Uvod u matematiku

M. Klaričić Bakula, S Braić

Split, 2008/09.

Sadržaj

Uvod **iii**

1. Građa matematike **1**
1.1. Simboli . . . 1
1.2. Apstrakcija . . . 2
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 nasuprot dijalektičkoj matematici . . . 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 . . . 13
2.2. Logika prvog reda . . . 15
2.2.1. Uvod . . . 15
2.2.2. Jezik logike prvog reda . . . 16

3. Skupovi **19**
3.1. Osnovni pojmovi . . . 19
3.2. Zadavanje skupova . . . 20
3.3. Booleove operacije na skupovima . . . 21
3.4. Kartezijev umnožak skupova . . . 25

4. Relacije **28**
4.1. Osnovni pojmovi . . . 28
4.2. Relacije ekvivalencije . . . 33
4.3. Relacije uređaja . . . 36
4.4. Funkcije . . . 38

5. Skupovi brojeva **44**
5.1. Skup prirodnih brojeva 44
5.1.1. Uvod 44
5.1.2. Rekurzivna definicija niza 45
5.1.3. Zbrajanje na skupu $\mathbb{N}$ 46
5.1.4. Množenje na skupu $\mathbb{N}$ 49
5.1.5. Daljnja svojstva skupa $\mathbb{N}$ 52
5.1.6. O uređenosti skupa $\mathbb{N}$ 54
5.2. Skup cijelih brojeva 55
5.2.1. Uvod 55
5.2.2. Zbrajanje i množenje na $\mathbb{Z}$ 56
5.2.3. O uređenosti skupa $\mathbb{Z}$ 58
5.2.4. Ulaganje prirodnih u cijele brojeve 60
5.3. Djeljivost i kongruencije 61
5.3.1. Djeljivost 61
5.3.2. Prosti brojevi 64
5.3.3. Kongruencije 66
5.4. Skup racionalnih brojeva 68
5.4.1. Uvod 68
5.4.2. Zbrajanje i množenje na $\mathbb{Q}$ 69
5.4.3. Ulaganje cijelih u racionalne brojeve 72
5.4.4. O uređenosti skupa $\mathbb{Q}$ 73
5.5. Skup realnih brojeva 74
5.5.1. Aksiomi skupa realnih brojeva 74
5.5.2. Apsolutna vrijednost 78
5.5.3. Cijeli i racionalni brojevi u skupu realnih brojeva 80
5.5.4. Binomni teorem 83
5.6. Skup kompleksnih brojeva 85
5.6.1. Uvod 85
5.6.2. Trigonometrijski oblik kompleksnog broja 89

6. Elementarne funkcije **90**
6.1. Polinomi 90
6.2. Racionalne funkcije 94

Bibliografija **96**

Uvod

Najstarije poznate matematičke pločice potječu iz 2400. godine prije Krista, no zasigurno se uporaba matematike proteže na cijelu civilizaciju. Tijekom 5000 godina razvila se golema količina postupaka i pojmova poznatih kao matematika i na mnogo načina se 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 je građa 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 treba 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 dijelom se bavi pitanjima prostornih mjerenja (udaljenost, površina), no bavi se i onim aspektima prostora koji imaju estetski značaj ili element iznanađenja. 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, no ne i pravilnim peterokutima.

Predajemo li geometriju po 2300 godina starom Euklidovom učenju, onda ona ima još jedan važan aspekt, a to je njena prezentacija kao *deduktivne znanosti.* Počevši od izvjesnog broja osnovnih ideja koje uzimamo 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 počevši od hipoteza dolazimo do zaključaka naziva se dokaz. 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 drevnim matematičarima, oni nisu bili naglašavani sve do 19. stoljeća kada se mislilo da u geometriji postoji dokaz, dok ga u algebri ili aritmetici nema. S povećanim naglaskom na deduk-

tivne 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 60000 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 je donedavno smatralo da dobar student može savladati cjelokupnu matematiku, no danas se to ne bi moglo reći. Sada se smatra da bi dobro obrazovani matematičar mogao imati osnovna znanja o otprilike 10% raspoloživog matematičkog saznanja. Naime, matematika se često prikazuje kao snažno stablo s korijenjem, deblom, granama i grančicama označenima prema pojedinim disciplinama. To je stablo koje 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 njen izdanak. Takve serijske ovisnosti uglavnom nema u drugim disciplinama.

Koliko bi matematičkih knjiga trebao poznavati budući matematičar? Ako računamo jednu knjigu po kolegiju, pa još udvostručimo rezultat zbog dodatne i neobavezne literature, doći ćemo do broja od oko 60 knjiga. Možemo tako gledati na onih 60000 knjiga kao na ocean znanja čija prosječna dubina iznosi 60 knjiga, iz čega slijedi da postoji oko 1000 uskih područja u matematici, no to je samo jednostavna i gruba procjena. Američko matematičko društvo daje finiju podjelu na otprilike 3000 kategorija matematičkih radova. U većini tih kategorija nova se znanja stvaraju sve većom brzinom: ocean se povećava i u dubinu i u širinu.

No 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 na nijednu 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 decimalnog sustava 0,1,2,3,4,5,6,7,8,9, znakove za aritmetičke operacije + , - , $\cdot$, : , znakove grupiranja ( ), {} , [ ] i znakove za relacije poput =,<,>. 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 novi.

Neki se često korišteni simboli mogu pripisati poznatim autorima: npr. oznaku $n!$ dugujemo Christianu Krampu (1808.), a slovo e kao oznaku za 2.71828... dugujemo Leonhardu Euleru (1707-1783). Neki su simboli skraćeni oblici riječi: tako je + skraćenica za riječ "et", π označava početno slovo riječi "periferija", $\int$ je početno slovo riječi "suma" i tako dalje. S druge strane, neki simboli se čine potpuno proizvoljnima.

Glavne su funkcije simbola u matematici da precizno i jasno označavaju i da skraćuju. Zapravo, bez korištenja kratica matematičko bi izražavanje jedva bilo moguće.

Posebno navodimo slova grčkog alfabeta jer se vrlo često koriste u matematici.

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

1.2. Apstrakcija

Smatra se da je matematika nastala kad je predodžba o tri jabuke oslobođena od jabuka i postala cijeli broj tri. To je primjer procesa apstrakcije, no kako se pojam apstrakcije u matematici koristi u nekoliko različitih smislova, potrebno ga je pobliže objasniti.

1.2.1. Apstrakcija kao idealizacija

Dijete olovkom, pomoću ravnala, povlači crtu po papiru da bi mu poslužila kao vodić dok bude rezalo. 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.

Uz ravnu crtu dolazimo do mnogih idealizacija: ravnine, kružnice, kvadrata, sfere, kocke. Neki od tih pojmova se ne definiraju (točka, pravac, ravnina). Drugi se, pak, definiraju pomoću jednostavnijih pojmova (kocka). Razumljivo je da će svaki stvarni primjer pokazivati nesavršenosti, no um će to velikodušno previdjeti.

Idealizacije koje su spomenute prešle su 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. Tu je riječ o stvarnim objektima, no s druge strane imamo apstraktne brojeve koji postoje bez obzira na ptice i naranče.

Danas matematika uglavnom ostavlja po strani pitanje kako su nastale takve apstrakcije i usredotočuje se na skupovno-teoretski opis oblikovanja apstrakcije. Apstraktni pojam "četiri" je skup 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 ABC jednakostraničan trokut, onda je kut uz vrh A jednak kutu uz vrh B." Zatim je neki drugi matematičar Y primijetio da iako je to točno, nije neophodno da trokut ABC

bude jednakostraničan. Y bi stoga mogao ustvrditi: 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) informacija: nekoliko usko povezanih činjenica ekonomično se umotaju u jedan paket. Pogledajmo primjer:

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 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, a s namjerom da učine matematički dokaz strožim. No ta se svrha nije mogla ispuniti sve dok je pisanje i čitanje dokaza bilo namjenjeno ljudima. 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 klasičnih djelova 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. Imenice označavaju matematičke objekte, npr. broj 3, skup prostih brojeva, logaritamsku funkciju... Matematičke strukture su nešto složenije i označavaju

matematičke objekte povezane izvjesnim relacijama, no razlika između njih i matematičkih objekata nije strogo određena. Ako se neka matematička struktura dugo koristi i na njoj se 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.

Termin "matematički objekt" podrazumijeva da objekt o kojemu se radi na neki način postoji. Mogli bismo pomisliti da je pojam postojanja sasvim jasan, no u stvarnosti su s njim 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 da li je matematička beskonačnost prijevara? Označava li ona nešto što zapravo uopće nije beskonačno? Zašto bismo povjerovali da beskonačno postoji? U formalnoj prezentaciji taj je zahtjev ispunjen aksiomatizacijom: uveden je aksiom beskonačnosti koji kaže da induktivni (beskonačni) skup postoji.

1.6. Oblici matematičkog mišljenja

Mišljenje se u psihologiji definira kao izdvajanje određenih strana i svojstava promatranog objekta i njihovo dovođenje u odgovarajuće veze s drugim objektima u cilju spoznaje tog objekta i 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*. *Sud* je svaka suvisla izjavna rečenica koja je istinita ili lažna, ali ne oboje. Pogledajmo primjer za svaki od ovih rezultata oblika razmišljanja.

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

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

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

Oblici mišljenja imaju veliki značaj u matematičkim teorijama. 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 nekog broja pojmova koji se ne definiraju, a nazivamo ih *osnovnim pojmovima*. To znači da 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*. Svaki novi pojam uvodimo *definicijom* pomoću osnovnih pojmova (to jest, unutar jezika teorije). Svaku novu *tvrdnju* dokazujemo logičkim zaključivanjem na osnovu definicija, aksioma i tvrdnji koje smo već dokazali. Obično se zahtjeva da izabrani aksiomi zadovoljavaju sljedeća tri principa:

1. **konzistentnost**, tj. iz sustava aksioma ne smije se moći dokazati istodobno neka tvrdnja i njena negacija;
2. **potpunost**, tj. svaka tvrdnja, ili njena negacija, je dokaziva u danom sustavu aksioma;
3. **neovisnost**, tj. niti jedan od aksioma se ne može dobiti kao posljedica ostalih.

Dakle, možemo reći da je neko matematičko područje tvorevina osnovnih pojmova, aksioma, izvedenih pojmova i dokazanih tvrdnji. No pogledajmo podrobnije na što mislimo pod tim nazivima.

1.6.1. Matematički pojmovi

Matematički pojam je oblik mišljenja u kojem se odražavaju bitna svojstva objekata koji se proučavaju. *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 točka, pravac, skup... *Izvedeni pojam* je pojam koji se jasno i precizno definira, što znači da se njegovo značenje opisuje pomoću osnovnih i ranije definiranih pojmova. Dakle, *definicija pojma* je nabrajanje nužnih i dovoljnih obilježja toga pojma povezanih logičkom rečenicom ili simboličkim zapisom.

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.

Dakle, neki se pojam može često definirati na više načina, no važno je da sve definicije moraju određivati isti skup objekata, tj. moraju biti međusobno ekvivalentne. Ako odaberemo jednu od tih definicija kao radnu definiciju toga pojma, onda njoj ekvivalentne definicije poprimaju značenje poučaka koji su njene posljedice. To su tzv. *karakterizacije* toga pojma.

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.
5. Definicija ne smije biti negativna ako može biti pozitivna.
6. Mora postojati barem jedan objekt kojeg definicija opisuje.

1.6.2. Aksiomi

Aksiom je polazna tvrdnja koja se smatra istinitom i koja 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 tim 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 skalar $\alpha \in \mathbb{R}$ 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 svaki izbor vektora $\overrightarrow{a}$, $\overrightarrow{b} \in V^3$.

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 (*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 u njemu razmatra određeni objekt, te

2. što se o tomu objektu tvrdi.

Prema tomu, u formuliranju teorema razlikujemo dva dijela: *pretpostavka* (uvjet, hipoteza, premisa) P i *tvrdnja* (zaključak, posljedica, konkluzija) Q. Ključne riječi su "**Ako je** P, **onda je** Q."

Pogledajmo nekoliko primjera.

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

U matematici je teorem za koji postoji kratki i jednostavni dokaz uobičajeno zvati *propozicija*. Teoreme koji sami za sebe nisu od posebnog značaja, nego služe kao etape u dokazu nekog važnijeg teorema, nazivamo *lemama*. Konačno, teorem koji je neposredna i jednostavna posljedica drugog, prethodno dokazanog teorema, nazivamo *korolarom* toga teorema. Dokazi korolara su često toliko očiti da ih 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 Q. Pogledajmo jedan primjer.

Teorem. Zbroj kutova u svakom trokutu je 180^0.

Dokaz. P: Neka je $\triangle$ABC po volji odabrani trokut, te označimo $\alpha = \measuredangle CAB$, $\beta = \measuredangle ABC$ i $\gamma = \measuredangle ACB$.

Q: $\alpha + \beta + \gamma = 180^0$.

Vrhom C trokuta 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 kutovi $\measuredangle DCA$ i $\measuredangle CAB$, odnosno $\measuredangle BCE$ i $\measuredangle ABC$ imaju paralelne krakove. Prema *Poučku o kutovima s paralelnim kracima* vrijedi

$$\begin{aligned} \measuredangle DCA &= \measuredangle CAB = \alpha, \\ \measuredangle BCE &= \measuredangle ABC = \beta. \end{aligned}$$

Kutovi $\measuredangle DCA$, $\measuredangle ACB$ i $\measuredangle BCE$ zajedno tvore ispruženi kut, pa je

$$\alpha + \beta + \gamma = \measuredangle DCA + \measuredangle ACB + \measuredangle BCE = 180^0.$$

■

Indirektni dokaz tvrdnje Q je direktni dokaz teorema u kome je pretpostavka negacija tvrdnje Q (u oznaci $-Q$), a tvrdnja neka očigledna neistina. Ako takav teorem dokažemo, onda po načelu isključenja trećega zaključujemo da je Q istinita.

Među indirektnim dokazima najčešće se primjenjuju sljedeća dva: dokaz svođenjem na kontradikciju i dokaz obratom po kontrapoziciji. Pogledajmo najprije primjer dokaza svođenjem na kontradikciju.

Teorem. Ako su a i b pozitivni realni brojevi, onda je $(a+b)/2 \geq \sqrt{ab}$.

Dokaz. Pretpostavimo 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 $(a+b)/2 \geq \sqrt{ab}$. ■

U narednom dajemo primjer dokaza obratom po kontrapoziciji.

Teorem. Ako je $n \in \mathbb{N}$ i n^2 neparan broj, onda je i n neparan broj.

Dokaz. Pretpostavimo da je n paran broj. On je tada oblika $n = 2k$, za neki $k \in \mathbb{N}$. No iz ovoga slijedi $n^2 = 4k^2 = 2\left(2k^2\right)$, pa je n^2 paran broj. Ovo je u kontradikciji s početnom pretpostavkom da je n^2 neparan broj $\Rightarrow\Leftarrow$. Dakle, n mora biti neparan. ■

1.7. Algoritamska nasuprot dijalektičkoj matematici

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

Algoritamsko rješenje. Iz $x^2 = 2$ slijedi $x = 2/x$. Ako je x neznatno podcijenjen, onda će $2/x$ biti neznatno precijenjen. Na pola puta između podcijenjenog i precijenjenog biti će pravo rješenje. Dakle, definiramo li niz (x_n) kao

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

onda taj 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 $x = 1$ je $f(1) = -1$, a za $x = 2$ je $f(2) = 2$. Kako se x neprekidno mijenja od -1 do 2, tako se $f(x)$ neprekidno mijenja od negativne prema pozitivnoj vrijednosti. stoga negdje između 1 i 2 mora biti vrijednost od x za koju je $f(x) = 0$, tj. $x^2 = 2$. Detalji argumentacije slijede iz svojstava skupa realnih brojeva i neprekidnih funkcija definiranih na njemu.

U izvjesnom smislu, ni prvo ni drugo rješenje nije uistinu rješenje. Prvo 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? U okviru algoritamske matematike postavili bismo na neki način problem nalaženja takvog pravca. U okviru dijalektičke matematike možemo odgovoriti da takav pravac postoji, a da ništa ne radimo. Treba samo primijetiti da ako pomičemo takav pravac s lijeva na desno, dio trokuta s lijeve strane pravca se neprekidno mijenja od 0% do 100%, pa tako mora postojati pozicija gdje je taj dio točno 50%. No također možemo primijetiti da specifična svojstva trokuta uopće nisu korištena; isti argument bi vrijedio za bilo kakvo područje. I tako ustvrđujemo da za svaki lik postoji vertikalni pravac koji ga raspolavlja, iako ga ne znamo naći, niti znamo površinu toga područja koje raspolavljamo. Ipak, 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 knjige *Doživljaj matematike* autora Davisa, Hersha i Marchisotta [2], te iz [1].

Poglavlje 2.

Osnove matematičke logike

2.1. Logika sudova

2.1.1. Uvod

Jedan od osnovnih problema u matematičkoj logici je ispitati istinitost neke rečenice (logičke forme) i to promatrajući samo njen oblik, a ne i sadržaj. Logika sudova, ili propozicijska logika, je jedna od najjednostavnijih formalnih teorija. U njoj rečenice promatramo kao forme sastavljene od "atomarnih" djelova koji su povezani veznicima: *ne*, *i*, *ili*, *ako...onda* i *ako i samo ako* (pišemo *akko*).

Podsjetimo se: sud je svaka suvisla izjavna rečenica koja je istinita ili lažna, ali ne oboje. Ovo svakako ne može biti definicija suda, jer se može postaviti pitanje što je rečenica, ili pak što je 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.

Sudovi (1) i (2) su jednostavnog oblika, tj. atomarni su. Pomoću veznika *ne*, *i*, *ili*, *ako...onda* i *ako i samo ako* iz jednostavnih sudova možemo graditi 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:

$$\frac{\begin{array}{c}\text{Ako pada kiša, onda nosim kišobran.}\\ \text{Pada kiša.}\end{array}}{\text{Nosim kišobran.}}$$

je primjer korektnog zaključivanja. Formalno zapisano, ono je oblika

$$\frac{\begin{array}{c}A \longrightarrow B\\ A\end{array}}{B},$$

a 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

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

Dakle, važno je razlučiti koje je zaključivanje korektno, odnosno što je logička posljedica.

Formalno matematičko zaključivanje čini se 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.

Ovo je poglavlje, uz manje izmjene, preuzeto iz [6].

2.1.2. Jezik logike sudova

Sada ćemo definirati koji su osnovni znakovi logike sudova i kako gradimo formule: kada je to zadano smatramo da je zadan jezik teorije. No prije definicije formula uvest ćemo još neke pojmove.

Skup je osnovni pojam u matematici 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", "familija" ili slično. Skupovima ćemo se više 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 u abecedi A. Po dogovoru smatramo da skup svih riječi proizvoljne abecede sadrži praznu riječ ε. Najvažnija operacija na skupu riječi je *konkatenacija*: ako su a i b oznake za riječi, onda kažemo da je riječ ab nastala konkatenacijom riječi a i b.

Primjer 1. *Neka je* $A = \{\alpha, \beta\}$. *Tada riječi* $\alpha\alpha\beta\alpha$ *i* $\beta\alpha\beta\beta\alpha$ *pripadaju skupu* A^*. *Njihovom konkatenacijom možemo dobiti riječ* $\alpha\alpha\beta\alpha\beta\alpha\beta\beta\alpha$ *koja je također u skupu* A^*.

Abeceda logike sudova je skup čiji su elementi:

1. $P_0, P_1, P_2, \ldots$ koje nazivamo propozicijskim varijablama,
2. $-, \wedge, \vee, \longrightarrow, \longleftrightarrow$ koje nazivamo logičkim veznicima,
3. pomoćni simboli $(\ ,\ )$.

Logičke veznike nazivamo redom: *negacija* $(-)$, *konjukcija* $(\wedge)$, *disjunkcija* $(\vee)$, *kondicional* $(\longrightarrow)$ i *bikondicional* $(\longleftrightarrow)$.

Sada ćemo definirati najvažnije riječi abecede logike sudova, a to su formule.

Definicija 2.1.1. *Atomarna formula je svaka propozicijska varijabla. Formula je definirana sa:*

a) svaka atomarna formula je formula,

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

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

Primjedba 2.1.1. *Općenito ćemo formule označavati velikim latiničnim slovima s početka abecede (A, B, C, F, G,...), dok ćemo za propozicijske varijable koristiti velika latinična slova s kraja abecede (P, Q, R, S, V,...).*

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 $(((-P) \wedge Q) \longrightarrow R)$ pišemo kao $(-P \wedge Q) \longrightarrow R$.

2.1.3. Semantika

Svako preslikavanje sa skupa propozicijskih varijabli u skup $\{0, 1\}$ nazivamo interpretacijom. Po složenosti formule definiramo interpretacije na proizvoljnim formulama u skladu s danom semantičkom tablicom:

P	Q	$-P$	$P \wedge Q$	$P \vee Q$	$P \longrightarrow Q$	$P \longleftrightarrow Q$
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

Ako je vrijednost interpretacije I na formuli F jednaka 1, tj. $I(F) = 1$, onda kažemo da je formula F istinita za interpretaciju I. Ako je vrijednost interpretacije I na formuli F jednaka 0, tj. $I(F) = 0$, onda kažemo da je formula F neistinita za interpretaciju I.

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

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

Dakle, $I(F) = 0$. Očito $I(F)$ ovisi o $I(P)$, $I(Q)$ i $I(R)$, pa bi za neke druge vrijednosti $I(P)$, $I(Q)$ i $I(R)$ imali različitu vrijednost $I(F)$. Pogledajmo sve moguće

interpretacije:

P	Q	R	$-P$	$-P \vee Q$	$-R$	$(-P \vee Q) \longrightarrow -R$
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

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

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

Uočimo da su valjane formule upravo one formule koje su istinite bez obzira na istinitost svojih atomarnih djelova. Sada ćemo navesti neke važne formule koje su valjane.

1. $--P \longleftrightarrow P$, princip dvojne negacije,
2. $P \vee -P$, princip isključenja trećeg,
3. $-(P \wedge -P)$, princip neproturječnosti,
4. $(P \longrightarrow Q) \longleftrightarrow (-Q \longrightarrow -P)$, princip kontrapozicije,
5. $-P \longrightarrow (P \longrightarrow Q)$, princip negacije premise,
6. $-(P \vee Q) \longleftrightarrow -P \wedge -Q$, De Morganov princip,
7. $-(P \wedge Q) \longleftrightarrow -P \vee -Q$, De Morganov princip.

2.1.4. Logička implikacija

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

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

Nije teško vidjeti da za proizvoljne formule A i B vrijedi

$$A \Rightarrow B \text{ ako i samo ako je } A \longrightarrow B \text{ valjana formula.}$$

Drugim riječima, implikacija se može svesti na valjanost kondicionala. Analogno,

$$A \Leftrightarrow B \text{ ako i samo ako je } A \longleftrightarrow B \text{ valjana formula,}$$

tj. ekvivalencija se može svesti 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 ($A \Leftrightarrow B$ 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.

Kao što smo vidjeli, logička implikacija je usko vezana uz kondicional. To je dovelo do tendencije da se "implicira" koristi za čitanje znaka " $\longrightarrow$ " za kondicional, što nikako nije ispravno! Naime, kada kažemo da jedna formula implicira drugu izričemo određenu tvrdnju o tim formulama, a kada među njima stavimo znak " $\longrightarrow$ " gradimo složeniju formulu. Slično vrijedi i za logičku ekvivalenciju i znak " $\longleftrightarrow$ ".

Pogledajmo sada u kakvoj su vezi logička implikacija i dokaz nekog matematičkog teorema s pretpostavkom P i tvrdnjom Q. U logičkoj notaciji to možemo pisati kao $P \Rightarrow Q$. Uz ovo 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? Podsjetimo se da $P \Rightarrow Q$ ako i samo ako je $P \longrightarrow Q$ valjana formula, pa možemo ispitati njihovu vezu pomoću semantičke tablice.

P	Q	$P \longrightarrow Q$	$-P \longrightarrow -Q$	$Q \longrightarrow P$	$-Q \longrightarrow -P$
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.

2.2. Logika prvog reda

2.2.1. Uvod

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

$$\frac{\begin{array}{c}\text{Svi ljudi su smrtni.}\\ \text{Grci su ljudi.}\end{array}}{\text{Grci su smrtni.}}$$

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:

$$\begin{aligned} &C(x) \ldots \text{"}x \text{ je čovjek"},\\ &S(x) \ldots \text{"}x \text{ je smrtan"},\\ &G(x) \ldots \text{"}x \text{ je Grk"}. \end{aligned}$$

U tom slučaju gornji primjer možemo zapisati u obliku:

$$\frac{\begin{array}{c}\forall x\,(C(x) \longrightarrow S(x))\\ \forall x\,(G(x) \longrightarrow C(x))\end{array}}{\forall x\,(G(x) \longrightarrow S(x))}$$

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

$$\begin{aligned} &E(x) \ldots \text{"}x \text{ je elipsa"},\\ &K(x) \ldots \text{"}x \text{ je krivulja"},\\ &C(x,y) \ldots \text{"}y \text{ crta } x\text{"}, \end{aligned}$$

onda gornji primjer možemo pisati kao

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

Logika sudova ne može formalno zapisati ni neke jednostavne matematičke pojmove. Jedan takav primjer je pojam neprekidnosti u točki. Neka je funkcija $f : \mathbb{R} \to \mathbb{R}$ neprekidna u točki x_0. Tada je istinita formula

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

Negacija gornje formule, tj. formula

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

je formalni zapis činjenice da funkcija f ima prekid u točki x_0. Primjenom pravila prijelaza za kvantifikatore dobivamo

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

Važno je uočiti da u prethodnim primjerima istinitost zaključaka 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.

Ovako dobivena logika, koju nazivamo *logikom prvog reda* ili *predikatnom logikom*, ima veću izražajnu moć, no gubi neka dobra svojstva logike sudova, a tu prije svega mislimo na odlučivost. Za svaku formulu logike sudova možemo u konačno mnogo koraka provjeriti je li valjana, no to nije moguće za formule logike prvog reda.

2.2.2. Jezik logike prvog reda

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

1. $A_1 = \{v_0, v_1, v_2, \ldots\}$ prebrojiv skup čije elemente nazivamo individualnim varijablama,
2. $A_2 = \{-, \wedge, \vee, \longrightarrow, \longleftrightarrow, \forall, \exists\}$ skup logičkih veznika,
3. $A_3 = \{R_k : k \in \mathbb{N}\}$ skup čije elemente nazivamo relacijskim simbolima (predikatima),
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.

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 se interpretira kao funkcija dvije varijable.

Definicija 2.2.1. *Term je riječ dane 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 koraka pravila a) i b).

Na primjer, uzmimo $\{\ln, \sin, \exp\} \subset A_4$, $\{v_1, x\} \subset A_1$ i $c_3 \in A_5$. Sljedeće su riječi termi: c_3, x, $\ln x$, $\exp(\sin v_1)$, $\ln(\exp(\sin c_3))$.

Definicija 2.2.2. *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 definirana sa:*

a) svaka atomarna formula je formula,

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

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

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

Primjedba 2.2.1. *Uobičajeno je umjesto $\exists x (x \in S \wedge P(x))$ pisati $(\exists x \in S) P(x)$, a umjesto $\forall x (x \in S \longrightarrow P(x))$ analogno pišemo $(\forall x \in S) P(x)$. Također, umjesto $\exists x (P(x) \wedge \forall y (P(y) \longrightarrow y = x))$ pišemo $\exists! x P(x)$. Dakle, treba uvijek voditi računa o tomu da se radi samo o uvriježenim zapisima.*

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 3", i to bi (za razliku od prethodna dva primjera) bio sud, i to lažan. "x je jednak 2" nije sud jer ne možemo utvrditi da li je ova izjavna rečenica istinita ili lažna, a isto vrijedi i za izjavnu rečenicu "x je jednak y". No uvođenjem odgovarajučeg broja kvantifikatora u gradnju formule kojoj je podformula $R(t_1, t_2)$, dobit ćemo sudove. Na primjer,

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

je neistina, dok su

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

istine. Ovo su bili primjeri *zatvorenih* formula, tj. formula kod kojih su sve varijable vezane kvantifikatorima, no definicija formule dozvoljava i *otvorene* formule, tj. formule kod kojih nisu sve varijable vezane kvantifikatorima. Jedna takva bi bila

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

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

Pogledajmo još neke primjere korektnih 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. $-\forall x \forall y\,(P\,(x,y) \longrightarrow R\,(x,y)) \Leftrightarrow \exists x \exists y\,(P\,(x,y) \wedge -R\,(x,y))$,
2. $-\,(\forall x \in A)\,(\forall y \in A)\,(x \neq y \longrightarrow f\,(x) \neq f\,(y))$
   $\Leftrightarrow (\exists x \in A)\,(\exists y \in A)\,(x \neq y \wedge f\,(x) = f\,(y))$,
3. $-\,(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\;\; x^2 + y^2 \geq 0 \Leftrightarrow (\exists x \in \mathbb{R})\,(\exists y \in \mathbb{R})\;\; x^2 + y^2 < 0.$

Poglavlje 3.

Skupovi

3.1. Osnovni pojmovi

Skup je osnovni matematički pojam koga je nemoguće definirati pomoću jednostavnijih pojmova, no intuitivno je jasno što podrazumijevamo pod pojmom "skup". Možemo reći da je to "množina", "mnoštvo", "kolekcija", "familija" ili slično, no time nismo rekli ništa novo, već smo samo koristili sinonime. Matematička disciplina koja se bavi skupovima zove se *teorija skupova*. Njen osnivač *Georg Cantor* o skupu je rekao sljedeće:

"Skup je mnoštvo koje shvaćamo kao jedno."

Dakle, skup možemo smatrati cjelinom sastavljenom od za tu cjelinu osnovnih dijelova koje nazivamo *elementima* tog skupa. Intuitivno pretpostavljamo da postoji određeni odnos između skupa i njegovih elemenata. I ne samo to, za svaki objekt možemo reći pripada li nekom skupu ili ne. Skupove ćemo u matematici najčešće označavati velikim latiničnim slovima $A, B, C, X, Y, \ldots$, a njihove elemente malim latiničnim slovima $a,\ b,\ c,\ x,\ y,\ \ldots$

Pojam "*biti element skupa*" je također osnovni matematički pojam. Činjenicu da je x element skupa S zapisujemo kao $x \in S$ i čitamo "x *je element skupa* S" ili "x *pripada skupu* S". Slično, činjenicu da y nije element skupa S zapisujemo kao $y \notin S$ i čitamo "y *nije element skupa* S" ili "y *ne pripada skupu* S". Na primjer, označimo li sa S skup svih riba u Jadranskom moru, onda vrijedi: tunj $\in S$, pirana $\notin S$, srdela $\in S$.

Definirajmo sada neke jednostavne pojmove vezane uz skupove.

Definicija 3.1.1. *Neka su A i B skupovi. Ako je svaki element skupa A ujedno i element skupa B, onda kažemo da je skup A podskup skupa B (ili da je skup A sadržan u skupu B) i pišemo $A \subseteq B$. Kažemo još i da je skup B nadskup skupa A (ili da skup B sadrži skup A), a to pišemo kao $B \supseteq A$. Oznaku $\subseteq$ čitamo kao "inkluzija".*

Definicija 3.1.2. *Ako je $A \subseteq B$ i ako postoji neki $b \in B$ takav da $b \notin A$, onda kažemo da je skup A pravi podskup skupa B i pišemo $A \subset B$ ili $A \subsetneq B$.*

Definicija 3.1.3. *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 prema tomu provjeriti jesu li dva skupa A i B jednaka znači provjeriti je li $A \subseteq B$ i $B \subseteq A$.

Ukoliko dva skupa A i B nisu jednaka pišemo $A \neq B$. Očito je da vrijedi

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

pri čemu je

$$A \nsubseteq B \Leftrightarrow \exists a\,(a \in A \wedge a \notin B).$$

Propozicija 3.1.1. *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. ■

U mnogim situacijama je potrebno promatrati samo podskupove nekog skupa U, koji tada poprima značenje *univerzalnog skupa* (univerzuma). Naravno, univerzalnost skupa U je relativna i varira od problema do problema. Drugi važni istaknuti skup je *prazni skup*, tj. skup bez ijednog elementa. Označavamo ga s $\emptyset$.

Skupove i njihove međusobne odnose ponekad zorno prikazujemo tzv. *Vennovim dijagramima*. Ipak, važno je istaknuti da takvi crteži ne predstavljaju dokaz.

3.2. Zadavanje skupova

Skup smatramo *zadanim* ako je nedvosmislemo 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.

Skupove 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 $S = \{a, e, i, o, u\}$. Pritom poredak nije važan i ponovljene elemente ne uzimamo u obzir. Vitičaste zagrade igraju dvostruku ulogu: one su simbol ujedinjavanja dijelova u cjelinu i klasifikator objekata na one koji koji pripadaju skupu i na one koji mu ne pripadaju.

2. Isticanjem nekog karakterističnog svojstva koje imaju samo elementi toga skupa, tj. nekim propisom.
   Na primjer, skup svih pozitivnih cijelih brojeva zadajemo s $\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\}$, a centralnu, jediničnu kružnicu sa $S_1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

3.3. Booleove operacije na skupovima

Definicija 3.3.1. *Neka je U proizvoljan skup. Partitivni skup skupa U, u oznaci $\mathcal{P}(U)$, je skup svih podskupova skupa U. Često pišemo i 2^U.*

Na primjer,

1. $\mathcal{P}(\emptyset) = \{\emptyset\}$,
2. $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$,
3. $\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

Uvedimo sada neke operacije sa skupovima.

Definicija 3.3.2. *Neka je U dani 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

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

Ove osnovne operacije sa skupovima nazivamo Booleovim operacijama. Uočimo odmah da je

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

Također

$$(\forall A, B \subseteq U)\,(A \cap B \subseteq A, B \subseteq A \cup B).$$

Definicija 3.3.3. *Neka je U dani skup i $A, B \subseteq U$. Kažemo da su skupovi A i B disjunktni ako je $A \cap B = \emptyset$.*

Propozicija 3.3.1. *Neka je U proizvoljan skup i $A, B \subseteq U$. Vrijedi*

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

Dokaz. Dokaz provodimo indirektno, reductio ad absurdum.

Pretpostavimo suprotno, tj. da je $(A \setminus B) \cap (B \setminus A) \neq \emptyset$. Tada postoji neki $x \in (A \setminus B) \cap (B \setminus A)$, pa za njega vrijedi $x \in (A \setminus B)$ i $x \in (B \setminus A)$. Odatle je $x \in A, x \notin B$ i $x \in B, x \notin A$, što je nemoguće. Budući da smo došli do kontradikcije, zaključujemo da je pretpostavka bila pogrešna. Zato mora vrijediti $(A \setminus B) \cap (B \setminus A) = \emptyset$. ■

Sada ćemo uvesti i jednu unarnu operaciju sa skupovima.

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

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

Uočimo da je za svaki $A \subseteq U$ ispunjeno $A^c \subseteq U$.

Pogledajmo jedan primjer: ako je $U = \{1, 2, 3, 4, 5, 6, 7\}$ i $A = \{2, 5, 6\}$, onda je $A^c = \{1, 3, 4, 7\}$.

Primjedba 3.3.1. *Neka je U dani skup i $A, B \subseteq U$. Uočimo da 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 sada koja svojstva imaju Booleove operacije.

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

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

Dokaz. Dokaz ćemo provesti direktno. S obzirom da u svim slučajevima dokazujemo jednakost skupova, svaki put treba dokazati dvije inkluzije. Tvrdnje $(1) - (4)$ su očigledne, pa ćemo dokazati samo tvrdnju (5).

Neka je $A \subseteq U$. Treba dokazati da je $(A^c)^c \subseteq A$ 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. 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

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

Prema tomu vrijedi $(A^c)^c \subseteq A$, čime je dokazano i $(A^c)^c = A$. ■

Teorem 3.3.2. *Neka je U dani 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. Svojstvo (1) je direktna posljedica 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, $(A \cup B)^c \subseteq A^c \cap B^c$, pa smo tako dokazali i jednakost tih skupova.

Drugu formulu u (2) dokazat ćemo 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 Napomeni 3.3.1. znamo da 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 skup i $A, B, C \subseteq U$. Vrijedi:*

1. $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ *(asocijativnost),*
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributivnost).*

Dokaz. Sami za vježbu. ■

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

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

4. $A \cap B$ *i* $A \cap B^c$ *su disjunktni skupovi,*

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

6. $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Partitivni skup $\mathcal{P}(U)$ zajedno s operacijama $\cup, \cap$ i $\setminus$ zove se *Booleova algebra skupova* na U.

Primjedba 3.3.2. *Pojam unije i presjeka dvaju skupova 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 s*

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

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

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

I u ovom slučaju vrijede de Morganove formule

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

U Zadatku 1. prikazali smo skupove $A \cup B$ i A kao unije disjunktnih skupova. 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 bilo koja familija* $\mathcal{F} \subseteq \mathcal{P}(A)$ *koja 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) $\bigcup_{X \in \mathcal{F}} X = A$.

Dakle, $\mathcal{F}$ je particija skupa A ako i samo ako za svaki $x \in A$ postoji jedinstveni skup $X \in \mathcal{F}$ takav da je $x \in X$.

Na primjer, $\mathcal{F}_1 = \{\{1\}, \{2,3\}, \{4\}\}$ i $\mathcal{F}_2 = \{\{1,2\}, \{3,4\}\}$ su dvije particije skupa $A = \{1,2,3,4\}$.

Osim Booleovih operacija, na skupu $\mathcal{P}(A)$ možemo definirati i neke druge operacije, a jedna od njih je *simetručna razlika skupova.*

Definicija 3.3.6. *Neka je* U *dani skup i* $A, B \subseteq U$*. Simetrična razlika skupova* A *i* B*, u oznaci* $A \triangle B$*, je skup definiran sa:*

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

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

Zadatak 2. *Neka je U dani 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. $A \triangle A = \emptyset$.

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). Uočimo da je važan poredak članova uređenog para.

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*

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

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, i to na način da ćemo dokazati istinitost dviju odgovarajućih implikacija.
Dokažimo najprije da $(a, b) = (a', b') \Rightarrow (a = a' \wedge b = b')$. 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) $a = b$
U ovom slučaju 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 $\{a\} = \{a'\} = \{a', b'\}$, a konačno (opet po definiciji jednakosti skupova) $a' = b' = a = b$.
Dakle, $a = a'$ i $b = b'$, što je i trebalo dokazati.

b) $a \neq b$

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 da $(a = a' \wedge b = b') \Rightarrow (a, b) = (a', b')$.

Ako je $a = a'$ i $b = b'$, onda je $\{a\} = \{a'\}$ i $\{a, b\} = \{a', b'\}$. Odatle odmah slijedi

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

čime je dokaz završen. ■

Primjedba 3.4.1. *Uočimo da je općenito* $(a, b) \neq (b, a)$. *Štoviše, iz* $(a, b) = (b, a)$ *slijedi* $a = b$. *Za razliku od toga,* $\{a, b\} = \{b, a\}$.

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 s*

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

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

Primjer 3. *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.

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*

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

a njegova dijagonala je skup

$$I_A = \{(a, a) : a \in A\}.$$

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

Primjer 4. *Dva poznata primjera su:*

1. $A = B = \mathbb{R}$ *(koordinatna ravnina)*

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

2. $A = B = [0, 1]$ *(jedinični kvadrat u koordinatnoj ravnini)*

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

Operacija Kartezijeva množenja ima neka 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. ■

Pojam Kartezijeva umnoška možemo poopćiti i na više od dva faktora.
Ako je $n \in \mathbb{N}$ i $A_1, A_2, \ldots, A_n$ neprazni skupovi, definiramo

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i,\ i = 1, 2, \ldots n\},$$

pri čemu $(a_1, a_2, \ldots, a_n)$ zovemo *uređena n-torka*. Ako je bilo koji od skupova $A_i,\ i = 1, 2, \ldots n$, prazan, definiramo $A_1 \times A_2 \times \cdots \times A_n = \emptyset$.
Naravno, možemo Kartezijev umnožak n skupova definirati i induktivno kao

$$\begin{aligned} A_1 \times A_2 \times A_3 &= (A_1 \times A_2) \times A_3, \\ &\vdots \\ A_1 \times A_2 \times \cdots \times A_{n-1} \times A_n &= (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n. \end{aligned}$$

Odatle posebno slijedi

$$(a_1, a_2, \ldots, a_n) = (a_1', a_2', \ldots, a_n') \Leftrightarrow a_1 = a_1' \wedge \cdots \wedge a_n = a_n'.$$

Zadatak 1. *Uvjerite se da Kartezijev umnožak nije asocijativan, tj. da postoje skupovi X, Y, Z takvi da je $(X \times Y) \times Z \neq X \times (Y \times Z)$. Dakle, ne valja definirati uređenu trojku (x, y, z) kao skup $\{\{x\}, \{x, y\}, \{x, y, z\}\}$.*

Primjer 5. *Dva poznata primjera su:*

1. $A = B = C = \mathbb{R}$ *(koordinatni prostor)*

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

2. $A = B = C = [0, 1]$ *(jedinična kocka u koordinatnom prostoru)*

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

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

Poglavlje 4.

Relacije

4.1. Osnovni pojmovi

Pojam *relacije* je jedan od najvažnijih matematičkih pojmova uopće, a kao poseban slučaj sadrži pojam funkcije.

Primjeri iz svakidašnjeg života pokazuju da je često potrebno između dvaju skupova uspostaviti nekakav odnos.

Neka je npr. A skup svih dnevnih listova koji izlaze u Splitu, a neka je B skup svih stanovnika grada Splita. Između skupova A i B postoji izvjestan odnos koji se sastoji u tomu da neki stanovnici Splita čitaju neke dnevne listove: pri tome neki čitaju samo jedan, neki više njih, a postoje također i oni stanovnici Splita koji ne čitaju nijedan dnevni list. Ako nam $a \in A$ označava *Slobodnu Dalmaciju*, onda je a u vezi s određenim brojem elemenata skupa B, tj. s određenim brojem stanovnika Splita. To su upravo oni $b \in B$ 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" ustanovljen (uočen) odnos između skupova A i B. Stoga je prirodno promatrati umnožak $A \times B$ budući se u njemu javljaju sve mogućnosti poznavanja. Imamo:

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

Odredimo li da su u parovima samo osobe koje se "poznaju", dobivamo skup

$$R = \{(a,e),(a,g),(b,f),(c,e),(c,f),(c,g)\} \subseteq A \times B.$$

Ovi primjeri ukazuju na potrebu proučavanja proizvoljnih podskupova Kartezijeva umnoška $A \times B$.

Definicija 4.1.1. *Neka su A i B skupovi. Svaki podskup R Kartezijeva umnoška $A \times B$ zove se (binarna) relacija. Skup A označavamo s $D_1(R)$, a skup B s $D_2(R)$. Za element $a \in A$ kažemo da je u relaciji R s $b \in B$ ako je $(a,b) \in R$. Domena relacije R je skup*

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

a slika relacije R skup

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

Činjenicu da je $(a,b) \in R$ često pišemo u obliku aRb i kažemo da a ima svojstvo da je u relaciji R s b.

Ako je $A \neq B$ kažemo da je $R \subseteq A \times B$ *heterogena* relacija, a ako je $A = B$ kažemo da je $R \subseteq A \times A$ *homogena* relacija na skupu A.

Posebno izdvajamo homogenu relaciju I_A (ili u oznaci Δ_A), koja je za bilo koji neprazan skup A definirana s

$$I_A = \{(a,a) : a \in A\},$$

a koju zovemo *dijagonala* ili *identična relacija* na skupu A.

Definiciju binarne relacije može se proširiti na podskupove Kartezijeva produkta $A_1 \times \cdots A_n, n \in \mathbb{N}$, i tada govorimo o *$n$-arnim relacijama*. Nama će ipak biti najvažnije binarne relacije koje ćemo u nastavku jednostavno zvati relacije.

Uvedimo sada još nekoliko pojmova vezanih uz relacije.

Definicija 4.1.2. *Neka je $R \subseteq A \times B$ neprazna relacija. Suprotna (inverzna) relacija relaciji R je relacija $R^{-1} \subseteq B \times A$ definirana sa*

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

Definicija 4.1.3. *Neka je $R \subseteq A \times B$. Komplement relacije R je relacija $R^c \subseteq A \times B$ definirana sa*

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

Definicija 4.1.4. *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*

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

Primjer 6. *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 7. *Neka je $A = \{1,2,3\}$. Definirajmo homogene relacije R i S na skupu A sa*

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

Tada je

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

pa je očito da kompozicija relacija općenito nije komutativna.

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

Ako je $Z \circ (S \circ R) = \emptyset$ onda tvrdnja trivijalno vrijedi, stoga pretpostavimo da je relacija $Z \circ (S \circ R)$ neprazna. Kako je $Z \circ (S \circ R) \subseteq A \times D$, 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 $(b,c) \in S$. Po definiciji kompozicije iz $(b,c) \in S$ i $(c,d) \in Z$ slijedi $(b,d) \in Z \circ S$ i analogno iz $(a,b) \in R$ i $(b,d) \in Z \circ S$ slijedi $(a,d) \in (Z \circ S) \circ R$, što je i trebalo dokazati.

Suprotnu inkluziju dokažemo analogno. ■

Prethodni teorem nam u stvari kaže da je kompozicija relacija asocijativna. Stoga za homogenu relaciju R na skupu A ima smisla definirati potencije relacije 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 je $R \subseteq A \times B$. Vrijedi:*

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

Dokaz. Dokazat ćemo samo prvi identitet jer se drugi dokazuje analogno.

Znamo da je $R \circ I_A \subseteq A \times B$. 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 $a = a'$, pa je $(a,b) \in R$. Dakle, $R \circ I_A \subseteq R$.

Obratno, uzmimo proizvoljan $(a,b) \in R$. Kako za svaki $a \in A$ vrijedi $(a,a) \in I_A$, to po definiciji kompozicije slijedi $(a,b) \in R \circ I_A$, pa je $R \subseteq R \circ I_A$. ■

Primjedba 4.1.1. *Posebno, ako je $R \subseteq A \times A$, iz prethodne propozicije slijedi*

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

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

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

No iz (4.1) *za $R = Q$ dobijemo $Q \circ I_A = I_A \circ Q = Q$ pa iz tog i* (4.2) *slijedi*

$$I_A = Q.$$

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. ■

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

Definicija 4.1.5. *Neka je R homogena relacija na skupu A. Kažemo da je relacija 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

$$(\forall x \in A)\,(\forall y \in A)\,((x, y) \in R \longrightarrow (y, x) \in R)\,,$$

d) antisimetrična ako vrijedi

$$(\forall x \in A)\,(\forall y \in A)\,((x, y) \in R \wedge (y, x) \in R \longrightarrow x = y)\,,$$

e) tranzitivna ako vrijedi

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

Geometrijski gledano, refleksivna relacija sadrži dijagonalu I_A skupa A, irefleksivna relacija ne siječe dijagonalu I_A, a simetrična relacija je simetrična s obzirom na dijagonalu I_A.

Gornja svojstva homogenih relacija se skupovno mogu opisati na sljedeći način.

Lema 4.1.2. *Neka je R 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 $R \subseteq R^{-1}$;*
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 $R = \emptyset \subseteq R^{-1}$, pa je tvrdnja trivijalno ispunjena. Pretpostavimo stoga da je R neprazna, te uzmimo proizvoljan $(x, y) \in R$. Relacija R je simetrična, pa je $(y, x) \in R$, a iz ovoga po definiciji inverzne relacije slijedi $(x, y) \in R^{-1}$. Dakle, dokazali smo da je $R \subseteq R^{-1}$. Obratno, neka je $R \subseteq R^{-1}$. Ako je $R = \emptyset$ tvrdnja trivijalno vrijedi (prazna relacija je simetrična). Pretpostavimo stoga da je $R \neq \emptyset$ i uzmimo proizvoljan par $(x, y) \in R$. Jer je $R \subseteq R^{-1}$ slijedi $(x, y) \in R^{-1}$, 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 $(y, z) \in R$. Jer je R tranzitivna slijedi i da je $(x, z) \in R$, pa zaključujemo da vrijedi $R \circ R \subseteq R$. Obratno, neka je $R \circ R \subseteq R$. Ako je $R = \emptyset$ tada 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 dokazati. ■

Primjedba 4.1.2. *Uočimo da iz $R \subseteq R^{-1}$ po Lemi 4.1.1. slijedi $R^{-1} \subseteq (R^{-1})^{-1} = R$, pa iz te dvije inkluzije zaključujemo da je $R = R^{-1}$. Dakle, može se reći da je relacija R simetrična ako i samo ako je $R = R^{-1}$.*

Sada ćemo navesti neka svojstva koja mogu imati heterogene relacije (naravno, mogu ih imati i homogene relacije kao poseban slučaj heterogenih relacija).

Definicija 4.1.6. *Neka su A i B skupovi, te $R \subseteq A \times B$. Kažemo da je relacija R :*

a) injektivna ako vrijedi

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

b) funkcionalna ako vrijedi

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

c) surjektivna ako vrijedi

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

d) totalna ako vrijedi

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

Lema 4.1.3. *Neka su A i B 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 $R \circ R^{-1} \supseteq I_B$;*

4. *R je totalna ako i samo ako je $R^{-1} \circ R \supseteq I_A$.*

Dokaz. Za ilustraciju ćemo dokazati samo prvu tvrdnju, a oba smjera dokaza ćemo provesti obratom po kontrapoziciji.

Pretpostavimo da $R^{-1} \circ R \nsubseteq I_A$. To svakako znači da je $R^{-1} \circ R \neq \emptyset$, te da

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

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.

Obratno, pretpostavimo 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 $R^{-1} \circ R \nsubseteq I_A$. ■

Definicija 4.1.7. *Funkcionalne relacije nazivamo parcijalnim funkcijama. Totalne funkcionalne relacije nazivamo funkcijama.*

4.2. Relacije ekvivalencije

Definicija 4.2.1. *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 simbolom $\sim$ ili $\cong$. Ako je $x \sim y$, onda kažemo da je x ekvivalentan s y. Važan primjer relacije ekvivalencije je relacija $=$ ("biti jednak").

Neka je $A \neq \emptyset$ proizvoljan skup i $\sim$ relacija ekvivalencije na njemu. Svakom elementu a skupa A možemo pridružiti skup

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

tj. skup svih onih elemenata skupa A koji su u relaciji $\sim$ s a. Skup $[a]$ nazivamo *klasom ekvivalencije* određenom elementom a, a sam element *a reprezentantom klase* $[a]$. Budući je $(\forall a \in A)\, a \sim a$, to je $(\forall a \in A)\, [a] \neq \emptyset$.

Pogledajmo još neka važna svojstva klasa ekvivalencije.

Teorem 4.2.1. *Neka je $A \neq \emptyset$ proizvoljan 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.

Neka su $x, y \in A$ takvi da $x \nsim y$. Dokažimo da je $[x] \cap [y] = \emptyset$. Pretpostavimo suprotno, tj. da je $[x] \cap [y] \neq \emptyset$. To znači da postoji neki $a \in [x] \cap [y]$. Iz $a \in [x]$ slijedi $a \sim x$, a iz $a \in [y]$ slijedi $a \sim y$. Kako je $\sim$ relacija ekvivalencije na A to je ona simetrična i tranzitivna, pa iz $a \sim x$ slijedi $x \sim a$, a iz $x \sim a$ i $a \sim y$ slijedi $x \sim y$. Obratom po kontrapoziciji dobijemo da iz $x \nsim y$ slijedi $[x] \cap [y] = \emptyset$.

Dokažimo još i drugu tvrdnju.

Pretpostavimo da je $x \sim y$. Treba dokazati $[x] \subseteq [y]$ i $[y] \subseteq [x]$. Dokažimo najprije $[x] \subseteq [y]$. Znamo da je $[x] \neq \emptyset$, pa uzmimo bilo koji element a iz $[x]$. To znači da je $a \sim x$. Zbog tranzitivnosti relacije $\sim$, iz $a \sim x$ i $x \sim y$ slijedi $a \sim y$, pa je $a \in [y]$. Dakle, $[x] \subseteq [y]$. Kako je relacija $\sim$ simetrična, to iz $x \sim y$ slijedi $y \sim x$, pa je po prethodnom $[y] \subseteq [x]$. ■

Prema prethodnom teoremu možemo zaključiti da za proizvoljne $x, y \in A$ vrijedi $[x] \cap [y] = \emptyset$ ili $[x] = [y]$. Odavde slijedi da za svaki $x \in A$ postoji jedinstvena klasa $[a]$ čiji je on član.

Stavimo li u jedan skup sve te različite klase koje definira relacija $\sim$ na skupu A, dobit ćemo skup čiji su elementi neprazni, po parovima disjunktni podskupovi skupa A, a čija je unija jednaka čitavom skupu A. Prema tomu, dobit ćemo jednu *particiju* skupa A. Tu particiju nazivamo *kvocijentnim skupom* skupa A po relaciji $\sim$ i označavamo je s $A/\sim$.

Dakle, svaka relacija ekvivalencije na skupu A definira jednu particiju skupa A na klase ekvivalencije. No kao što ćemo vidjeti, vrijedi i obrat. No prije nego to dokažemo uvest ćemo funkciju koja elementima skupa pridružuje njima pripadne klase po nekoj relaciji ekvivalencije.

Propozicija 4.2.1. *Neka je $\sim$ relacija ekvivalencije na skupu A i relacija τ na $A \times (A/\sim)$ definirana sa*

$$(a, [x]) \in \tau \quad \textit{ako i samo ako} \quad a \in [x].$$

Relacija τ je funkcionalna, totalna i surjektivna.

Dokaz. Kako je za svaki $a \in A$ ispunjeno $a \in [a]$, to je relacija τ očigledno totalna i surjektivna. Pokažimo još da je funkcionalna. Neka je $a \in A$, te $[x]$ i $[y]$ dvije klase iz $A/\sim$ takve da je $(a, [x]) \in \tau$ i $(a, [y]) \in \tau$. Iz ovoga slijedi $a \in [x]$ i $a \in [y]$, tj. $a \in [x] \cap [y]$. Po svojstvima klasa relacije ekvivalencije τ zaključujemo da je $[x] = [y]$, pa je relacija τ funkcionalna. ■

Definicija 4.2.2. *Neka je $\sim$ relacija ekvivalencije na skupu A. Funkcija $\tau : A \to A/\sim$ definirana izrazom*

$$\tau(a) = [a]$$

zove se projekcija skupa A na kvocijentni skup $A/\sim$.

Teorem 4.2.2. *Svaka relacija ekvivalencije na skupu A definira jednu particiju skupa A. U istom elementu particije nalaze se oni i samo oni elementi skupa A koji su međusobno ekvivalentni.*

Dokaz. Neka je $\sim$ neka relacija ekvivalencije na skupu A. Pokazat ćemo da $A/\sim$ određuje jednu particiju skupa A.

Kako je relacija $\sim$ refleksivna, to je za svaki $x \in A$ ispunjeno $x \in [x]$. Iz ovoga slijedi $A = \cup_{x\in A}[x]$ i $[x] \neq \emptyset$ za sve $x \in A$. Nadalje, znamo da je za sve $x, y \in A$ ispunjeno $[x] \cap [y] = \emptyset$ ili $[x] = [y]$, pa $A/\sim$ zaista određuje jednu particiju skupa A. ■

Zanimljivo je da vrijedi i obrat prethodnog teorema: svaka particija skupa A definira jednu relaciju ekvivalencije na A. O tome nam govori naredni teorem.

Teorem 4.2.3. *Neka je $\mathcal{F}$ jedna particija skupa A. Tada je relacija $R_{\mathcal{F}}$ na skupu 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 A.

Dokaz. Neka su $x, y \in A$ u istom elementu particije $\mathcal{F}$. Po definiciji relacije $R_{\mathcal{F}}$ tada je $(x, y) \in R_{\mathcal{F}}$ i $(y, x) \in R_{\mathcal{F}}$, pa je relacija $R_{\mathcal{F}}$ simetrična. Posebno, ako je $x = y$ slijedi $(x, x) \in R_{\mathcal{F}}$, pa je $R_{\mathcal{F}}$ refleksivna. Dokažimo još i da je $R_{\mathcal{F}}$ tranzitivna. Pretpostavimo da 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 je $x, y \in S_1$ i $y, z \in S_2$. No to znači da je $y \in S_1 \cap S_2$, pa mora vrijediti $S_1 = S_2$ iz čega slijedi da su i x i z u istom elementu particije $\mathcal{F}$, pa je $(x, z) \in R_{\mathcal{F}}$. Dakle, $R_{\mathcal{F}}$ je i tranzitivna, pa je $R_{\mathcal{F}}$ relacija ekvivalencije na skupu A. ■

Primjer 8. *Neka je $\mathcal{P}$ skup svih pravaca neke ravnine. Na skupu $\mathcal{P}$ definiramo relaciju $\parallel$* ("biti paralelan"). *Podsjetimo se da su dva pravca u ravnini paralelna ako nemaju nijednu zajedničku točku ili ako se podudaraju.*
Očito je $\parallel$ relacija ekvivalencije na $\mathcal{P}$ (provjerite sami!). Klase ekvivalencije nazivamo smjerovima u ravnini.
Da li je relacija $\perp$ ("biti okomit") *relacija ekvivalencije na $\mathcal{P}$? (Nije!)*

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 $\mathcal{T}$.*

Primjer 10. *Neka je E^3 prostor točaka.* Orijentirana dužina *u E^3 je svaki uređeni par točaka $(A, B) \in E^3 \times E^3$. Oznaka za orjentiranu dužinu je $(A, B) = \overrightarrow{AB}$.*
Označimo sa $\mathcal{O}$ skup svih orjentiranih dužina u E^3, tj.

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

Na skupu $\mathcal{O}$ definiramo relaciju $\equiv$ (biti ekvivalentan) na sljedeći način: reći ćemo da je orijentirana dužina $\overrightarrow{AB}$ ekvivalentna orijentiranoj dužini $\overrightarrow{CD}$, i pist ćemo $\overrightarrow{AB} \equiv \overrightarrow{CD}$ ako i samo ako dužine $\overline{AD}$ i $\overline{BC}$ imaju zajedničko polovište-
Provjerite sami da je relacija $\equiv$ relacija ekvivalencije na $\mathcal{O}$. Kvocijentni skup $\mathcal{O}/\equiv$ označavamo kao V^3, a njegove elemente (klase ekvivalencije) nazivamo vektorima.

4.3. Relacije uređaja

Osim relacija ekvivalencije s kojima smo se upoznali u prethodnoj točki, važan je još jedan tip binarnih homogenih relacija.

Definicija 4.3.1. *Homogenu binarnu relaciju koja je refleksivna, antisimetrična i tranzitivna nazivamo relacijom djelomičnog (parcijalnog) uređaja.*

Definicija 4.3.2. *Uređeni par (A, ρ) sastavljen od skupa A i relacije djelomičnog uređaja ρ na skupu A zove se djelomično (parcijalno) uređen skup.*

kao i u prethodnom, za relacije djelomičnog uređaja često se umjesto $(x, y) \in \rho$ piše $x \rho y$.

Primjer 11. *Definirajmo relaciju ρ na skupu $\mathbb{N}$ sa*

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

Očito je ova relacija refleksivna, antisimetrična i tranzitivna, pa je $(\mathbb{N}, \rho)$ djelomično uređen skup. Ipak, nisu svi elementi skupa $\mathbb{N}$ "usporedivi". Npr. $(2, 5) \notin \rho$ i također $(5, 2) \notin \rho$.

Gornji primjer nas motivira za sljedeću definiciju.

Definicija 4.3.3. *Neka je ρ realcija djelomičnog uređaja na skupu A. Ako vrijedi*

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

onda kažemo da je ρ relacija linearnog (totalnog) uređaja na skupu A.
Uređeni par (A, ρ) u tom slučaju nazivamo linearno (totalno) uređenim skupom ili jednostavno uređenim skupom.

Poznati primjer uređenog skupa je $(\mathbb{R}, \leq)$, dok je poznati primjer djelomično uređenog skupa $(\mathcal{P}(S), \subseteq)$, gdje je S neki neprazan skup. Relaciju $\subseteq$ nazivamo *relacijom sadržavanja*.

Djelomično uređene skupove se često prikazuje shematski.

Radi jasnoće ćemo nadalje za relaciju djelomičnog uređaja koristiti oznaku $\preceq$ da je ne bismo miješali s oznakom $\leq$ koju koristimo za relaciju uređaja "manje ili jednako" na skupovima brojeva.

Definicija 4.3.4. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$. 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

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

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

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

Očigledno je da je najmanji element ujedno i minimalan, a najveći element ujedno i maksimalan. Obrat, međutim, ne mora vrijediti. Također, djelomično uređen skup može imati više minimalnih i maksimalnih elemenata, a ne mora imati ni najveći ni najmanji element.

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

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

Elementi a i e su minimalni, a elementi b, d i f su maksimalni po $\preceq$. No u A nema po $\preceq$ 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*

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

Element a je minimalan i najmanji, a element e maksimalan i najveći po $\preceq$.

Definicija 4.3.5. *Neka je $(A, \preceq)$ djelomično uređen skup, te $X \subseteq A$.*
Element d skupa A je donja međa skupa X u A ako za svaki $x \in X$ vrijedi $d \preceq x$.
Najveća donja međa, ako postoji, zove se infimum skupa X i označava $\inf X$.
Element g skupa A je gornja međa skupa X u A ako za svaki $x \in X$ vrijedi $x \preceq g$.
Najmanja gornja međa, ako postoji, zove se supremum skupa X i označava $\sup X$.

Na primjer, u uređaju $(\mathbb{N}, \leq)$ je $\inf \mathbb{N} = 1$, a $\sup \mathbb{N}$ ne postoji. U djelomičnom uređaju $(\mathcal{P}(S), \subseteq)$ je $\inf \mathcal{P}(S) = \emptyset$, a $\sup \mathcal{P}(S) = S$.

Podsjetimo se da smo kod uspoređivanja brojeva često koristili relaciju $<$. Općenito su takve relacije definirane na sljedeći način.

Definicija 4.3.6. *Homogenu binarnu relaciju koja je irefleksivna i tranzitivna nazivamo relacijom strogog djelomičnog (parcijalnog) uređaja.*

Definicija 4.3.7. *Neka je $\prec$ relacija strogog djelomičnog uređaja na skupu A. Ako vrijedi*

$$(\forall x \in A)\, (\forall y \in A)\, [x \neq y \longrightarrow ((x,y) \in \rho \vee (y,x) \in \rho)]$$

onda kažemo da je $\prec$ relacija strogog uređaja na skupu A.
Uređeni par $(A, \prec)$ u tom slučaju nazivamo strogo uređenim skupom.

4.4. Funkcije

Već smo rekli da su *funkcije* posebne relacije, tj. binarne relacije koje su funkcionalne i totalne. No kako su funkcije same po sebi važan matematički pojam posvetit ćemo im posebnu točku. Pogledajmo najprije jedan primjer.

Primjer 14. *Neka je H skup svih državljana Republike Hrvatske, $Z = \{0, 1, \ldots, 9\}$ skup znamenki dekadskog 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 $f \subseteq H \times J$ ovako

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

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

Napomenimo da se često funkcije definira kao uređene trojke (A, B, f), gdje su A i B neprazni skupovi, a f pravilo pridruživanja po kojemu se svakom elementu skupa A pridružuje jedan i samo jedan element skupa B. Mi nećemo koristiti takvu definiciju da bismo izbjegli uvođenje pojma "pravila pridruživanja" koji intuitivno nije jasan.

No koristit ćemo uobičajene oznake: za funkciju f umjesto $f \subseteq A \times B$ pisat ćemo $f : A \to B$, a umjesto $(x, y) \in f$ pisat ćemo $y = f(x)$. Element x nazivamo *argumentom* (neovisnom varijablom), a element y *slikom* ili vrijednošću funkcije (ovisnom varijablom).

Funkcije se često prikazuju *dijagramima*.

Već smo se upoznali s inverznom relacijom i slikom relacije, no kada je relacija funkcija uvode se neke posebne oznake i pojmovi.

Definicija 4.4.1. *Neka je $f : A \to B$ funkcija i $C \subseteq A$, $D \subseteq B$.*

a) Slika skupa C u odnosu na funkciju f je skup

$$f(C) = \{f(x) : x \in C\} \subseteq B,$$

b) Praslika skupa D u odnosu na funkciju f je skup

$$f^{-1}(D) = \{x \in A : f(x) \in D\} \subseteq A.$$

Očito je

$$\begin{aligned} f(A) &\subseteq B, \quad f^{-1}(B) = A, \\ f(\emptyset) &= \emptyset, \quad f^{-1}(\emptyset) = \emptyset. \end{aligned}$$

Napomenimo da kada se radi o jednočlanim podskupovima ne pišemo vitičaste zagrade, već jednostavno stavljamo

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

Primjer 15. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana s* $f(x) = 7$ *za sve* $x \in \mathbb{R}$. *Vrijedi:*

$$K(f) = \{7\}, \ f([1,2]) = \{7\}, \quad f^{-1}(\mathbb{R}) = f^{-1}(7) = \mathbb{R},$$
$$f^{-1}([1,4]) = \emptyset, \quad f^{-1}([3,8]) = \mathbb{R}, \quad f^{-1}(\{6,7\}) = \mathbb{R}.$$

Primjer 16. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana s* $f(x) = x^2$ *za sve* $x \in \mathbb{R}$. *Vrijedi:*

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

Propozicija 4.4.1. *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. $f(X \cap Y) \subseteq f(X) \cap f(Y)$.

Dokaz. Dokažimo najprije $f(X \cup Y) = f(X) \cup f(Y)$.

Neka je $y \in f(X \cup Y)$ proizvoljan. To znači da postoji neki $x \in X \cup Y$ takav da je $y = f(x)$. Jer je $x \in X \cup Y$, to je $x \in X$ ili $x \in Y$. Iz ovoga slijedi $y = f(x) \in f(X)$ ili $y = f(x) \in f(Y)$, pa je $y \in f(X) \cup f(Y)$. Dakle, dokazali smo 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 $y \in f(Y)$. 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 $x \in X \cup Y$ takav da je $y = f(x)$, pa je $y \in f(X \cup Y)$. Dakle, dokazali smo i da je $f(X) \cup f(Y) \subseteq f(X \cup Y)$, čime je dokaz prve tvrdnje završen.

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 $y = f(x)$. Za x vrijedi $x \in X$ i $x \in Y$, pa je $y \in f(X)$ i $y \in f(Y)$. Dakle, vrijedi $y \in f(X) \cap f(Y)$, pa je tvrdnja dokazana. ■

Pokazat ćemo protuprimjerom da ne vrijedi $f(X \cap Y) \supseteq f(X) \cap f(Y)$.

Neka je $A = \{a,b\}$, $a \neq b$, i $B = \{b\}$. Definirat ćemo funkciju $f : A \to B$ sa $f(a) = f(b) = b$. Neka je $X = \{a\}$ i $Y = \{b\}$. Vrijedi $X \cap Y = \emptyset$, pa je $f(X \cap Y) = \emptyset$. No s druge strane je $f(X) = f(Y) = \{b\}$, pa je $f(X) \cap f(Y) = \{b\} \neq \emptyset$. Dakle, $f(X) \cap f(Y) \not\subseteq f(X \cap Y)$.

Propozicija 4.4.2. *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. Preostale tvrdnje dokažite sami.

Uzmimo proizvoljan $x \in f^{-1}(X \cup Y)$. Iz ovoga odmah slijedi $f(x) \in X \cup Y$. 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 $x \in f^{-1}(X) \cup f^{-1}(Y)$. Dakle, dokazali smo 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 $f(x) \in X$ 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 $f^{-1}(X) \cup f^{-1}(Y) \subseteq f^{-1}(X \cup Y)$. Zajedno s prethodnim to daje $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. ■

Iz prethodne dvije propozicije vidimo da se praslike ponašaju bolje nego slike.

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 vidimo da se u okviru naše definicije funkcije kao posebne relacije graf funkcije f i sama funkcija f poklapaju, pa nećemo posebno definirati graf funkcije. Točnije, kao što bilo koju relaciju možemo prikazati grafički, tako to možemo napraviti i kada je riječ o funkciji.

Primjer 17. *Nacrtaj funkcije* $f, g : \mathbb{R} \to \mathbb{R}$ *definirane formulama* $f(x) = 2x$ *odnosno* $g(x) = x^2$ *za sve* $x \in \mathbb{R}$.

Definicija 4.4.2. *Neka su* A, B *proizvoljni skupovi i* $C \subseteq A$. *Kažemo da je funkcija* $g : C \to B$ *restrikcija ili ograničenje funkcije* $f : A \to B$ *(odnosno da je funkcija* f *ekstenzija ili proširenje funkcije* g*) ako je* $g \subset f$. *Pišemo* $g = f|_C$.

Primjedba 4.4.1. *Može se pokazati da je* $g \subset f$ *ako i samo ako je* $D(g) \subset D(f)$ *i* $(\forall x \in D(g))\, g(x) = f(x)$.

Primjer 18. *Neka je funkcija* $f : \mathbb{R} \to \mathbb{R}$ *definirana izrazom* $f(x) = |x|$ *za sve* $x \in \mathbb{R}$,*a funkcija* $g : \mathbb{R}_0^+ \to \mathbb{R}$ *izrazom* $g(x) = x$ *za sve* $x \in \mathbb{R}_0^+$. *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 sve* $x \in \mathbb{R}$,*a funkcija* $g : \mathbb{R}_0^+ \to \mathbb{R}$ *izrazom* $g(x) = x$ *za sve* $x \in \mathbb{R}_0^+$. *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 sve* $x \in \mathbb{R}$, *a funkcija* $g : \left[\frac{\pi}{2}, \frac{3\pi}{2}\right] \to \mathbb{R}$ *izrazom* $g(x) = -\cos x$ *za sve* $x \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]$. *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 to nije slučaj s proširenjem. Pogledajmo jedan primjer.

Primjer 21. *Neka je funkcija* $f : [0,1] \to \mathbb{R}$ *definirana izrazom* $f(x) = \sqrt{1 - x^2}$ *za sve* $x \in [0,1]$, *a funkcija* $g : [-1,1] \to \mathbb{R}$ *izrazom*

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

za sve $x \in [-1,1]$. *Tada je* $f = g|_{[0,1]}$. *No funkcija* $h : [-1,1] \to \mathbb{R}$ *definirana izrazom*

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

za sve $x \in [-1,1]$ *je također proširenje funkcije* f, *tj.* $f = h|_{[0,1]}$.

Već smo definirali kompoziciju relacija i pokazali da je ona asocijativna. Sada ćemo dokazati da je kompozicija dviju funkcija funkcija.

Teorem 4.4.1. *Neka su dane funkcije $f : A \to B$ i $g : B \to C$. Tada je i $g \circ f$ funkcija, te $g \circ f : A \to C$.*

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 $D(g) = B$, to je $(\forall x \in A)(\exists y \in B) f(x) = y$ i $(\forall y \in B)(\exists z \in C) g(y) = z$. Dakle, $(\forall x \in A)(\exists z \in C)(g \circ f)(x) = z$, 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 $(g \circ f)(x) = z$ i $(g \circ f)(x) = z'$. Jer je $(g \circ f)(x) = z$ to postoji neki $y \in B$ takav da je $f(x) = y$ i $g(y) = z$. Jer je $(g \circ f)(x) = z'$ to postoji neki $y' \in B$ takav da je $f(x) = y'$ i $g(y') = z'$. Jer je f funkcionalana slijedi $y = y'$, a jer je i g funkcionalna slijedi $z = z'$. Dakle, $g \circ f$ je funkcionalna. ■

Primjedba 4.4.2. *Iz dokaza prethodnog teorema se vidi da se analogna tvrdnja može izreći i za parcijalne funkcije.*

Primjedba 4.4.3. *Posljedica prethodnog teorema jest da je za sve $x \in D(f)$ ispunjeno*

$$(g \circ f)(x) = g(f(x)).$$

Među funkcijama važnu ulogu igraju one koje su injektivne i surjektivne, tj. injekcije i surjekcije. Podsjetimo se da je funkcija $f : A \to B$ injektivna ako vrijedi

$$(\forall x \in A)(\forall x' \in A)(\forall y \in B)(f(x) = y \wedge f(x') = y \longrightarrow x = x'),$$

te da je surjektivna ako vrijedi

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

Mogli bismo to izreći i ovako: funkcija $f : A \to B$ je injektivna ako vrijedi

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

a surjektivna ako vrijedi

$$K(f) = B.$$

Primjer 22. *Funkcija $f : \mathbb{R} \to \mathbb{R}_0^+$ definirana izrazom $f(x) = |x|$ za sve $x \in \mathbb{R}$ je surjektivna, ali nije injektivna (npr. $f(-1) = f(1)$). Funkcija $g : \mathbb{R} \to \mathbb{R}$ definirana izrazom $g(x) = 2x + 2$ za sve $x \in \mathbb{R}$ je injektivna i surjektivna.*

Definicija 4.4.3. *Funkcija je bijekcija ako je injekcija i surjekcija.*

Posebno, homogenu bijekciju $f : A \to A$ nazivamo *permutacijom* skupa A.

Primjer 23. *Funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana izrazom $f(x) = x^3$ za sve $x \in \mathbb{R}$ je bijekcija. Funkcija $g : [0,1] \to [0,1]$ definirana izrazom $g(x) = \sqrt{1 - x^2}$ za sve $x \in \mathbb{R}$ je također bijekcija.*

Primjedba 4.4.4. *Posebno važna bijekcija koju ćemo često spominjati je tzv. identiteta na skupu A, tj. funkcija $i_A : A \to A$ definirana izrazom $i_A(x) = x$ za sve $x \in A$. Svojstva ove funkcije ispitana su još kada je bila općenito riječ o relacijama, pa znamo da je za svaku funkciju $f : A \to B$ ispunjeno*

$$f \circ id_A = id_B \circ f = f.$$

Zadatak 1. *Dokaži da je:*

1. *kompozicija dviju injekcija injekcija,*
2. *kompozicija dviju surjekcija surjekcija,*
3. *kompozicija dviju bijekcija bijekcija.*

Sljedeći teorem će nam omogućiti da uvedemo pojam inverzne funkcije.

Teorem 4.4.2. *Neka je dana funkcija $f : A \to B$. Relacija f^{-1} je funkcija ako i samo ako je f bijekcija. Štoviše, f^{-1} je i sama bijekcija.*

Dokaz. Pretpostavimo najprije da je f bijekcija i pokažimo da je u tom slučaju f^{-1} funkcija, i to bijekcija.

Kako je f surjekcija, to za svaki $y \in B$ postoji neki $x \in A$ takav da je $f(x) = y$. Dakle, za svaki $y \in B$ postoji neki $x \in A$ takav da je $f^{-1}(y) = x$, iz čega odmah slijedi da je f^{-1} totalna relacija. Dokažimo još da je f^{-1} funkcionalna. Uzmimo stoga proizvoljan $y \in B$ i neke $x, x' \in A$ takve da je $f^{-1}(y) = x$ i $f^{-1}(y) = x'$. Iz ovoga slijedi $f(x) = y$ i $f(x') = y$. Jer je f injektivna slijedi $x = x'$, pa je f^{-1} funkcionalna relacija. Dakle, f^{-1} je funkcija.

Dokažimo da je f^{-1} surjekcija. Kako je f totalna, to za svaki $x \in A$ postoji neki $y \in B$ takav da je $f(x) = y$. Dakle, za svaki $x \in A$ postoji neki $y \in B$ takav da je $f^{-1}(y) = x$, pa je f surjekcija. Dokažimo još i da je f^{-1} injekcija. Uzmimo proizvoljne $y, y' \in B$ i neki $x \in A$ takve da je $f^{-1}(y) = f^{-1}(y') = x$. Slijedi $f(x) = y$ i $f(x) = y'$. Jer je f funkcionalna mora vrijediti $y = y'$, pa je f^{-1} injekcija. Dakle, f^{-1} je bijekcija.

Treba još pokazati da kad god je f^{-1} funkcija da je onda f bijekcija. No ovo slijedi iz drugog dijela već provedenog dokaza: zamjenimo li f sa f^{-1} i iskoristimo li činjenicu da je $(f^{-1})^{-1} = f$ možemo uočiti da se funkcionalnost i totalnost relacije f^{-1} na f prenose kao injektivnost i surjektivnost, pa je u tom slučaju f bijekcija. ■

Primjedba 4.4.5. *Iz dokaza prethodnog teorema se vidi da je f^{-1} parcijalna funkcija ako i samo ako je f injekcija.*

Teorem 4.4.3. *Neka je $f : A \to B$ bijekcija. Vrijedi*

$$f^{-1} \circ f = id_A, \qquad f \circ f^{-1} = id_B \quad ,$$

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

Dokaz. Po Teoremu 4.4.2. znamo da je f^{-1} bijekcija, a po teoremu 4.4.1. 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 proizvoljne $x \in A,\ y \in B$. Jer su f i f^{-1} bijekcije vrijedi

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

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 pri tomu $g \neq f^{-1}$. 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 da je $g \neq f^{-1}$, pa je f^{-1} jedinstvena funkcija s ovim svojstvima. ■

Primjedba 4.4.6. *Posljedica prethodnog teorema jest da je za sve $x \in D(f)$ i sve $y \in K(f)$ ispunjeno*

$$\left(f^{-1} \circ f\right)(x) = x, \qquad \left(f \circ f^{-1}\right)(y) = y.$$

Ovo poglavlje je dijelom preuzeto iz [3].

Poglavlje 5.

Skupovi brojeva

5.1. Skup prirodnih brojeva

5.1.1. Uvod

S prirodnim brojevima se upoznajemo već u osnovnoj školi, no naše znanje o njima tada nije podvrgnuto kritici: šutke 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. No 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:

1. $\mathbb{N}$ nije prazan.
2. $\mathbb{N}$ je uređen.
3. Ako je $n \in \mathbb{N}$, onda je skup svih prirodnih brojeva manjih od n konačan.
4. Skup $\mathbb{N}$ nema najvećeg elementa.

Ova svojstva imaju za posljedicu funkciju $s : \mathbb{N} \to \mathbb{N}$, koja elementu $n \in \mathbb{N}$ pridružuje direktnog sljedbenika $s(n) = n + 1$. 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. $1 \in M$,
2. $(\forall x \in \mathbb{N})\,(x \in M \longrightarrow s(x) \in M)$,

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

Pokazuje se da je prilikom aksiomatske izgradnje skupa prirodnih brojeva najbolje navedeno svojstvo uzeti kao jedan od aksioma. Evo kako bi izgledala aksiomatska izgradnja skupa $\mathbb{N}$.

Definicija 5.1.1. *Neprazni skup $\mathbb{N}$ zove se skup prirodnih brojeva, a njegovi elementi prirodni brojevi, ako vrijede sljedeći aksiomi:*

A1 *Postoji funkcija* $s : \mathbb{N} \to \mathbb{N}$.

A2 *Postoji barem jedan element u* $\mathbb{N}$, *označimo ga s* 1, *takav da je* $(\forall n \in \mathbb{N})\, s(n) \neq 1$.

A3 *Ako je* $s(m) = s(n)$ *za* $m, n \in \mathbb{N}$, *onda je* $m = n$.

A4 *Ako je* M *podskup skupa* $\mathbb{N}$ *i ako vrijedi:*

(a) $1 \in M$,

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

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

Navedeni aksiomi poznati su pod imenom *Peanovi aksiomi skupa prirodnih brojeva*, prema talijanskom matematičaru G. Peanu (1858-1931). U ovoj točki pokazujemo da skup $\mathbb{N}$, koji zadovoljava navedena četiri aksioma, ima sva ona svojstva za koja vjerujemo da ih ima skup prirodnih brojeva s 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.

Naglasimo da četvrti aksiom ima posebnu ulogu: koristimo ga pri dokazivanju teorema i prilikom rekurzivnog definiranja funkcija na $\mathbb{N}$.

5.1.2. Rekurzivna definicija niza

Neka je S neprazan skup, $a \in S$ i $g : S \to S$. Pomoću funkcije g ćemo definirati funkciju $f : \mathbb{N} \to S$ na *rekurzivivni* način: najprije broju 1 pridružimo uočeni element $a \in S$, tj. definiramo da je $f(1) = a$. Funkcija g pridružuje elementu a novi element b iz S, a funkcija s broju 1 broj $s(1)$. Sada se pridruže $s(1)$ i b, tj. definiramo da je $f(s(1)) = g(a) = b$. Taj postupak se nastavlja. Recimo da je za neko $n \in \mathbb{N}$ već definirano $f(n) = x$. Funkcija g pridružuje elementu x element $y = g(x)$, a funkcija s broju n broj $s(n)$. Sada se definira $f(s(n)) = g(x) = y$. Naša tvrdnja je da se ovim postupkom stvarno dobiva jedna funkcija sa $\mathbb{N}$ u S i da je ona jedinstvena. Za funkciju f kažemo da je zadana rekurzivno, odnosno da je definirana induktivno. Prilikom takvog definiranja treba uočiti dvoje:

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

Teorem 5.1.1. *(Rekurzivni teorem) Neka je* S *neprazan skup i* a *zadani element iz* S. *Neka je svakom elementu* n *skupa* $\mathbb{N}$ *pridružena funkcija* $g_n : S \to S$. *Tada postoji jedna i samo jedna funkcija* $f : \mathbb{N} \to S$ *takva da je*

$$f(1) = a \qquad i \qquad (\forall n \in \mathbb{N})\, f(s(n)) = g_n(f(n)).$$

Dokaz. Dokaz ove tvrdnje nije jednostavan, pa ga dajemo samo u skici.

Sa $\mathcal{F}$ označimo familiju svih skupova $B \subseteq \mathbb{N} \times S$ koji 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, to je $\mathcal{F} \neq \emptyset$. Označimo

$$f = \bigcap\nolimits_{B \in \mathcal{F}} B.$$

Lako se vidi da relacija f ima tražena svojstva. Sada se korištenjem aksioma $A1 - A4$ provede dokaz da je relacija f totalna i funkcionalna, tj. da je funkcija sa $\mathbb{N}$ u S, a po konstrukciji relacije f slijedi i da je jedinstvena. ■

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

$$f(1) = a \qquad i \qquad (\forall n \in \mathbb{N})\, f(s(n)) = g(f(n)).$$

Definicija 5.1.2. *Neka je S neprazan skup. Funkcija $f : \mathbb{N} \to S$ zove se niz.*

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 5.1.2. *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.

U Korolaru 5.1.1. uzmimo $S = \mathbb{N}$, $g = s$ i za dani $m \in \mathbb{N}$ stavimo $a = s(m)$. Sada prema Korolaru 5.1.1. postoji jedinstvena funkcija $f_m : \mathbb{N} \to \mathbb{N}$ za koju vrijedi

$$f_m(1) = a = s(m),$$

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

Na taj način je svakom uređenom paru $(m, n) \in \mathbb{N} \times \mathbb{N}$ pridružen jedinstven prirodan broj $f_m(n)$, što znači da imamo funkciju $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ takvu da je

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

Odavde je

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

i

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

Time je egzistencija funkcije f dokazana.

Dokažimo sada jedinstvenost.

Pretpostavimo da postoje dvije funkcije, f i g, koje zadovoljavaju uvjete teorema. Za dani $n \in \mathbb{N}$ označimo s F_n skup svih prirodnih brojeva m takvih da je $f(m,n) = g(m,n)$. Također, označimo s F skup svih prirodnih brojeva n takvih da je $F_n = \mathbb{N}$.

Budući da je

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

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

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

iz čega slijedi

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

a ovo po svojstvima funkcija f i g povlači

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

Dakle, $F_{s(n)} = \mathbb{N}$. Prema tomu imamo:

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

pa $A4$ povlači $F = \mathbb{N}$, tj. $(\forall n \in \mathbb{N})\, F_n = \mathbb{N}$. Drugim riječima, vrijedi

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

pa je $f = g$. ■

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

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

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

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

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

Teorem 5.1.3. *(Asocijativnost zbrajanja) Za proizvoljne brojeve $m,n,p \in \mathbb{N}$ vrijedi*

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

Dokaz. Označimo za dane, ali proizvoljne, $m,n \in \mathbb{N}$ s $M_{m,n}$ skup svih prirodnih brojeva p takvih da je

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

Dokazat ćemo da je $M_{m,n} = \mathbb{N}$. Vrijedi:

$$(m+n)+1 = f(m+n,1) = s(m+n),$$

i isto tako:

$$m+(n+1)=m+f(n,1)=m+s(n)=f(m,s(n))=s(f(m,n))=s(m+n),$$

pa je stoga

$$(m+n)+1=m+(n+1),$$

tj. $1\in M_{m,n}$.

Uzmimo sada $p\in M_{m,n}$ i pokažimo da je u tom slučaju i $s(p)\in M_{m,n}$. Vrijedi:

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

S druge strane je

$$\begin{aligned} m+(n+s(p)) &= m+f(n,s(p))=m+s(f(n,p))=f(m,s(n+p)) \\ &= s(f(m,n+p))=s(m+(n+p)). \end{aligned}$$

Iz ovoga slijedi:

$$\begin{aligned} (m+n)+s(p) &= s((m+n)+p), \\ m+(n+s(p)) &= s(m+(n+p)). \end{aligned}$$

Budući je po pretpostavci $p\in M_{m,n}$, to vrijedi $(m+n)+p=m+(n+p)$, pa je

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

Kombinirajući dobiveno možemo zaključiti da je

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

pa je $s(p)\in M_{m,n}$. Prema tomu, skup $M_{m,n}$ ima svojstva potrebna za primjenu $A4$ i slijedi $M_{m,n}=\mathbb{N}$. Dakle, za dane, a inače proizvoljne $m,n\in\mathbb{N}$ i proizvoljni $p\in\mathbb{N}$ vrijedi

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

što je i trebalo dokazati. ■

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

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

Dokaz. Označimo za dani $m\in\mathbb{N}$ s M_m skup svih prirodnih brojeva n takvih da je $m+n=n+m$. Dalje, označimo s M skup svih prirodnih brojeva m takvih da je $M_m=\mathbb{N}$. Dokazat ćemo da su u skupu M svi prirodni brojevi.

Najprije, lako se vidi da je $M_1=\mathbb{N}$. Naime, po već dokazanoj asocijativnosti zbrajanja prirodnih brojeva imamo:

$$1+s(n)=1+(n+1)=_{as}(1+n)+1.$$

Ako je $n\in M_1$ vrijedi $n+1=1+n$, pa dobijemo

$$1+s(n)=(n+1)+1=s(n)+1,$$

pa je u tom slučaju i $s(n) \in M_1$. Nadalje,

$$1 + 1 = s(1) = 1 + 1,$$

pa je i $1 \in M_1$. Po $A4$ zaključujemo da je $M_1 = \mathbb{N}$.

Prema tomu, vrijedi $1 \in M$. Uzmimo sad neki $m \in \mathbb{N}$ takav da je $m \in M$, tj. $M_m = \mathbb{N}$. Zbog toga je za bilo koji $n \in \mathbb{N}$ ispunjeno

$$n + m = m + n,$$

a kako je $M_1 = \mathbb{N}$ slijedi

$$\begin{aligned} n + s(m) &= n + (m + 1) \overset{as}{=} (n + m) + 1 \overset{pp}{=} (m + n) + 1 \\ &\overset{M_1=\mathbb{N}}{=} 1 + (m + n) \overset{as}{=} (1 + m) + n \overset{M_1=\mathbb{N}}{=} (m + 1) + n \\ &= s(m) + n, \end{aligned}$$

tj. $s(m) \in M$. Dakle, po $A4$ zaključujemo da je $M = \mathbb{N}$, tj. da vrijedi tvrdnja teorema. ■

Primjedba 5.1.1. *Pišemo* $s(1) = 2,\ s(2) = 3,\ s(3) = 4, \ldots$

Teorem 5.1.5. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, m + n \neq n.$

Dokaz. Za dani, ali proizvoljni, $m \in \mathbb{N}$ označimo

$$M_m = \{n \in \mathbb{N} : m + n \neq n\}.$$

Prema $A2$ je sigurno $s(m) \neq 1$, pa je $m + 1 \neq 1$. Dakle, $1 \in M_m$.

Uzmimo sada $n \in M_m$. Iz $m + n \neq n$ slijedi

$$m + s(n) = m + (n + 1) \overset{as}{=} (m + n) + 1 = s(m + n) \overset{A3}{\neq} s(n),$$

pa je i $s(n) \in M_m$. Po $A4$ slijedi $M_m = \mathbb{N}$. Kako je $m \in \mathbb{N}$ bio proizvoljan dobijemo

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

■

Primjedba 5.1.2. *Uočimo da* $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\, m + n \neq n$ *zbog komutativnosti zbrajanja na* $\mathbb{N}$ *zanči 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 5.1.6. *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.

U Korolaru 5.1.1. uzmimo $S = \mathbb{N}$, $a = m$ i $(\forall x \in \mathbb{N})\, g(x) = x + m$. Tada postoji jedinstvena funkcija $h_m : \mathbb{N} \to \mathbb{N}$ takva da je

$$h_m(1) = a = m,$$

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

Odavde slijedi da je sa

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

definirana funkcija h sa $\mathbb{N} \times \mathbb{N}$ u $\mathbb{N}$.

Pri tomu je

$$h(m,1) = h_m(1) = m,$$

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

Time je dokazana egzistencija funkcije h s traženim svojstvima (1) i (2).

Dokažimo da je h jedina takva funkcija.

Pretpostavimo da su h, k funkcije s traženim svojstvima. Za dani, ali proizvoljni, $m \in \mathbb{N}$ definiramo

$$F_m = \{n \in \mathbb{N} : h(m,n) = k(m,n)\}.$$

Dokazat ćemo da je $F_m = \mathbb{N}$.

Očito je $1 \in F_m$, jer je $h(m,1) = m = k(m,1)$. Ako je $n \in F_m$, tj. $h(m,n) = k(m,n)$, onda je

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

pa je i $s(n) \in F_m$. Po $A4$ zaključujemo da je $F_m = \mathbb{N}$. Dakle, za dani ali proizvoljni $m \in \mathbb{N}$ i za svaki $n \in \mathbb{N}$ vrijedi $h(m,n) = k(m,n)$, pa su funkcije h i k jednake. ■

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

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

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

zove se množenje na skupu $\mathbb{N}$ i umjesto $h(m,n)$ pišemo mn. Nadalje, umjesto $h(m,n) + p = f(h(m,n), p)$ pišemo $mn + p$.

Uočimo da $mn + p$ označava superpoziciju dviju funkcija od kojih najprije treba izvršiti množenje. Zato se obično kaže da je množenje operacija višeg reda od zbrajanja.

Teorem 5.1.7. *(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

$$M_{m,n} = \{p \in \mathbb{N} : m(n+p) = mn + mp\}.$$

U skupu $M_{m,n}$ je broj 1 jer je

$$m(n+1) = ms(n) = mn + m = mn + m1.$$

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

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

pa je i $s(p) \in M_{m,n}$. Po $A4$ zaključujemo da je $M_{m,n} = \mathbb{N}$. Kako su m i n proizvoljni slijedi da za bilo koja tri prirodna broja m, n, p vrijedi

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

■

Zbrajanje i množenje su dvije algebarske operacije na skupu $\mathbb{N}$. Prethodnim teoremom uspostavljena je veza među njima: lijevi i desni zakon distribucije.

Teorem 5.1.8. *(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

$$M_{m,n} = \{p \in \mathbb{N} : m(np) = (mn)p\}.$$

Znamo da vrijedi

$$m(n1) = mn = (mn)1,$$

pa je $1 \in M_{m,n}$. Dalje, ako je $p \in M_{m,n}$, tj. ako je $m(np) = (mn)p$, imamo

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

pa je $s(p) \in M_{m,n}$. Po $A4$ zaključujemo da je $M_{m,n} = \mathbb{N}$. Kako su m i n bili proizvoljni zaključujemo da za sve prirodne brojeve m, n, p vrijedi

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

■

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

$$mn = nm.$$

Dokaz. Za dani $m \in \mathbb{N}$ definiramo

$$M_m = \{n \in \mathbb{N} : mn = nm\},$$

i zatim

$$M = \{m \in \mathbb{N} : M_m = \mathbb{N}\}.$$

Znamo da vrijedi $1 \cdot 1 = 1$, pa je $1 \in M_1$. Dalje, ako je $n \in M_1$, tj. ako je $1n = n1$, imamo

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

pa je i $s(n) \in M_1$. Po $A4$ zaključujemo da je $M_1 = \mathbb{N}$, tj. $1 \in M$.

Pretpostavimo sada da je $m \in M$, tj. da je $M_m = \mathbb{N}$. Pokazat ćemo da je i $s(m) \in M$. Naime,

$$s(m)\,n = (m+1)\,n = mn + 1n = mn + n1 = nm + n1 = n(m+1) = ns(m).$$

Dakle,

$$s(m)\,n = ns(m),$$

pa je $M_{s(m)} = \mathbb{N}$, tj. $s(n) \in M$. Opet po $A4$ zaključimo da je $M = \mathbb{N}$. Dakle,

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

pa je

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

■

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. *Za dva skupa S i S' kažemo da su 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 klasi svih skupova, pa se skupovi mogu svrstati u međusobno disjunktne klase ekvivalencije s obzirom na ovu relaciju. Klasu kojoj neki skup S pripada nazivamo njegovim *kardinalnim brojem* i označavamo s $\mathrm{kard}(S)$.

Definicija 5.1.6. *Reći ćemo da je skup S beskonačan ako postoji pravi podskup $S' \subset S$ takav da je $S \cong S'$. Ako skup nije beskonačan, onda kažemo da je konačan.*

Definicija 5.1.7. *Neka je S konačan skup. Reći ćemo da je n broj elemenata skupa S i pisati 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. *Ako je $n \in \mathbb{N} \setminus \{1\}$, onda postoji barem jedan $m \in \mathbb{N}$ takav da je $n = s(m)$. Drugim riječima, s je preslikavanje sa $\mathbb{N}$ na $\mathbb{N} \setminus \{1\}$.*

Dokaz. Označimo $M = s(\mathbb{N}) \cup \{1\}$. Pretpostavimo da je $m \in M$. Tada je očito i $s(m) \in M$. Po $A4$ zaključujemo da je $M = \mathbb{N}$, pa je za svaki $n \in \mathbb{N}$ ispunjeno $n = 1$ ili $n \in s(\mathbb{N})$. No u posljednjem slučaju postoji neki $m \in \mathbb{N}$ takav da je $s(m) = n$. ■

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

Dokaz. Iz $A3$ slijedi da $n \neq m$ povlači $s(m) \neq s(n)$ za bilo koje $m, n \in \mathbb{N}$, a to znači da je s bijekcija sa $\mathbb{N}$ na $s(\mathbb{N})$. Po prethodnoj lemi znamo da je $s(\mathbb{N})$ pravi podskup skupa $\mathbb{N}$, pa je $\mathbb{N}$ ekvipotentan svome pravom podskupu. Dakle, $\mathbb{N}$ je beskonačan. ■

Posebno , kardinalni broj kard$(\mathbb{N})$ skupa prirodnih brojeva označavamo s $\aleph_0$ (čitamo *alef-nula*).

Definicija 5.1.8. *Reći ćemo da je skup S prebrojiv ako je ekvipotentan skupu $\mathbb{N}$.*

Primjedba 5.1.3. *Lako se vidi da je svaki beskonačan podskup skupa $\mathbb{N}$ ekvipotentan skupu $\mathbb{N}$, te 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 svaki skup $\mathbb{N}^k$, gdje je k neki prirodan broj. 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 5.1.10. *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 5.1.11. *(O regularnosti zbrajanja i množenja prirodnih brojeva) Ako su $m, p, q \in \mathbb{N}$, onda*

$$m + p = m + q \Rightarrow p = q,$$

i

$$mp = mq \Rightarrow p = q.$$

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

Na osnovi Teorema 5.1.10. i Teorema 5.1.11. može se na skupu $\mathbb{N}$ uvesti strogi uređaj na sljedeći način: s $<$ označimo onaj podskup skupa $\mathbb{N}\times\mathbb{N}$ koji sadrži samo one parove $(n,m)\in\mathbb{N}\times\mathbb{N}$ koji imaju svojstvo da postoji neki $p\in\mathbb{N}$ takav da je $m=n+p$. 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 $(n,n)\in<$, odnosno $n<n$, postojao bi $p\in\mathbb{N}$ takav da je $n=n+p$ što nije moguće po Teoremu 5.1.11.. Nadalje, ako je za neke n,m i l 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 5.1.10. slijedi da su svaka dva različita elementa skupa $\mathbb{N}$ usporediva po $<$.

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

1. ako je $m=n+p$ i $m'=n'+p'$, onda je

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

pa $n<m$ i $n'<m'$ povlači $n+n'<m+m'$;

2. ako je $m=n+p$, onda je

$$mq=(n+p)\,q=nq+pq,\quad q\in\mathbb{N}$$

pa $n<m$ povlači $nq<mq$ za bilo koji $q\in\mathbb{N}$.

Uvakvo uređenje skupa $\mathbb{N}$ nazivamo *prirodnim uređenjem.* U odnosu na njega postoji 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 slijedi $1<n$.

Teorem 5.1.12. $\mathbb{N}$ *je diskretno uređen skup, tj. za svaki* $n\in\mathbb{N}$ *postoji jedinstveni element* $n'\in\mathbb{N}$ *takav da je* $n<n'$ *i da u* $\mathbb{N}$ *nema elementa koji je između* n *i* n'. *Nadalje, ako je* $n>1$, *onda postoji jedinstveni element* $n''\in\mathbb{N}$ *takav da je* $n''<n$ *i da između* n'' *i* n *nema elemenata skupa* $\mathbb{N}$.

Dokaz. Znamo da je $n<s(n)=n+1$. Pretpostavimo da postoji neki $m\in\mathbb{N}$ takav da je $n<m<s(n)$. Tada je za neki $p\in\mathbb{N}$ ispunjeno $m=n+p$. Ako je $p=1$ onda je $m=s(n)$, a to je u suprotnosti s $m<s(n)$. Dakle, mora biti $p\neq 1$. No u tom slučaju postoji $q\in\mathbb{N}$ takav da je $p=s(q)$, pa je $m=n+s(q)=s(n)+q$, što povlači $s(n)<m$. No ovo nije moguće zbog $m<s(n)$. Dakle, ne postoji nijedan prirodan broj između n i $s(n)$, tj. $s(n)$ je *neposredni sljedbenik* elementa 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* elementa n. ■

Teorem 5.1.13. *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 5.1.14. *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. ■

5.2. 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 se vidi da cijele brojeve treba promatrati kao uređene parove prirodnih brojeva, odnosno 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 $\mathbb{N} \times \mathbb{N}/\sim$ ima svojstva skupa cijelih brojeva na koja smo navikli. No čitava konstrukcija se oslanja na sljedeći teorem.

Teorem 5.2.1. *Definiramo relaciju $\sim$ na $\mathbb{N} \times \mathbb{N}$ sa*

$$(m, n) \sim (p, q) \quad \textit{ako i samo ako je} \quad m + q = p + n.$$

Vrijedi:

1. *$\sim$ 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, $\sim$ 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

$$\begin{aligned} m+q &= p+n,\\ p+s &= r+q, \end{aligned}$$

pa je

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

odnosno $m+s=r+n$ po Teoremu 5.1.11.. Iz ovoga, pak, slijedi $(m,n)\sim(r,s)$, pa je relacija $\sim$ i tranzitivna, tj. ona je 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 $m+n'=m'+n$ i $p+q'=p'+q$. Odavde 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 $(m+p,n+q)\sim(m'+p',n'+q')$.

Druga ekvivalencija se dokaže na sličan način. ■

Definicija 5.2.1. *Neka je $\sim$ relacija na $\mathbb{N}\times\mathbb{N}$ definirana s*

$$(m,n)\sim(p,q) \quad \textit{ako i samo ako je} \quad m+q=p+n.$$

Skup $\mathbb{N}\times\mathbb{N}/\sim$ nazivamo skupom cijelih brojeva. Označavamo ga sa $\mathbb{Z}$, a njegove elemente nazivamo cijelim brojevima.

5.2.2. Zbrajanje i množenje na $\mathbb{Z}$

Podsjetimo se da smo sa τ označavali funkciju projekcije vezanu uz neku relaciju ekvivalencije. U našem slučaju ćemo promatrati relaciju ekvivalencije $\sim$ na skupu $\mathbb{N}\times\mathbb{N}$ pomoću koje smo definirali cijele brojeve. Projekcija $\tau:\mathbb{N}\times\mathbb{N}\to\mathbb{N}\times\mathbb{N}/\sim$ svakom uređenom paru prirodnih brojeva (m,n) pridružuje odgovarajuću klasu ekvivalnecije po relaciji $\sim$, tj. odgovarajući cijeli broj. Može se pokazati (dokaz zbog duljine preskačemo, vidi [4]) da za bilo koje $(m,n),(p,q)\in\mathbb{N}\times\mathbb{N}$ 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 $\mathbb{Z}$. Štoviše, pri tomu se sačuvaju sva ona svojstva zbrajanja i množenja koja smo već opisali u prethodnoj točki (komutativnost, asocijativnost i distributivnost).

Posebno izdvajamo cijeli broj $\tau(1,1)$. Taj se element označava s 0 i zove se *nula* u $\mathbb{Z}$. lako se vidi da vrijedi

$$a+0=0+a=a$$

za svaki $a\in\mathbb{Z}$ i 0 je jedini element s ovim svojstvom.

No elementi skupa $\mathbb{Z}$ imaju još jedno važno svojstvo koje je opisano u narednom teoremu.

Teorem 5.2.2. *Za svaki $a\in\mathbb{Z}$ postoji jedan i samo jedan $a'\in\mathbb{Z}$ takav da je*

$$a+a'=a'+a=0.$$

Dokaz. Neka je $a=\tau(m,n)$. 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

$$m+n+1=1+m+n,$$

to je

$$(m+n,m+n)\sim(1,1),$$

pa je

$$\tau(m+n,m+n)=\tau(1,1)=0,$$

tj.,

$$a+a'\overset{kom}{=}a'+a=0.$$

Dokažimo jedinstvenost elementa a'. Pretpostavimo da za neki $b\in\mathbb{Z}$ vrijedi

$$a+b=b+a=0.$$

Tada je

$$b=b+0=b+(a+a')=(b+a)+a'=0+a'=a'.$$

■

Element a' sa svojstvom $a+a'=0$ 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 $\tau(m,n)=-\tau(n,m)$, što se lako 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 se *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 prvobitnomu poretku.

5.2.3. O uređenosti skupa $\mathbb{Z}$

Uređajnu relaciju na skupu $\mathbb{Z}$ uvodimo na osnovi sljedećeg teorema.

Teorem 5.2.3. *$P = \{\mathbb{Z}_-, \mathbb{Z}_0, \mathbb{Z}_+\}$ je jedna particija skupa $\mathbb{Z}$, pri ćemu 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 $a = \tau(p,q)$. Po Teoremu 5.1.10. znamo da za prirodne brojeve p i q postoji samo jedna od tri mogućnosti:

$$\begin{aligned} p &= q+n, \quad n \in \mathbb{N}, \\ q &= p+n, \quad n \in \mathbb{N}, \\ p &= q. \end{aligned}$$

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

$$\mathbb{Z} \subseteq \mathbb{Z}_- \cup \mathbb{Z}_0 \cup \mathbb{Z}_+,$$

no kako su $\mathbb{Z}_-, \mathbb{Z}_0, \mathbb{Z}_+ \subset \mathbb{Z}$ odmah slijedi i

$$\mathbb{Z} = \mathbb{Z}_- \cup \mathbb{Z}_0 \cup \mathbb{Z}_+.$$

Dalje, za bilo koji $n \in \mathbb{N}$ je $\tau(n+1,1) \neq 0$ i $\tau(1,n+1) \neq 0$, pa 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 $(n+1,1) \sim (1,m+1)$, 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 $\mathbb{Z}$.

Također, lako se vidi da iz $a \in \mathbb{Z}_+$ slijedi $-a \in \mathbb{Z}_-$ i obratno.

Teorem 5.2.4. *Skup*

$$\rho = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : b - a \in \mathbb{Z}_+\}$$

je uređajna relacija na $\mathbb{Z}$.

Dokaz. Iz $a, b \in \mathbb{Z}$ slijedi $b - a \in \mathbb{Z}$. Po Teoremu 5.2.3. znamo da vrijedi samo jedno od troje: $b - a \in \mathbb{Z}_-$, $b - a \in \mathbb{Z}_0$ ili $b - a \in \mathbb{Z}_+$.

Ako je $b - a \in \mathbb{Z}_0$, tj. $a = b$, onda sigurno znamo da $b - a \notin \mathbb{Z}_+$, pa je ρ irefleksivna.

Ako je $b - a \in \mathbb{Z}_-$, onda postoji $n \in \mathbb{N}$ takav da je $b - a = \tau(1,n+1)$. Iz ovoga slijedi $a - b = -\tau(1,n+1) = \tau(n+1,1)$, pa je $a - b \in \mathbb{Z}_+$, tj. $(b,a) \in \rho$. Ako je, pak, $b - a \in \mathbb{Z}_+$, onda je $(a,b) \in \rho$. Dakle, svi različiti elementi $\mathbb{Z}$ su usporedivi.

I na kraju, relacija ρ je i tranzitivna. Naime, ako je $(a,b)\in\rho$ i $(b,c)\in\rho$, onda je

$$\begin{aligned} b-a &\in \mathbb{Z}_+, \quad \text{tj.} \quad b-a=\tau(n+1,1),\ n\in\mathbb{N},\\ c-b &\in \mathbb{Z}_+, \quad \text{tj.} \quad c-b=\tau(m+1,1),\ m\in\mathbb{N}. \end{aligned}$$

Odatle slijedi

$$\begin{aligned} c-a &= c+0-a=c+[(-b)+b]-a=(c-b)+(b-a)\\ &= \tau(m+1,1)+\tau(n+1,1)=\tau(n+m+1+1,1+1)\\ &= \tau(n+m+1,1)\in\mathbb{Z}_+, \end{aligned}$$

pa je $(a,c)\in\rho$. ■

Dakle, Teorem 5.2.4. nam garantira da je ρ uređajna relacija na $\mathbb{Z}$. Tu relaciju označavamo s $<$, i za svaka dva cijela a i b broja vrijedi točno jedno od troje: $a=b$, $a<b$ (tj. $(a,b)\in\rho$) ili $b<a$ (tj. $(b,a)\in\rho$). Također, iz $a<b$ i $b<c$ slijedi $a<c$.

Očito je da iz $a\in\mathbb{Z}_+$ slijedi $a>0$, a iz $a\in\mathbb{Z}_-$ slijedi $a<0$ i obratno.

Teorem 5.2.5. *Za elemente skupa $\mathbb{Z}$ vrijede sljedeće izreke:*

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 samo 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

$$\begin{aligned} ab &= \tau(1,n+1)\,\tau(1,m+1)\\ &= \tau(1\cdot 1+(n+1)(m+1),1\cdot(m+1)+(n+1)\cdot 1)\\ &= \tau(mn+m+n+1+1,m+n+1+1)\\ &= \tau(mn+1,1)\in\mathbb{Z}_+. \end{aligned}$$

■

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 ova 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 $\mathbb{Z}_+$).

Štoviše, može se pokazati da uređena trojka $(\mathbb{Z}_+, s', j(1))$, gdje je $s' : \mathbb{Z}_+ \to \mathbb{Z}_+$ definirana sa $s'(j(n)) = j(n+1)$, zadovoljava Peanove aksiome A1-A4. Prema tomu, $\mathbb{Z}_+$ je skup prirodnih brojeva isto toliko koliko je i $\mathbb{N}$.

Zahvaljujući svojstvima funkcije j možemo na neki način poistovijetiti skupove $\mathbb{N}$ i $\mathbb{Z}_+ = j(\mathbb{N})$: svaki teorem dokazan u $\mathbb{N}$ pomoću j prelazi u teorem u $\mathbb{Z}_+$ i obratno. Kažemo da smo $\mathbb{N}$ *uložili* u $\mathbb{Z}$. Koristeći prije spomenutu identifikaciju 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

$$(-1)\,n = \tau(1,2)\,\tau(n+1,1) = \tau(n+1+2, 1+2n+2) = \tau(1,n+1) = -n.$$

Dakle, 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 ili konačnih skupova prebrojiva ili konačna 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 $\mathrm{kard}(\mathbb{Z}) = \aleph_0$.

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 i 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.

Dakle, $\mathbb{Z} \cong \mathbb{N}$ i 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. ■

5.3. Djeljivost i kongruencije

U ovom poglavlju ćemo se detljnije pozabaviti dvjema relacijama vezanim uz skup cijelih brojeva $\mathbb{Z}$, no također i uz skup prirodnih brojeva $\mathbb{N}$. Te su relacije *djeljivost* i *kongruencija*. Prva je relacija parcijalnog uređaja, dok je druga relacija ekvivalencije.

Matematička disciplina koja, općenito govoreći, proučava svojstva prirodnih brojeva zove se *teorija brojeva*. Njen najstariji dio je *elementarna teorija brojeva*, koja svoje začetke ima još u starohebrejskoj, starogrčkoj i starokineskoj matematici.

5.3.1. Djeljivost

Temeljni pojam teorije brojeva je *djeljivost*.

Definicija 5.3.1. *Kažemo da broj $a \in \mathbb{N}$ dijeli broj $b \in \mathbb{N}$ ako postoji broj $k \in \mathbb{N}$ 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 (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 $a \nmid b$.

Definicija 5.3.2. *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 je na sljedeći način:

$$\mid = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \mid b\}.$$

Pogledajmo neka važna svojstva ove relacije.

Propozicija 5.3.1. *Vrijedi:*

1. $(\forall a \in \mathbb{N})\, a \mid a$;
2. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(a \mid b \wedge b \mid a \longrightarrow a = b)$;
3. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \wedge b \mid c \longrightarrow a \mid c)$,

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 5.3.2. *Vrijedi:*

1. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \wedge a \mid c \longrightarrow a \mid b + c)$;
2. $(\forall a \in \mathbb{N})\,(\forall b \in \mathbb{N})\,(\forall c \in \mathbb{N})\,(a \mid b \longrightarrow a \mid bc)$.

Dokaz. Sami za vježbu. ■

Pojam djeljivosti možemo lako proširiti i na cijele brojeve. U tom slučaju 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. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(a \mid b \wedge b \mid a \longrightarrow a = \pm b)$;
3. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \wedge b \mid c \longrightarrow a \mid c)$;
4. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \wedge a \mid c \longrightarrow a \mid b \pm c)$;
5. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \mid b \longrightarrow a \mid bc)$.

Sično 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 5.3.1. *(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. 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 $0 \leq r < a$. Pretpostavimo suprotno, tj. da vrijedi $r = b - aq \geq a$. Tada je $0 \leq b - (q + 1)\, a = r - a < r$, 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.

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* (kvocijent), a broj r *ostatak* pri dijeljenju broja b brojem a. Broj a zovemo *djelitelj* (divizor), a broj b *djeljenik* (dividend).

Primjer 24. $25 = 3 \cdot 7 + 4,\ -25 = (-4) \cdot 7 + 3,$ *ali ne* $-25 = (-3) \cdot 7 - 4.$

Primjedba 5.3.1. *Primijetimo da $a \mid b$ ako i samo ako je ostatak r pri dijeljenju b s a jednak nuli.*

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

Primjedba 5.3.2. *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 $m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ na uređenom paru $(a, b) \in \mathbb{N} \times \mathbb{N}$, $a < b$, dobiva se tzv. *Euklidovim algoritmom*

$$\begin{aligned} b &= q_1 a + r_1, \quad 0 < r_1 < a \\ a &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1}, \quad r_{n+1} = 0. \end{aligned}$$

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 tom uzimamo da je $r_0 = a$). No tada je $r_{n-1} = q_{n+1} r_n$, pa iz

$$m(a, b) = m(r_1, a) = m(r_2, r_1) = \cdots = m(r_n, r_{n-1}) = r_n$$

slijedi

$$m(a,b) = r_n.$$

Iz gornjeg algoritma se odmah dobije da za bilo koje prirodne brojeve a i b postoje cijeli brojevi c i d takvi da je

$$m(a,b) = ac + bd.$$

Primjer 25. *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 26. *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

$$\begin{aligned} 3 &= 42 - 1 \cdot 39 = 42 - 1 \cdot (165 - 3 \cdot 42) \\ &= 42 + 3 \cdot 42 - 1 \cdot 165 = 4 \cdot 42 + (-1) \cdot 165. \end{aligned}$$

Definicija 5.3.3. *Kažemo da su prirodni brojevi a i b relativno prosti ako je $m(a,b) = 1$.*

Zadatak 2. *Dokaži 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 $a \mid c$;*

5.3.2. 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 5.3.4. *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 brojvima.*

Dakle, skup prirodnih brojeva možemo podijeliti na tri međusobno disjunktna podskupa: $\{1\}$, skup P prostih brojeva i skup S složenih brojeva.

Početni dio skupa 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.

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots, n.$$

Najprije prekrižimo 1. Najmanji prosti broj je $p_1 = 2$, pa prekrižimo sve višekratnike broja 2 iza 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. ostalo je

$$2, 3, 5, 7, 11, 13, 17, \ldots, n.$$

Postupak za $p_3 = 5$ nastavimo s višekratnicima broja 5 i tako dalje. 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 nisu riješeni do dana današnjeg. 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 5.3.2. *(Euklid) Prostih brojeva ima beskonačno mnogo.*

Da bismo dokazali ovaj teorem trebat će nam jedna lema.

Lema 5.3.1. *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, a koji nije umnožak prostih brojeva. Tada je skup $M \subset \mathbb{N}$ u kojemu su svi takvi brojevi neprazan, pa ima najmanji element koji ćemo označiti 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. Prema tomu, postoje prirodni brojevi m_1 i m_2 takvi da je $1 < m_1, m_2 < m$ i $m = m_1 m_2$. No kako je m najmanji element skupa M i $1 < m_1, m_2 < m$, to odmah slijedi da se brojevi m_1 i m_2 mogu prikazati kao umnošci prostih brojeva, a time da 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.

Označimo $N = p_1 p_2 p_3 \cdots p_n + 1$. Očito je $N > 1, p_1, p_2, p_3, \ldots, p_n$ i N nije djeljiv ni s jednim od brojeva $p_1, p_2, p_3, \ldots, p_n$ (pri dijeljenju sa svakim od njih on daje ostatak 1). 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. ■

Dokazali smo da se svaki prirodni broj veći od 1 može prikazati kao umnožak jednog ili više prostih brojeva, tj. *rastaviti na proste faktore*. U Lemi 5.3.1. smo dokazali egzistenciju takvog rastava, no može se pokazati i da je takav rastav jedinstven do na poredak faktora. O tomu govori sljedeći teorem.

Teorem 5.3.3. *(Osnovni teorem aritmetike) Za svaki prirodni broj $n > 1$ postoje jedinstveni prirodni brojevi $k, \alpha_1, \alpha_2, \ldots, \alpha_k$ i jedinstveni prosti brojevi $p_1 < \cdots < p_k$ takvi da je*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Dokaz. Jedinstvenost brojeva $k, \alpha_1, \alpha_2, \ldots, \alpha_k$ 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 27. $18 = 2^1 3^2,\ 35 = 5^1 7^1,\ 180 = 2^2 3^2 5^1$.

5.3.3. Kongruencije

Teorem o dijeljenju s ostatkom direktno se nadovezuje na jedan važan primjer relacije ekvivalencije.

Definicija 5.3.5. *Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$. Kažemo da je a kongruentno b modulo n i pišemo*

$$a \equiv b \,(\mathrm{mod}\, n)$$

ako $n \mid a - b$.

Primjer 28. $17 \equiv 2 \,(\mathrm{mod}\, 5)$, $17 \equiv -3 \,(\mathrm{mod}\, 5)$, *ali nije* $12 \equiv 5 \,(\mathrm{mod}\, 4)$.

Za neki dani $n \in \mathbb{N}$ ovim je definirana jedna relacija na skupu $\mathbb{Z}$. Označavamo je s $\equiv (\mathrm{mod}\, n)$ i zovemo "kongruencija modulo n". ovaj pojam je uveo Gauss 1801. godine.

Propozicija 5.3.3. *Neka je dan neki $n \in \mathbb{N}$. Vrijedi:*

1. $(\forall a \in \mathbb{Z})\, a \equiv a \,(\mathrm{mod}\, n)$;
2. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(a \equiv b \,(\mathrm{mod}\, n) \longrightarrow b \equiv a \,(\mathrm{mod}\, n))$;
3. $(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(a \equiv b \,(\mathrm{mod}\, n) \wedge b \equiv c \,(\mathrm{mod}\, n) \longrightarrow a \equiv c \,(\mathrm{mod}\, n))$.

Drugim riječima, relacija $\equiv (\mathrm{mod}\, n)$ je relacija ekvivalencije na skupu $\mathbb{Z}$.

Dokaz. Za svaki $a \in \mathbb{Z}$ vrijedi $n \mid a - a = 0$, tj. $a \equiv a \,(\mathrm{mod}\, n)$.

Neka su $a, b \in \mathbb{Z}$ takvi da je $a \equiv b \,(\mathrm{mod}\, n)$. Iz toga slijedi da $n \mid a-b$, pa $n \mid b-a$, odakle je $b \equiv a \,(\mathrm{mod}\, n)$.

Neka su $a, b, c \in \mathbb{Z}$ takvi da je $a \equiv b \,(\mathrm{mod}\, n)$ i $b \equiv c \,(\mathrm{mod}\, n)$. Tada vrijedi $n \mid a - b$ i $n \mid b - c$, pa zbog svojstava djeljivosti $n \mid (a - b) + (b - c) = a - c$. Dakle, $a \equiv c \,(\mathrm{mod}\, n)$. ■

Budući je $\equiv (\mathrm{mod}\, n)$ relacija ekvivalencije na skupu $\mathbb{Z}$, ona tvori jednu particiju skupa $\mathbb{Z}$. Za $a \in \mathbb{Z}$ pripadna je klasa ekvivalencije skup

$$[a] = \{b \in \mathbb{Z} : a \equiv b \,(\mathrm{mod}\, n)\}.$$

Znamo da vrijedi:

$$\begin{aligned} a \;&\equiv\; b \,(\mathrm{mod}\, n) \Leftrightarrow b \equiv a \,(\mathrm{mod}\, n) \Leftrightarrow n \mid b - a \\ &\Leftrightarrow\; b - a = kn,\ k \in \mathbb{Z} \Leftrightarrow b = a + kn,\ k \in \mathbb{Z}. \end{aligned}$$

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 5.3.4. *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 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 $\{[0], [1], \ldots, [n-1]\}$ jedna particija skupa $\mathbb{Z}/_{\equiv(\mathrm{mod}\, n)}$, 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 pretstavnike 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 skup $\{a_0, a_1, \ldots, a_{n-1}\}$ s ovim svojstvom nazivamo *potpunim skupom ostataka modulo n*.

Kongruencije imaju još neka lijepa svojstva.

Propozicija 5.3.5. *Neka je dan neki $n \in \mathbb{N}$. 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 $n \mid a - c$ 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, $cd - ab = c(d - b) + b(c - a)$, pa $n \mid cd - ab$, iz čega odmah slijedi $ab \equiv cd\,(\mathrm{mod}\, n)$. ■

Propozicija 5.3.6. *Neka su $d, n \in \mathbb{N}$ relativno prosti brojevi. Tada za bilo koje $a, b \in \mathbb{Z}$ vrijedi $ad \equiv bd\,(\mathrm{mod}\, n)$ ako i samo ako $a \equiv b\,(\mathrm{mod}\, n)$.*

Dokaz. Sami za vježbu. ■

5.4. Skup racionalnih brojeva

5.4.1. 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 $\mathbb{Z}\setminus\{0\}$), a 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 5.4.1. *Za dva elementa (a, b) i (c, d) iz $\mathbb{Z} \times \mathbb{Z}^*$ definiramo*

$$(a, b) \sim (c, d) \quad \text{ako i samo ako je } ad = cb.$$

Tada je $\sim$ relacija ekvivalencije na $\mathbb{Z}\times\mathbb{Z}^*$. Nadalje, ako je

$$(a,b)\sim(a',b') \quad i \quad (c,d)\sim(c',d'),$$

onda je

$$(ad+cb,bd)\sim(a'd'+c'b',b'd'),$$

i

$$(ac,bd)\sim(a'c',b'd').$$

Dokaz. Da je $\sim$ refleksivna i simetrična očigledno je. Dokažimo još da je tranzitivna. Neka su $(a,b),(c,d)$ i (e,f) elementi $\mathbb{Z}\times\mathbb{Z}^*$ 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

$$d(af)=(ad)f=(bc)f=(cf)b=(de)b=d(eb),$$

a jer je $d\neq 0$ po regularnosti množenja je tada

$$af=eb,$$

tj. $(a,b)\sim(e,f)$. Dakle, $\sim$ je relacija ekvivalencije na $\mathbb{Z}\times\mathbb{Z}^*$.

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 $\mathbb{Z}\times\mathbb{Z}^*$. Da bi vrijedila tvrdnja $(ad+cb,bd)\sim(a'd'+c'b',b'd')$ treba dokazati 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. Druga se dokaže lako na sličan način. ■

Definicija 5.4.1. *Neka je $\sim$ relacija ekvivalencije kao u Teoremu 5.4.1.. Skup*

$$\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}^*/\sim$$

nazivamo skupom racionalnih brojeva.

Sa τ nadalje označavamo projekciju skupa $\mathbb{Z}\times\mathbb{Z}^*$ na skup $\mathbb{Q}$.

Primjer 29.

$$\tau(1,2)=[(1,2)]=\{(1,2),(-1,-2),(2,4),(-2,-4),(3,6),(-3,-6),\ldots\}.$$

5.4.2. Zbrajanje i množenje na $\mathbb{Q}$

Do relacije ekvivalencije $\sim$ dosli smo zamjenivši $\frac{a}{b}$ s paromm (a,b). Na sličan način, formule $\frac{a}{b}+\frac{c}{d}$ i $\frac{a}{b}\frac{c}{d}$ pređu 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

$$\tau(a,b)+\tau(c,d)=\tau(ad+cb,bd), \tag{5.1}$$

$$\tau(a,b)\,\tau(c,d)=\tau(ac,bd). \tag{5.2}$$

Teorem 5.4.2. *Sa* (5.1) *i* (5.2) *definirane su funkcije sa* $\mathbb{Q}\times\mathbb{Q}$ *u* $\mathbb{Q}$. *Funkcija* $+$ *definirana s* (5.1) *zove se zbrajanje, a funkcija* $\cdot$ *definirana s* (5.2) *zove se množenje na* $\mathbb{Q}$.

Dokaz. Treba pokazati da su relacije $+$ i $\cdot$ funkcionalne i totalne. Totalnost je u oba slučaja očigledna (svakako su za bilo koje $\tau(a,b)$, $\tau(c,d)$ iz $\mathbb{Q}$ i $\tau(ad+cb,bd)$, kao i $\tau(ac,bd)$, iz $\mathbb{Q}$). Dokažimo funkcionalnost.

Neka su $(\tau(a,b),\tau(c,d))$, $(\tau(a',b'),\tau(c',d'))$ dva jednaka elementa iz $\mathbb{Q}\times\mathbb{Q}$. Tada je $\tau(a,b)=\tau(a',b')$ i $\tau(c,d)=\tau(c',d')$, odnosno $(a,b)\sim(a',b')$ i $(c,d)\sim(c',d')$. Iz ovoga je po Teoremu 5.4.1.

$$(ad+cb,bd)\sim(a'd'+c'b',b'd'),$$

pa je $\tau(ad+cb,bd)=\tau(a'd'+c'b',b'd')$.

Analogno se dokaže funkcionalnost i za množenje. ■

Teorem 5.4.3. *Zbrajanje i množenje su komutativne i asocijativne operacije na* $\mathbb{Q}$. *Također je zbrajanje distributivno prema množenju na* $\mathbb{Q}$.

Dokaz. Sami. ■

Teorem 5.4.4. *Za svaki element* $\tau(a,b)$ *skupa* $\mathbb{Q}$ *vrijedi*

$$\tau(a,b)+\tau(0,1)=\tau(0,1)+\tau(a,b)=\tau(a,b),$$

$$\tau(a,b)\,\tau(1,1)=\tau(1,1)\,\tau(a,b)=\tau(a,b),$$

$$\tau(a,b)\,\tau(0,1)=\tau(0,1)\,\tau(a,b)=\tau(0,1).$$

Štoviše, $\tau(0,1)$ *i* $\tau(1,1)$ *su jedinstveni elementi skupa* $\mathbb{Q}$ *s ovim svojstvima.*

Dokaz. Vrijedi:

$$\tau(a,b)+\tau(0,1)=\tau(a\cdot1+0\cdot b,b\cdot1)=\tau(a,b)=\tau(0,1)+\tau(a,b),$$

$$\tau(a,b)\,\tau(1,1)=\tau(a\cdot1,b\cdot1)=\tau(a,b)=\tau(1,1)\,\tau(a,b)$$

i

$$\tau(a,b)\,\tau(0,1)=\tau(a\cdot0,b\cdot1)=\tau(0,b)=\tau(0,1)=\tau(0,1)\,\tau(a,b)$$

zbog $(0,b)\sim(0,1)$ za svaki $b\in\mathbb{Z}^*$.

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

$$\tau(x,y)=\tau(x,y)+\tau(0,1)=\tau(0,1).$$

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

$$\tau(x,y) = \tau(x,y)\,\tau(1,1) = \tau(1,1).$$

■

Zbog prethodnog teorema ima, dakle, smisla označiti

$$\tau(0,1) \equiv 0,\ \tau(1,1) \equiv 1.$$

Teorem 5.4.5. *Za svaki element $\tau(a,b)$ skupa $\mathbb{Q}$ postoji jedinstveni element x skupa $\mathbb{Q}$ takav da vrijedi*

$$\tau(a,b) + x = x + \tau(a,b) = \tau(0,1).$$

Nadalje, za svaki element $\tau(a,b)$ skupa $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$ postoji jedinstveni element $y \in \mathbb{Q}^*$ takav da vrijedi

$$\tau(a,b)\cdot y = y\cdot\tau(a,b) = \tau(1,1).$$

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

$$x' = x' + 0 = x' + (\tau(a,b) + x) = (x' + \tau(a,b)) + x = \tau(0,1) + x = x.$$

Definiramo li da je za $\tau(a,b) \in \mathbb{Q}^*$

$$y = \tau(b,a) \in \mathbb{Q}^*,$$

vrijedi

$$\tau(a,b)\,\tau(b,a) = \tau(ab,ba) = \tau(ab,ab) = \tau(1,1),$$

zbog $\tau(c,c) = \tau(1,1)$ za svaki $c \in \mathbb{Z}^*$.

Na sličan način kao kod zbrajanja dokažemo i jedinstvenost elementa y s navedenim svojstvima. ■

Primjedba 5.4.1. *Za svaki $\tau(a,b) \in \mathbb{Q}$ označavat ćemo $\tau(-a,b) = -\tau(a,b)$ (inverzni element za zbrajanje na $\mathbb{Q}$), a za svaki $\tau(a,b) \in \mathbb{Q}^*$ označavat ćemo $\tau(b,a) = \tau(a,b)^{-1}$ (inverzni element za množenje na $\mathbb{Q}$). 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.*

5.4.3. Ulaganje cijelih u racionalne brojeve

Lako se pokaže da je funkcija $j : \mathbb{Z} \to \mathbb{Q}$ definirana s

$$j(m) = \tau(m, 1)$$

za svaki $m \in \mathbb{Z}$ dobro definirana i da je injekcija. Štoviše, ona ima svojstva da je za sve $m, m' \in \mathbb{Z}$ ispunjeno

$$j(m + m') = \tau(m + m', 1) = \tau(m, 1) + \tau(m', 1) = j(m) + j(m'),$$

$$j(mm') = \tau(mm', 1) = \tau(m, 1)\,\tau(m', 1) = j(m)\,j(m'),$$

te

$$j(1) = \tau(1, 1) = 1_Q.$$

Ove činjenice nam omogućavaju da poistovijetimo cijeli broj m s racionalnim brojem $j(m) = \tau(m, 1)$, odnosno da uložimo slup cijelih brojeva u skup racionalnih brojeva.

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 ćemu 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

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb,$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Također je

$$-\frac{a}{b} = \frac{-a}{b} \quad \text{i} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \quad a \neq 0.$$

Teorem 5.4.6. *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 $\mathrm{kard}\mathbb{Q} = \aleph_0$. ■

5.4.4. O uređenosti skupa $\mathbb{Q}$

Uređajnu relaciju na $\mathbb{Q}$ uvodimo na osnovi sljedećeg teorema.

Teorem 5.4.7. *$\mathcal{P} = \{\mathbb{Q}_-, \mathbb{Q}_0, \mathbb{Q}_+\}$ je particija skupa $\mathbb{Q}$, pri ćemu 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 $ad = bc$, a odavde je $(ab)(cd) = (bc)^2 > 0$. Dakle, ab i cd moraju biti istog predznaka, tj. istodobno su u $\mathbb{Q}_+$, odnosno $\mathbb{Q}_-$. 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 $\mathbb{Q}_+$ dobro definirani i međusobno disjunktni. Pokažimo 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 je $\mathbb{Q} = \mathbb{Q}_- \cup \mathbb{Q}_0 \cup \mathbb{Q}_+$, 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 5.4.8. *Skup*

$$\rho = \{(x,y) \in \mathbb{Q} \times \mathbb{Q} : y - x \in \mathbb{Q}_+\}$$

je stroga uređajna relacija 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 $z - y \in \mathbb{Q}_+$. Da bismo dokazali da je $z - x \in \mathbb{Q}_+$, mi ćemo dokazati 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 ćemu 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, $x + y \in \mathbb{Q}_+$.

Sada imamo:

$$z - x = (z - y) + (y - x) \in \mathbb{Q}_+,$$

pa je relacija ρ tranzitivna. Ovime smo dokazali da je relacija ρ relacija strogog uređaja na skupu $\mathbb{Q}$. ■

Ova relacija uređaja na $\mathbb{Q}$ ima mnoga lijepa svojstva. Tako vrijedi

$$(\forall m \in \mathbb{Z})\,(\forall n \in \mathbb{Z})\,(m < n \longrightarrow j\,(m) < j\,(n))\,,$$

pa preslikavanje j čuva uređaj na $\mathbb{Z}$. Također vrijedi i sljedeće.

Teorem 5.4.9. *Zbrajanje i množenje na $\mathbb{Q}$ su kompatibilne operacije s uređajem na $\mathbb{Q}$. Točnije vrijedi:*

1. $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x < y \longrightarrow x + z < y + z)\,;$
2. $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,((x < y \wedge 0 < z) \longrightarrow xz < yz)\,.$

Sada ćemo ukazati na još jedno važno svojstvo skupa $\mathbb{Q}$ koje nemaju ni skup $\mathbb{N}$ ni skup $\mathbb{Z}$.

Definicija 5.4.2. *Za uređeni skup $(S, <)$ kažemo da je gust ako između svaka dva elementa skupa S postoji treći element skupa S, tj. ako vrijedi*

$$(\forall a \in S)\,(\forall b \in S)\,(a < b \longrightarrow (\exists c \in S)\,(a < c < b))\,.$$

Teorem 5.4.10. *Skup $\mathbb{Q}$ je gust.*

Dokaz. Neka su a, b proizvoljni elementi skupa $\mathbb{Q}$ za koje vrijedi $a < b$. Definiramo li

$$c = \frac{a+b}{2} \in \mathbb{Q},$$

vrijedit će $a < c < b$. ■

5.5. Skup realnih brojeva

5.5.1. Aksiomi skupa realnih brojeva

Vidjeli smo da elemente skupa $\mathbb{Q}$ možemo zbrajati i množiti, te oduzimati i dijeliti (izuzev s nulom). Pri tome zbrajanje i množenje na $\mathbb{Q}$ imaju ova svojstva:

A1 $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,x + (y + z) = (x + y) + z$ (asocijativnost zbrajanja);

A2 $(\exists 0 \in \mathbb{Q})\,(\forall x \in \mathbb{Q})\,0 + x = x + 0 = x$ (neutralni el. za zbrajanje);

A3 $(\forall x \in \mathbb{Q})\,(\exists -x \in \mathbb{Q})\,x + (-x) = (-x) + x = 0$ (inverzni el. 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 el. 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 el. 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 P koji ima barem dva različita elementa i na kojem su definirane algebarske operacije zbrajanje i množenje s navedenih devet svojstava zove se *polje*.

Dakle je skup racionalnih brojeva $\mathbb{Q}$ polje uz standardne operacije zbrajanja i množenja.

No na skupu $\mathbb{Q}$ osim navedene strukture polja postoji i uređajna struktura. Pokazali smo da je skup $\mathbb{Q}$ uređen i pri tome taj uređaj ima ova svojstva:

Aa $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x < y \wedge y < z \longrightarrow x < z)$ (tranzitivnost rel. $<$);

Ab $(\forall x \in \mathbb{Q})\,(x \not< x)$ (irefleksivnost re. $<$);

Ac $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(x \neq y \longrightarrow x < y \vee y < x)$ (linearnost rel. $<$);

Ad $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(\forall z \in \mathbb{Q})\,(x < y \longrightarrow x + z < y + z)$;

Ae $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(0 < x \wedge 0 < y \longrightarrow 0 < xy)$.

Kratko kažemo da je $\mathbb{Q}$ uređeno polje. Štoviše, kako u skupu $\mathbb{Q}$ vrijedi i

Af $(\forall x \in \mathbb{Q})\,(\forall y \in \mathbb{Q})\,(0 < x \wedge 0 \leq y \longrightarrow (\exists n \in \mathbb{N})\; y \leq nx)$,

to $\mathbb{Q}$ nazivamo *Arhimedovim poljem*.

Općenito, svako polje P koje je uređen skup i u kome vrijede svojstva d) i e) nazivamo *uređenim poljem*.

Ova svojstva racionalnih brojeva i želja da svaki odozgo omeđen rastući niz elemenata iz $\mathbb{Q}$ ima i supremum u $\mathbb{Q}$ vodi na definiciju *skupa realnih brojeva*.

Definicija 5.5.1. *Neka je A podskup uređena skupa S. Kažemo da je skup A omeđen (ograničen) odozgo ako postoji barem jedan element g skupa S (zvan majoranta) takav da je za svaki element x skupa A ispunjeno $x \leq g$.*
Kažemo da je skup A omeđen odozdo ako postoji barem jedan element d skupa S (zvan minoranta) takav da je za svaki element x skupa A ispunjeno $d \leq x$.
Kažemo da je A omeđen skup ako postoje elementi d, g skupa S takvi da je za svaki element x slupa A ispunjeno $d \leq x \leq g$.

Negacijom ovih pojmova dobivamo pojmove *neomeđenih* skupova.

Definicija 5.5.2. *Neka su S_1 i S_2 dva uređena skupa. Za funkciju $f : S_1 \to S_2$ kažemo da je rastuća ako*

$$(\forall x \in S_1)\,(\forall x' \in S_1)\,(x < x' \longrightarrow f(x) \leq f(x'))\,,$$

a da je strogo rastuća ako

$$(\forall x \in S_1)\,(\forall x' \in S_1)\,(x < x' \longrightarrow f(x) < f(x'))\,.$$

Za funkciju $f : S_1 \to S_2$ kažemo da je padajuća ako

$$(\forall x \in S_1)\,(\forall x' \in S_1)\,(x < x' \longrightarrow f(x) \geq f(x'))\,,$$

a da je strogo padajuća ako

$$(\forall x \in S_1)\,(\forall x' \in S_1)\,(x < x' \longrightarrow f(x) > f(x'))\,.$$

Definicija 5.5.3. *Neka su S_1 i S_2 dva uređena skupa. Za funkciju $f : S_1 \to S_2$ kažemo da je monotona ako je rastuća ili padajuća, odnosno da je strogo monotona ako je strogo rastuća ili strogo padajuća.*

Posebno, ako je S_1 skup prirodnih brojeva $\mathbb{N}$ onda umjesto o monotonim funkcijama ovorimo o *monotonim nizovima* elemenata skupa S_2.

Sada možemo dati definiciju skupa realnih brojeva.

Definicija 5.5.4. *Skup $\mathbb{R}$ zove se skup realnih brojeva, a njegovi elementi realni brojevi, ako $\mathbb{R}$ ima sljedeća dva svojstva:*

a) $\mathbb{R}$ *je uređeno polje;*

b) svaki rastući niz elemenata skupa $\mathbb{R}$ koji je odozgo omeđen ima u $\mathbb{R}$ supremum. Pri tome pod supremumom niza $a : \mathbb{N} \to \mathbb{R}$ podrazumijevamo supremum skupa $\{a_n : n \in \mathbb{N}\}$.

Naravno, posebno se u matematici dokazuje da postoji ovakav skup. Sam dokaz se provodi pomoću tzv. *Dedekindovih rezova*, no mi to ovdje preskačemo.

Teorem 5.5.1. *Neka su $x, y, z, x_1, \ldots, x_n, y_1, \ldots, y_n$ realni brojevi. Tada vrijedi:*

1. $(\forall i \in \{1, \ldots, n\})\,(x_i \leq y_i) \longrightarrow x_1 + \cdots + x_n \leq y_1 + \cdots y_n$;
2. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq y \longleftrightarrow (\exists z \in \mathbb{R})\,x + z \leq y + z)\,;$
3. $(\forall x \in \mathbb{R})\,(2x = x \longrightarrow x = 0)\,;$
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. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(\forall z \in \mathbb{R})\,(x \leq y \wedge 0 \leq z \longrightarrow xz \leq yz)\,;$
7. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq 0 \wedge 0 \leq y \longrightarrow xy \leq 0)\,;$

8. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \leq 0 \wedge y \leq 0 \longrightarrow 0 \leq xy)\,;$

9. $(\forall x \in \mathbb{R})\,(x \neq 0 \longrightarrow x^2 > 0)\,;$

10. $(\forall x \in \mathbb{R})\,(x > 0 \longrightarrow x^{-1} > 0)\,;$

11. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(0 < x < y \longleftrightarrow 0 < y^{-1} < x^{-1})\,.$

Dokaz. 1) Iz $x_1 \leq y_1$, $x_2 \leq y_2$ i uređenosti polja $\mathbb{R}$ slijedi

$$x_1 + x_2 \leq y_1 + x_2\ , \quad y_1 + x_2 \leq y_1 + y_2,$$

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 aksiomu (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 opet 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 je po tvrdnji 3 $0 \cdot x = 0$.

5)Pomnožimo li s x jednakost $y + (-y) = 0$ dobijemo

$$x\,[y + (-y)] = x \cdot 0 = 0 \cdot x = 0 = xy + x\,(-y)\,,$$

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) dobijemo

$$x + (-x) \leq y + (-x)\,,$$

tj.

$$0 \leq y + (-x).$$

Za $0 \leq z$ je onda po (Ae)

$$0 \leq z\,(y + (-x)),$$

odnosno

$$xz \leq yz.$$

7) i 8) se dokazuje slično kao prethodno.

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 polaznom pretpostavkom. Dakle, ako je $x \neq 0$, onda 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

$$0 = x^{-1} \cdot 0 < x^{-1}\left(y^{-1}x\right) = y^{-1} < x^{-1} \cdot 1 = x^{-1}.$$

■

5.5.2. Apsolutna vrijednost

Definicija 5.5.5. *Skup* $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\} = \langle 0, +\infty\rangle$ *zove se skup pozitivnih realnih brojeva, a njegove elemente nazivamo pozitivnim realnim brojevima. Skup* $\mathbb{R}_+ \cup \{0\} = \{x \in \mathbb{R} : x \geq 0\} = [0, +\infty\rangle$ *zove se skup svih nenegativnih realnih brojeva.*
Skup $\mathbb{R}_- = \{x \in \mathbb{R} : x < 0\} = \langle -\infty, 0\rangle$ *zove se skup negativnih realnih brojeva, a njegove elemente nazivamo negativnim realnim brojevima.*

Primjedba 5.5.1. *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

$$(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(x \in \mathbb{R}_- \wedge y \in \mathbb{R}_+ \longrightarrow x < y).$$

Definicija 5.5.6. *Funkcija* $|\cdot| : \mathbb{R} \to \mathbb{R}_+ \cup \{0\}$ *zove se apsolutna vrijednost (modul) ako je*

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}.$$

Dakle je za bilo koji $x \in \mathbb{R}$ ispunjeno $|x| = \max\{-x, x\}$. Broj $|x|$ nazivamo apsolutnom vrijednošću broja x. Npr. $|7| = 7,\ |0| = 0$ i $|-3| = 3$.

Teorem 5.5.2. *Vrijedi:*

1. $(\forall x \in \mathbb{R})\,(\forall a \in \mathbb{R}_+)\,(-a \leq x \leq a \longleftrightarrow |x| \leq a)$;
2. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,|x+y| \leq |x| + |y|$, *s tim da će vrijediti jednakost u slučaju* $x, y \neq 0$ *ako i samo ako je za neki* $t > 0$ *ispunjeno* $x = ty$;
3. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,||x| - |y|| \leq |x - y|$;
4. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,|xy| = |x| \cdot |y|$.

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 zbog $a > 0$ sigurno $-a \leq x$, 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 $x \leq 0 \leq |x|$ ispunjeno

$$x + y \leq y \leq y + |x| = |x| + |y|.$$

Nadalje je zbog $-|y| \leq 0 \leq y$

$$x + y \geq x \geq x - |y| = -|x| - |y| = -(|x| + |y|).$$

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 je i

$$|y| - |x| \leq |y - x| = |x - y|\,,$$

pa je

$$-|x - y| \leq |x| - |y| \leq |x - y|\,.$$

opet po prvoj tvrdnji slijedi

$$||x| - |y|| \leq |x - y|\,.$$

4) Sami. ■

Teorem 5.5.3. *Funkcija* $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ *definirana za sve* $x, y \in \mathbb{R}$ *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. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(d(x, y) = 0 \longleftrightarrow x = y)$;
3. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,d(x, y) = d(y, x)$;
4. $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,(\forall z \in \mathbb{R})\,d(x, z) \leq d(x, y) + d(y, z)$.

Dokaz. Sve tvrdnje lako slijede iz svojstava apsolutne vrijednosti. Za vježbu dokaze provedite sami. ■

Definicija 5.5.7. *Funkcija* d *zove se razdaljinska funkcija, a broj* $d(x, y) = |x - y|$ *zove se udaljenost realnih brojeva* x *i* y.

5.5.3. Cijeli i racionalni brojevi u skupu realnih brojeva

Neka je $\mathbb{R}$ skup realnih brojeva i 1 neutralni element za množenje u polju $\mathbb{R}$ (odnosno jedinica). Po Teoremu 5.5.1. iz $1 \neq 0$ slijedi $1^2 = 1 > 0$. No tada je i $1 + 1 = 2 \cdot 1 > 0$ i analogno $n \cdot 1 > 0$ za svaki prirodan broj n.

Neka je funkcija $j : \mathbb{N} \to \mathbb{R}$ za svaki prirodan broj n definirana izrazom

$$j(n) = n \cdot 1.$$

Označimo

$$\mathbb{N}' = j(\mathbb{N}) \subset \mathbb{R}.$$

Funkcija j ima svojstva:

1. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\,j(m + n) = j(m) + j(n)$;
2. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\,j(m \cdot n) = j(m) \cdot j(n)$;
3. $(\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\,(m \leq n \longrightarrow j(m) \leq j(n))$.

Ovo pokazuje da je na $\mathbb{N}'$ definirano zbrajanje, množenje i uređaj u skladu sa zbrajanjem, množenjem i uređajem na skupu prirodnih brojeva $\mathbb{N}$.

U stvari, lako je dokazati da skup $\mathbb{N}'$ zajedno s funkcijom $s : \mathbb{N}' \to \mathbb{N}'$ definiranom sa

$$s(n \cdot 1) = (n+1) \cdot 1$$

zadovoljava sve aksiome skupa prirodnih brojeva. Elementi skupa $\mathbb{N}'$ zovu se *prirodni realni brojevi*, ili jednostavno prirodni brojevi. U daljnjemu ćemo umjesto $\mathbb{N}'$ pisati $\mathbb{N}$ (dakle shvaćamo $\mathbb{N}$ kao podskup skupa $\mathbb{R}$), a umjesto $n \cdot 1$ jednostavno n.

Slično, s $-n$ ćemo označavati broj $n \cdot (-1)$. Skup

$$\mathbb{Z}' = \{0, n \cdot 1, n \cdot (-1) : n \in \mathbb{N}\} \subset \mathbb{R}$$

zove se skup *cijelih realnih brojeva*, ili jednostavno skup cijelih brojeva, a njegove elemente nazivamo *cijelim realnim brojevima*, ili jednostavno cijelim brojevima. I opet ćemo pisati jednostavno $\mathbb{Z}$ umjesto $\mathbb{Z}'$ i $-n$ umjesto $n \cdot (-1)$.

Kada smo u skupu $\mathbb{R}$ pronašli analogone prirodnih i cijelih brojeva, lako napravimo isto i za racionalne brojeve. Naime, za svaki element $a \in \mathbb{R} \setminus \{0\}$ postoji inverzni (*recipročni*) element $a^{-1} \in \mathbb{R}$ kojeg ćemo označiti s

$$a^{-1} = \frac{1}{a}.$$

Sada za $n \in \mathbb{N}$ i $m \in \mathbb{Z}$ realni broj $mn^{-1} \in \mathbb{R}$ označimo kao

$$mn^{-1} = \frac{m}{n}$$

i zovemo *racionalni realni broj* ili jednostavno racionalni broj. Skup

$$\mathbb{Q}' = \left\{ \frac{m}{n} \in \mathbb{R} : n \in \mathbb{N} \wedge m \in \mathbb{Z} \right\} \subset \mathbb{R}$$

zovemo skupom *racionalnih realnih brojeva* i jednostavno ga označavimo s $\mathbb{Q}$.

Teorem 5.5.4. *Skup realnih brojeva $\mathbb{R}$ je Arhimedovo polje.*

Dokaz. Neka su a i b realni brojevi za koje vrijedi $a > 0$ i $b \geq 0$. Označimo

$$A = \{na : n \in \mathbb{N}\} \subset \mathbb{R}.$$

Pretpostavimo da je

$$(\forall x \in A)\, x \leq b,$$

tj. da je b majoranta skupa A. Budući je $a > 0$ $(A4)$ povlači da je $2a = a + a \geq a$, $3a \geq 2a, \ldots, (n+1)\, a \geq na$. Dakle niz $f : \mathbb{N} \to A$ definiran izrazom

$$f(n) = na$$

je rastući i odozgo omeđen niz realnih brojeva. To znači da on ima u $\mathbb{R}$ supremum, tj. postoji

$$M = \sup A \in \mathbb{R}.$$

S druge strane je

$$a + A = \{a + x : x \in A\} \subseteq A,$$

pa je

$$a + M \leq M,$$

iz čega slijedi $a \leq 0$. ovo je u kontradikciji s pretpostavkom $a > 0$, pa b ne može biti majoranta skupa A. Dakle, postoji barem jedan $x \in A$ takav da je $b \leq x$. Drugim riječima, postoji neki $n \in \mathbb{N}$ takav da je

$$b \leq na.$$

Dakle, $\mathbb{R}$ je Arhimedovo polje. ■

Teorem 5.5.5. *Između bilo koja dva različita realna broja postoji barem jedan racionalni broj.*

Dokaz. Neka su $a, b \in \mathbb{R}$ i $a < b$. Uzmimo najprije da je $b > 0$ i stavimo da je $c = b - a$. Jer je $c > 0$, to je i $c^{-1} > 0$. Za realne brojeve 1 i c postoji prirodni broj n takav da je $n \cdot 1 > c^{-1}$ (ako po prethodnom teoremu postoji neki $m \in \mathbb{N}$ takav da je $m \cdot 1 \geq c^{-1}$, onda se lako vidi da postoji i ovakav n). Dakle je

$$c > n^{-1}.$$

Sada analogno postoji prirodni broj k takav da je $b \leq k \cdot n^{-1}$, pa je

$$K = \left\{k \in \mathbb{N} : b \leq k \cdot n^{-1}\right\} \neq \emptyset.$$

Znamo da tada skup K ima najmanji element, neki m. Dakle je

$$\begin{aligned} b &\leq m \cdot n^{-1}, \\ b &> (m-1) \cdot n^{-1}. \end{aligned}$$

Pretpostavka da je

$$a \geq (m-1) \cdot n^{-1}$$

vodi na

$$b \leq m \cdot n^{-1} = [(m-1)+1] \cdot n^{-1} = (m-1) \cdot n^{-1} + n^{-1} \leq a + n^{-1},$$

a to se protivi uvjetu

$$c = b - a > n^{-1}.$$

Prema tome je

$$a < \frac{m-1}{n} < b.$$

U slučaju $b < 0$ imamo $a < b < 0$, pa je $0 < -b < -a$ i po prethodnome

$$-b < \frac{m-1}{n} < -a,$$

iz čega slijedi

$$a < \frac{1-m}{n} < b.$$

Ako je $b = 0$, onda je $b \in \mathbb{Q}$. ■

Teorem 5.5.6. *(G. Cantor, 1874.) Skup* $\Delta_0 = [a, b]$, $a < b$, *svih realnih brojeva između brojeva a i b je neprebrojiv.*

Dokaz. Vidi [4]. ■

Korolar 5.5.1. *Skup* $\mathbb{R}$ *je neprebrojiv.*

Dokaz. Kako je $\Delta_0 = [a, b] \subset \mathbb{R}$ i Δ_0 neprebrojiv, to mora i $\mathbb{R}$ biti takav. ■

Vidjeli smo da se kardinalni broj skupa $\mathbb{N}$ označava s $\aleph_0$. Kardinalni broj skupa $\mathbb{R}$ označava se s c (čitamo *continuum*) a po prethodnom je $\aleph_0 \neq c$.

Korolar 5.5.2. *Postoji barem jedan rastući, odozgo omeđen niz racionalnih brojeva koji u skupu racionalnih brojeva nema supremum.*

Dokaz. Kada ne bi bilo tako, onda bi skup $\mathbb{Q}$ zadovoljavao sve aksiome skupa realnih brojeva, pa bi bio neprebrojiv, a ovo nije moguće jer smo dokazali da je skup $\mathbb{Q}$ prebrojiv. ■

Definicija 5.5.8. *Realni broj koji nije racionalan zove se iracionalan broj.*

Korolar 5.5.3. *Skup svih iracionalnih brojeva je neprebrojiv.*

Dokaz. Unija dvaju prebrojivih skupova je prebrojiv skup, a kako je skup racionalnih brojeva prebrojiv i skup realnih brojeva neprebrojiv, to skup iracionalnih brojeva koji je komplement skupa $\mathbb{Q}$ u $\mathbb{R}$ mora biti neprebrojiv. ■

5.5.4. Binomni teorem

Neka je $n \in \mathbb{N}$. Označit ćemo

$$n! = 1 \cdot 2 \cdot \cdots \cdot n.$$

Posebno se uzima da je $0! = 1$.

Očito je za svaki prirodan broj n ispunjeno

$$(n+1)! = (n+1)\, n!.$$

Dalje ćemo za $n \in \mathbb{N}$ i $k \in \{0, 1, \ldots, n\}$ označiti

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

Broj $\binom{n}{k}$ nazivamo *binomnim koeficijentom*, a zašto vidjet ćemo u narednom teoremu.

Lako se pokaže da vrijedi:

$$\binom{n}{k} = \binom{n}{n-k},$$

$$\binom{n}{0} = \binom{n}{n} = 1,$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Teorem 5.5.7. *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 s 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 $n \in M$. 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 je i $n+1 = s(n) \in M$, pa je po aksiomu indukcije $M = \mathbb{N}$. ■

Primjer 30. *Vrijedi:*

1. $(a+b)^2 = a^2 + 2ab + b^2$;
2. $(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$;
3. $(a+b)^4 = a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4$.

Dakle, binomni koeficijenti su dobili svoje ime zahvaljujući činjenici da se pojavljuju kao koeficijenti prilikom razvoja binoma. Oni se mogu poredati u tzv. *Pascalov trokut.*

Primjedba 5.5.2. *Binomni je teorem važan kod dokazivanja egzistencije supremuma niza $a : \mathbb{N} \to \mathbb{R}$ definiranog izrazom*

$$a(n) = \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k}.$$

Pomoću binomnog teorema se pokaže da je za sve $n \in \mathbb{N}$ ispunjeno

$$2 < a_n < 3,$$

a kako je ovaj niz realnih brojeva očigledno rastući, to on u skupu $\mathbb{R}$ ima supremum. Označimo

$$\begin{aligned} e &= \sup\{a_n : n \in \mathbb{N}\} \\ &= \sup\left\{\left(2 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right) : n \in \mathbb{N}\right\} \\ &= 2,718281828459045\cdots . \end{aligned}$$

Iracionalni broj e zovemo bazom prirodnih ili Neperovih logaritama.

5.6. Skup kompleksnih brojeva

5.6.1. Uvod

Slično kao što smo skupove cijelih i racionalnih brojeva izgradili pomoću prirodnih, tako ćemo sada i skup kompleksnih brojeva izgraditi pomoću skupa realnih brojeva. Osnova za to nam je sljedeći teorem.

Teorem 5.6.1. *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

$$\begin{aligned} & (a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \\ = \; & \left(\frac{a^2}{a^2 + b^2} - \frac{-b^2}{a^2 + b^2}, \frac{-ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2} \right) = (1, 0) \\ = \; & \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \cdot (a, b), \end{aligned}$$

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 ditributivno s obzirom na zbrajanje. ■

Polje $\mathbb{R} \times \mathbb{R}$, u oznaci $\mathbb{C}$, nazivamo *poljem kompleksnih brojeva*, a njegove elemente nazivamo *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 za sve $a \in \mathbb{R}$ sa

$$j(a) = (a, 0)$$

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 ovoga smijemo poistovijetiti skupove $\mathbb{R}$ i $\mathbb{R}'$ i za $a \in \mathbb{R}$ pisati

$$(a, 0) \equiv a,$$

pa skup $\mathbb{R}'$ nazivamo skupom *realnih kompleksnih brojeva*.

No 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

$$i \equiv (0, 1)$$

dobijemo

$$z = a + bi = \mathrm{Re}(z) + \mathrm{Im}(z)\, i.$$

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: da li je uz neku operaciju uređaja skup $\mathbb{C}$ uređeno polje? Naredni teorem to opovrgava.

Teorem 5.6.2. *Na skupu* $\mathbb{C}$ *ne postoji relacija uređaja* $<$ *takva da je* $\mathbb{C}$ *uređeno polje.*

Dokaz. Pretpostavimo da je $\mathbb{C}$ uređeno polje u odnosu na neku relaciju uređaja $<$. 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 sam skup $\mathbb{C}$ izgrađen pomoću skupa $\mathbb{R}$.

Definicija 5.6.1. *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. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$;
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" $|\cdot| : \mathbb{C} \to \mathbb{R}_+ \cup \{0\}$. 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 5.5.3.).

5.6.2. 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 kompleksnoih 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 ne lako zbrajati kompleksne brojeve.

Primjer 31. *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. Polinomi

Ako je S proizvoljan neprazan skup i $f : S \to \mathbb{R}$ funkcija, onda kažemo da je f *realna funkcija*. Ako je još i $S \subset \mathbb{R}$, onda kažemo da je f *realna funkcija realne varijable*. U ovomu poglavlju bavit ćemo se samo realnim funkcijama realne varijable. Među najjednostavnije funkcije te vrste spadaju *polinomi*.

Definicija 6.1.1. *Neka je $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ i neka su $a_0, \ldots, a_n$ realni brojevi. Funkcija $p_n : \mathbb{R} \to \mathbb{R}$ definirana izrazom*

$$p_n(x) = a_0 + a_1 x + \cdots + a_n x^n$$

za sve $x \in \mathbb{R}$ zove se polinom. 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.

Polinom o za koga vrijedi

$$(\forall x \in \mathbb{R})\, o(x) = 0$$

zovemo *nul-polinom* i on je jedini polinom nedefiniranoga stupnja.

Polinom nultoga stupnja je za sve $x \in \mathbb{R}$ definiran izrazom

$$p_0(x) = a_0, \quad a_0 \neq 0.$$

Polinom prvoga stupnja je za sve $x \in \mathbb{R}$ definiran izrazom

$$p_1(x) = a_0 + a_1 x, \quad a_1 \neq 0,$$

a polinom drugoga stupnja izrazom

$$p_2(x) = a_0 + a_1 x + a_2 x^2, \quad a_2 \neq 0.$$

Općenito s $\mathcal{P}_n$ označavamo skup svih polinoma stupnja manjega ili jednakoga n uključujući i nul-polinom, a s $\mathcal{P}$ skup svih polinoma definiranih nad $\mathbb{R}$. Dakle, vrijedi

$$\mathcal{P} = \bigcup_{n \in \mathbb{N}_0} \mathcal{P}_n.$$

Teorem 6.1.1. *Za polinom p_n vrijedi $p_n = o$ ako i samo ako je*

$$a_0 = a_1 = \cdots = a_n = 0.$$

Dokaz. Očito da iz $a_0 = a_1 = \cdots = a_n = 0$ odmah slijedi $p_n = o$. Pretpostavimo stoga da je $p_n = o$, tj. da vrijedi

$$(\forall x \in \mathbb{R})\, p_n(x) = 0.$$

Dokaz ćemo provesti kontradikcijom: pretpostavimo da postoji neki $m \in \{0, 1, \ldots, n\}$ takav da je

$$a_0 = a_1 = \cdots = a_{m-1} = 0 \quad \text{i} \quad a_m \neq 0.$$

Tada je

$$(\forall x \in \mathbb{R})\, q(x) = a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n = 0,$$

iz čega odmah slijedi

$$(\forall x \in \mathbb{R} \setminus \{0\})\, a_m + a_{m+1} x + \cdots + a_n x^{n-m} = 0,$$

odnosno

$$(\forall x \in \mathbb{R} \setminus \{0\})\, a_{m+1} x + \cdots + a_n x^{n-m} = -a_m. \tag{6.1}$$

Stavimo

$$M = \max\{|a_m|, \ldots, |a_n|\}.$$

Svakako je $M > 0$, pa za $x \in \langle 0, 1/2\rangle$ iz (6.1) 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,za $x \in \langle 0, 1/2\rangle$ vrijedi

$$x \geq \frac{|a_m|}{2M}. \tag{6.2}$$

Uzmemo li u (6.2) redom za x brojeve

$$\frac{1}{2^2}, \frac{1}{2^3}, \ldots, \frac{1}{2^k}, \ldots \in \langle 0, 1/2\rangle$$

dobijemo

$$\frac{|a_m|}{2M} \leq \frac{1}{2^k}, \qquad k \in \{2, 3, \ldots\}.$$

Kako je $|a_m|/2M \neq 0$, onda bismo iz činjenice da je $\mathbb{R}$ Arhimedovo polje dobili da za svaki $k \in \{2, 3, \ldots\}$ postoji prirodni broj n_k takav da je

$$n_k \frac{|a_m|}{2M} > 1,$$

pa imamo da je za svaki $k \in \{2,3,\ldots\}$ ispunjeno (koristeći $i \leq 2^i$)

$$1 < n_k \frac{|a_m|}{2M} \leq 2^{n_k} \frac{|a_m|}{2M} \leq 1,$$

odnosno $1 < 1$, što nije moguće. Dakle, mora biti $|a_m|/2M = 0$, iz čega slijedi $a_m = 0$, a ovo je u kontradikciji s početnom pretpostavkom. Dakle, mora biti $a_0 = a_1 = \cdots = a_n = 0$. ■

Korolar 6.1.1. *Dva polinoma*

$$p_n(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0,$$

i

$$q_m(x) = b_0 + b_1 x + \cdots + b_m x^m, \quad b_m \neq 0$$

su jednaka ako i samo ako je $n = m$ i

$$(\forall i \in \{1,\ldots,n\})\, a_i = b_i.$$

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

$$(\forall i \in \{1,\ldots,n\})\, a_i - b_i = 0.$$

■

Definicija 6.1.2. *Zbroj dviju funkcija $f, g : \mathbb{R} \to \mathbb{R}$ je funkcija $f + g : \mathbb{R} \to \mathbb{R}$ takva za sve $x \in \mathbb{R}$ vrijedi*

$$(f+g)(x) = f(x) + g(x).$$

Lako se vidi da je zbrajanje funkcija asocijativno i komutativno, jer je takvo zbrajanje realnih brojeva.

Još ćemo uvesti i sljedeću oznaku: za funkciju $f : \mathbb{R} \to \mathbb{R}$ s $-f$ ćemo označiti funkciju $-f : \mathbb{R} \to \mathbb{R}$ takvu da za sve $x \in \mathbb{R}$ vrijedi

$$(-f)(x) = -f(x).$$

Primjedba 6.1.1. *Uočimo da za svaku funkciju $f : \mathbb{R} \to \mathbb{R}$ vrijedi*

$$f + o = o + f = f,$$

pa je nul-polinom o neutralni element za zbrajanje funkcija. To posebno znači i to da je o neutralni element za zbrajanje polinoma.
Također, za svaku funkciju $f : \mathbb{R} \to \mathbb{R}$ vrijedi

$$f + (-f) = (-f) + f = o,$$

pa svaka funkcija $f : \mathbb{R} \to \mathbb{R}$ ima inverzni element s obzirom na zbrajanje funkcija.

Još ćemo posebno istaknuti tzv, *jediničnu* polinom, tj. polinom $j : \mathbb{R} \to \mathbb{R}$ stupnja nula definiran za sve $x \in \mathbb{R}$ izrazom $j(x) = 1$. On će nam biti važan kada u sljedećem teoremu uvedemo množenje među funkcijama.

Definicija 6.1.3. *Umnožak dviju funkcija $f, g : \mathbb{R} \to \mathbb{R}$ je funkcija $fg : \mathbb{R} \to \mathbb{R}$ takva za sve $x \in \mathbb{R}$ vrijedi*

$$(fg)(x) = f(x)\, g(x).$$

Lako se vidi da je množenje funkcija asocijativno i komutativno, jer je takvo množenje realnih brojeva.

Primjedba 6.1.2. *Uočimo da za svaku funkciju $f : \mathbb{R} \to \mathbb{R}$ vrijedi*

$$fj = jf = f,$$

pa je jedinični polinom neutralni element za množenje funkcija. To posebno znači i to da je j neutralni element za množenje polinoma.

Posebno, pomnožimo li dva polinoma p_n i q_m stupnja n odnosno m, rezultat će biti opet polinom stupnja $n + m$.

Teorem 6.1.2. *Neka je p_m polinom stupnja m. Za svaki polinom P_n stupnja n postoji jedinstveni uređeni par polinoma (q, r) takav da je*

$$P_n = qp_m + r,$$

pri čemu je $\partial r < m$ kad god je $r \neq o$, a $\partial q = n - m$ kad god je $n \geq m$.

Dokaz. Dokaz radi duljine preskačemo. Može se naći u [4]. ■

Definicija 6.1.4. *Neka su sve oznake kao u prethodnom teoremu. Polinom q zovemo kvocijentom, a polinom p_m djeliteljem ili divizorom. Ako je $r = o$ kažemo da je polinom P_n djeljiv s polinomom p_m ili da je p_m njegova mjera. Ako je $r \neq o$ zovemo ga ostatkom pri djeljenju polinoma P_n polinomom p_m.*

Definicija 6.1.5. *Normirani polinom $m(p, q)$ zove se najveća zajednička mjera polinoma $p, q \neq o$ ako on ima ova dva svojstva:*

a) $m(p, q)$ je mjera polinoma p i q;

b) ako r dijeli i p i q, onda r dijeli i $m(p, q)$.

Egzistencija i stvarni postupak za nalaženje takve najveće zajedničke mjere dvaju ne-nul polinoma dobiva se iz tzv. Euklidova algoritma za polinome koji je analogan onomu za prirodne brojeve.

Teorem 6.1.3. *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

$$\partial a < \partial q, \quad \partial b < \partial p.$$

Dokaz. Dokaz se lako provede iz Euklidova algoritma za polinome. ■

Definicija 6.1.6. *Kažemo da su polinomi $p, q \neq o$ relativno prosti ako je $m(p,q) = j$.*

Definicija 6.1.7. *Kažemo da je polinom p ireducibilan nad poljem $\mathbb{R}$ ako $p = qr$ povlači $\partial q = 0$ ili $\partial r = 0$.*

Korištenjem prethodnog teorema lako se pokaže da vrijede sljedeće tvrdnje:

1. Ako je p relativno prost s q i r, onda je relativno prost i s qr;
2. Ako je q djelitelj umnoška pr, te p i q relativno prosti, onda q dijeli r;
3. Ako su relativno prosti polinomi q i r djelitelji polinoma p, onda je i qr djelitelj polinoma p;
4. Svaki polinom p je umnožak ireducibilnih polinoma;
5. Faktorizacija na ireducibilne polinome je jedinstvena do na permutaciju.

Uočimo da nam Tvrdnja 4 ne kaže kojega su stupnja ti ireducibilni faktori. No sada ćemo bez dokaza dati teorem koji nam kazuje da se nad poljem $\mathbb{C}$ (za razliku od polja $\mathbb{R}$) svaki polinom može prikazati kao umnožak ireducibilnih faktora stupnja jedan.

Teorem 6.1.4. *Neka je p polinom n-tog stupnja nad poljem $\mathbb{C}$, $n \in \mathbb{N}$. Tada postoji barem jedna kompleksni broj z_0 takav da je $p(z_0) = 0$. Štoviše, postoje kompleksni brojevi $z_1, \ldots, z_n$ takvi da je*

$$p(z) = a_n (z - z_1) \cdots (z - z_n).$$

Primjer 32. *Npr. polinom p definiran s $p(x) = 1 + x^2$ ireducibilan nad $\mathbb{R}$ i nema nijednu nul-točku. S druge strane je*

$$p(x) = (x - i)(x + i),$$

pa ovaj polinom nad $\mathbb{C}$ ima dvije nul-točke i reducibilan je.

6.2. Racionalne funkcije

Definicija 6.2.1. *Funkcija $Q : S \to \mathbb{R}$ koja je za sve $x \in S$ definirana izrazom*

$$Q(x) = \frac{p_n(x)}{q_m(x)},$$

pri ćemu je

$$S = \{x \in \mathbb{R} : q_m(x) \neq 0\}, \quad p_n, q_m \in \mathcal{P} \quad i \quad q_m \neq o,$$

zove se racionalna funkcija. Racionalna funkcija $Q \neq o$ je u kanonskom obliku ako je $m(p_n, q_m) = j$. Racionalna funkcija Q je prava racionalna funkcija ako je $n < m$.

Podsjetimo se da se može pisati

$$p_n = qq_m + r,$$

pa je

$$Q = \frac{p_n}{q_m} = q + \frac{r}{q_m},$$

pri čemu je r/q_m prava racionalna funkcija. Očito je ovaj prikaz jedinstven.

Definicija 6.2.2. *Pravi razlomak r/q je prost (parcijalni razlomak) ako je $q = p^k$, pri čemu je polinom p ireducibilan nad $\mathbb{R}$ i $\partial r < \partial p$.*

Teorem 6.2.1. *Svaka prava racionalna funkcija $Q = p/q$, $p, q \neq o$, može se na jedinstven način prikazati kao zbroj prostih razlomaka.*

Dokaz. 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] P. Papić, *Uvod u teoriju skupova*, Hrvatsko matematičko društvo, Zagreb, 2000.

[6] M. Vuković, *Matematička logika I*, skripta Matematičkog odjela PMF-a, 2004.