točno n nul-točaka (računajući višestruke).

Ovo nas vodi do sljedećeg teorema koji kazuje da se nad poljem $\mathbb{C}$ (za razliku od polja $\mathbb{R}$) svaki polinom može prikazati kao umnožak ireducibilnih polinoma stupnja točno jedan.

Teorem 6.2.4. *Neka je p_n polinom n-tog stupnja nad poljem $\mathbb{C}$, $n \in \mathbb{N}$. Tada postoji barem jedan kompleksni broj z_0 takav da je $p_n(z_0) = 0$. Štoviše, postoje kompleksni brojevi $z_1, \ldots, z_n \in \mathbb{C}$ (ne nužno različiti) takvi da je*

$$p_n(z) = a_n (z - z_1) \cdots (z - z_n).$$

Primjer 33. *Polinom p_2 definiran s $p_2(x) = 1 + x^2$ je ireducibilan nad $\mathbb{R}$ i nema nijednu nul-točku. S druge strane, $p_2(x) = (x - i)(x + i)$, pa ovaj polinom nad $\mathbb{C}$ ima dvije nul-točke i reducibilan je.*

6.2.2. Racionalne funkcije

Definicija 6.2.6. *Neka su p_n i q_m polinomi stupnja n i m, te $S = \{x \in \mathbb{R} : q_m(x) \neq 0\} \subseteq \mathbb{R}$. Funkciju $Q = \frac{p_n}{q_m} : S \to \mathbb{R}$ definiranu s*

$$Q(x) = \frac{p_n(x)}{q_m(x)} = \frac{a_n x^n + \ \ldots \ + a_1 x + a_0}{b_m x^m + \ \ldots \ + b_1 x + b_0}, \quad za\ sve\ x \in S,$$

*nazivamo **racionalnom** funkcijom.*
*Kažemo da je racionalna funkcija $Q \neq o$ **kanonskog oblika** ako je $m(p_n, q_m) = j$.*
*Racionalna funkcija Q je **prava** ako je $n < m$.*

Nultočke polinoma q_m nazivamo **polovima** racionalne funkcije. Primijetimo, ako je $m = 0$, onda je funkcija Q polinom.

Kako je $p_n = qq_m + r$, za neki par polinoma (q, r), to se Q može prikazat u obliku

$$Q = \frac{p_n}{q_m} = q + \frac{r}{q_m},$$

gdje je $\frac{r}{q_m}$ prava racionalna funkcija i ovaj prikaz je jedinstven.

Definicija 6.2.7. *Prava racionalna funkcija* $\frac{r}{q}$ *je* ***prosti*** *ili* ***parcijalni razlomak*** *ako je* $q = p^k$, *pri čemu je polinom* p *neki ireducibilni polinom nad* $\mathbb{R}$ *i* $\partial r < \partial p$.

Teorem 6.2.5. *Svaka prava racionalna funkcija* $Q = \frac{p}{q}$, $p, q \neq o$, *može se na jedinstven način prikazati kao zbroj prostih razlomaka.*

6.2.3. Algebarske funkcije

Definicija 6.2.8. *Elementarne funkcije koje se mogu dobiti komponiranjem općih potencija s racionalnim eksponentima i racionalnih funkcija s racionalnim koeficijentima nazivamo* ***algebarskim funkcijama****.*

Primjer 34. *Funkcija* $f : X \subseteq \mathbb{R} \longrightarrow \mathbb{R}$,

$$f(x) = \sqrt[4]{\left(\frac{x^2+1}{2x^3-5x}\right)^5} \quad \text{je algebarska funkcija,}$$

a funkcije $g_1, g_2 : \mathbb{R} \longrightarrow \mathbb{R}$, $g_1(x) = (x^4+7)^{\sqrt{2}}$, $g_2(x) = \left(\sqrt{3}x + 2\right)$ *nisu algebarske funkcije.*

Očito je da su racionalne funkcije s racionalnim koeficijentima ujedno algebarske funkcije. Algebarske funkcije koje nisu racionalne nazivamo **iracionalnim** funkcijama.

6.2.4. Transcendentne funkcije

Definicija 6.2.9. *Elementarne funkcije koje nisu algebarske nazivamo* ***transcendentnim*** *funkcijama.*

Dakle, u ovu klasu funkcija ubrajaju se sve eksponencijalne, logaritamske, trigonometrijske i ciklometrijske, kao i većina racionalnih fukcija (sve one kojima je neki koeficijent iracionalan broj).

Važne transcendentne funkcije su i tzv. **hiperbolne funkcije**, koje se dobiju pomoću prirodne eksponencijalne funkcije $f(x) = \mathrm{e}^x$.

6.2.5. Hiperbolne funkcije

Definiramo:

sinus hiperbolni: $\operatorname{sh} : \mathbb{R} \longrightarrow \mathbb{R}, \qquad \operatorname{sh} x = \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{2},$

kosinus hiperbolni: $\operatorname{ch} : \mathbb{R} \longrightarrow \mathbb{R}, \qquad \operatorname{ch} x = \dfrac{\mathrm{e}^x + \mathrm{e}^{-x}}{2},$

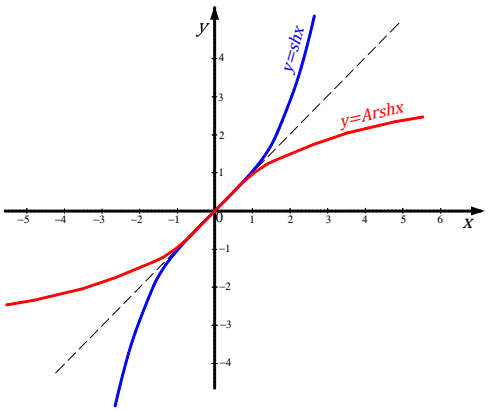
tangens hiperbolni: $\operatorname{th} : \mathbb{R} \longrightarrow \mathbb{R}, \qquad \operatorname{th} x = \dfrac{\operatorname{sh} x}{\operatorname{ch} x} = \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{\mathrm{e}^x + \mathrm{e}^{-x}},$

kotangens hiperbolni : $\operatorname{cth} : \mathbb{R}\setminus\{0\} \longrightarrow \mathbb{R}, \qquad \operatorname{cth} x = \dfrac{1}{\operatorname{th} x} = \dfrac{\mathrm{e}^x + \mathrm{e}^{-x}}{\mathrm{e}^x - \mathrm{e}^{-x}}.$

Vrijedi: $\operatorname{ch}^2 t - \operatorname{sh}^2 t = 1$,pa preslikavanje $t \mapsto (\operatorname{ch} t, \operatorname{sh} t)$ svakoj točki $t \in \mathbb{R}$ pravca pridružuje točku na hiperboli (desne grane) $x^2 - y^2 = 1 \quad (x \geq 1)$, slično kao što je i $(\cos t, \sin t)$ točka kružnice $x^2 + y^2 = 1$ za svaki $t \in \mathbb{R}$.

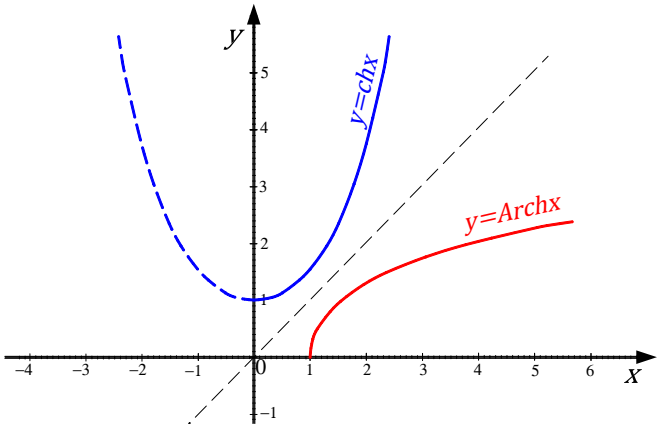
6.2.6. Area funkcije

Funkcija sinus hiperbolni $\operatorname{sh} : \mathbb{R} \longrightarrow \mathbb{R}$, $\operatorname{sh} x = \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}$ je bijekcija, pa postoji njoj inverzna funkcija **area sinus hiperbolni:** $\operatorname{Arsh} : \mathbb{R} \longrightarrow \mathbb{R}$, $\operatorname{Arsh} x = \ln\left(x + \sqrt{x^2+1}\right)$.



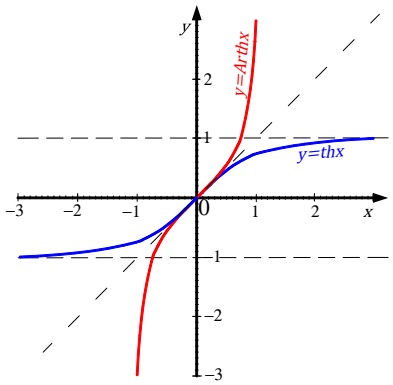
Funkcija kosinus hiperbolni $\operatorname{ch} : [0,\infty\rangle \longrightarrow [1,\infty\rangle\,,\ \operatorname{ch} x = \dfrac{\mathrm{e}^x + \mathrm{e}^{-x}}{2}$ je bijekcija, pa postoji inverzna funkcija **area kosinus hiperbolni** :

$\operatorname{Arch} : [1,\infty\rangle \longrightarrow [0,\infty\rangle\,,\ \operatorname{Arch} x = \ln\left(x + \sqrt{x^2-1}\right)$.



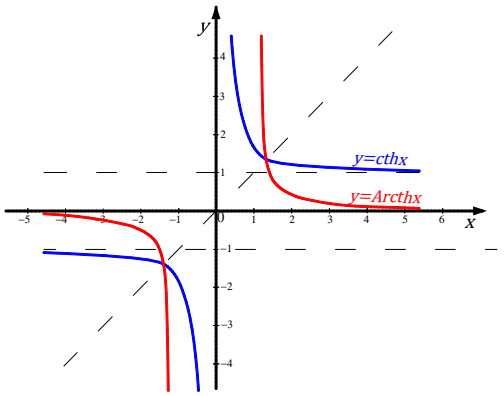
Funkcija tangens hiperbolni $\operatorname{th} : \mathbb{R} \longrightarrow \langle -1,1\rangle\,,\ \operatorname{th} x = \dfrac{\mathrm{e}^x - \mathrm{e}^{-x}}{\mathrm{e}^x + \mathrm{e}^{-x}}$ je bijekcija, pa postoji inverzna funkcija te funkcije **area tangens hiperbolni** :

$\operatorname{Arth} : \langle -1,1\rangle \longrightarrow \mathbb{R},\ \operatorname{Arth} x = \frac{1}{2}\ln\frac{1+x}{1-x}$.



Funkcija kotangens hiperbolni $\operatorname{cth} : \mathbb{R}\setminus\{0\} \longrightarrow \mathbb{R}\setminus[-1,1]\,,\ \operatorname{cth} x = \dfrac{\mathrm{e}^x + \mathrm{e}^{-x}}{\mathrm{e}^x - \mathrm{e}^{-x}}$ je bijekcija, pa postoji inverzna funkcija te funkcije **area kotangens hiperbolni**:

$\operatorname{Arcth} : \mathbb{R}\setminus[-1,1] \longrightarrow \mathbb{R}\setminus\{0\}\,,\ \operatorname{Arcth} x = \frac{1}{2}\ln\frac{x+1}{x-1}$.



Dokaz radi duljine preskačemo. Može se naći u [4].

Bibliografija

[1] A. Čižmešija, *Elementarna matematika I*, predavanja.

[2] P. J. Davis, R. Hersh, E. A. Marchisotto, *Doživljaj matematike*, Tehnička knjiga, Zagreb, 2004.

[3] K. Kuratowski, A. Mostowski, *Set Theory*, North-Holand Publishing Company Amsterdam, 1968.

[4] S. Kurepa, *Uvod u matematiku*, Tehnička knjiga, Zagreb, 1979.

[5] S. Mardešić, *Matematička analiza I*, Školska knjiga, Zagreb, 1988.

[6] P. Papić, *Uvod u teoriju skupova*, Hrvatsko matematičko društvo, Zagreb, 2000.

[7] N. J. Vilenkin, *Priče o skupovima*, Školska knjiga, Zagreb, 1975.

[8] M. Vuković, *Matematička logika I*, skripta Matematičkog odjela PMF-a, 2004.