ZVONIMIR BUJANOVIĆ

BORIS MUHA

ELEMENTARNA MATEMATIKA 1

MATEMATIČKI ODSJEK
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
SVEUČILIŠTE U ZAGREBU

Verzija
28/9/2018

Sadržaj

Uvod

Elementarna matematika 1 je obavezan kolegij koji se izvodi u prvom semestru Prediplomskog sveučilišnog studija matematike. Glavni cilj ovog kolegija je "premostiti" prazninu između nivoa srednjoškolske matematike i matematike koje se predaje na sveučilištu. Radi toga smo se, s jedne strane, odlučili na strogo formalan stil izlaganja, a s druge strane, dokazi su u pravilu provedeni tako da uključuju sve detalje. Naime, cilj nam je studente naučiti preciznom matematičkom izražavanju te pokazati na primjerima izgradnju matematičke teorije počevši od aksioma.

Materijali se sastoje od 7 poglavlja. U prvom poglavlju uvodimo logičke veznike i kvantifikatore. Drugo poglavlje bavi se osnovama teorije skupova. Iako je glavni cilj napraviti naivnu teoriju i operativno savladati skupovne operacije, uveden je pojednostavljen sustav pravila izgradnje teorije skupova. Cilj takvog pristupa je ilustrirati kako se formalno može definirati pojam skupa. Treće poglavlje se bavi relacijama i u njemu su dani neki osnovni primjeri relacija koji se često javljaju u raznim matematičkim disciplinama. Skupovi brojeva su uvedeni u četvrtom poglavlju. Najprije se pomoću Peanovih aksioma definiraju prirodni brojevi, a pomoću njih se definiraju cijeli i racionalni brojevi. Realni brojevi su konstruirani pomoću Dedekinovih rezova, ali samo na informativnoj razini. Sljedeće poglavlje bavi se osnovama teorije brojeva. Tako je dokazan osnovni teorem aritmetike, teorem o dijeljenju sa ostatkom i teorem o rješivosti linearnih kongruencija. Osnovni pojmovi vezani za funkcije su tema šestog poglavlja. U tom poglavlju se također uvodi pojam ekvipotentnosti skupa, te prebrojivog i neprebrojivog skupa. Dokazana je prebrojivost skupa racionalnih brojeva, te neprebrojivost skupa realnih brojeva. U zadnjem poglavlju bavimo se polinomima. Polinomi će biti proučavani koristeći algebarski pristup.

Ovi nastavni materijali nastali su na temelju predavanja koje su autori držali akademskih godina 2014/15, 2015/16 i 2016/17, knjiga profesora Pavkovića i Veljana[1,2] (koje preporučujemo studentima kao dodatnu literaturu), te na materijalima koje su nam velikodušno ustupili nastavnici koji su ovaj kolegij predavali prije nas. Jedan od njih bio je i naš dragi prijatelj Ante Mimica, kojemu posvećujemo ovu skriptu.

Zahvaljujemo se profesoru Mladenu Vukoviću na pažljivom čitanju ovih materijala, te brojnim korisnim sugestijama i korekcijama.

[1] Boris Pavković and Darko Veljan. *Elementarna matematika 1*. Tehnička knjiga, 1992

[2] Boris Pavković and Darko Veljan. *Elementarna matematika II: trigonometrija, stereometrija-geometrija prostora, analitička geometrija, elementarna teorija brojeva*. Školska knjiga, 1995

1
Osnove matematičke logike

Svaki suvremeni matematički tekst lako je prepoznati po simbolima i formulama koje koristi. Iako nam se može činiti da su matematičari i znanstvenici oduvijek koristili ovakav zapis, povijest je posve drugačija: na primjer, simbol $+$ za zbrajanje prvi put se pojavio tek u 14. stoljeću, simbol $\leq$ tek u 17. stoljeću, a oznake za uniju i presjek skupova tek pred kraj 19. stoljeća. Umjesto formulama, jednadžbe i identiteti su bili iskazivani opisno, riječima umjesto simbolima. Matematička notacija koju koristimo danas omogućava nam da iskažemo vrlo složene tvrdnje isključivo pomoću simbola. Da bismo ju mogli razumjeti, trebamo prvo savladati standardiziranu osnovnu notaciju koju koriste sve grane matematike, a koja se zasniva na logici sudova i korištenju kvantifikatora.

1.1 Logički veznici

Matematičke tvrdnje koje ćemo proučavati u ovom poglavlju nazivaju se sudovi. SUD je izjavna rečenica za koju se može utvrditi je li istinita ili lažna (neistinita). Sama rečenica može biti zapisana standardnim govornim jezikom ili simbolima. Promotrimo nekoliko primjera.

(a) Izjava "2+2=4" je sud, i to istinit.

(b) Izjava "0 = 1" je sud, i to lažan.

(c) Izjava "Koliko je sati?" nije sud jer to nije izjavna (već upitna) rečenica.

(d) Izjava "x+2 = 8" nije sud jer joj se ne može utvrditi je li istinita ili lažna (ako ne znamo koliki je x).

(e) Izjava "Za sve prirodne brojeve x vrijedi x+2 = 8" je sud, i to lažan.

(f) Izjava "Postoji beskonačno mnogo prostih brojeva" je sud, i to istinit—dokaz ćemo napraviti u Poglavlju 5. Što ako nemamo dokaz tvrdnje, pa ne znamo je li istinita ili lažna? Takve tvrdnje nazivamo HIPOTEZAMA.

(g) Izjava "Broj 0.0001 je malen" nije sud jer pojam "malenog broja" nije dobro definiran.

(h) Izjava "Ova izjava je lažna" nije sud, jer nije niti istinita niti lažna. Naime, kad bi ta izjava bila istinita, onda bi vrijedilo da je "Ova izjava lažna", tj. da nije istinita, a nemoguće je da je istovremeno istinita i nije istinita. Kad bi ta izjava bila lažna, onda ne bi vrijedilo da je "Ova izjava lažna", tj. izjava bi bila istinita, pa ponovno dobivamo da je istovremeno i istinita i nije istinita.

Iako se iz zadnja dva primjera može činiti da je problematično utvrditi što je sud, a što nije, u praksi nas tvrdnje ovog tipa uopće neće zamarati. Za tipične matematičke tvrdnje se vrlo lako može utvrditi jesu li sudovi (odnosno, hipoteze). Ono što će nam često trebati je povezivanje više jednostavnih sudova u složeniji, te utvrđivanje je li taj složeniji sud istinit ili lažan ako znamo istinitost jednostavnih sudova od kojih je sastavljen. Za takvo povezivanje služe nam logički veznici. Da bismo olakšali i skratili zapis prilikom utvrđivanja istinitosti složenih sudova, sudove ćemo umjesto punim rečenicama simbolički označavati velikim slovima. Na primjer,

$$A \equiv \text{“}2+2=4\text{”}, \quad B \equiv \text{“}0<1\text{”}.$$

Oznake $\equiv$ i $=$ naizmjenično ćemo koristiti u daljnjem tekstu kada budemo pridruživali oznake sudovima i kada budemo govorili o jednakosti sudova. Osim $=$ koristimo i $\equiv$ radi lakšeg čitanja, jer se znak $=$ često pojavljuje i u iskazu suda, kao kod "$2+2=4$".

Definicija 1.1. KONJUNKCIJA *sudova A i B je složeni sud koji je istinit točno onda kada su istiniti i sud A i sud B. Konjunkciju označavamo sa $A\&B$ ili $A \wedge B$, te čitamo "A i B".*

U računarstvu se za konjunkciju često koristi još i $A \cdot B$.

Promotrimo dva primjera:

(a) $A \equiv \text{“}3<4\text{”}$, $B \equiv \text{“}4=3+1\text{”}$.
Sud $A \wedge B$ je istinit jer su istiniti i sud A i sud B.

(b) $A \equiv \text{“}2<1\text{”}$, $B \equiv \text{“}4\cdot 3=12\text{”}$.
Sud $A \wedge B$ je lažan jer je sud A lažan (iako je B istinit).

Definicija 1.2. DISJUNKCIJA *sudova A i B je složeni sud koji je lažan samo onda kada su lažni i sud A i sud B. Disjunkciju označavamo sa $A \vee B$, te čitamo "A ili B".*

U računarstvu se za disjunkciju često koriste još i $A + B$ te $A|B$.

Promotrimo ponovno prethodna dva primjera:

(a) $A \equiv \text{“}3<4\text{”}$, $B \equiv \text{“}4=3+1\text{”}$.
Sud $A \vee B$ je istinit jer su istiniti i sud A i sud B.

(b) $A \equiv \text{“}2<1\text{”}$, $B \equiv \text{“}4\cdot 3=12\text{”}$.
Sud $A \vee B$ je istinit jer je sud B istinit (iako je A lažan).

Definicija 1.3. IMPLIKACIJA *sudova A i B je složeni sud koji je lažan samo onda kada je A istinit, a B lažan. Implikaciju označavamo sa $A \Rightarrow B$, te čitamo "A povlači B" ili "A implicira B" ili "Ako A, onda B" ili "Iz A slijedi B" ili "B je* NUŽAN UVJET *za A" ili "A je* DOVOLJAN UVJET *za B".*

Pravilo za implikaciju lakše pamtimo ovako: "Iz istine ne može slijediti laž".

Promotrimo ponovno prethodna dva primjera:

(a) $A \equiv$ "$3 < 4$", $B \equiv$ "$4 = 3 + 1$".
Sud $A \Rightarrow B$ je istinit, kao i sud $B \Rightarrow A$.

(b) $A \equiv$ "$2 < 1$", $B \equiv$ "$4 \cdot 3 = 12$".
Sud $A \Rightarrow B$ je istinit, a sud $B \Rightarrow A$ lažan.

Definicija 1.4. EKVIVALENCIJA *sudova A i B je složeni sud koji je istinit kada su i sud A i sud B oba istiniti, te kada su i sud A i sud B oba lažni. Ekvivalenciju označavamo sa $A \Leftrightarrow B$, te čitamo "A je ekvivalentno sa B" ili "A vrijedi ako i samo ako vrijedi B" (kraće "A vrijedi akko vrijedi B") ili "A je* NUŽAN I DOVOLJAN UVJET *za B".*

Promotrimo prethodna dva primjera, uz još jedan dodatni:

(a) $A \equiv$ "$3 < 4$", $B \equiv$ "$4 = 3 + 1$".
Sud $A \Leftrightarrow B$ je istinit, kao i sud $B \Leftrightarrow A$.

(b) $A \equiv$ "$2 < 1$", $B \equiv$ "$4 \cdot 3 = 12$".
Sud $A \Leftrightarrow B$ je lažan, kao i sud $B \Leftrightarrow A$.

(c) $A \equiv$ "$7 < 4$", $B \equiv$ "Broj 6 je prost".
Sud $A \Leftrightarrow B$ je istinit, kao i sud $B \Leftrightarrow A$.

Definicija 1.5. NEGACIJA *suda A je sud koji je istinit samo onda kada je sud A lažan. Negaciju označavamo sa $\neg A$, te čitamo "nije A" ili "ne A" ili "non A".*

Vrlo je važno naučiti negirati složene sudove. Promotrimo za početak nekoliko primjera; kasnije ćemo razviti mehanizam kako to raditi gotovo automatski:

(a) $A \equiv$ "$3 < 4$". Tada $\neg A \equiv$ "$3 \geq 4$".

(b) $A \equiv$ "Svaka kuća ima krov". Tada $\neg A \equiv$ "Postoji kuća bez krova".

(c) $A \equiv$"Postoji stolac s dvije noge". Tada $\neg A \equiv$"Ne postoji stolac s dvije noge" ili, manje u duhu hrvatskog jezika, a bliže matematičkoj terminologiji, $\neg A \equiv$"Svaki stolac ima broj nogu različit od dva".

Logičke veznike možemo kombinirati i tako dobiti još složenije sudove, na primjer:

$$C \equiv \neg((A \wedge B) \vee ((\neg A) \Rightarrow B)).$$

Kao i kod aritmetičkih operacija, zagradama označavamo redoslijed primjenjivanja logičkih veznika. Također, kao što operacija množenja ima veći prioritet od operacije zbrajanja, pa možemo pisati $2 + 3 \cdot 5$ umjesto $2 + (3 \cdot 5)$, tako uvodimo i prioritet logičkih veznika:

1. Najviši prioritet ima logički veznik $\neg$.
2. Srednji prioritet ima logički veznik $\wedge$.
3. Najniži prioritet imaju logički veznici $\vee$, $\Rightarrow$ i $\Leftrightarrow$. Ta tri veznika imaju jednak prioritet.

U matematičkoj logici obično se definira da veznici $\wedge$ i $\vee$ imaju isti prioritet. Mi ćemo u ovoj skripti ipak koristiti prioritete kako su navedeni u glavnom tekstu, prvenstveno zbog analogije s aritmetikom koja se koristi u računarstvu, kao i načina kako su prioriteti definirani u kolegiju Programiranje 1.

Koristeći ovako postavljene prioritete, u gornjoj formuli možemo ispustiti neke zagrade bez da joj promijenimo smisao:

$$C \equiv \neg(A \wedge B \ \vee \ (\neg A \Rightarrow B)).$$

Uočite da zagradu oko implikacije ne možemo ispustiti bez da promijenimo smisao formule jer $\vee$ i $\Rightarrow$ imaju isti prioritet. Ako imamo dvojbu oko prioriteta ili želimo otkloniti sumnju oko redoslijeda izračunavanja, bolje je ostaviti dodatne zagrade.

Tu je situacija slična kao u izrazu $2-(3+5)$, koji nema istu vrijednost kao $2-3+5$ iako $+$ i $-$ imaju isti prioritet. Ako dvije operacije ili veznika imaju isti prioritet, rezultat se izračunava s lijeva na desno.

Ako želimo utvrditi istinitost složenog suda u ovisnosti o istinitosti sudova od kojih je sastavljen, onda koristimo TABLICE ISTINITOSTI. U toj tablici sa 0 označavamo laž, a sa 1 istinu. Za sve moguće kombinacije istinitosti sudova koji čine složeni sud, ispisujemo istinitost složenog suda. Prema definicijama logičkih veznika, njihove tablice istinitosti izgledaju ovako:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\neg A$
0	0	0	0	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	0	0
1	1	1	1	1	1	0

Definicija 1.6. *Kažemo da je složeni sud A* TAUTOLOGIJA *ako se njegov pripadni stupac u tablici istinitosti sastoji isključivo od oznaka* 1.

Definicija 1.7. *Kažemo da su složeni sudovi A i B* (SEMANTIČKI) JEDNAKI *ako i samo ako je sud $A \Leftrightarrow B$ tautologija. Tada pišemo $A \equiv B$.*

Uočimo da vrijedi $A \equiv B$ ako i samo ako sudovi A i B imaju identične tablice istinitosti.

Propozicija 1.8. *Neka su A i B sudovi. Tada vrijedi:*

(a) $\neg(\neg A) \equiv A$;

(b) $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$;

(c) $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$;

(d) $A \Rightarrow B \equiv \neg A \vee B$.

(e) $\neg(A \Rightarrow B) \equiv A \wedge \neg B$.

Tvrdnje (b) i (c) zovemo De Morganovi zakoni.

Dokaz. Dovoljno je napraviti tablice istinitosti za formule s lijeve i desne strane jednakosti i uvjeriti se da se pripadni stupci podudaraju. Pokažimo tvrdnje (a) i (b).

(a)

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

Prvi i treći stupac se podudaraju, pa vrijedi $A \equiv \neg(\neg A)$.

(b)

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Četvrti i posljednji stupac se podudaraju, pa vrijedi $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$.

□

Koristeći tablice istinitosti, možemo dokazati mnogo jednakosti koje će nam biti korisne za transformiranje složenih sudova u oblik koji je pogodniji za ispitivanje njihove istinitosti. Neke od tih jednakosti navedene su u sljedećoj propoziciji.

Propozicija 1.9. *Neka su A i B sudovi. Tada vrijedi:*

(a) $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$;

(b) $A \wedge B \equiv B \wedge A$; $\quad A \vee B \equiv B \vee A$;

(c) $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$; $\quad (A \vee B) \vee C \equiv A \vee (B \vee C)$;

(d) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$;

(e) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$;

(f) $A \vee 0 \equiv A$; $\quad A \wedge 1 \equiv A$;

(g) $A \wedge \neg A \equiv 0$; $\quad A \vee \neg A \equiv 1$.

Uočimo da logički veznici $\wedge$ i $\vee$ imaju mnoga svojstva koja imaju i aritmetičke operacije zbrajanja i množenja: uvjerite se u to tako da zamijenite $\wedge$ operacijom množenja, a $\vee$ operacijom zbrajanje. Svojstvo (b) nazivamo komutativnost, (c) asocijativnost, (d) i (e) distributivnost.

Dokaz. Dokaz svih tvrdnji se provodi pisanjem tablice istinitosti i u uspoređivanjem odgovarajućih stupaca. To ćemo napraviti za tvrdnju (a), dok ostale ostavljamo za vježbu.

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Usporedbom trećeg i posljednjeg stupca, vidimo da vrijedi $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$. □

Uz jednakosti navedene u prethodne dvije propozicije, više nije nužno uvijek pisati tablice istinitosti da bismo pokazali jednakost dvaju sudova. Na primjer:

$$\begin{aligned}(A \vee B) \vee (\neg A \wedge \neg B) &\equiv (A \vee B) \vee \neg(A \vee B) \\ &\equiv 1. \end{aligned} \tag{1.1}$$

Ovdje smo u prvom retku iskoristili De Morganov zakon, a u drugom Propoziciju 1.9(g). Iz jednakosti (1.1) zaključujemo da će tablica

istinitosti za sud $(A \vee B) \vee (\neg A \wedge \neg B)$ u svim recima sadržavati samo "jedinice", to jest, taj sud je tautologija!

Tako su, na primjer, sudovi $A \vee \neg A$, $(A \wedge B) \Rightarrow B$ i $(A \vee B) \vee (\neg A \wedge \neg B)$ tautologije, dok $\neg(A \wedge B)$ nije tautologija. Dokažite ove tvrdnje tako da napravite tablice istinitosti za navedene sudove!

Brojne matematičke tvrdnje imaju oblik implikacije, tj. $A \Rightarrow B$. Kada imamo sud tog oblika, često će nam biti korisne i varijante navedene u sljedećoj definiciji.

Definicija 1.10. *Neka je $A \Rightarrow B$ sud. Tada kažemo:*

(a) Sud $B \Rightarrow A$ je OBRAT *suda $A \Rightarrow B$;*

(b) Sud $\neg B \Rightarrow \neg A$ je OBRAT PO KONTRAPOZICIJI *suda $A \Rightarrow B$;*

(c) Sud $\neg A \Rightarrow \neg B$ je SUPROTNI SUD *od $A \Rightarrow B$.*

Promotrimo tablicu istinitosti za navedene sudove.

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

Primjećujemo da vrijede sljedeće važne (ne)jednakosti:

(a) $A \Rightarrow B \;\equiv\; \neg B \Rightarrow \neg A$;

(b) $A \Rightarrow B \;\not\equiv\; B \Rightarrow A$;

(c) $A \Rightarrow B \;\not\equiv\; \neg A \Rightarrow \neg B$;

(d) $B \Rightarrow A \;\equiv\; \neg A \Rightarrow \neg B$.

Drugim riječima, ako je tvrdnja $A \Rightarrow B$ istinita, onda je istinita i tvrdnja $\neg B \Rightarrow \neg A$ i obratno. Stoga: ako želimo dokazati da tvrdnja A povlači tvrdnju B, ponekad je jednostavnije dokazati da tvrdnja $\neg B$ povlači tvrdnju $\neg A$. Taj dokaz će biti posve ispravan kao dokaz tvrdnje $A \Rightarrow B$, te ga nazivamo dokaz obratom po kontrapoziciji. Primjere ćemo vidjeti u Poglavlju 1.3. Za sada, napišimo nekoliko implikacija, te njihovih obrata i obrata po kontrapoziciji.

Primjer 1.11. *Promotrimo sljedeće sudove.*

(a) "Ako je α obodni kut nad promjerom kružnice k, onda je α pravi kut."
Ovaj sud, oblika $A \Rightarrow B$, je istinit.
Njegov obrat $B \Rightarrow A$ glasi ovako: "Ako je α pravi kut, onda je α obodni kut nad promjerom kružnice k." Obrat nije (uvijek) istinit, pravi kut možemo nacrtati i izvan kružnice k.
Obrat po kontrapoziciji, $\neg B \Rightarrow \neg A$, glasi ovako: "Ako α nije pravi kut, onda α nije obodni kut nad promjerom kružnice k." Ovaj sud je također istinit.

(b) "Ako je $x > 0$ i $y > 0$, onda je $x \cdot y > 0$." Ovaj sud, oblika $(A \wedge B) \Rightarrow C$, je istinit.
Njegov obrat $C \Rightarrow (A \wedge B)$ glasi ovako: "Ako je $x \cdot y > 0$, onda je $x > 0$ i $y > 0$." Obrat nije istinit, na primjer za $x = -2$ i $y = -5$ je $x \cdot y > 0$, ali nije istina da je $x > 0$ i $y > 0$.
Obrat po kontrapoziciji ima oblik $\neg C \Rightarrow \neg(A \wedge B)$, što korištenjem De Morganovog pravila možemo zapisati i kao $\neg C \Rightarrow (\neg A \vee \neg B)$. Zapisano riječima, glasi ovako: "Ako vrijedi $x \cdot y \leq 0$, onda vrijedi $x \leq 0$ ili $y \leq 0$." Ovaj sud je također istinit.
Suprotni sud ima oblik $\neg(A \wedge B) \Rightarrow \neg C$, odnosno, $(\neg A \vee \neg B) \Rightarrow \neg C$. Zapisano riječima: "Ako vrijedi $x \leq 0$ ili $y \leq 0$, onda vrijedi $x \cdot y \leq 0$." Ovaj sud ponovno nije istinit, na primjer za $x = -2$ i $y = -5$.

Formalno gledajući, ovo nije sud jer ne znamo vrijednosti od x i y. U ovom primjeru zapravo podrazumijevamo da piše: "Za sve realne brojeve x, y, vrijedi: ako je $x > 0$ i $y > 0$, onda je $x \cdot y > 0$".

1.2 *Predikati i kvantifikatori*

Kako smo naveli na početku prethodne cjeline, izjavu "$x + 2 = 8$" ne smatramo sudom jer joj ne možemo utvrditi istinitost budući da ne znamo vrijednost od x. Međutim, uvrstimo li bilo koju vrijednost umjesto x, dobivamo sud. Drugim riječima, promotrimo "funkciju"

$$P(x) \equiv \text{"}x + 2 = 8\text{"}.$$

Tada je, na primjer, $P(6) \equiv$ "$6 + 2 = 8$" istinit sud, a $P(3) \equiv$ "$3 + 2 = 8$" lažan sud. Kažemo da je $P(x)$ primjer jednomjesnog PREDIKATA.

Slično, ako istinitost neke izjave ovisi o dvije varijable, govorimo o dvomjesnim predikatima. Na primjer, ako označimo

$$Q(x, y) \equiv \text{"Prirodni broj } x \text{ je djeljiv prirodnim brojem } y\text{"},$$

onda je $Q(12, 3)$ istinit sud, a $Q(5, 7)$ lažan sud. Dakle, $Q(x, y)$ je primjer dvomjesnog predikata. Općenito, *n*-MJESNI PREDIKAT je izjavna rečenica koja sadrži n varijabli, te koja postaje sud nakon uvrštavanja konkretnih vrijednosti umjesto tih varijabli.

Osim uvrštavanjem konkretnih vrijednosti na mjesto varijabli, postoji još jedan način kako od predikata možemo napraviti sudove: pomoću tzv. *kvantifikatora*.

Definicija 1.12. *Neka je $P(x)$ predikat. Sud*

$$(\forall x)\ P(x)$$

je istinita točno onda kada je $P(x)$ istiniti sud za sve vrijednosti varijable x. Čitamo: "Za svaki x, vrijedi $P(x)$", a oznaku $\forall$ zovemo UNIVERZALNI KVANTIFIKATOR.

Nadalje, sud

$$(\exists x)\ P(x)$$

je istinita točno onda kada postoji barem jedna vrijednost varijable x za koju je sud $P(x)$ istinit. Čitamo: "Postoji x za koji vrijedi $P(x)$", a oznaku $\exists$ zovemo EGZISTENCIJALNI KVANTIFIKATOR.

Iz kojeg skupa dolaze varijable x u gornjoj definiciji? To će ili biti jasno iz konteksta ili će biti eksplicitno navedeno unutar predikata $P(x)$. Pogledajmo jedan primjer.

Primjer 1.13. *Pretpostavimo da je varijabla x realan broj.*

(a) Sud $(\forall x)\ x \geq 3$ *je lažan, jer predikat* $P(x) \equiv x \geq 3$ *nije istinit, na primjer, za* $x = -5$.

(b) Sud $(\exists x)\ x \geq 3$ *je istinit, jer je predikat* $P(x) \equiv x \geq 3$ *istinit, na primjer, za* $x = 5$.

(c) Sud $(\forall x)\ (x > -1 \Rightarrow x^2 > 1)$ *je lažan, jer predikat* $P(x) \equiv (x > -1 \Rightarrow x^2 > 1)$ *nije istinit, na primjer, za* $x = 0$.

(d) Sud $(\exists x)\ x^2 = -1$ *je lažan.*

Ako unutar samog suda želimo eksplicitno navesti iz kojeg skupa dolaze dozvoljene varijable, to možemo napraviti ovako:

$$(\forall x)\ (x \in \mathbb{R} \Rightarrow x \geq 3),$$

u slučaju univerzalnog kvantifikatora, odnosno,

$$(\exists x)\ (x \in \mathbb{R} \wedge x \geq 3),$$

u slučaju egzistencijalnog kvantifikatora. Ovakve zapise često skraćujemo na sljedeći način:

$$(\forall x)\ (x \in S \Rightarrow P(x)) \text{ kraće zapisujemo kao } (\forall x \in S)\ P(x);$$
$$(\exists x)\ (x \in S \wedge P(x)) \text{ kraće zapisujemo kao } (\exists x \in S)\ P(x).$$

Tako je, na primjer, sud

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

istinit, a sud

$$(\exists x \in \mathbb{Q})\ x^2 = 2$$

lažan.

Ako želimo izjaviti da postoji točno jedna vrijednost varijable za koju je sud istinit (a ne više njih!), onda koristimo KVANTIFIKATOR JEDINSTVENE EGZISTENCIJE, u oznaci $\exists!$. Na primjer,

$$(\exists! x \in \mathbb{R})\ x^2 = 2 \text{ je lažan sud,}$$
$$(\exists! x \in \langle 0, +\infty \rangle)\ x^2 = 2 \text{ je istinit sud,}$$
$$(\exists! x \in \mathbb{R})\ x^2 = -1 \text{ je lažan sud.}$$

Uočite da kvantifikator jedinstvene egzistencije možemo zapisati pomoću univerzalnog i egzistencijalnog kvantifikatora:

$$(\exists! x)\ P(x) \ \equiv\ (\exists x)\big(P(x)\ \wedge\ ((\forall y)\ (P(y) \Rightarrow x = y))\big).$$

Kvantifikatore možemo i ulančavati, pa bismo tako tvrdnju

$$(\forall x)(\exists y)\ P(x, y)$$

čitali "Za svaki x, postoji y takav da vrijedi $P(x, y)$".

Primjer 1.14.

(a) Sud $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\ x + 17 = y$ *je istinit.*

(b) Sud $(\forall x \in \mathbb{R})(\exists y \in R)\ x \cdot y > 0$ *je lažan.*

(c) Sud $(\exists x \in \mathbb{R})(\forall y \in R)\ x \cdot y > 0$ *je lažan.*

(d) Sud $(\exists x \in \mathbb{R})(\exists y \in R)\ x \cdot y > 0$ *je istinit.*

Često prilikom dokazivanja tvrdnji trebamo napraviti negaciju nekog suda koji sadrži kvantifikatore. U tu svrhu će nam poslužiti sljedeća pravila:

$$\neg((\forall x)\ P(x)) \ \equiv\ (\exists x)\ \neg P(x);$$
$$\neg((\exists x)\ P(x)) \ \equiv\ (\forall x)\ \neg P(x).$$

Uvjerimo se da je prvo pravilo ispravno: po definiciji negacije, sud $\neg((\forall x)\ P(x))$ je istinit ako i samo ako je sud $(\forall x)\ P(x)$ lažan. Po definiciji univerzalnog kvantifikatora, taj sud je lažan ako i samo ako sud $P(x)$ nije istinit za sve vrijednosti varijable x. Dakle, $\neg((\forall x)\ P(x))$ je istinit ako i samo ako postoji neka vrijednost varijable x za koju $P(x)$ nije istinit, odnosno, ako i samo ako postoji neka vrijednost varijable x takva da vrijedi $\neg P(x)$. Po definiciji egzistencijalnog kvantifikatora, to je ako i samo ako $(\exists x)\ P(x)$.

Primjer 1.15. *Promotrimo sada nekoliko primjera sudova koji uključuju kvantifikatore, te napišimo njihove negacije koristeći gornja pravila.*

(a) $A \equiv (\forall x \in \mathbb{R})\ x^2 > x + 2$
$\neg A \equiv (\exists x \in \mathbb{R})\ \neg(x^2 > x + 2) \equiv (\exists x \in \mathbb{R})\ x^2 \leq x + 2$

(b) $A \equiv (\exists x \in \mathbb{Q})\ x^3 = 8$
$\neg A \equiv (\forall x \in \mathbb{Q})\ \neg(x^3 = 8) \equiv (\forall x \in \mathbb{Q})\ x^3 \neq 8$

(c) $A \equiv (\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\ x^2 + y^2 \geq 0$
$\neg A \equiv (\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\ x^2 + y^2 < 0$

(d) $A \equiv$ *"Svaka kuća je bijela."*
Tvrdnju je puno lakše ispravno negirati ako ju zapišemo simbolima, te primijenimo pravila za negaciju. Neka je S skup svih kuća, a $P(K) \equiv$ "Kuća K je bijela" predikat. Tada $A \equiv (\forall K \in S)\ P(K)$, pa je $\neg A \equiv (\exists K \in S)\ \neg P(K)$. Kada pročitamo zapis suda $\neg A$, dobivamo $\neg A \equiv$ "Postoji kuća koja nije bijela".

(e) $A \equiv$ *"Postoji crna ovca."*
Ponovno zapisujemo sud pomoću simbola: neka je S skup svih ovaca, a $P(o) \equiv$ "Ovca o ima crnu boju". Tada $A \equiv (\exists o \in S)\ P(o)$, pa je $\neg A \equiv (\forall o \in S)\ \neg P(o)$, odnosno, $\neg A \equiv$ "Svaka ovca ima boju koja je različita od crne".

Ako bismo ovdje uzeli $P(o) \equiv$ "Ovca o je crna", onda bi nas doslovno čitanje suda $\neg A$ moglo navesti na izjavu $\neg A \equiv$ "Svaka ovca nije crna". Ovu bismo tvrdnju, zbog nepreciznosti govornog jezika, mogli shvatiti na dva načina: "Nijedna ovca nije crna" (što je ispravna negacija tvrdnje A) ili "Nisu sve ovce crne" (što je pogrešna negacija tvrdnje A jer zapravo znači "Postoji ovca koja nije crna", te dozvoljava da neke ovce imaju crnu boju). Jedan ispravan način čitanja bi bio $\neg A \equiv$ "Za svaku ovcu vrijedi da nije crna".

(f) $A \equiv (\forall x)(\forall y)\ (P(x,y) \Rightarrow Q(x,y))$.
Ovdje primjenjujemo pravilo za negiranje implikacije, dokazano u Propoziciji 1.8(e):

$$\begin{aligned}\neg A &\equiv (\exists x)(\exists y)\ \neg(P(x,y) \Rightarrow Q(x,y)) \\ &\equiv (\exists x)(\exists y)\ (P(x,y) \wedge \neg Q(x,y)).\end{aligned}$$

(g) Ako je f funkcija, onda je sud A istinit ako i samo ako je f injekcija:

$$A \equiv (\forall x \in S)(\forall y \in S)\ (x \neq y \Rightarrow f(x) \neq f(y)).$$

Negacija će biti istinita kada funkcija f nije injekcija:

$$\neg A \equiv (\exists x \in S)(\exists y \in S)\ (x \neq y \wedge f(x) = f(y)).$$

Korištenjem obrata po kontrapoziciji, dobivamo sljedeći zapis suda A:

$$A \equiv (\forall x \in S)(\forall y \in S)\ (f(x) = f(y) \Rightarrow x = y).$$

Ovaj zapis često koristimo kada želimo dokazati da je f injekcija, o čemu će biti više riječi u Poglavlju 6.

(h) Sud A je istinit ako je niz $(a_n)_n$ ima limes, tj. ako je konvergentan:

$$A \equiv (\exists L \in \mathbb{R})(\forall \varepsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})\ (n \geq n_0 \Rightarrow |a_n - L| < \varepsilon).$$

Negacija će biti istinita kada niz $(a_n)_n$ nema limes:

$$\neg A \equiv (\forall L \in \mathbb{R})(\exists \varepsilon > 0)(\forall n_0 \in \mathbb{N})(\exists n \in \mathbb{N})\ (n \geq n_0 \wedge |a_n - L| \geq \varepsilon).$$

(i) Negirajmo još i kvantifikator jedinstvene egzistencije:

$$A \equiv (\exists! x)\ P(x) \equiv (\exists x)\ \big(P(x) \wedge ((\forall y)\ P(y) \Rightarrow x = y)\big);$$
$$\neg A \equiv (\forall x)\ \big(\neg P(x)\ \vee\ ((\exists y)\ P(y) \wedge x \neq y)\big).$$

1.3 *Vrste matematičkih tvrdnji*

U svakoj matematičkoj teoriji pojavljuju se slični tipovi tvrdnji. Neke tvrdnje predstavljaju osnovne činjenice na kojima se bazira cijela teorija, nekim tvrdnjama se uvode novi pojmovi na temelju već postojećih pojmova kako bi se pojednostavnila terminologija teorije, a nekim tvrdnje predstavljaju činjenice koje je potrebno dokazati. Krenimo redom.

AKSIOM je tvrdnja koja se smatra istinitom i koja se ne dokazuje. Na primjer, tvrdnja "1 je prirodan broj" je jedan od Peanovih aksioma kojima se uvodi skup prirodnih brojeva. Tu činjenicu prihvaćamo kao istinitu, nju ne dokazujemo, te pomoću nje dokazujemo druge tvrdnje o prirodnim brojevima. Slično, postoje aksiomi kojima se uvodi pojam geometrije euklidske ravnine. Jedan od tih aksioma je tzv. aksiom o paralelama, odnosno, "Euklidov peti postulat" koji glasi: "Ako je T točka koja ne leži na pravcu p, onda postoji jedinstveni pravac q koji prolazi točkom T, a ne siječe pravac q".

Svaka matematička teorija sadrži skup aksioma na kojima se ona zasniva. Počevši od skupa aksioma, logičkim zaključivanjem zatim dokazujemo sve složenije i složenije tvrdnje. Svaka dokazana tvrdnja, koliko god bila netrivijalna, u konačnici mora slijediti iz aksioma i mora se moći svesti na njih. Stoga je vrlo važno ispravno odabrati aksiome teorije, te želimo da oni imaju sljedeća svojstva:

1. Skup aksioma treba biti *konzistentan*, tj. ne smije se dogoditi da pomoću njih možemo dokazati da je istinit i sud A i sud $\neg A$.
2. Skup aksioma treba biti *potpun*, tj. za svaku tvrdnju A teorije trebamo, koristeći aksiome, biti u stanju dokazati da je A istina ili da je $\neg A$ istina.

Kurt Gödel (1906.–1978.), austrijski i američki matematičar i logičar

S druge strane, Kurt Gödel je 1931. dokazao da svaki konzistentni skup aksioma u kojem se mogu provesti elementarne aritmetičke operacije ne može biti potpun, tj. postoje tvrdnje koje se neće moći niti dokazati niti opovrgnuti koristeći aksiome! Više o ovoj problematici možete doznati na kolegiju "Matematička logika", koji je izborni kolegij na trećoj godini preddiplomskog studija. Također, preporučamo knjigu Apostolos Doxiadis: "*Stric Petros i Goldbachova slutnja*".

3. Skup aksioma treba biti *nezavisan*, tj. ne smije se dogoditi da jedan aksiom možemo dokazati pomoću preostalih.

Drugi tip matematičkih tvrdnji su definicije. DEFINICIJA je izjava kojom se na jednoznačan način, nabrajanjem njegovih nužnih i dovoljnih svojstava, opisuje neki matematički pojam. Već u ovom poglavlju smo se susreli s definicijama—definirali smo, primjerice, logičke veznike. Uloga definicija je, zapravo, da pojednostave terminologiju teorije: umjesto da svaki puta kažemo "Promotrimo sud koji je istinit točno onda kada su istiniti i sud A i sud B", jednostavno ćemo reći "Promotrimo konjunkciju sudova A i B" ili "Promotrimo sud $A \wedge B$".

Jedan te isti pojam možemo definirati na više načina. Na primjer, ako su nam poznati pojmovi pravokutnika i romba, te ako želimo uvesti pojam kvadrata, to možemo napraviti na neki od sljedećih načina:

(a) Pravokutnik kojemu susjedne stranice imaju jednaku duljinu nazivamo KVADRAT.

(b) Kažemo da je pravokutnik KVADRAT ukoliko su mu dijagonale međusobno okomite.

(c) KVADRAT je romb kojemu je kut između susjednih stranica pravi.

Svaka od ovih definicija kvadrata je ispravna. Kada uvodimo pojam kvadrata, odlučit ćemo se za jednu (bilo koju) od gornje tri definicije. Preostale dvije definicije tada postaju tvrdnje koje je potrebno dokazati—one više neće biti definicije, nego tzv. KARAKTERIZACIJE pojma kvadrat.

Kada definiramo novi pojam, potrebno je obratiti pažnju da ne napravimo neku od tipičnih pogreška:

1. Definicija treba obuhvaćati točno onaj pojam koji želimo definirati, a ne i neke druge pojmove.
   Na primjer, pogrešna je definicija: "Kažemo da su dva pravca u prostoru PARALELNI, ako se ne sijeku i ne podudaraju." Ova "definicija" obuhvaća i mimoilazne pravce u prostoru, a ne samo one koje želimo nazvati paralelnima.

2. Definicija treba navesti minimalan broj svojstava kojima je novi pojam u potpunosti opisan.
   Na primjer, pogrešna je definicija: "JEDNAKOSTRANIČNI TROKUT je trokut kojem su sve tri stranice jednake i sva tri kuta jednaka". Naime, jednakostranični trokut možemo definirati kao trokut kojemu su sve tri stranice jednake, a zatim pomoću toga *dokazati* da su mu i sva tri kuta jednaka.

3. Definicija ne smije biti cirkularna, tj. ne smije uvoditi novi pojam pomoću njega samog.
   Na primjer, pogrešna je definicija: "KRUŽNICA je skup svih točaka ravnine koje su jednako udaljene od središta kružnice". Ispravno bi bilo reći: "Zadana je točka T. Kružnica sa središtem u točki T je skup svih točaka ravnine koje su jednako udaljene od točke T".

Posljednju grupu matematičkih tvrdnji čine teoremi, propozicije, leme i korolari—to su matematičke tvrdnje čiju istinitost je potrebno utvrditi dokazom, tj. logičkim zaključivanjem iz aksioma i već ranije dokazanih tvrdnji. TEOREM obično označava važan i netrivijalan matematički sud, koji predstavlja značajan i istaknuti rezultat neke matematičke teorije. PROPOZICIJA je matematički sud nešto manje važnosti. LEMA je pomoćna tvrdnja koja se koristi da bi se dokazao neki složeniji teorem. KOROLAR je tvrdnja koja slijedi jednostavnim zaključivanjem kao direktna posljedica nekog teorema ili propozicije.

Sve ove vrste tvrdnji možemo zajednički obuhvatiti pojmom "teorem". Teoremi tipično imaju oblik implikacije $P \Rightarrow Q$, a kada izričemo neki teorem, potrebno je vrlo jasno razlučiti i navesti:

1. Što je PRETPOSTAVKA teorema: sud P koji se smatra istinitim;
2. Što je TVRDNJA teorema: sud Q koji je potrebno dokazati.

Na primjer, Talesov teorem kaže: "Obodni kut nad promjerom kružnice je pravi kut". Iako nije eksplicitno zapisan u obliku $P \Rightarrow Q$, za njegovo ispravno razumijevanje moramo ga formulirati u tom obliku:

$$\begin{aligned} P &\equiv \text{"Kut } \alpha \text{ je obodni kut nad promjerom kružnice."} \\ Q &\equiv \text{"Kut } \alpha \text{ je pravi kut."} \\ P \Rightarrow Q &\equiv \text{"Ako je } \alpha \text{ obodni kut nad promjerom kružnice, onda je } \alpha \\ &\qquad \text{pravi kut."} \end{aligned}$$

Objasnimo još što znači dokazati neki teorem oblika $P \Rightarrow Q$. Razlikujemo direktne i indirektne dokaze:

(a) Napraviti DIREKTNI DOKAZ tvrdnje $P \Rightarrow Q$ znači, uz pretpostavku da su istinite tvrdnja P i aksiomi teorije, logičkim zaključivanjem pronaći tvrdnje $Q_1, Q_2, \ldots, Q_n$ takve da vrijedi

$$(P \Rightarrow Q_1) \wedge (Q_1 \Rightarrow Q_2) \wedge \ldots \wedge (Q_n \Rightarrow Q).$$

Tada, zbog toga što vrijedi $(A \Rightarrow B) \wedge (B \Rightarrow C) \equiv (A \Rightarrow C)$, vrijedi $P \Rightarrow Q$.

(b) Napraviti DOKAZ OBRATOM PO KONTRAPOZICIJI znači dokazati da vrijedi $\neg Q \Rightarrow \neg P$. Kako smo pokazali ranije, ovaj sud je semantički jednak sudu $P \Rightarrow Q$, pa smo, dokazavši $\neg Q \Rightarrow \neg P$ ujedno dokazali i $P \Rightarrow Q$.

(c) Napraviti DOKAZ SVOĐENJEM NA KONTRADIKCIJU znači dokazati da vrijedi $(P \wedge \neg Q) \Rightarrow L$, pri čemu je L neka očito lažna tvrdnja. Naime, ako je $P \wedge \neg Q$ laž, onda je $\neg(P \wedge \neg Q) \equiv P \Rightarrow Q$ istina.

Dokaze obratnom po kontrapoziciji i svođenjem na kontradikciju još zovemo i INDIREKTNI DOKAZI. Kako se možda nismo susretali do sada sa ovom vrstom dokaza, napravimo po jedan primjer za svaki od njih.

Primjer 1.16. *Dokažimo sljedeću tvrdnju:*

"Ako je $n \in \mathbb{N}$ takav da je n^2 neparan, onda je i n također neparan".

Zapišimo ovu tvrdnju u obliku $P \Rightarrow Q$:

$$P \equiv \text{"Broj } n^2 \text{ je neparan"};$$
$$Q \equiv \text{"Broj } n \text{ je neparan"}.$$

Umjesto dokaza tvrdnje $P \Rightarrow Q$, lakše je napraviti dokaz obratom po kontrapoziciji, odnosno, dokazati tvrdnju $\neg Q \Rightarrow \neg P$:

"Ako je $n \in \mathbb{N}$ paran, onda je i n^2 također paran".

Dakle, pretpostavimo da vrijedi $\neg Q$, odnosno, da je broj n paran. Tada ga možemo zapisati u obliku $n = 2k$, za neki prirodni broj k. No tada je $n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$, pa je i broj n^2 također paran, to jest, vrijedi tvrdnja $\neg P$. Stoga smo pokazali $\neg Q \Rightarrow \neg P$, pa obratom po kontrapoziciji vrijedi i $P \Rightarrow Q$.

Primjer 1.17. *Dokažimo da je $\log 3$ iracionalan broj.*
Tvrdnju dokazujemo svođenjem na kontradikciju: pretpostavimo suprotno, tj. da je $\log 3$ racionalan broj. Tada postoje $p, q \in \mathbb{N}$ takvi da je $\log 3 = \frac{p}{q}$. Po definiciji funkcije logaritam, tada vrijedi $3 = 10^{\frac{p}{q}}$. Cijelu jednakost potenciramo potencijom q, čime dobivamo $3^q = 10^p$. S obje strane ove jednakosti su prirodni brojevi, no lijeva strana je djeljiva brojem 3, a desna nije. To je nemoguće, odnosno, dobili smo kontradikciju. Zbog toga je početna pretpostavka bila kriva, pa $\log 3$ nije racionalan broj.

Uočimo da je $\log 3 > 0$ jer je logaritam rastuća funkcija, a $\log 1 = 0$.

Ako je $P \Rightarrow Q$ neki teorem, onda kažemo da je tvrdnja $Q \Rightarrow P$ OBRAT TEOREMA. Međutim, obrat teorema nije nužno istinit!

Primjer 1.18. *Promotrimo sljedeći lako dokazivi teorem: "Neka su $a, b, c \in \mathbb{N}$. Ako je broj a djeljiv brojem c, onda je i broj $a \cdot b$ također djeljiv brojem c".*
Obrat ovog teorema glasi: "Neka su $a, b, c \in \mathbb{N}$. Ako je broj $a \cdot b$ djeljiv brojem c, onda je i broj a također djeljiv brojem c".
Međutim, obrat očito ne vrijedi: brojevi $a = 5$, $b = 27$ i $c = 3$ su takvi da je $a \cdot b$ djeljivo sa c, no a nije djeljiv brojem c.

U gornjem primjeru smo željeli pokazati da obrat teorema nije istinit. To smo napravili tako da smo pronašli KONTRAPRIMJER. Zbog čega je to dovoljno? Obrat teorema je bio tvrdnja oblika $(\forall x)P(x)$. Da bismo pokazali da je ova tvrdnja lažna, dovoljno je pokazati da je tvrdnja

$$\neg((\forall x)\ P(x)) \equiv (\exists x)\ \neg P(x)$$

istinita. Ta tvrdnja je istinita ako postoji vrijednost varijable x za koju predikat $P(x)$ nije istinit—takav x zovemo kontraprimjer.

U Primjeru 1.18 obrat zapravo ima ovaj oblik:

$$(\forall a, b, c \in \mathbb{N})\ Q(a, b, c) \Rightarrow P(a, b, c),$$

gdje je $P(a, b, c) \equiv$ "Broj a je djeljiv brojem c", te $Q(a, b, c) \equiv$ "Broj $a \cdot b$ je djeljiv brojem c". Negacija gornjeg suda glasi:

$$(\exists a, b, c \in \mathbb{N})\ Q(a, b, c) \wedge \neg P(a, b, c),$$

pa je dovoljno pronaći vrijednosti za a, b, c takve da vrijedi $Q(a, b, c)$, ali ne vrijedi $P(a, b, c)$.

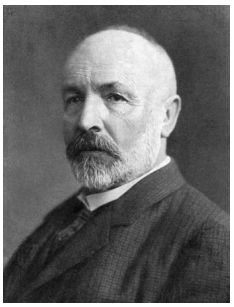
Ako vrijedi i teorem $P \Rightarrow Q$ i njegov obrat $Q \Rightarrow P$, onda u iskazu teorema često koristimo frazu "ako i samo ako". Da dokažemo takav teorem, potrebno je dokazati i jednu i drugu implikaciju! Primjer ovakvog teorema je Pitagorin poučak: "Trokut čije su duljine stranica a, b i c je pravokutan s pravim kutem nasuprot stranice c ako i samo ako vrijedi $a^2 + b^2 = c^2$".

2
Skupovi

Pojam skupa jedan je od osnovnih pojmova u matematici i javlja se u praktički svakom njenom području. Govorimo o skupovima prirodnih i realnih brojeva; kada zadajemo funkcije, zadajemo njihovu domenu i kodomenu koje su skupovi; kada proučavamo jednadžbe, dobivamo skupove njihovih rješenja. Čak i pojmove iz geometrije, poput kružnice ili kocke, definiramo kao skupove točaka u ravnini ili prostoru.

Zbog tih razloga, već od nižih razreda osnovne škole stekli smo intuitivno razumijevanje pojma skupa. Skup je jednostavno kolekcija nekih objekata; ako imamo više kolekcija objekata, jasno nam je što znači njihova unija ili presjek. Ovakve operacije nad skupovima smo navikli zamišljati i prikazivati Vennovim dijagramima. Problem nam ne predstavljaju niti beskonačni skupovi, poput skupa svih prirodnih brojeva ili intervala $\langle 0, 1\rangle$.

Ovakav pristup razumijevanju pojma skupa prevladavao je u matematici sve do kraja 19. stoljeća. Tada su se, prvenstveno motivirani radovima Georga Cantora u kojima je proučavao beskonačne skupove, najednom počeli pojavljivati paradoksi—tvrdnje koje su, uz intuitivno shvaćanje pojma skupa, jednostavno bile kontradiktorne. Stoga se javila potreba za strogim pravilima koja bi jasno definirala što se može smatrati skupom, a što ne, odnosno, potreba za uvođenjem aksioma teorije skupova. Tako je nastalo nekoliko sustava aksioma, od kojih se danas u matematici najčešće koristi Zermelo–Frankelov sustav (ZFC).



Georg Cantor (1845.–1912.), začetnik teorije skupova

Strogo formalna definicija aksioma ZFC i obrazloženja razloga za njihovo uvođenje izlazi izvan okvira ovog kolegija[1]. Iako nam je intuitivno razumijevanje skupova sasvim dovoljno za svladavanje svog gradiva Elementarne matematike 1, ipak ćemo uvesti nešto pojednostavljeni sustav aksioma teorije skupova kojim ćemo ilustrirati kako se može formalno definirati pojam skupa. Tako ćemo u ovom poglavlju navesti niz pravila pomoću kojih se grade skupovi. Nešto ćemo smatrati skupom jedino u slučaju da to nešto možemo dobiti koristeći ta pravila, i nikako drugačije.

[1] Mnogo više detalja ove problematike upoznat ćete na kolegiju "Teorija skupova" na trećoj godini preddiplomskog studija.

2.1 Prazan skup i jednočlani skupovi

Skupove i dalje smatramo kolekcijama objekata. Ti objekti mogu biti, na primjer, prirodni ili realni brojevi, točke u prostoru, funkcije, i tako dalje. Neki skup možemo zapisati tako da sve objekte od kojih se sastoji navedemo unutar vitičastih zagrada.

Na primjer, $\{3,\ 6,\ 20\}$ će biti skup koji je kolekcija objekata 3, 6 i 20.

Kažemo da je objekt x ELEMENT skupa S ako objekt x pripada kolekciji objekata koji čine S. To označavamo ovako: $x \in S$. U protivnom, x nije element skupa S i pišemo $x \notin S$.

$3 \in \{3,\ 6,\ 20\}$
$5 \notin \{3,\ 6,\ 20\}$

Prva dva pravila opisuju najjednostavnije moguće skupove: prvo kaže da postoji prazan skup, a drugo definira jednočlane skupove.

Pravilo S1. *Postoji skup $\emptyset$, kojeg zovemo* PRAZAN SKUP *i koji ne sadrži niti jedan element. Drugim riječima, za svaki objekt x vrijedi $x \notin \emptyset$.*

Pravilo S2. *Ako je x objekt, onda je $\{x\}$ skup. Jedini element tog skupa je x.*

Ako promatramo objekte 3, 6 i 20, jedini skupovi koje možemo napraviti koristeći ova dva pravila su: $\emptyset$, $\{3\}$, $\{6\}$ i $\{20\}$.

2.2 Booleove operacije nad skupovima

Sljedeće pravilo dat će nam mehanizam pomoću kojeg od dva "manja" skupa možemo napraviti "veći".

Pravilo S3. *Ako su A i B dva skupa, onda postoji skup $A \cup B$ čiji elementi su svi oni objekti koji pripadaju skupu A ili skupu B. Skup $A \cup B$ zovemo* UNIJA *skupova A i B. Zapisano simbolima,*

$$(\forall x)\ \Big(x \in A \cup B \ \Leftrightarrow\ (x \in A \vee x \in B)\Big). \tag{2.1}$$

Pomoću ovih pravila možemo *dokazati* da je $\{3, 6, 20\}$ zaista skup: od ranije već znamo da su $A = \{3\}$, $B = \{6\}$ i $C = \{20\}$ skupovi. Primjenom Pravila S3, skup je i $S := A \cup B = \{3, 6\}$. Ako ponovno primijenimo Pravilo S3 na skupove S i C, dobivamo da je $\{3, 6, 20\}$ zaista skup.

Trebamo li zasebnim pravilima specificirati da su presjek, razlika i komplement dvaju skupova također skupovi? Mogli bismo, no umjesto toga uvest ćemo samo jedno pravilo pomoću kojeg ćemo lako dokazati da navedenim operacijama dobivamo skupove.

Pravilo S4. *Neka je A skup, te neka je $P(x)$ predikat definiran za sve elemente x iz skupa A. Tada postoji skup, kojeg označavamo sa*

Uobičajen je i zapis: $\{x \in A \mid P(x)\}$.

$$\{x \in A\ :\ P(x)\},$$

čiji elementi su svi oni elementi x skupa A za koje je $P(x)$ istina.

Primjer 2.1. *Koristeći prva tri pravila možemo pokazati da je $A = \{1,\ 2,\ 3,\ 4,\ 5\}$ skup. Neka je $P(x)$ = "broj x je paran". Iz Pravila S4 slijedi da je $\{x \in A\ :\ P(x)\} = \{2, 4\}$ također skup. Ovo smo, naravno, mogli pokazati i samo pomoću prva tri pravila.*

U Primjeru 2.1 vidjeli smo da neki skup možemo pomoću pravila izgraditi na više načina. Zbog toga se prirodno javlja potreba za provjerom kada su dva skupa jednaka.

Definicija 2.2. *Neka su A i B skupovi. Kažemo da je A* PODSKUP *od B i pišemo $A \subseteq B$ ako vrijedi*

$$(\forall x)\ \Big(x \in A \Rightarrow x \in B\Big).$$

Simbol $\subseteq$ zovemo "inkluzija".

Ako je $A \subseteq B$ i $B \subseteq A$, kažemo da su skupovi A i B JEDNAKI *i pišemo $A = B$.*

Iz gornje definicije i iz svojstava logičkih operacija implikacije i ekvivalencije slijedi da za skupove A i B vrijedi

$$A = B \equiv (\forall x)\ \Big(x \in A \Leftrightarrow x \in B\Big). \tag{2.2}$$

Zbog toga je lako[2] provjeriti da je

$$\{1,2,3,4,5\} = \{3,5,4,5,2,4,3,1,2,1\}.$$

[2] Jednostavno redom za svaki element skupa $\{1,2,3,4,5\}$ provjerimo je li on element od $\{3,5,4,5,2,4,3,1,2,1\}$ i obratno. "Višestruke" kopije pojedinog elementa su posve nebitne kad govorimo o skupovima. Isto vrijedi i za poredak elemenata unutar vitičastih zagrada.

Kako opovrgnuti tvrdnju $A \subseteq B$? U Poglavlju 1 naučili smo negirati logičke formule s kvatifikatorima, pa sada možemo iskoristiti to znanje:

$$\begin{aligned}\neg(A \subseteq B) &\equiv \neg((\forall x)\ x \in A \Rightarrow x \in B)\\ &\equiv (\exists x)\ \neg(x \in A \Rightarrow x \in B)\\ &\equiv (\exists x)\ (x \in A \wedge \neg(x \in B))\\ &\equiv (\exists x)\ (x \in A \wedge x \notin B).\end{aligned} \tag{2.3}$$

Drugim riječima, ako želimo dokazati da A nije podskup od B, dovoljno je pronaći element x skupa A koji nije element skupa B. Na primjer, skup $X = \{1,2,3\}$ nije podskup skupa $Y = \{1,5,6\}$ zato jer $2 \in X$, ali $2 \notin Y$.

Na posve isti način se može dokazati

$$A \neq B \equiv (\exists x)\ \Big((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\Big).$$

Često će nam se javiti i pojam "pravi podskup", pa navedimo i njegovu definiciju.

Definicija 2.3. *Neka su A i B skupovi takvi da je $A \subseteq B$, ali $A \neq B$. Tada kažemo da je A* PRAVI PODSKUP *od B i pišemo $A \subsetneq B$.*

Ponekad se koristi i oznaka $A \subsetneqq B$.

Uz pomoć formule (2.3), lako se vidi da vrijedi:

$$A \subsetneq B \equiv ((\forall x)\ x \in A \Rightarrow x \in B) \wedge ((\exists x)\ x \in B \wedge x \notin A).$$

Ovdje smo zapravo simbolima zapisali ekvivalentnu tvrdnju:

$$A \subsetneq B \ \Leftrightarrow\ (A \subseteq B) \wedge \neg(B \subseteq A).$$

Sljedeća propozicija nam daje prve jednostavne rezultate o odnosima skupova.

Propozicija 2.4. *Neka su A, B i C proizvoljni skupovi. Tada vrijedi:*

(a) $\emptyset \subseteq A$;

(b) $A \subseteq A$;

(c) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$;

(d) $(A = B \wedge B = C) \Rightarrow A = C$;

(e) $A \subseteq A \cup B$.

Dokaz.

(a) Prema definiciji pojma podskup, tvrdnja $\emptyset \subseteq A$ je istina ako vrijedi

$$(\forall x)\ \Big(x \in \emptyset \Rightarrow x \in A\Big).$$

No tvrdnja $x \in \emptyset$ je uvijek lažna, pa je implikacija $x \in \emptyset \Rightarrow x \in A$ istinita za sve objekte x.

(b)(c)(d) Dokazi ovih tvrdnji su očiti ili vrlo jednostavni, pa ih ostavljamo za vježbu.

(e) Prema definiciji pojma podskup, treba dokazati

$$(\forall x)\ \Big(x \in A \Rightarrow x \in A \cup B\Big).$$

Neka je, dakle, x proizvoljni objekt takav da je $x \in A$ istinit sud. No tada je istinit i sud $(x \in A) \vee (x \in B)$, a to prema Pravilu S3 znači $x \in A \cup B$.

□

Kao što smo i spomenuli, kada imamo Pravilo S4, nije potrebno uvesti pojam presjeka pomoću pravila, nego to možemo dokazati. Ako su A i B skupovi, za $x \in A$ promotrimo predikat $P(x) =$ "$x \in B$". Prema Pravilu S4, $\{x \in A\ :\ P(x)\}$ je skup—upravo onaj kojeg nazivamo presjek.

Definicija 2.5. *Neka su A i B skupovi. Skup*

$$A \cap B := \{x \in A\ :\ x \in B\}$$

zovemo PRESJEK *skupova A i B.*

Možda je prirodnije definirati presjek simetrično s obzirom na skupove A i B, tj. ovako:

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

No iz definicije lijevo i Pravila S4 je odmah jasno da je $A \cap B$ skup.

Lako se vidi da vrijedi

$$(\forall x)\ \Big(x \in A \cap B\ \Leftrightarrow\ (x \in A \wedge x \in B)\Big). \tag{2.4}$$

Uz uniju i presjek, često su nam korisne i skupovne razlike.

Definicija 2.6. *Neka su A i B skupovi.* RAZLIKA SKUPOVA *A i B je skup*

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

SIMETRIČNA RAZLIKA SKUPOVA *A i B je skup*

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

Iz Pravila S4 slijedi da su $A \setminus B$ i $B \setminus A$ skupovi.
Iz Pravila S3 onda slijedi da je skup i $A \triangle B$.

Na primjer, neka je $A = \{1, 2, 4, 5, 7\}$ i $B = \{1, 3, 5, 9\}$. Tada:

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 7, 9\}, \\ A \cap B &= \{1, 5\}, \\ A \setminus B &= \{2, 4, 7\}, \\ B \setminus A &= \{3, 9\}, \\ A \triangle B &= \{2, 3, 4, 7, 9\}. \end{aligned}$$

Pripadnost skupovnim razlikama također možemo lako izraziti pomoću logičkih formula.

Propozicija 2.7. *Neka su A i B skupovi. Tada*

$$(\forall x)\ \Big(x \in A \setminus B \ \Leftrightarrow (x \in A) \wedge (x \notin B)\Big); \tag{2.5}$$

$$(\forall x)\ \Big(x \in A \triangle B \ \Leftrightarrow ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))\Big). \tag{2.6}$$

Dokaz. Prva tvrdnja je trivijalna; pokažimo drugu. Potrebno je pokazati istinitost ekvivalencije, što ćemo pokazati tako da pokažemo istinitost obje implikacije.

($\Rightarrow$) Neka je $x \in A \triangle B$. Po definiciji simetrične razlike, tada $x \in (A \setminus B) \cup (B \setminus A)$. Prema formuli (2.1), slijedi

$$x \in A \setminus B \ \vee \ x \in B \setminus A,$$

pa imamo dva slučaja.
Ako je $x \in A \setminus B$, onda je, prema prvoj tvrdnji ove propozicije, $(x \in A) \wedge (x \notin B)$, pa stoga[3] i $((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$, što je i trebalo pokazati.
Analogno, ako je $x \in B \setminus A$, onda je $(x \in B) \wedge (x \notin A)$, pa stoga i $((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$, što je i trebalo pokazati.

[3] Ako je istinit sud P, onda je istinit i sud $P \vee Q$, bez obzira na istinitost suda Q.

($\Leftarrow$) Obratno, neka je $((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$. Ponovno razlikujemo dva slučaja.
Prvi slučaj: $(x \in A) \wedge (x \notin B)$. Tada po prvoj tvrdnji ove propozicije slijedi $x \in A \setminus B$, pa onda[4] i $x \in (A \setminus B) \cup (B \setminus A)$, odnosno $x \in A \triangle B$.
Drugi slučaj: $(x \in B) \wedge (x \notin A)$. Tada po prvoj tvrdnji ove propozicije slijedi $x \in B \setminus A$, pa onda i $x \in (A \setminus B) \cup (B \setminus A)$, odnosno $x \in A \triangle B$.

[4] To je zbog Propozicije 2.4: za skupove $A \setminus B$ i $B \setminus A$ vrijedi

$$A \setminus B \subseteq (A \setminus B) \cup (B \setminus A);$$

zatim primijenimo definiciju pojma podskup.

□

Kada razvijamo neku matematičku teoriju, obično su svi skupovi koje promatramo u sklopu te teorije podskupovi nekog većeg skupa kojeg onda zovemo *univerzalni skup*. Na primjer, ako proučavamo djeljivost i proste brojeve, svi skupovi koji će nas zanimati će sadržavati isključivo cijele brojeve, odnosno, bit će podskupovi od $\mathbb{Z}$. U tom kontekstu ulogu univerzalnog skupa ima skup $\mathbb{Z}$. U slučaju kada imamo univerzalni skup, moguće je definirati još jednu skupovnu operaciju.

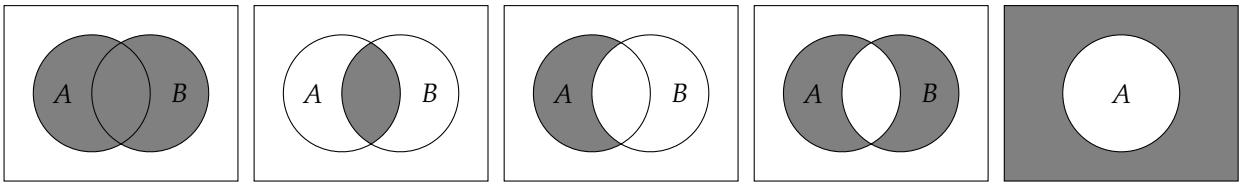
Definicija 2.8. *Neka je U skup i $A \subseteq U$. Skup*

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

zovemo KOMPLEMENT SKUPA *A (s obzirom na skup U).*

Ovdje U ima ulogu univerzalnog skupa.

Na Slici 2.1 smo ilustrirali *Booleove operacije* nad skupovima: uniju, presjek, razliku, simetričnu razliku, te komplement.



(a) $A \cup B$ (b) $A \cap B$ (c) $A \setminus B$ (d) $A \triangle B$ (e) A^c

Slika 2.1: Booleove operacije nad skupovima ilustrirane Vennovim dijagramima.

Sada ćemo nizom teorema utvrditi odnose između skupova dobivenih Booleovim operacijama. U prvom teoremu ispitujemo odnos jednog skupa A s univerzalnim i s praznim skupom.

Teorem 2.9. *Neka je U skup i $A \subseteq U$. Tada:*

(a) $A \cup A = A; \quad A \cap A = A;$

(b) $A \cup U = U; \quad A \cap \emptyset = \emptyset;$

(c) $A \cup \emptyset = A; \quad A \cap U = A;$

(d) $A \cup A^c = U; \quad A \cap A^c = \emptyset;$

(e) $(A^c)^c = A.$

Svojstvo (a) zovemo idempotentnost, a svojstvo (e) involutivnost.

Dokaz. Dokažimo samo (a) i (d); ostale ostavljamo za vježbu.

(a) $x \in A \cup A \;\Leftrightarrow\; (x \in A) \vee (x \in A) \;\Leftrightarrow\; x \in A.$

(d) Pokažimo prvo inkluziju $A \cup A^c \subseteq U$: neka je $x \in A \cup A^c$ proizvoljan. Po definiciji unije, slijedi $(x \in A) \vee (x \in A^c)$. Uočimo da je $A \subseteq U$ i $A^c \subseteq U$, pa $x \in A$ povlači $x \in U$ i $x \in A^c$ također povlači $x \in U$. Stoga, $x \in A \cup A^c \Rightarrow (x \in U) \vee (x \in U) \Rightarrow x \in U$, odnosno, $A \cup A^c \subseteq U$.
Obratno, treba pokazati $U \subseteq A \cup A^c$. Neka je $x \in U$ proizvoljan. Razlikujemo dva slučaja: $x \in A$ i $x \notin A$. Ako je $x \in A$, onda je zbog Propozicije 2.4(e) također i $x \in A \cup A^c$. Ako je $x \notin A$, onda je $x \in U \setminus A$, odnosno $x \in A^c$, pa zbog iste propozicije ponovno imamo $x \in A \cup A^c$.

□

Sljedeći teorem navodi još neka svojstva Booleovih operacija.

Teorem 2.10. *Neka su A, B i U skupovi takvi da je $A \subseteq U$ i $B \subseteq U$. Tada vrijedi:*

(a) $A \cup B = B \cup A; \quad A \cap B = B \cap A;$

(b) $(A \cup B)^c = A^c \cap B^c; \quad (A \cap B)^c = A^c \cup B^c;$

(c) $A \setminus B = A \cap B^c; \quad (A \setminus B) \cap (B \setminus A) = \emptyset;$

(d) $A \subseteq B \Leftrightarrow B^c \subseteq A^c.$

Iz svojstva (a) vidimo da su operacije unije i presjeka komutativne. Formule (b) ponovno zovemo De Morganove formule.

Dokaz. Budući da smo formulama (2.1), (2.4), (2.5) operacije nad skupovima sveli na logičke formule, svi dokazi će se svesti na svojstva logičkih veznika.

(a) Slijedi direktno iz komutativnosti logičkih veznika "i" i "ili".

(b) U četvrtom retku koristimo De Morganovu formulu za logički veznik "ili".

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

Drugu formulu je lako dokazati pomoću prve i involutivnosti komplementa:

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

Ovdje smo "unatrag" primijenili De Morganovu formulu za komplement unije skupova A^c i B^c:

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

(c) Prvu jednakost skupova dokazujemo ovako:

$$\begin{aligned} x \in A \setminus B &\Leftrightarrow (x \in A) \wedge (x \notin B), \text{ zbog (2.5)} \\ &\Leftrightarrow (x \in A) \wedge (x \in U) \wedge (x \notin B), \text{ zbog } A \subseteq U \\ &\Leftrightarrow (x \in A) \wedge (x \in B^c) \\ &\Leftrightarrow x \in A \cap B^c. \end{aligned}$$

Drugu jednakost dokazujemo svođenjem na kontradikciju:

$$\begin{aligned} x \in (A \setminus B) \cap (B \setminus A) &\Rightarrow (x \in A \wedge x \notin B) \wedge (x \in B \wedge x \notin A) \\ &\Rightarrow (x \in A \wedge x \notin A) \wedge (x \in B \wedge x \notin B), \end{aligned}$$

no to nije istina niti za jedan objekt x, pa je $(A \setminus B) \cap (B \setminus A) = \emptyset$.

(d) Neka je $A \subseteq B$. Treba dokazati da je tada $B^c \subseteq A^c$, pa uzmimo proizvoljni $x \in B^c$; želimo dokazati da je $x \in A^c$. Pretpostavimo suprotno, to jest $x \notin A^c$. Kako smo u Teoremu 2.9(d) pokazali da je $A \cup A^c = U$, slijedi $x \in A$. Zbog $A \subseteq B$, slijedi $x \in B$, no to je kontradikcija s pretpostavkom $x \in B^c$ i pokazanom činjenicom da je $B \cap B^c = \emptyset$. Dakle, mora biti $x \in A^c$, pa je $B^c \subseteq A^c$.
Obratno, neka je $B^c \subseteq A^c$. Prema upravo dokazanom, slijedi $(A^c)^c \subseteq (B^c)^c$. No zbog involutornosti komplementa iz ovog imamo odmah $A \subseteq B$.

□

Kao u (c) dijelu prethodnog teorema, česta je situacija u kojoj je presjek dva skupa prazan, pa uvodimo poseban pojam za takve skupove.

Definicija 2.11. *Za skupove A i B takve da vrijedi $A \cap B = \emptyset$ kažemo da su* DISJUNKTNI.

Preostao nam je još teorem koji ispituje odnose unije i presjeka triju skupova.

Teorem 2.12. *Neka su A, B, C skupovi. Tada:*

(a) Operacije unije i presjeka su asocijativne, odnosno, vrijedi:

Da li je skupovna razlika asocijativna?

$$(A \cup B) \cup C = A \cup (B \cup C);$$
$$(A \cap B) \cap C = A \cap (B \cap C).$$

(b) Operacije unije i presjeka su distributivne jedna prema drugoj:

Ove, kao i većina drugih skupovnih jednakosti su u direktnoj vezi s odgovarajućim jednakostima logičkih izraza. Uniju obično povezujemo s veznikom "ili", a presjek s veznikom "i". Stoga bi prvi izraz odgovarao logičkom izrazu

$$A \cdot (B + C) = A \cdot B + A \cdot C,$$

a drugi

$$A + (B \cdot C) = (A + B) \cdot (A + C).$$

Za oba smo pokazali da su istiniti u prvom poglavlju. Usporedite i ostale skupovne jednakosti u ovom poglavlju; $\emptyset$ poistovjetite s 0, a U s 1.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Dokaz.

(a) Dokaz se svodi na asocijativnost logičkih veznika.

$$\begin{aligned} x \in (A \cup B) \cup C &\Leftrightarrow (x \in A \cup B) \vee (x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \vee (x \in C) \\ &\Leftrightarrow [\text{asocijativnost veznika } \vee] \\ &\Leftrightarrow x \in A \vee (x \in B \vee x \in C) \\ &\Leftrightarrow x \in A \vee (x \in B \cup C) \\ &\Leftrightarrow x \in A \cup (B \cup C). \end{aligned}$$

(b) Dokaz se svodi na distributivnost logičkih veznika.

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge (x \in B \vee x \in C) \\ &\Leftrightarrow [\text{distributivnost veznika } \wedge \text{ prema } \vee] \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\Leftrightarrow ((x \in A \cap B)) \vee ((x \in A \cap C) \\ &\Leftrightarrow (x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

□

Za kraj ove cjeline, pokažimo i neka svojstva simetrične razlike.

Teorem 2.13. *Neka su A, B, C, U skupovi takvi da je $A \subseteq U$, $B \subseteq U$, $C \subseteq U$. Tada:*

Kojem logičkom vezniku bi odgovarala skupovna razlika?

(a) $A \triangle A = \emptyset$;

(b) $A \triangle \emptyset = \emptyset \triangle A = A$;

(c) $A \triangle B = (A \cup B) \setminus (A \cap B)$;

(d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Dokaz. Pokažimo samo tvrdnju (c), koju najčešće i koristimo pri radu sa simetričnom razlikom.

$$\begin{aligned} x \in A \triangle B &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B) \\ &\Leftrightarrow [(P \wedge \neg Q) \vee (\neg P \wedge Q) \equiv (P \vee Q) \wedge (\neg P \vee \neg Q)] \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in A^c \cup B^c) \\ &\Leftrightarrow [\text{De Morganova formula}] \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in (A \cap B)^c) \\ &\Leftrightarrow x \in (A \cup B) \setminus (A \cap B). \end{aligned}$$

Dokažite identitet logike sudova koji smo koristili u drugom retku! □

2.3 *Partitivni skup*

Nakon što smo uveli osnovne skupovne operacije, vratimo se na pravila teorije skupova. Premda ćemo dodati još nekoliko pravila, svi rezultati i dokazi koje smo proveli u prethodnoj cjelini i dalje ostaju ispravni! Do sada imamo četiri pravila: prva dva omogućuju izgradnju praznog i jednočlanih skupova, treće kaže da je unija dvaju skupova ponovno skup, a četvrto omogućava da pomoću jednomjesnog predikata odaberemo neke elemente postojećeg skupa i tako stvorimo novi skup.

Uz sljedeće pravilo, skupovi koje možemo izgraditi će postati bitno složeniji.

Pravilo S5. *Svaki skup je ujedno i objekt.*

Drugim riječima, skupovi mogu biti elementi drugih skupova.

Izuzetno je važno u potpunosti razumjeti sljedeći primjer.

Primjer 2.14. *Koristeći prva tri pravila, znamo da su* $\{1\}, \{2,3\}$ *i* $\emptyset$ *skupovi. Zbog Pravila S5, to su ujedno i objekti, što znači da ih smijemo "uvrstiti" u preostale pravila. Prema Pravilu S2,*

$\{\{1\}\}$ *je skup čiji je jedini element* $\{1\}$*, dakle,* $\{1\} \in \{\{1\}\}$.

Uočite:

$$1 \in \{1\}, \quad \{1\} \in \{\{1\}\}, \quad \textit{ali } 1 \notin \{\{1\}\}.$$

Slično, uvjerite se da su i ovo skupovi:

$$\begin{aligned} A &= \{\emptyset\}, \\ B &= \{1,\ \{1\},\ \{2,3\}\}, \\ C &= \{\emptyset,\ \{\emptyset\}\}, \\ D &= \{1,\ \{1,\ \{2,\ 3\}\}\}, \end{aligned}$$

te da vrijedi:

$$\emptyset \in A,\ \emptyset \subseteq A,\ \{\emptyset\} \subseteq A;$$
$$1 \in B,\ \{1\} \in B,\ \{1\} \subseteq B,\ 2 \notin B,\ \{2,3\} \in B,\ \{2,3\} \not\subseteq B;$$
$$\emptyset \in C,\ \{\emptyset\} \in C,\ \{\emptyset\} \subseteq C,\ \{\{\emptyset\}\} \subseteq C;$$
$$1 \in D,\ \{1\} \notin D,\ \{1\} \subseteq D,\ \{2,3\} \notin D,\ \{1,\{2,3\}\} \in D.$$

Ako su svi elementi skupa $\mathcal{F}$ i sami skupovi, kažemo da je $\mathcal{F}$ FAMILIJA SKUPOVA. Na primjer,

Familije skupova obično označavamo kaligrafskim slovima, na primjer $\mathcal{A}, \mathcal{F}, \mathcal{S}$.

$$\mathcal{F} = \{\{2,3\},\ \{1,2,3\},\ \{3\},\ \{1,3\}\}$$

je jedna familija skupova. Svaki od elemenata te familije je podskup skupa $\{1,2,3\}$. Jedna vrlo važna familija skupova sastoji se od svih podskupova nekog skupa.

Pravilo S6. *Neka je A skup. Postoji skup $\mathcal{P}(A)$ takav da je svaki podskup skupa A element skupa $\mathcal{P}(A)$.*
Skup $\mathcal{P}(A)$ zovemo PARTITIVNI SKUP *skupa A.*

Ovo pravilo dobiva puni smisao tek kada uvedemo beskonačne skupove, vidi Pravilo S7. Možete li dobiti skup $\mathcal{P}(\mathbb{N})$ bez ovog pravila?

Na primjer, za $A = \{1,2,3\}$ je

$$\mathcal{P}(A) = \{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,\ 2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\},$$

za $B = \emptyset$ je

$$\mathcal{P}(B) = \{\emptyset\},$$

a za $C = \{1,\ \{2,3\}\}$ je

$$\mathcal{P}(C) = \{\emptyset,\ \{1\},\ \{\{2,3\}\},\ \{1,\{2,3\}\}\}.$$

Nije teško pokazati da, ako skup A ima n elemenata, onda skup $\mathcal{P}(A)$ ima 2^n elemenata. Naime, skup $\mathcal{P}(A)$ ima onoliko elemenata koliko ima različitih podskupova od A. Svaki podskup od A možemo dobiti na sljedeći način: napišimo sve elemente od A jedan do drugog, a zatim ispod svakog elementa napišimo ili 0 ili 1. Oni elementi ispod kojih piše 1 čine jedan podskup od A. Pisanjem svih mogućih kombinacija 0 i 1 (a njih ima 2^n) očito dobivamo sve moguće podskupove od A.

Na primjer, ako je $A = \{1,2,3,4,5\}$, onda kombinacijom

1	2	3	4	5
0	1	1	0	1

dobivamo podskup $\{2,3,5\}$.

Također, prirodan je i sljedeći rezultat.

Propozicija 2.15. *Neka su A i B skupovi. Tada vrijedi:*

$$A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Dokaz.

($\Rightarrow$) Pretpostavimo da je $A \subseteq B$, te neka je $X \in \mathcal{P}(A)$ proizvoljan. Po definiciji partitivnog skupa, slijedi $X \subseteq A$. Kako je $A \subseteq B$, prema Propoziciji 2.4(c) slijedi $X \subseteq B$, što znači $X \in \mathcal{P}(B)$. Dakle, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Uočimo da je ovdje X skup koji je element od $\mathcal{P}(A)$.

($\Leftarrow$) Pretpostavimo da je $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Zbog $A \subseteq A$ vrijedi $A \in \mathcal{P}(A)$, pa onda i $A \in \mathcal{P}(B)$, a to po definiciji partitivnog skupa znači $A \subseteq B$.

□

Primijetimo da ako je $A, B \subseteq U$, onda su i $A \cup B$, $A \cap B$, $A \setminus B$, A^c i $A \triangle B$ također podskupovi od U. Dakle,

$$A, B \in \mathcal{P}(U) \;\Rightarrow\; A \cup B,\; A \cap B,\; A \setminus B,\; A^c,\; A \triangle B \in \mathcal{P}(U).$$

2.4 *Beskonačni skupovi*

Svi skupovi koje možemo konstruirati pomoću do sada navedenih pravila su konačni jer svako od pravila smijemo primijeniti samo konačno mnogo puta. Budući da su beskonačni skupovi vrlo česti u matematici, bit će nam potrebno dodatno pravilo pomoću kojeg ćemo ih uvesti. Vrlo je zanimljiva činjenica da, ako skupom proglasimo "kolekciju" svih prirodnih brojeva, onda pomoću ostalih pravila možemo izgraditi i sve druge beskonačne skupove, poput $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$! Taj postupak ćemo opisati u Poglavlju 4, a za sada dodajmo odgovarajuće pravilo. Kako bismo mogli promatrati raznovrsnije primjere, u ostatku ovog poglavlja ćemo pretpostavljati da smo već pokazali da su navedene kolekcije objekata zapravo skupovi.

Pravilo S7. *Kolekcija svih prirodnih brojeva $\mathbb{N}$ je skup.*

Preciznije, kolekcija svih objekata koju ćemo definirati Peanovim aksiomima u Poglavlju 4.1 je skup.

Sada možemo uz pomoć preostalih pravila pokazati da, primjerice, svi prosti brojevi čine skup:

$$A = \{x \in \mathbb{N} \;:\; x \text{ je prost broj}\}.$$

Slično, možemo pokazati i da su intervali realnih brojeva također skupovi, na primjer:

$$\langle -\infty, a\rangle = \{x \in \mathbb{R} \;:\; x < a\};$$
$$[a, b\rangle = \{x \in \mathbb{R} \;:\; a \leq x \wedge x < b\}.$$

Sad kada smo uveli beskonačne skupove, više nam neće biti dovoljne skupovne operacije u kojima sudjeluju samo dva, tri, pa ni konačno mnogo skupova, nego ćemo promatrati unije i presjeke od po volji mnogo skupova. Na primjer, često se javljaju situacije u kojima za svaki prirodni broj n imamo definiran skup A_n i zanimaju nas svi elementi koji se javljaju barem u jednom od tih skupova, ili oni elementi koji se javljaju u svakom od tih skupova. Koristeći Pravilo S4, možemo definirati unije i presjeke familija[5] skupova.

[5] Uočite da u donjoj definiciji promatramo familije podskupova nekog univerzalnog skupa U. Ako bismo htjeli promatrati proizvoljne familije skupova, onda ne bismo mogli iskoristiti Pravilo S4, nego bi bilo potrebno uvesti novo pravilo koje kaže da su i takve unije skupovi!

Definicija 2.16. *Neka je U skup, te $\mathcal{F}$ neka familija podskupova od U (tj. $\mathcal{F} \subseteq \mathcal{P}(U)$). Tada skup*

$$\bigcup_{A \in \mathcal{F}} A := \{x \in U \;:\; (\exists A \in \mathcal{F})\; x \in A\}$$

zovemo UNIJA FAMILIJE $\mathcal{F}$*, a skup*

$$\bigcap_{A \in \mathcal{F}} A := \{x \in U \;:\; (\forall A \in \mathcal{F})\; x \in A\}$$

zovemo PRESJEK FAMILIJE $\mathcal{F}$.

Promotrimo nekoliko primjera.

(a) Neka su $X \subseteq U$ i $Y \subseteq U$ skupovi, te neka je $\mathcal{F} = \{X, Y\}$. Tada je

$$\bigcup_{A \in \mathcal{F}} A = X \cup Y,$$

odnosno, unija familije $\mathcal{F}$ koja sadrži samo skupove X i Y je upravo njihova unija. Analogna tvrdnja vrijedi i za presjek.

(b) Za $n \in \mathbb{N}$, neka je $A_n = \langle \frac{1}{n}, 1 \rangle$. Promotrimo familiju skupova čiji su elementi $A_1, A_2, \ldots$:

$$\mathcal{F} = \{A_n \ : \ n \in \mathbb{N}\}. \tag{2.7}$$

Pokažimo da vrijedi

$$\bigcup_{n=1}^{\infty} A_n := \bigcup_{A \in \mathcal{F}} A = \langle 0, 1 \rangle.$$

(Oznaku $\bigcup_{n=1}^{\infty} A_n$ redovito koristimo za ovakve unije familija.) Treba dokazati jednakost skupova:

($\subseteq$) Pokažimo prvo da je $\bigcup_{n=1}^{\infty} A_n \subseteq \langle 0, 1 \rangle$. Neka je $x \in \bigcup_{n=1}^{\infty} A_n$. Prema Definiciji 2.16, tada postoji $n \in \mathbb{N}$ takav da je $x \in A_n$. No tada $x \in \langle \frac{1}{n}, 1 \rangle$, pa je $\frac{1}{n} < x < 1$, a onda i $0 < x < 1$, odnosno, $x \in \langle 0, 1 \rangle$.

($\supseteq$) Obratno, pokažimo da je $\langle 0, 1 \rangle \subseteq \bigcup_{n=1}^{\infty} A_n$. Neka je $x \in \langle 0, 1 \rangle$, odnosno, $0 < x < 1$. Tada postoji $n \in \mathbb{N}$ takav da je $\frac{1}{n} < x$. No tada je $x \in \langle \frac{1}{n}, 1 \rangle = A_n$, pa onda i $x \in \bigcup_{n=1}^{\infty} A_n$.

Kako odrediti takav n? Na primjer, ako je $x = 0.001$, možemo uzeti $n = \frac{1}{x} + 1 = 1001$. Ovaj trik radi i općenito: uvijek možemo za n uzeti prvi prirodni broj veći od $\frac{1}{x}$.

S druge strane, imamo

$$\bigcap_{n=1}^{\infty} A_n := \bigcap_{A \in \mathcal{F}} A = \emptyset.$$

Naime, ako bi postojao $x \in \bigcap_{n=1}^{\infty} A_n$, onda je $x \in \langle \frac{1}{n}, 1 \rangle$ za sve $n \in \mathbb{N}$. Specijalno, za $n = 1$ imamo $x \in \langle \frac{1}{1}, 1 \rangle = \emptyset$, a takav x ne postoji.

(c) Označimo sa $\mathbb{R}_+$ skup svih pozitivnih realnih brojeva. Za $\alpha \in \mathbb{R}_+$, neka je $X_\alpha = \langle -\alpha, \alpha \rangle$, te promotrimo sljedeću familiju skupova:

$$\mathcal{F} = \{X_\alpha \ : \ \alpha \in \mathbb{R}_+\}. \tag{2.8}$$

Tada je

$$\bigcup_{\alpha \in R_+} X_\alpha := \bigcup_{X \in \mathcal{F}} X = \langle -\infty, \infty \rangle = \mathbb{R},$$
$$\bigcap_{\alpha \in R_+} X_\alpha := \bigcap_{X \in \mathcal{F}} X = \{0\}.$$

Dokaz ovih tvrdnji posve je analogan kao u (b), pa ga ostavljamo za vježbu.

Primjerinavedeni u (b) i (c) su primjeri *indeksiranih familija podskupova*.

Definicija 2.17. *Neka je $\mathcal{I}$ neprazni skup i $A_\alpha \subseteq U$ za svako $\alpha \in \mathcal{I}$. Tada*

$$\mathcal{F} = \{A_\alpha \,:\, \alpha \in \mathcal{I}\} \tag{2.9}$$

zovemo INDEKSIRANA FAMILIJA PODSKUPOVA, *a $\mathcal{I}$ zovemo* INDEKSNI SKUP. *Umjesto $\bigcup_{A\in\mathcal{F}} A$ pišemo $\bigcup_{\alpha\in\mathcal{I}} A_\alpha$, a umjesto $\bigcap_{A\in\mathcal{F}} A$ pišemo $\bigcap_{\alpha\in\mathcal{I}} A_\alpha$. Specijalno, kao u primjeru (b), ako je $\mathcal{I} = \mathbb{N}$, pišemo $\bigcup_{n=1}^{\infty} A_n$ i $\bigcap_{n=1}^{\infty} A_n$.*

Ovdje smo "prešutili" jedan detalj: da bismo mogli uopće govoriti o uniji familije podskupova, nužno je da su kolekcije $\mathcal{F}$ definirane u (2.7), (2.8), (2.9) skupovi. Zbog čega je to tako? U slučaju (2.7), možemo iskoristiti Pravilo S4:

$$\mathcal{F} = \{A \in \mathcal{P}(\mathbb{R}) \,:\, (\exists n \in \mathbb{N})\ A = \langle \frac{1}{n}, 1\rangle\}.$$

Slično je i za (2.8). No općenito, da bi (2.9) bio skup, nužno je uvesti još jedno novo pravilo. Radi jednostavnosti, umjesto toga ćemo ovdje prihvatiti da su indeksirane familije podskupova, kako smo ih definirali, uvijek skupovi.

I u slučaju unija i presjeka familija podskupova vrijede De Morganove formule.

Teorem 2.18. *Neka je U skup i $\mathcal{F} \subseteq \mathcal{P}(U)$ neka familija podskupova. Tada vrijedi:*

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

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

Dokaz. Pokažimo tvrdnju (a); dokaz druge tvrdnje je analogan.

$$\begin{aligned}
x \in \left(\bigcup_{A\in\mathcal{F}} A\right)^c &\Leftrightarrow x \in U \ \wedge\ x \notin \left(\bigcup_{A\in\mathcal{F}} A\right)\\
&\Leftrightarrow x \in U \ \wedge\ \neg\left(x \in \bigcup_{A\in\mathcal{F}} A\right)\\
&\Leftrightarrow x \in U \ \wedge\ \neg\left((\exists A \in \mathcal{F})\ x \in A\right)\\
&\Leftrightarrow x \in U \ \wedge\ \left((\forall A \in \mathcal{F})\ x \notin A\right)\\
&\Leftrightarrow (\forall A \in \mathcal{F})\ (x \in U \wedge x \notin A)\\
&\Leftrightarrow (\forall A \in \mathcal{F})\ x \in A^c\\
&\Leftrightarrow x \in \bigcap_{A\in\mathcal{F}} A^c.
\end{aligned}$$

□

Ako nam je dan neki skup A, često će nas zanimati jedna posebna vrsta familije podskupova od A koju ćemo zvati particija skupa A. Da bismo lakše razumjeli definiciju, promotrimo prvo jedan jednostavni primjer. Neka je $A = \{1,2,3,4,5\}$ i familiju $\mathcal{F} = \{A_1, A_2, A_3\}$ koju čine sljedeći skupovi:

$$A_1 = \{3,4\},\ A_2 = \{1\},\ A_3 = \{2,5\}.$$

Skupovi A_1, A_2 i A_3 u uniji daju cijeli skup A, a presjek svaka dva je prazan: $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$. Familija $\mathcal{F}$ je primjer jedne particije skupa A.

Još neke particije $\{1,2,3,4,5\}$ su, na primjer,

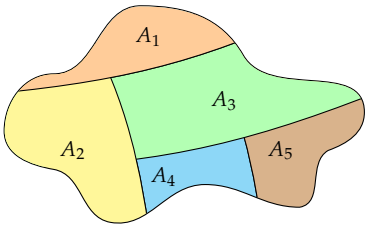
$\{\{1,3,4\},\ \{2,5\}\}$,
$\{\{1,2,3,4,5\}\}$,
$\{\{1\},\ \{2\},\ \{3\},\ \{4\},\ \{5\}\}$.

Postoje ukupno 52 particije tog skupa!

Definicija 2.19. *Neka je A proizvoljan skup.* PARTICIJA SKUPA *A je bilo koja familija skupova $\mathcal{F} \subseteq \mathcal{P}(A)$ sa sljedećim svojstvima:*

(a) Za sve $X \in \mathcal{F}$ vrijedi $X \neq \emptyset$;

(b) Za sve $X, Y \in \mathcal{F}$ vrijedi $X = Y$ ili $X \cap Y = \emptyset$;



Vizualizacija jedne particije skupa u ravnini, $\mathcal{F} = \{A_1, A_2, A_3, A_4, A_5\}$.

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

Možemo promatrati i particije beskonačnih skupova.

(a) Neka je X skup svih parnih, a Y skup svih neparnih prirodnih brojeva. Tada je $\mathcal{F} = \{X, Y\}$ jedna particija skupa $\mathbb{N}$.

(b) Neka je $A_n = [n, n+1\rangle$, za svaki prirodni broj n. Tada je $\mathcal{F} = \{A_n : n \in \mathbb{N}\}$ jedna particija skupa $[1, +\infty\rangle$. S druge strane, ako označimo $B_n = [n, n+1]$ i $C_n = \langle n, n+1\rangle$, onda $\mathcal{G} = \{B_n : n \in \mathbb{N}\}$ i $\mathcal{H} = \{C_n : n \in \mathbb{N}\}$ *nisu* particije skupova $[1, +\infty\rangle$ ni $\langle 1, +\infty\rangle$.

2.5 *Kartezijev produkt skupova*

Još jedan pojam koji ćemo često koristiti u nastavku je pojam uređenog para.

Definicija 2.20. *Neka su A i B skupovi, te $a \in A$ i $b \in B$. Objekt (a, b) zovemo* UREĐENI PAR, *pri čemu a zovemo* PRVI ČLAN PARA, *a b zovemo* DRUGI ČLAN PARA. *Dva uređena para (a_1, b_1) i (a_2, b_2) su* JEDNAKI *ako je $a_1 = a_2$ i $b_1 = b_2$; pišemo $(a_1, b_1) = (a_2, b_2)$.*

Napomenimo da ovdje nismo morali uvesti *novi* objekt (a, b), nego da smo mogli staviti $(a, b) := \{\{a\}, \{a, b\}\}$. Pogledajte Zadatak 2.1: možemo dokazati i da je Kartezijev produkt skupova A i B iz Definicije 2.21 zaista skup.

Skup svih uređenih parova zovemo Kartezijev produkt.

Definicija 2.21. *Neka su A i B skupovi.* KARTEZIJEV PRODUKT *skupova A i B je skup*

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

Ako je $A = \emptyset$ ili $B = \emptyset$, dogovorno uzimamo $A \times B = \emptyset$.

Promotrimo nekoliko primjera.

(a) Neka je $A = \{\sqrt{2}, \pi\}$, $B = \{1\}$. Tada je:

$$A \times B = \{(\sqrt{2}, 1),\ (\pi, 1)\},$$
$$B \times A = \{(1, \sqrt{2}),\ (1, \pi)\}.$$

Vidimo da je općenito $A \times B \neq B \times A$, odnosno, Kartezijev produkt *nije* komutativan.

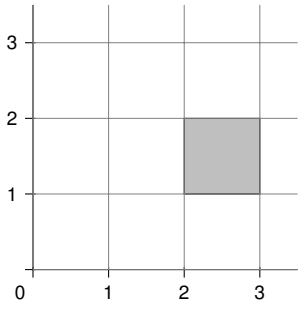
(b) Neka je $A = \{1, \{2\}\}$ i $B = \{\{\pi\}, 1\}$. Tada je:

$$A \times B = \{(1, \{\pi\}),\ (1, 1),\ (\{2\}, \{\pi\}),\ (\{2\}, 1)\}.$$

(c) Neka je $A = [2, 3]$ i $B = [1, 2]$. Tada je:

$$A \times B = [2, 3] \times [1, 2] = \{(x, y) \ : \ x \in [2, 3],\ y \in [1, 2]\}.$$

Skup $A \times B$ možemo prikazati u ravnini; vidi Sliku 2.2.



Slika 2.2: Osjenčani pravokutnik reprezentira skup $[2, 3] \times [1, 2]$.

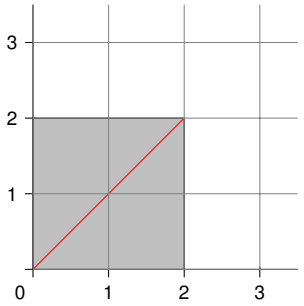
Definicija 2.22. *Neka je A skup. Tada skup $A^2 := A \times A$ zovemo* KARTEZIJEV KVADRAT, *skup*

$$D = \{(x, y) \in A^2 \ : \ x = y\}$$

zovemo DIJAGONALA.

Pokažimo sada nekoliko svojstava Kartezijevog produkta skupova. Na primjer, uz $A = [0,2]$ imamo

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



Slika 2.3: Osjenčani kvadrat reprezentira skup A^2 za $A = [0,2]$. Dijagonala je označena crveno.

Teorem 2.23. *Neka su A, B, C, D skupovi. Tada vrijedi:*

(a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;

(b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;

(c) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;

(d) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$;

(e) $(A \times B) \cap (B \times A) = (A \cap B)^2$.

Dokaz. Pokažimo, na primjer, tvrdnju (c):

$$\begin{aligned}(x,y) \in (A \times B) \cap (C \times D) &\Leftrightarrow (x,y) \in (A \times B) \ \wedge \ (x,y) \in (C \times D)\\ &\Leftrightarrow (x \in A \ \wedge y \in B) \ \wedge \ (x \in C \ \wedge \ y \in D)\\ &\Leftrightarrow (x \in A \ \wedge x \in C) \ \wedge \ (y \in B \ \wedge \ y \in D)\\ &\Leftrightarrow (x \in A \cap C) \ \wedge \ (y \in B \cap D)\\ &\Leftrightarrow (x,y) \in (A \cap C) \times (B \cap D).\end{aligned}$$

Zbog čega ne možemo primijeniti isti dokaz u (d), tako da samo zamijenimo presjek unijom? Zbog toga što vrijedi samo

$$\begin{aligned}(x,y) \in (A \times B) \cup (C \times D) &\Leftrightarrow (x,y) \in (A \times B) \ \vee \ (x,y) \in (C \times D)\\ &\Leftrightarrow (x \in A \ \wedge y \in B) \ \vee \ (x \in C \ \wedge \ y \in D)\\ &\Rightarrow (x \in A \ \vee x \in C) \ \wedge \ (y \in B \ \vee \ y \in D),\end{aligned}$$

a obrat zadnje implikacije općenito nije istinit (dokažite to!). □

Osim uređenih parova, možemo promatrati i u uređene trojke, četvorke, i tako dalje. Općenito, za skupove $A_1, A_2, \ldots, A_n$ definiramo UREĐENU n-TORKU $(a_1, a_2, \ldots, a_n)$ gdje je $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$. Dvoje n-torke $(a_1, a_2, \ldots, a_n)$ i $(b_1, b_2, \ldots, b_n)$ su JEDNAKE ako vrijedi $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. Nadalje, KARTEZIJEV PRODUKT skupova $A_1, A_2, \ldots, A_n$ definiramo kao skup svih uređenih n-torki:

$$\begin{aligned}&A_1 \times A_2 \times \ldots \times A_n\\ &\qquad := \{(a_1, a_2, \ldots, a_n) \ : \ a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.\end{aligned}$$

Na primjer, za $A = [0,1]$ je $A^3 := A \times A \times A = \{(x,y,z) \ : \ x,y,z \in [0,1]\}$, što možemo skicirati kao jediničnu kocku u prostoru.

Za kraj, uočimo jedan mali detalj. Iz naših definicija Kartezijevog skupa slijedi:

$$(A \times B) \times C \neq A \times (B \times C) \neq A \times B \times C.$$

Naime, ako su $a \in A$, $b \in B$ i $c \in C$, onda je

$$\begin{aligned}((a,b),c) &\in (A \times B) \times C,\\ (a,(b,c)) &\in A \times (B \times C),\\ (a,b,c) &\in A \times B \times C;\end{aligned}$$

dakle, elementi skupa $(A \times B) \times C$ imaju kao prvi član uređeni par $(a,b) \in A \times B$, a elementi skupa $A \times (B \times C)$ imaju kao prvi član $a \in A$. Kartezijev produkt nije asocijativan.

2.6 *Russellov paradoks i preostali aksiomi teorije skupova*

Za kraj ovog poglavlja, pokažimo da pravila koja smo uveli mogu spriječiti pojavu nekih paradoksa. Također, navest ćemo i ostala aksiome koji upotpunjuju Zermelo-Frankelov sustav. Aksiome nećemo formulirati posve precizno, već ćemo ispustiti neke (bitne) detalje, pa ćemo ih i dalje nazivati pravilima. Ova sekcija je informativnog tipa i sadrži neke naprednije koncepte, te se može preskočiti.

Primjer 2.24. *(Russellov paradoks) Već smo ranije vidjeli da elementi skupova mogu biti ponovno skupovi. Postoje li možda skupovi koji su sami sebi element? To bi bilo malo neobično, ali $P(x) =$ "$x \notin x$" je sasvim legitiman predikat (koji je istinit za sve skupove koje smo dosad promatrali). Promotrimo sada kolekciju S definiranu ovako:*

$$S = \{x \,:\, P(x)\} = \{x \,:\, x \notin x\}$$

Dakle, gledamo sve one skupove koji nisu sami sebi elementi. Da li je i sam S takav skup?

(1) Pretpostavimo da je $S \in S$. Kako se u S nalaze svi x za koje vrijedi $P(x)$, zbog $S \in S$ onda mora biti istinito $P(S)$. Ali, $P(S) =$ "$S \notin S$", što je kontradikcija s pretpostavkom $S \in S$.

(2) Pretpostavimo da je $S \notin S$. Dakle, vrijedi $P(S)$, a kako se u S nalaze svi x za koje vrijedi $P(x)$, slijedi da je i $S \in S$. No to je kontradikcija s pretpostavkom $S \notin S$.

Kako je moguće da ne vrijedi niti $S \in S$ niti $S \notin S$?

Russellov paradoks ima zgodnu i lako razumljivu formulaciju "iz stvarnog života". Zamislimo selo u kojem živi jedan brijač. Brijač brije sve one ljude koji ne briju sami sebe i ne brije nikog drugog. Da li brijač brije sam sebe? I prepostavka da brije sam sebe i pretpostavka da ne brije sam sebe vode na kontradikciju! Rješenje ovog paradoksa je isto kao u formulaciji sa skupovima: selo s takvim svojstvom *ne postoji*.

Rješenje Russelovog paradoksa je vrlo jednostavno: kolekcije poput S neće biti skupovi. Odnosno, aksiomi teorije skupova moraju biti takvi da se pomoću njih nikada ne može napraviti kolekcija poput S. U Pravilu S4 smo zahtijevali da svi objekti koji zadovoljavaju svojstvo $P(x)$ moraju dolaziti iz nekog skupa A. Sada smo vidjeli što se događa ako uklonimo ograničenje da elementi moraju dolaziti iz nekog skupa i promatramo *sve objekte* koji zadovoljavaju $P(x)$—dolazi do paradoksa.

Slično, pojmovi poput "skup svih skupova" također vode na paradokse. Uočite da pomoću pravila ne možemo napraviti takav "skup", kao ni skup S iz Primjera 2.24.

U sustavu aksioma postoji još jedno pravilo koji sprječava slične paradokse:

Pravilo S8. *Ako je A neprazan skup, onda postoji barem jedan element $x \in A$ takav da ili x nije skup ili vrijedi $x \cap A = \emptyset$.*

Kako bi mogli uopće nastati takvi skupovi? Pomoću Pravila S1-S8 ih ne možemo napraviti. Međutim, za neke matematičke teorije potrebni su mnogo složeniji skupovi zbog kojih je potrebno uvesti još neka dodatna pravila. Već smo spomenuli da smo prilikom definicija unije familije uveli ograničenje zahtjevom da svi elementi familije moraju biti podskupovi nekog univerzalnog skupa. To ograničenje se može ukloniti pomoću sljedeća dva pravila.

Pravilo S9. *Neka je A skup, a f funkcija koja svakom elementu od A pridružuje neki skup. Tada je kolekcija*

$$\{f(a) \,:\, a \in A\}$$

ponovno skup.

Na primjer, pretpostavimo da imamo skupove $A_1, A_2, \ldots, A_n, \ldots$ Znamo da je $\mathbb{N}$ skup, pa promotrimo funkciju takvu da je $f(n) = A_n$ za svaki $n \in \mathbb{N}$. Sada iz Pravila S9 slijedi da je $\{A_1, A_2, \ldots, A_n, \ldots\}$ zaista skup, bez zahtjeva $A_n \subseteq U$ za svako $n \in \mathbb{N}$. Na posve analogan način možemo pokazati da je bilo koja indeksirana familija skupova i sama skup. No sada nam je potrebno i pravilo unije proizvoljne familije skupova:

Pravilo S10. *Neka je $\mathcal{F}$ familija skupova. Tada postoji skup S za koji vrijedi*

$$x \in S \;\Leftrightarrow (\exists A \in \mathcal{F})\; x \in A.$$

Skup S označavamo sa $\bigcup_{A \in \mathcal{F}} A$.

Posljednje pravilo je tzv. aksiom izbora. Opišimo prvo riječima jedan vrlo jednostavan oblik ovog aksioma: zamislimo da imamo nekoliko nepraznih i disjunktnih skupova: $A_1 = \{2,5,7\}$, $A_2 = \{1,6\}$, $A_3 = \{4,8\}$. Aksiom izbora kaže da postoji skup X koji sadrži točno jedan element iz A_1, jedan element iz A_2 i jedan element iz A_3. Na primjer, $X = \{1,5,8\}$—no ključni detalj je da aksiom ne daje sam skup X niti način kako ga napraviti, nego samo kaže da takav skup postoji. Formalna definicija dozvoljava da napravimo skup koji sadrži po jedan element iz svakog člana bilo koje familije skupova.

Pravilo S11. *Neka je $\mathcal{F}$ neprazna familija u parovima disjunktnih nepraznih skupova. Tada postoji skup X za koji vrijedi*

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

Naizgled, ovo je jedan vrlo prirodan i jednostavan aksiom, koji nam često može pomoći da dobijemo željene skupove. I zaista, u brojnim granama matematike nije moguće izbjeći ovaj aksiom da bi se dokazali neki fundamentalni rezultati (na primjer: "Svaki vektorski prostor ima bazu.") Međutim, korištenjem ovog aksioma mogu se dobiti neke paradoksalne tvrdnje—najpoznatija je tzv. Banach-Tarskijev paradoks. Zbog toga je običaj da se uz svaki dokaz teorema koji koristi aksiom izbora eksplicitno istakne ta činjenica.

Popularna formulacija Banach-Tarskijevog paradoksa je sljedeća: zamislimo da imamo jednu naranču, te ju na izvjestan način podijelimo na 5 dijelova. Nakon toga te dijelove na izvjestan način pomičemo (translatiramo i rotiramo) u prostoru. Koristeći taj postupak, moguće je dobiti dvije naranče koje su u potpunosti identične početnoj! To je paradoks, jer se translacijama i rotacijama ne može promijeniti volumen.

2.7 Zadaci

Zadatak 2.1. *U ovom zadatku ćemo pokazati kako pomoću pravila možemo definirati pojam Kartezijevog produkta dvaju skupova. Neka su X i Y skupovi. Za $x \in X$ i $y \in Y$, definiramo $(x, y) := \{\{x\}, \{x, y\}\}$.*

Ovdje zapravo pokazujemo da nam ne treba novi simbol (x, y), nego da je taj simbol samo kraći zapis za $\{x, \{x, y\}\}$. Također, dokazujemo da je kolekcija svih (x, y), gdje je $x \in X$ i $y \in Y$, skup, za koji onda uvodimo oznaku $X \times Y$.

(a) Dokažite da za $x_1, x_2 \in X$ i $y_1, y_2 \in Y$ vrijedi

$$(x_1, y_1) = (x_2, y_2) \Leftrightarrow (x_1 = x_2 \wedge y_1 = y_2).$$

Oprez, X i Y ne moraju biti disjunktni!

(b) Dokažite da je $(x, y) \in \mathcal{P}(\mathcal{P}(X \cup Y))$.

Kao Kartezijev produkt skupova X i Y tada možemo definirati skup svih elemenata tog partitivnog skupa koji imaju upravo oblik kao (x, y):

$$X \times Y := \{S \in \mathcal{P}(\mathcal{P}(X \cup Y)) \ : P(S)\},$$

pri čemu je predikat $P(S)$ dan sa:

$$P(S) \equiv (\exists x \in X)(\exists y \in Y)\ S = \{\{x\}, \{x, y\}\}.$$

Dakle, iskoristili smo Pravilo S6 i Pravilo S4 kako bismo pokazali da je $X \times Y$ skup.

3
Relacije

U prethodnom poglavlju smo upoznali pojam uređenog para i Kartezijevog produkta dvaju skupova. Ti pojmovi će nam sada poslužiti za proučavanje jednog novog važnog pojma, koji će se vrlo često javljati u ovom i drugim kolegijima: pojam relacije.

Ako su zadana dva skupa A i B, te ako želimo reći da su neki elementi skupa A na izvjestan način povezani s nekim elementima skupa B, onda je to prirodno izraziti koristeći podskup Kartezijevog produkta $A \times B$. Na primjer, neka je $A = \{\text{Ana}, \text{Marko}, \text{Maja}\}$ skup studenata, a $B = \{\text{EM1}, \text{MA1}, \text{Prog1}\}$ skup kolegija koje ti studenti slušaju. Zamislimo da Ana i Marko vole kolegij EM1, Maja voli Prog1. Ovu činjenicu možemo "matematički" zapisati kao skup koji se sastoji od tri uređena para—svaki par sadrži ime jednog studenta i jednog kolegija kojeg taj student voli:

$$\text{voli} = \{(\text{Ana}, \text{EM1}),\ (\text{Marko}, \text{EM1}),\ (\text{Maja}, \text{Prog1})\}.$$

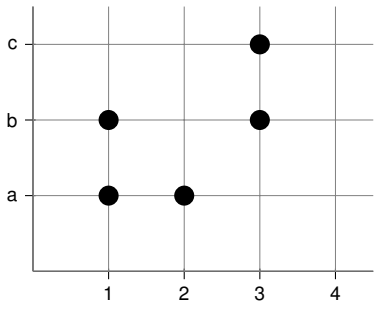
3.1 Pojam relacije

Definicija 3.1. *Neka su A i B skupovi. Podskup $\rho \subseteq A \times B$ zovemo* RELACIJA.
Ako $(a, b) \in \rho$, kažemo da "a je u relaciji ρ sa b" i pišemo: $a\ \rho\ b$.
Ako $(a, b) \notin \rho$, kažemo da "a nije u relaciji ρ sa b" i pišemo: $a \not\rho b$.

Pogledajmo još jedan primjer: stavimo $A = \{1, 2, 3, 4\}$ i $B = \{a, b, c\}$. Tada je

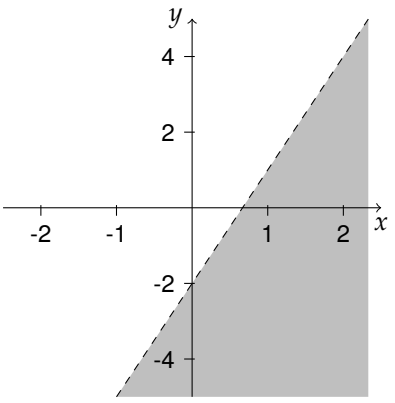
$$\rho = \{(1, a),\ (1, b),\ (2, a),\ (3, b),\ (3, c)\}$$

jedna relacija. Relacije možemo prikazivati u koordinatnom sustavu ovako: na x-osi navedemo sve elemente skupa A, a na y-osi sve elemente skupa B. Tada označimo sve uređene parove koji se nalaze u relaciji. U koordinatnom sustavu možemo prikazivati i relacije $\rho \subseteq \mathbb{R} \times \mathbb{R}$; pogledajte Sliku 3.2.

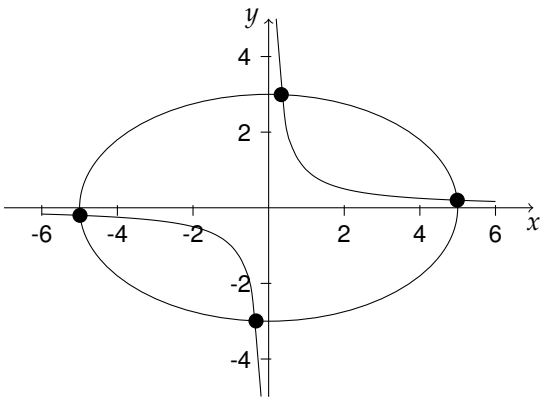


Slika 3.1: Prikaz relacije ρ u koordinatnom sustavu.

Napomenimo da pojamo relacije možemo poopćiti i na Kartezijeve produkte više skupova. Ako su $A_1, A_2, \ldots, A_n$ skupovi, onda ćemo reći da je $\rho \subseteq A_1 \times A_2 \times \ldots \times A_n$ jedna n-ARNA RELACIJA. Specijalno, kada je $n = 2$ (što je situacija opisana u Definiciji 3.1), kažemo da je ρ BINARNA RELACIJA. Ukoliko je $\rho \subseteq A \times A$, onda kažemo da je ρ RELACIJA NA SKUPU A.



(a) $\rho = \{(x,y) \in \mathbb{R} \times \mathbb{R} \ : \ y < 3x - 2\}$



(b) $\rho = \{(x,y) \in \mathbb{R} \times \mathbb{R} \ : \ \frac{x^2}{25} + \frac{y^2}{9} = 1 \ \wedge \ xy = 1\}$

Slika 3.2: Dvije relacije $\rho \subseteq \mathbb{R} \times \mathbb{R}$ prikazane u ravnini. Na lijevoj slici, relaciji pripadaju sve sivo osjenčane točke ravnine. Na desnoj slici, relaciji pripadaju samo četiri točke koje se nalaze na presjeku elipse i hiperbole.

Mnoge relacije koje se javljaju u nastavku će imati posebna svojstva, od kojih neka navodimo u sljedećoj definiciji.

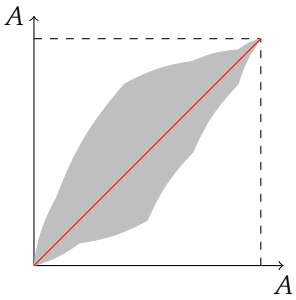
Definicija 3.2. *Neka je A skup i neka je ρ binarna relacija na A. Kažemo da je ρ:*

(a) REFLEKSIVNA *ako vrijedi:*
$(\forall x \in A)\ (x,x) \in \rho$;

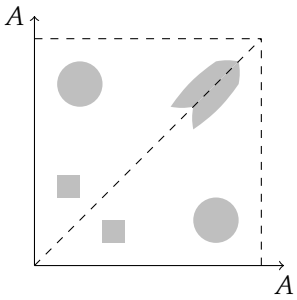
(b) SIMETRIČNA *ako vrijedi:*
$(\forall x,y \in A)\ \Big((x,y) \in \rho \ \Rightarrow \ (y,x) \in \rho\ \Big)$;

(c) ANTISIMETRIČNA *ako vrijedi:*
$(\forall x,y \in A)\ \Big(((x,y) \in \rho \ \wedge \ (y,x) \in \rho) \ \Rightarrow \ x = y\Big)$;

(d) TRANZITIVNA *ako vrijedi:*
$(\forall x,y,z \in A)\ \Big(((x,y) \in \rho \ \wedge \ (y,z) \in \rho) \Rightarrow \ (x,z) \in \rho\Big)$.



(a) Refleksivna relacija ρ na skupu A: dijagonala od $A \times A$ je podskup od ρ.



(b) Simetrična relacija ρ na skupu A: prikaz u ravnini je simetričan s obzirom na dijagonalu.

Slika 3.3: Prikaz refleksivne i simetrične relacije u koordinatnom sustavu. Tranzitivne relacije nije lako prepoznati samo na temelju prikaza u koordinatnom sustavu.

Primjer 3.3. *Promotrimo sada nekoliko primjera relacija, te proučimo koja od svojstava iz prethodne definicije zadovoljavaju.*

(a) Na skupu $\mathbb{R}$ promotrimo relaciju "biti manji ili jednak", odnosno, relaciju $\leq$. Tada je relacija $\leq$:

(1) *refleksivna, jer za svaki* $a \in \mathbb{R}$ *vrijedi* $a \leq a$;

(2) *nije simetrična*[1] *: na primjer, vrijedi* $3 \leq 5$, *ali ne vrijedi* $5 \leq 3$;

(3) *antisimetrična, jer ako je* $a \leq b$ *i* $b \leq a$, *onda slijedi* $a = b$;

(4) *tranzitivna, jer iz* $a \leq b$ *i* $b \leq c$ *slijedi* $a \leq c$.

[1] Ovdje koristimo negaciju definicije simetrične relacije: relacija *nije* simetrična ako

$$(\exists x \in A)(\exists y \in A)\ (x,y) \in \rho \wedge (y,x) \notin \rho.$$

(b) Na skupu $\mathbb{R}$ *promotrimo relaciju "biti manji", odnosno, relaciju* $<$. *Tada relacija* $<$:

(1) *nije refleksivna*[2] *: na primjer, ne vrijedi* $3 < 3$;

(2) *nije simetrična: na primjer, vrijedi* $3 < 5$, *ali ne vrijedi* $5 < 3$;

(3) *antisimetrična*[3] *, jer ako je* $a < b$ *i* $b < a$, *onda slijedi* $a = b$;

(4) *tranzitivna, jer iz* $a < b$ *i* $b < c$ *slijedi* $a < c$.

[2] Ovdje koristimo negaciju definicije refleksivne relacije: relacija *nije* refleksivna ako

$$(\exists x \in A)(x,x) \notin \rho.$$

[3] Uočite da je tvrdnja $a < b \wedge b < a$ uvijek lažna, pa iz nje možemo implicirati bilo što, uključujući i $a = b$.

(c) Na skupu $\mathbb{Z} \setminus \{0\}$ *promotrimo relaciju "dijeli", odnosno, relaciju* $|$. *Tada je relacija* $|$:

(1) *refleksivna, jer za svaki* $a \in \mathbb{Z} \setminus \{0\}$ *vrijedi* $a \mid a$;

(2) *nije simetrična: na primjer, vrijedi* $3 \mid 6$, *ali ne vrijedi* $6 \mid 3$;

(3) *nije antisimetrična: na primjer,* $-2 \mid 2$ *i* $2 \mid -2$, *ali* $2 \neq -2$;

(4) *tranzitivna, jer iz* $a \mid b$ *i* $b \mid c$ *slijedi* $a \mid c$.

(d) Na skupu $\mathbb{N}$ *promotrimo relaciju "dijeli", odnosno, relaciju* $|$. *Tada je relacija* $|$:

(1) *refleksivna, jer za svaki* $a \in \mathbb{N}$ *vrijedi* $a \mid a$;

(2) *nije simetrična: na primjer, vrijedi* $3 \mid 6$, *ali ne vrijedi* $6 \mid 3$;

(3) *antisimetrična, jer za sve* $a, b \in \mathbb{N}$ *iz* $a \mid b$ *i* $b \mid a$ *slijedi* $a = b$;

(4) *tranzitivna, jer iz* $a \mid b$ *i* $b \mid c$ *slijedi* $a \mid c$.

(e) Na skupu svih pravaca u ravnini, promotrimo relaciju "biti paralelan", odnosno, relaciju $\parallel$. *Tada je relacija* $\parallel$:

(1) *refleksivna, jer za svaki pravac* p *vrijedi* $p \parallel p$;

(2) *simetrična, jer ako vrijedi* $p \parallel q$, *onda je i* $q \parallel p$;

(3) *nije antisimetrična: uzmimo dva različita paralelna pravca* p *i* q. *Tada je* $p \parallel q$ *i* $q \parallel p$, *ali ne i* $p = q$;

(4) *tranzitivna, jer ako* $p \parallel q$ *i* $q \parallel r$ *onda vrijedi i* $p \parallel r$.

(f) Na skupu svih pravaca u ravnini, promotrimo relaciju "biti okomit", odnosno, relaciju $\perp$. *Tada relacija* $\perp$:

(1) *nije refleksivna: uzmimo bilo koji pravac* p. *Tada ne vrijedi* $p \perp p$;

(2) *simetrična, jer ako vrijedi* $p \perp q$, *onda je i* $q \perp p$;

(3) *nije antisimetrična: uzmimo bilo koja dva okomita pravca* p *i* q. *Tada je* $p \perp q$ *i* $q \perp p$, *ali ne i* $p = q$;

(4) *nije tranzitivna: uzmimo bilo koje pravce* p, q *i* r *takve da je* $p \perp q$ *i* $q \perp r$. *Tada vrijedi* $p \parallel r$, *odnosno, ne vrijedi* $p \perp r$.

(g) Na skupu svih trokutova u ravnini, promotrimo relaciju "biti sukladan", odnosno, relaciju $\cong$. *Tada je relacija* $\cong$:

(1) *refleksivna, jer za svaki trokut A vrijedi $A \cong A$;*

(2) *simetrična, jer ako vrijedi $A \cong B$, onda je i $B \cong A$;*

(3) *nije antisimetrična: uzmimo bilo koja dva različita, ali sukladna trokuta A i B. Tada je $A \cong B$ i $B \cong A$, ali ne i $A = B$;*

(4) *tranzitivna, jer ako vrijedi $A \cong B$ i $B \cong C$, onda je i $A \cong C$.*

(h) Neka je S skup. Na skupu $\mathcal{P}(S)$ definiramo relaciju "biti podskup", odnosno, relaciju $\subseteq$. Tada je relacija $\subseteq$:

(1) *refleksivna, jer za svaki $A \in \mathcal{P}(S)$ vrijedi $A \subseteq A$;*

(2) *općenito nije simetrična, jer ako vrijedi $A \subseteq B$, ne mora nužno biti $B \subseteq A$;*

(3) *antisimetrična, jer ako je $A \subseteq B$ i $B \subseteq A$, onda slijedi $B = A$;*

(4) *tranzitivna, jer iz $A \subseteq B$ i $B \subseteq C$ slijedi $A \subseteq C$.*

3.2 *Relacije ekvivalencije*

U prethodnom primjeru možemo uočiti da su relacija "biti paralelan" na skupu svih pravaca u ravnini, kao i relacija "biti sukladan" na skupu svih trokuta u ravnini istovremeno refleksivne, simetrične i tranzitivne. Relacije koje imaju sva ova tri svojstva se vrlo često pojavljuju i zbog toga zaslužuju zaseban naziv.

Definicija 3.4. *Relaciju koja je refleksivna, simetrična i tranzitivna zovemo* RELACIJA EKVIVALENCIJE.

Ako je na nekom skupu A dana relacija ekvivalencije, onda će skup svih elemenata koji su u relaciji s nekim elementom $a \in A$ imati posebna svojstva. U nekom smislu, moći ćemo sve takve elemente poistovjetiti s elementom a: u odgovarajućem kontekstu, bit će posve svejedno koji od tih elemenata koristimo, te ćemo uvijek dobivati isti rezultat. U ovu, zasad apstraktnu tvrdnju, ćemo se mnogo puta uvjeriti u nadolazećim poglavljima.

Definicija 3.5. *Neka je $\sim$ relacija ekvivalencije na nepraznom skupu A, te neka je $a \in A$. Skup*

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

zovemo KLASA EKVIVALENCIJE *elementa a. Nadalje, kažemo da je a* REPREZENTANT *klase $[a]$. Skup svih klasa ekvivalencije zovemo* KVOCIJENTNI SKUP *i označavamo ga sa*

$$A/_{\sim} := \{[a] \ : \ a \in A\}.$$

Promotrimo prvo nekoliko primjera.

Primjer 3.6. *Neka je $A = \{1, 2, 3\}$. Definirajmo relaciju $\sim$ ovako:*

$$\sim = \{(1,1),\ (2,2),\ (3,3),\ (1,2),\ (2,1)\}.$$

Lako se provjeri da je $\sim$ relacija ekvivalencije na A. Njezine klase su:

$$[1] = [2] = \{1,\ 2\},$$
$$[3] = \{3\}.$$

Dakle, $A/_{\sim} = \{\{1,2\},\ \{3\}\}$.

Primjer 3.7. *Neka je A skup svih pravaca u ravnini. Promotrimo relaciju $\parallel$, "biti paralelan". Već smo ranije vidjeli da je to relacija ekvivalencije. Za zadani pravac p, što je $[p]$? To je skup svih elemenata od A koji su u relaciji sa p—dakle, to je skup svih pravaca q koji su paralelni sa p:*

$$[p] = \{q \in A\ :\ p \parallel q\}.$$

Po definiciji, $A/_{\parallel} = \{[p]\ :\ p \in A\}$. Intuitivno, svaka klasa predstavlja jedan smjer u ravnini jer svi paralelni pravci pripadaju istoj klasi. Tako možemo reći da je $A/_{\parallel}$ skup svih smjerova u ravnini. Uoči: svaki pravac pripada točno jednoj klasi!

U prethodna dva primjera možemo vidjeti da za bilo koja dva elementa skupa A vrijedi da su njihove klase ili jednake ili disjunktne. To će uvijek biti slučaj sa relacijama ekvivalencije.

Teorem 3.8. *Neka je $\sim$ relacija ekvivalencije na skupu A, te neka su $x, y \in A$ proizvoljni. Tada:*

(a) $x \in [x]$;

(b) ako $x \not\sim y$, onda $[x] \cap [y] = \emptyset$;

(c) ako $x \sim y$, onda $[x] = [y]$.

Dokaz.

(a) Relacija $\sim$ je refleksivna, pa za svaki $x \in A$ vrijedi $x \sim x$. Kako se u $[x]$ nalazi svi elementi koji su u relaciji sa x, slijedi $x \in [x]$.

(b) Neka je $x \not\sim y$. Pretpostavimo suprotno, tj. da $[x] \cap [y] \neq \emptyset$. Dakle, postoji neki $z \in A$ takav da je $z \in [x] \cap [y]$. Kako je $z \in [x]$, slijedi $x \sim z$. Kako je $z \in [y]$, slijedi $y \sim z$, pa zbog simetričnosti relacije $\sim$ imamo i $z \sim y$. No zbog tranzitivnosti iz $x \sim z$ i $z \sim y$ slijedi $x \sim y$, što je kontradikcija. Dakle, $[x] \cap [y] = \emptyset$.

(c) Neka je $x \sim y$. Treba dokazati $[x] = [y]$, odnosno, $[x] \subseteq [y]$ i $[y] \subseteq [x]$. Pokažimo prvu inkluziju; druga slijedi posve analogno. Neka je $z \in [x]$. Trebamo dokazati da je tada $z \in [y]$. Iz $z \in [x]$ slijedi $x \sim z$, pa zbog simetričnosti imamo $z \sim x$. Ovo i $x \sim y$ zbog tranzitivnosti povlače $z \sim y$, a ponovnom primjenom simetričnosti dobivamo $y \sim z$, što znači $z \in [y]$.

□

Uočimo da je kvocijentni skup jedna familija skupova koja zadovoljava Definiciju 2.19 particije skupa. Dakle, ako imamo relaciju ekvivalencije na skupu A, onda pomoću nje možemo napraviti jednu particiju skupa A. Članovi te particije su upravo klase ekvivalencije.

Korolar 3.9. *Neka je A neprazan skup i $\sim$ relacija ekvivalencije na A. Tada je $A/_\sim$ particija skupa A.*

Međutim, možemo lako provesti i obratni postupak: ako imamo neku particiju skupa A, onda pomoću te particije možemo napraviti jednu relaciju ekvivalencije na A. Postupak kojeg ćemo sada opisati na primjeru će funkcionirati i općenito (vidi Zadatak 3.1). Neka je $A = \{1,2,3,4\}$, te neka je

$$\mathcal{F} = \{\{1\},\ \{2,3\},\ \{4\}\}.$$

Očito je $\mathcal{F}$ particija skupa A. Definirajmo relaciju $\sim$ na A ovako: za $a, b \in A$ neka je $a \sim b$ ako su a i b elementi istog člana particije $\mathcal{F}$. Dakle,

$$\sim = \{(1,1),\ (2,2),\ (3,3),\ (2,3),\ (3,2),\ (4,4)\}.$$

Lako se vidi da je $\sim$ relacija ekvivalencije sa klasama

$$[1] = \{1\},\ [2] = [3] = \{2,3\},\ [4] = \{4\}.$$

Dakle, klase ekvivalencije su upravo članovi particije i vrijedi $A/_\sim = \mathcal{F}$.

Za kraj ove cjeline pogledajmo još jedan primjer relacije ekvivalencije, u kojem se vidi tipičan način korištenja klasa ekvivalencije: nakon uvođenja relacije ekvivalencije definiramo operacije nad njezinim klasama, te nas nakon toga zanimaju samo klase, a ne i pojedini reprezentanti (elementi) tih klasa. Ovaj primjer ćemo puno detaljnije proučavati u kolegiju Elementarna matematika 2.

Primjer 3.10. *Neka je E^2 Euklidska ravnina; njezine elemente nazivamo točke u ravnini. Uvedimo još jedan zapis uređenih parova točaka: za točke $A, B \in E^2$ označimo $\overrightarrow{AB} := (A, B)$. Takve objekte zovemo orijentirane dužine. Promotrimo skup svih orijentiranih dužina:*

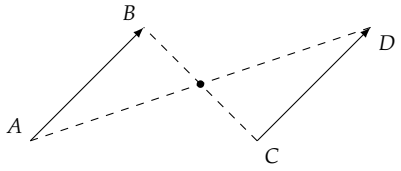
$$S := \{\overrightarrow{AB} \ :\ A, B \in E^2\},$$

te na S definirajmo relaciju $\sim$ ovako: $\overrightarrow{AB} \sim \overrightarrow{CD}$ ako dužine $\overline{AD}$ i $\overline{BC}$ imaju isto polovište.

Pokažite da je $\sim$ jedna relacija ekvivalencije na S. Kvocijentni skup $S/_\sim$ označavamo sa V^2, a njegove elemente zovemo vektori:

$$\vec{a} = [\overrightarrow{AB}] = \{\overrightarrow{CD} \in S \ :\ \overrightarrow{AB} \sim \overrightarrow{CD}\};$$
$$\vec{0} = [\overrightarrow{AA}] = \{\overrightarrow{CD} \in S \ :\ \overrightarrow{AA} \sim \overrightarrow{CD}\} = \{\overrightarrow{CC} \in S \ :\ C \in E^2\}.$$

Ovdje smo pokazali kako definirati nul-vektor $\vec{0}$. Na skupu svih vektora možemo uvesti uobičajene operacije zbrajanja i skalarnog i vektorskog množenja. Dakle, te operacije ćemo definirati na klasama ekvivalencije, a ne na orijentiranim dužinama: govorit ćemo o zbrajanju i množenju vektora, a ne o zbrajanju i množenju orijentiranih dužina.



Slika 3.4: Orijentirane dužine $\overrightarrow{AB}$ i $\overrightarrow{CD}$ su u relaciji: $\overrightarrow{AB} \sim \overrightarrow{CD}$. Alternativno, mogli bismo reći da su $\overrightarrow{AB}$ i $\overrightarrow{CD}$ u relaciji ako je $ABDC$ paralelogram, no to ne pokriva slučaj kada su sve četiri točke na istom pravcu.

3.3 Relacije parcijalnog uređaja

Poput relacija ekvivalencije, često se pojavljuju i relacije koje ispunjavaju drugu grupu svojstava: istovremeno su refleksivne, antisimetrične i tranzitivne. Ako pogledamo Primjer 3.3, takve su bile relacija $\leq$ na $\mathbb{R}$, relacija "dijeli" na $\mathbb{N}$ i relacija $\subseteq$ na $\mathcal{P}(S)$.

Sve ove relacije nas podsjećaju na relaciju "biti manji" u nekom smislu: zbog $8 \mid 24$ možemo reći da je 8 "manji" od 24 jer je njegov faktor; zbog $\{1,2\} \subseteq \{0,1,2,3\}$ možemo reći da je $\{1,2\}$ "manji" od $\{0,1,2,3\}$.

Definicija 3.11. *Neka je ρ relacija na skupu A. Ako je ρ refleksivna, antisimetrična i tranzitivna, onda kažemo da je ρ* RELACIJA PARCIJALNOG UREĐAJA *ili jednostavno* PARCIJALNI UREĐAJ. *Ako još vrijedi:*

$$(\forall x, y \in A)\ \Big((x\ \rho\ y)\ \vee\ (y\ \rho\ x)\Big), \tag{3.1}$$

onda ρ zovemo RELACIJA TOTALNOG UREĐAJA *ili* TOTALNI UREĐAJ. *Skup A zajedno s totalnim uređajem ρ zovemo* (TOTALNO) UREĐENI SKUP.

Često još kažemo da je ρ LINEARNI UREĐAJ.

Pogledajmo koje su od spomenutih relacija ujedno i relacije parcijalnog, a koje relacije totalnog uređaja.

Primjer 3.12. *(a) Skup $\mathbb{R}$ zajedno s relacijom $\leq$ je uređeni skup, jer je $\leq$ relacija totalnog uređaja. Naime, već smo ranije vidjeli da je $\leq$ relacija parcijalnog uređaja jer je refleksivna, antisimetrična i tranzitivna. Sada još uočavamo da za bilo koja dva broja $x, y \in \mathbb{R}$ uvijek vrijedi ili $x \leq y$ ili $y \leq x$ (ili oboje). Zato je $\leq$ totalni uređaj.*

(b) Već smo ranije vidjeli da je relacija "dijeli" na skupu $\mathbb{N}$ jedna relacija parcijalnog uređaja. Međutim, to nije relacija totalnog uređaja: za brojeve 5 i 7 ne vrijedi niti $5 \mid 7$ niti $7 \mid 5$.

Da pokažemo da nešto nije relacija totalnog uređaja, koristimo negaciju od (3.1):

$$(\exists x, y \in A)\ \Big(\neg(x\ \rho\ y)\ \wedge\ \neg(y\ \rho\ x)\Big).$$

(c) Ako je $S \neq \emptyset$ skup, onda je $\subseteq$ relacija parcijalnog uređaja na $\mathcal{P}(S)$, ali nije nužno relacija totalnog uređaja. Na primjer, neka je $S = \{1,2,3\}$. Uočimo da je $\{1,2\} \in \mathcal{P}(S)$ i $\{1,3\} \in \mathcal{P}(S)$, ali ne vrijedi $\{1,2\} \subseteq \{1,3\}$ niti $\{1,3\} \subseteq \{1,2\}$. Za koje sve skupove S relacija $\subseteq$ je totalni uređaj na $\mathcal{P}(S)$?

Sljedeći pojmovi se često javljaju u matematičkoj analizi.

Definicija 3.13. *Neka je ρ relacija parcijalnog uređaja na skupu A i neka je $B \subseteq A$. Kažemo da je $a \in A$* DONJA MEĐA *skupa B ako*

$$(\forall b \in B)\ a\ \rho\ b.$$

Element $a \in A$ je NAJVEĆA DONJA MEĐA *ili* INFIMUM *skupa B ako vrijedi:*

(1) a je donja međa skupa B;

(2) za svaku donju među $x \in A$ skupa B vrijedi $x\ \rho\ a$.

Pišemo $a = \inf B$.

Definicija 3.14. *Neka je ρ relacija parcijalnog uređaja na skupu A i neka je $B \subseteq A$. Kažemo da je $a \in A$* GORNJA MEĐA *skupa B ako*

$$(\forall b \in B)\ b\ \rho\ a.$$

Element $a \in A$ je NAJMANJA GORNJA MEĐA *ili* SUPREMUM *skupa B ako vrijedi:*

(1) a je gornja međa skupa B;

(2) za svaku gornju među $x \in A$ skupa B vrijedi $a \rho x$.

Pišemo $a = \sup B$.

Promotrimo ponovno nekoliko primjera.

Primjer 3.15.

(a) Promotrimo totalni uređaj $\leq$ na skupu $\mathbb{R}$. Tada:

$$A = \{-10,\ 1,\ 3,\ 5,\ 10,\ 12\} \ \Rightarrow\ \inf A = -10,\ \sup A = 12;$$
$$B = [1,2\rangle \ \Rightarrow\ \inf B = 1,\ \sup B = 2;$$
$$C = \mathbb{N} \ \Rightarrow\ \inf C = 1,\ \sup C \text{ ne postoji.}$$

(b) Promotrimo parcijalni uređaj $\subseteq$ na skupu $\mathcal{P}(S)$, gdje je $S = \{1,\ 2,\ \ldots,\ 10\}$. Neka je

$$A = \{\{1,4,5,7\},\ \{1,4,7,8\},\ \{2,3,4,7\}\}.$$

Tada $\inf A = \{4,7\}$, *te* $\sup A = \{1,2,3,4,5,7,8\}$. *Uočimo da niti* $\inf A$ *niti* $\sup A$ *nisu elementi od A.*

(c) Promotrimo parcijalni uređaj $\subseteq$ na skupu $\mathcal{P}(\mathbb{R})$. Neka je

$$A = \{[-n,n] \ :\ n \in \mathbb{N} \cup \{0\}\}.$$

Tada je $\inf A = \{0\}$, *te* $\sup A = \mathbb{R}$.

Primijetimo da neki skup A ne može imati više infimuma niti supremuma. To vidimo ovako: pretpostavimo da su i a_1 i a_2 infimumi skupa A. Specijalno tada su i a_1 i a_2 donje međe od A. Kako je a_1 infimum, a a_2 donja međa, po definiciji infimuma mora vrijediti $a_2 \rho a_1$. Kako je a_2 infimum, a a_1 donja međa, po definiciji infimuma mora vrijediti $a_1 \rho a_2$. No relacija ρ je antisimetrična, pa slijedi $a_1 = a_2$. Slično se vidi i da je supremum, ako postoji, jedinstven.

Definicija 3.16. *Neka je ρ relacija parcijalnog uređaja na skupu A, te neka je $B \subseteq A$. Ako postoji* $\inf B$ *i vrijedi* $\inf B \in B$, *onda kažemo da je* $\inf B$ NAJMANJI ELEMENT *skupa B i taj element označavamo sa* $\min B$. *Ako postoji* $\sup B$ *i vrijedi* $\sup B \in B$, *onda kažemo da je* $\sup B$ NAJVEĆI ELEMENT *skupa B i taj element označavamo sa* $\max B$.

U Primjeru 3.15(a) vrijedi $\min A = -10$, $\max A = 12$, $\min B = 1$, $\max B$ ne postoji, $\min C = 1$, $\max C$ ne postoji. U Primjeru 3.15(b) skup nema niti najmanji niti najveći element, dok u (c) vrijedi $\min A = \{0\}$, a najveći element ne postoji.

Za kraj, uvedimo još jedan pojam vezan uz totalne uređaje.

Definicija 3.17. *Neka je ρ totalni uređaj na skupu A. Kažemo da je A* DOBRO UREĐEN *ako svaki neprazni podskup $B \subseteq A$ ima najmanji element (minimum).*

Na primjer:

(a) Skup $A = \{1,\ 2,\ 3,\ 4,\ 5\}$ je uz relaciju $\leq$ jedan dobro uređen skup.

(b) Skup svih negativnih cijelih brojeva uz relaciju $\leq$ nije dobro uređen.

(c) Skup $\mathbb{N}$ uz relaciju $\leq$ je dobro uređen.

3.4 Zadaci

Zadatak 3.1. *Neka je A skup i neka je $\mathcal{F}$ particija skupa A. Definirajmo relaciju $\sim$ na skupu A ovako:*

$$\sim := \{(x, y) \in A \times A \ :\ (\exists S \in \mathcal{F})\ \Big((x \in S) \wedge (y \in S)\Big)\}.$$

Dokažite da je $\sim$ relacija ekvivalencije, te da vrijedi $A/_{\sim} = \mathcal{F}$.

4
Skupovi brojeva

U ovom poglavlju bavit ćemo se skupovima brojeva. Glavni cilj bit će nam definirati brojeve, pripadne algebarske relacije i uređaj, te rigorozno dokazati njihova svojstva. Većina rezultata ovog poglavlja poznata je studenatima iz njihovog srednješkolskog obrazovanja.[1] Međutim, uočite da nije isto znati slijediti pravila za računanje s brojevima (koristiti pravila algebre) i razumjeti zašto ta pravila vrijede. U svrhu dokazivanja i razumijevanja tih svojstava najprije je potrebno definirati brojeve, tj. zadati njihova osnovna svojstva (aksiome) iz kojih ćemo moći dokazati sva ostala svojstva. U tom smislu u ovom poglavlju ćemo dokazati mnogo naizgled očitih tvrdnji.[2] Osim dubljeg razumijevanja brojeva, svrha ovog pristupa je i naučiti studente rigorozno razmišljati te prikazati razvoj matematičke teorije počevši od aksioma. Ovo poglavlje će većinom pratiti[3] knjigu T. Tao, Analysis I.[4]

[1] Pravila za računanje s brojevima - zbrajanje, oduzimanje, množenje, dijeljenje, uspoređivanje.

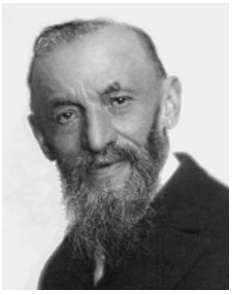
[2] Recimo prvi dokazani rezultat će glasiti da za sve prirodne brojeve a, b vrijedi $a + b = b + a$.

[3] Osim konstrukcije realnih i kompleksnih brojeva

[4] Terence Tao. *Analysis. I*, volume 37 of *Texts and Readings in Mathematics*. Hindustan Book Agency, New Delhi, third edition, 2014

4.1 Prirodni brojevi

Najprije ćemo krenuti od najosnovnijeg sistema brojeva - prirodnih brojeva. Intuitivno govoreći, želimo definirati skup $\mathbb{N} = \{1, 2, \dots\}$ sa pripadnim operacijama. Prirodne brojeve ćemo definirati na standardan način koristeći Peanove aksiome. Krenut ćemo od dva fundamentalna koncepta: broja 1 i funkcije sljedbenik s.



Guiseppe Peano (1858.–1932.), talijanski matematičar

Aksiom P1. 1 *je prirodan broj.*

Aksiom P2. *Ako je n prirodan broj, tada je i $s(n)$ prirodan broj.*

Aksiom P2 nam kaže da je sljedbenik prirodnog broja također prirodan broj. Koristeći prva dva aksioma možemo definirati prirodne brojeve $2 := s(1)$, $3 := s(2) = s(s(1))$, itd. Međutim, koristeći samo ova dva aksioma ne možemo dokazati npr. da je $3 \neq 1$. Naime, brojevni sustav koji se sastoji samo od brojeva 1 i 2, i funkcijom sljedbenik definiranom sa $s(1) = 2$, $s(2) = 1$ zadovoljava oba aksioma P1 i P2. Da bi izbjegli takvu situaciju dodajemo treći aksiom:

Aksiom P3. 1 *nije sljedbenik niti jednog prirodnog broja, tj.* $s(n) \neq 1$ *za svaki prirodan broj* n.

Uočite da dodavanje aksioma P3 ne isključuje patološki brojevni sustav u kojem vrijedi npr. $2 = 3$.[5]

[5] Definirajte $s(1) = 2$, $s(2) = 2$.

Aksiom P4. *Ako vrijedi $s(n) = s(m)$, tada je $m = n$.*[6]

[6] Drugim riječima s je injekcija.

Koristeći aksiome P1-P4 lako možemo dokazati da npr. vrijedi $3 \neq 5$.[7] Na kraju će nam trebati i aksiom koji kaže da su prirodni brojevi samo oni koji se mogu dobiti ponavljanjem postupka uzimanja sljedbenika od 1. Neformalno, želimo isključiti sljedeći skup $\{1, 1.5, 2, 2.5, \dots\}$. Također, potrebno je preciznije reći što mislimo sa "mogu se dobiti ponavljanjem postupka".

[7] Pretpostavimo suprotno, tj. $3 = 5$. Tada iz aksiomoma P4 imamo da vrijedi $2 = 4$. Ponovnim korištenjem istog aksioma zaključujemo da je $1 = 3$ što je u kontradikciji sa aksiomom P3.

Aksiom P5 (Aksiom matematičke indukcije)**.** *Neka je $S \subset \mathbb{N}$ takav da:*

1. $1 \in S$,
2. $(\forall n \in \mathbb{N})(n \in S \Rightarrow s(n) \in S)$.

Tada je $S = \mathbb{N}$.

Aksiom matematičke indukcije koristit ćemo ukoliko želimo dokazati da neko svojstvo vrijedi za sve prirodne brojeve. Aksiomi P1-P5 omogućuju nam i rekurzivne definicije.[8]

[8] a_1, $a_2 = f_1(a_1)$, $a_3 = f_2(a_2), \dots$

Dokažimo sada i teorem koji slijedi direktno iz aksioma P5 i koji ćemo često koristiti pri dokazivanju tvrdnji za prirodne brojeve:

Teorem 4.1 (Princip matematičke indukcije)**.** *Neka je $P(n)$ predikat koji ovisi o prirodnom broju $n \in \mathbb{N}$. Neka vrijedi:*

Baza*: $P(1)$ je istina.*

Korak*: Ako je $P(n)$ istina za neki $n \in \mathbb{N}$, onda je i $P(s(n))$ istina.*

Tada je $P(n)$ istina za svaki $n \in \mathbb{N}$.

Dokaz. Definirajmo skup $S = \{n \in \mathbb{N} : P(n) \text{ je istina}\}$. Tada vrijedi $1 \in S$ i $(\forall n \in \mathbb{N})(n \in S \Rightarrow s(n) \in S)$. Iz aksioma P5 slijedi $S = \mathbb{N}$, što je i tvrdnja teorema. □

Sada možemo definirati prvu složeniju operaciju na prirodnim brojevima[9]:

[9] Definicija je rekurzivna, tj. koristi Aksiom P5, vidi Zadatak 4.1

Definicija 4.2 (Zbrajanje prirodnih brojeva)**.** *Neka je $m \in \mathbb{N}$. Tada* ZBRAJANJE PRIRODNIH BROJEVA *definiramo na sljedeći način:*

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

Uočimo da iz definicije nije potpuno trivijalno dokazati niti komutativnost[10] zbrajanja. U tu svrhu dokažimo najprije sljedeće dvije leme:

[10] $a + b = b + a$, $a, b \in \mathbb{N}$

Lema 4.3. *Za svaki prirodan broj m vrijedi $1 + m = s(m)$.*[11]

[11] Iz definicije slijedi samo $m + 1 = s(m)$

Dokaz. Tvrdnju ćemo dokazati indukcijom. Iz Definicije 4.2 direktno slijedi $1 + 1 = s(1)$. Pretpostavimo sada da tvrdnja vrijedi za neki $n \in \mathbb{N}$, tj. $1 + n = s(n)$. Tada imamo:

$$1 + s(n) = (Def.\ 4.2) = s(1 + n) = (\text{pretp. indukcije}) = s(s(n)).$$

Koristeći aksiom matematičke indukcije, zaključujemo da tvrdnja vrijedi za svaki prirodan broj n. □

Lema 4.4. *Za sve prirodne brojeve m, n vrijedi $s(m) + n = s(m + n)$.*

Dokaz. Tvrdnju ćemo dokazati indukcijom po n (m je fiksan). Za $n = 1$, tvrdnja slijedi direktno iz Definicije 4.2.[12]

Pretpostavimo sada da tvrdnja vrijedi za neki n, tj. $s(m) + n = s(m + n)$. Dokaz ćemo završiti ukoliko pokažemo da tada vrijedi $s(m) + s(n) = s(m + s(n))$. Međutim, vrijedi:

$$s(m)+s(n) = (Def.\ 4.2) = s(s(m)+n) = (\text{pretp. indukcije}) = s(s(m+n))$$

$$= (Def.\ 4.2) = s(m+s(n)).$$

□

[12] $s(m) + 1 = s(s(m)) = s(m + 1)$

Propozicija 4.5 (Komutativnost zbrajanja prirodnih brojeva)**.** *Za sve prirodne brojeve n, $m \in \mathbb{N}$, vrijedi $m + n = n + m$.*

Dokaz. Fiksirajmo $m \in \mathbb{N}$ i tvrdnju dokazujemo indukcijom po n. Tvrdnja za $n = 1$ slijedi iz Leme 4.3 i Definicije 4.2.

Pretpostavimo sada da vrijedi $m + n = n + m$. Tada imamo:

$$m + s(n) = (Def.\ 4.2) = s(m + n) = (\text{pretp. indukcije}) = s(n + m)$$

$$= (Lema\ 4.4) = s(n) + m.$$

□

Koristeći slične argumente možemo dokazati:

Propozicija 4.6 (Asocijativnost zbrajanja prirodnih brojeva)**.** *Za sve prirodne brojeve $a, b, c \in \mathbb{N}$, vrijedi $(a + b) + c = a + (b + c)$.*[13]

[13] Zbog asocijativnosti možemo pisati samo $a + b + c$ budući da je svejedno kojim redom zbrajamo 3 priordna broja.

Dokažimo sada svojstvo kraćenja za zbrajanje.

Propozicija 4.7. *Neka su a, b, c prirodni brojevi takvi da vrijedi $a + c = b + c$. Tada je $a = b$.*[14]

[14] Uočite da oduzimanje još nismo definirali pa ovu propoziciju ne možemo dokazati tako da "oduzmemo" c od obje strane jednakosti!

Dokaz. Dokaz provodimo indukcijom po c. Baza indukcije $c = 1$ je ekvivalentna s Aksiomom P4. Pretpostavimo da tvrdnja vrijedi za neki c i provedimo korak indukcije:

$$a + s(c) = b + s(c) \underbrace{\Rightarrow}_{Def.\ 4.2} s(a + c) = s(b + c)$$

Dakle, $a + c = b + c$. Sada iz pretpostavke indukcije zaključujemo da $a = b$. □

Definicija 4.8 (Uređaj na $\mathbb{N}$)**.** *Neka su $m, n \in \mathbb{N}$. Kažemo da je n* MANJI ILI JEDNAK *m, pišemo $n \leq m$, ako i samo ako je $n = m$ ili postoji $c \in \mathbb{N}$ takav da $n + c = m$.*[15]

[15] Kažemo da je n strogo manji od m, pišemo $n < m$, akko $n \leq m$ i $n \neq m$.

Propozicija 4.9. *Relacija $\leq$ je parcijalni uređaj na skupu $\mathbb{N}$, tj. relacija $\leq$ je refleksivna, tranzitivna i antisimetrična.*

Dokaz. **Refleksivnost** je direktna posljedica Definicije 4.8.

Tranzitivnost. Neka su $a, b, c \in N$ takvi da vrijedi $a < b$ i $b < c$[16]. Iz

[16] Slučaj $a = b$ ili $b = c$ dokaže se analogno.

definicije slijedi da postoje $n_1, n_2 \in \mathbb{N}$ takvi da $a + n_1 = b$ i $b + n_2 = c$. Sada imamo:

$$a + (n_1 + n_2) = (Prop.\ 4.6) = (a + n_1) + n_2 = b + n_2 = c.$$

Dakle, $a < c$[17] čime je tranzitivnost dokazana.

Antisimetričnost. Neka su $a, b \in \mathbb{N}$ takvi da $a \leq b$ i $b \leq a$. Pretpostavimo suprotno, tj. $a \neq b$. Po Definiciji 4.8, zbog $a < b$ postoji $c \in \mathbb{N}$ takav da $a + c_1 = b$. S druge strane, vrijedi i $b < a$ pa postoji c_2 takava da $b + c_2 = a$. Kombinirajući ove dvije jednakosti dobivamo $a + c_1 + c_2 = a$, što je kontradikcija.[18] □

[17] $n_1 + n_2 \in \mathbb{N}$

[18] $a + c \neq a$, $a, c \in \mathbb{N}$. Dokažite!

Na sličan način može se dokazati i sljedeća propozicija koja povezuje uređaj i zbrajanje i čiji dokaz ćemo izostaviti:

Propozicija 4.10. *Neka su $a, b, c \in \mathbb{N}$. Tada vrijedi:*

1. *$a \leq b$ ako i samo ako $a + c \leq b + c$.*
2. *$a < b$ ako i samo ako $s(a) \leq b$.*

Često ćemo koristiti i sljedeću verziju principa matematičke indukcije:

Teorem 4.11 (Princip potpune matematičke indukcije)**.** *Neka je $P(n)$ predikat koji ovisi o prirodnom broju $n \in \mathbb{N}$. Neka vrijedi:*

Baza: *$P(1)$ je istina.*

Korak: *Ako je $n \in \mathbb{N}$ takav da su $P(1),\ P(2), \ldots, P(n)$ istiniti, onda je i $P(n+1)$ istina.*

Tada je $P(n)$ istina za svaki $n \in \mathbb{N}$.

Dokaz. Definiramo skup $S = \{n \in \mathbb{N} : P(1),\ P(2), \ldots, P(n)$ je istina$\}$. Dokaz je sada analogan dokazu Teorema 4.1. □

Propozicija 4.12. *Skup $\mathbb{N}$ je dobro uređen, tj. svaki neprazan podskup od $\mathbb{N}$ ima minimalni element.*

Dokaz. Pretpostavimo suprotno, tj. da postoji $T \neq \emptyset$ takav da T nema minimalni element. Definirajmo $S = \mathbb{N} \setminus T$. Koristeći Teorem 4.11 dokazat ćemo da $S = \mathbb{N}$:

Baza[19]**:** $1 \in S$. U suprotnom bi vrijedilo $1 \in T$ pa bi 1 bio minimalni element od T što je u kontradikciji s definicijom skupa T.

Korak: Pretpostavimo da $1, 2, \ldots, n \in S$ za neki $n \in \mathbb{N}$. Tada je i $n + 1 \in S$. Naime, u suprotnom bi $n + 1$ bio minimalni element[20] od T, što je kontradikcija. □

[19] Dokažite da vrijedi $1 \leq n$, $n \in \mathbb{N}$.

[20] $1, 2, \ldots, n \notin T$

Propozicija 4.13 (Trihotomija uređaja prirodnih brojeva)**.** *Neka su $a, b \in \mathbb{N}$. Tada je istinita točno jedna od sljedećih tvrdnji: $a < b$, $a = b$, $a > b$.*

Dokaz. Dokaz provodimo idukcijom po a.[21].

Baza: $a = 1 \leq b$. Ukoliko je $b = 1$ tada vrijedi $a = b$. Inače $a < b$.

Korak: Pretpostavimo da tvrdnja vrijedi za neko a. Ukoliko je $a < b$, onda je $s(a) \leq b$[22]. Ako vrijedi $a = b$ ili $a > b$ tada je $s(a) > b$.

□

[21] b je fiksan

[22] ili $a < b$ ili $a = b$

Definicija 4.14 (Množenje prirodnih brojeva)**.** *Neka je $m \in \mathbb{N}$. Tada* MNOŽENJE PRIRODNIH BROJEVA *definiramo na sljedeći način:*[23]

$$m \cdot 1 := m,$$

$$m \cdot s(n) := m \cdot n + m,\ n \in \mathbb{N}.$$

[23] Obično ćemo pisati mn umjesto $m \cdot n$

U sljedećoj propoziciji ćemo odmah navesti neka osnovna svojstva množenja. Dokaz propozicije provodi se indukcijom i sličan je dokazima svojstava zbrajanja pa ga izostavljamo.

Propozicija 4.15. *Neka su $a, b, c \in \mathbb{N}$. Tada vrijedi:*

1. $ab = ba$ *(komutativnost množenja),*
2. $(ab)c = a(bc)$ *(asocijativnost množenja),*
3. $\left.\begin{array}{r} a(b+c) = ab + ac, \\ (b+c)a = ba + ca \end{array}\right\}$ *(distributivnost množenja prema zbrajanju).*[24]

[24] Svojstvo distributivnosti nam grubo govoreći kaže da su ovako definirane operacije zbrajanja i množenja kompatibilne.

Sljedeća propozicija nam kaže da su uređaj i množenje također usklađeni.

Propozicija 4.16. *Neka su $a, b, c \in \mathbb{N}$ takvi da vrijedi $a < b$. Tada vrijedi $ac < bc$.*

Dokaz. Iz definicije uređaja slijedi da postoji $d \in \mathbb{N}$ takav da $a + d = b$. Sada iz distributivnosti množenja prema zbrajanju (Propozicija 4.15, 3) imamo

$$bc = (a + d)c = ac + dc.$$

Dakle, $ac < bc$. □

Korolar 4.17. *Neka su $a, b, c \in \mathbb{N}$ takvi da $ac = bc$. Tada je $a = b$.*

Dokaz. Iz Propozicije 4.13 slijedi da vrijedi točno jedna od sljedećih tvrdnji: $a < b$, $a = b$ i $a > b$. Međutim, po Propoziciji 4.16, tvrdnje $a < b$[25] i $a > b$[26] su u kontradikciji s pretpostavkom $ac = bc$. Dakle, ostaje samo mogućnost $a = b$, što je upravo tvrdnja korolara. □

[25] $ac < bc$
[26] $ac > bc$

Definicija 4.18. *Neka je $m \in \mathbb{N}$. Tada* POTENCIRANJE PRIRODNIH BROJEVA *definiramo na sljedeći način:*

$$m^1 := m,$$

$$m^{s(n)} := m^n \cdot m,\ n \in \mathbb{N}.$$

Napomena 4.19. *Skup $\mathbb{N}_0$ možemo neformalno definirati na sljedeći način:*

$$\mathbb{N}_0 = \{0, 1, 2, 3 \dots\}.$$

Međutim, uočite da skup $\mathbb{N}_0$ možemo također izgraditi iz Peanovih aksioma na potpuno analogan načina kao što smo izgradili skup $\mathbb{N}$. Jedina razlika je što će koncept 0 zamjeniti koncept 1 u Peanovim aksioima koji ostaju isti. Također, potrebno je modificirati inicijalni korak definicija operacija.[27] *Svi dokazani rezultati i dalje vrijede sa istim dokazima.*

[27] $n + 0 = 0$, $n \cdot 0 = 0$, $n^0 = 1$.

Ovo poglavlje ćemo završiti navođenjem dva primjera primjene principa matematičke indukcije, tj. Teorema 4.1 i 4.11.

Primjer 4.20. *Dokažimo da za svaki $n \in \mathbb{N}$ vrijedi:*

$$1+3+5+\cdots+(2n-1)=n^2.$$

Neka je $P(n) :=$ "$1+3+5+\cdots+(2n-1)=n^2$."
Baza: $P(1) =$ "$1=1^2$ je istina.
Korak: Pretpostavimo da je $P(n)$ istina za neko $n \in \mathbb{N}$. Tada

$$\underbrace{1+3+5+\cdots+(2n-1)}_{=n^2}+(2n+1)=n^2+2n+1=(n+1)^2.$$

Dakle, po principu matematičke indukcije (Teorem 4.1), $P(n)$ je istina za svako $n \in \mathbb{N}$, čime je tvrdnja dokazana.

Primjer 4.21. *Svaki $n \in \mathbb{N}$ može se zapisati u binarnom zapisu, tj. postoje $k \in \mathbb{N}_0$ i $c_0, c_1, \ldots, c_k \in \{0,1\}$ takvi da*

$$n = c_k 2^k + c_{k-1}2^{k-1} + \cdots + c_1 2 + c_0. \tag{4.1}$$

Neka je $P(n) :=$"broj n se može zapisati u binarnom zapisu (4.1).
Baza: $P(1)$ je istina jer $1 = 1$[28].
Korak: Pretpostavimo da za neki $n \in \mathbb{N}$ vrijede tvrdnje $P(1)$, $P(2)$, $\ldots$, $P(n)$. Cilj nam je dokazati da vrijedi $P(n+1)$. Broj $n+1$ je paran ili neparan. Promotrimo ta dva slučaja odvojeno:

[28] $k = 0$, $c_0 = 1$

- $n+1 = 2m$ za neki $m \in \mathbb{N}$. Uočite da vrijedi $m \leq n$[29]. Po pretpostavci indukcije vrijedi $P(m)$, tj. m se može zapisati u zapisu (4.1):
$$m = c_k 2^k + \cdots + c_1 2 + c_0.$$
Dakle, vrijedi $n+1 = 2m = c_k 2^{k+1} + c_{k-1}2^k + \ldots c_1 2^2 + c_0 2$, čime smo dokazali da je $P(n+1)$ istina za parne $n+1$.

[29] U protivnom iz $m > n$ slijedi $n+1 = 2m > 2n$. Dakle, $1 > n$, što je kontradikcija.

- $n+1 = 2m+1$. Opet analognim argumentom kao u prvom slučajo zaključujemo da vrijedi $m \leq n$, pa po pretpostavci vrijedi $P(m)$. Sada imamo:
$$n+1 = 2m+1 = c_k 2^{k+1} + c_{k-1}2^k + \ldots c_1 2^2 + c_0 2 + 1.$$
Dakle, dokazali smo da je $P(n+1)$ istina i za neparne $n+1$.

Po principu potpune matematičke indukcije (Teorem 4.11) zaključujemo da je $P(n)$ istina za sve $n \in \mathbb{N}$.

4.2 *Cijeli brojevi*

Neformalno, skup cijelih brojeva definiramo na sljedeći način:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Naravno, gornja definicija nije zadovoljavajuća jer operaciju oduzimanja još nismo definirali; također, prema Poglavlju 2 nismo sigurni

je li navedena kolekcija zaista skup. Prije formalne definicije promotrimo osnovnu motivaciju za uvođenje cijelih brojeva. Naime, jednadžbu tipa $n + 4 = 2$ ne možemo rješiti u prirodnim brojevima. Zbog toga nam je cilj proširiti prirodne brojeve objektima koji će biti rješenja jednadžbi gornjeg tipa. Neformalno, rješenje gornje jednadžbe je $n = 2 - 4$. Dakle, rješenje je opisano uređenim parom prirodnih brojeva $(2, 4)$. Međutim, znamo da je to rješenje[30] opisano i drugim parovima prirodnih brojeva, npr. $(3, 5)$ ili $(12, 14)$. Cilj nam je "poistovjetiti" sve parove prirodnih brojeva koji definiraju isti cijeli broj. U tu svrhu definiramo sljedeću relaciju na $\mathbb{N}_0 \times \mathbb{N}_0$:

[30] $n = -2$

Definicija 4.22.

$$(a, b) \sim (c, d) :\Leftrightarrow a + d = b + c,\ (a, b),\ (c, d) \in \mathbb{N}_0 \times \mathbb{N}_0.$$

Lako se vidi da je $\sim$ relacije ekvivalencije[31]

[31] Vidi zadatak 4.4.

Definicija 4.23. SKUP CIJELIH BROJEVA *definiramo kao*

$$\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0 /_{\sim}.$$

Primjer 4.24. *Dakle, cijeli brojevi su klase ekvivalencije relacije $\sim$, tj. klase ekvivalencije uređenih parova prirodnih brojeva*[32]. *Vratimo se primjeru s početka poglavlja:*

$$-2 = [(2, 4)] = \{(0, 2), (1, 3), (2, 4), \dots\}.$$

[32] Preciznije, skupa $\mathbb{N}_0$, tj. prirodnih brojeva s 0. Potpuno ekvivalentno mogli smo definirati cijele brojeve kao kvocijentni skup od $\mathbb{N} \times \mathbb{N}$. Odlučili smo se za $\mathbb{N}_0$ radi tehničke i notacijske jednostavnosti.

Definicija 4.25 (Zbrajanje cijelih brojeva)**.** *Neka su $[(a, b)], [(c, d)] \in \mathbb{Z}$. Tada definiramo:*

$$[(a, b)] + [(c, d)] := [(a + c, b + d)].$$

Napomena 4.26. *Intuicija iza definicije zbrajanja je dana sljedećim računom:*

$$(a - b) + (c - d) = (a + c) - (b + d).$$

Uočite da smo zbrajanje definirali pomoću reprezentanata klasa ekvivalencije. Apriori nije jasno da je ta definicija dobra, tj. da će dati isti rezultat ukoliko izaberemo neke druge reprezentante. Recimo da želimo zbrojiti cijele brojeve -2 i 3. Definicija 4.25 nam definira zbroj pomoću formule koja uključuje reprezentante klasa ekvivalencija. Recimo, $-2 = [(3, 5)] = [(1, 3)]$, a $3 = [(3, 0)] = [6, 3]$. Imamo:

$$\begin{aligned}[(3, 5)] + [(3, 0)] &= (def\ 4.25) = [(6, 5)] = [(7, 6)] = (def) \\ &= [(1, 3)] + [(6, 3)].\end{aligned}$$

Dakle, rezultat je isti iako smo uzeli druge predstavnike. Da bi Definicija 4.25 bila dobra potrebno je dokazati da gornja tvrdnja vrijedi općenito, tj. da je definicija neovisna o izboru reprezentanata klase ekvivalencije[33].

[33] Ovakvu tvrdnju treba dokazati općenito kod bilo koje definicije operacije na kvocijentnom skupu koja koristi reprezentante.

Lema 4.27. *Zbrajanje cijelih brojeva je dobro definirano, tj. za $(a, b) \sim (a', b')$ i $(c, d) \sim (c', d')$ vrijedi:*

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

Dokaz. Računamo:

$$\begin{aligned}(a'+c')+(b+d) &= (Prop.\ 4.5, 4.6) = (a'+b)+(c'+d)\\ &= (a+b')+(c+d') = (a+c)+(b'+d').\end{aligned}$$

Tvrdnja slijedi iz Definicije 4.22. □

Definicija 4.28 (Množenje cijelih brojeva)**.** *Neka su* $[(a,b)], [(c,d)] \in \mathbb{Z}$*. Tada definiramo:*

$$[(a,b)] \cdot [(c,d)] := [(ac+bd, ad+bc)].$$

Napomena 4.29. *Intuicija iza definicije množenja dana je sljedećim računom:*

$$(a-b)\cdot(c-d) = (ac+bd)-(bc+ad).$$

Kao i kod definicije zbrajanja, potrebno je dokazati da je i množenje cijelih brojeva dobro definirano. Dokaz je analogan dokazu dobre definiranosti zbrajanja i ostavljamo ga kao zadatak[34].

[34] Zadatak 4.5.

Lema 4.30. *Množenje cijelih brojeva je dobro definirano, tj. za* $(a,b) \sim (a',b')$ *i* $(c,d) \sim (c',d')$ *vrijedi:*

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

Intuitivno znamo da vrijedi $\mathbb{N} \subset \mathbb{Z}$ i bilo bi poželjno da ta inkluzija vrijedi i za našu konstrukciju. Međutim, primijetite da to nije istina: formalno gledajući, $\mathbb{N} \nsubseteq \mathbb{Z}$. Naime, elementi od $\mathbb{Z}$ su klase ekvivalencije oblika $[(n,m)]$ pa $n \notin \mathbb{Z}$ za svaki $n \in \mathbb{N}$. Situaciju možemo spasiti tako da definiramo preslikavanje $i : \mathbb{N} \to \mathbb{Z}$ sa $i(n) = [(n,0)]$. Preslikavanje i je injekcija,[35] pa ćemo skup $\mathbb{N}$ identificirati s njegovom slikom $i(\mathbb{N})$. Uz tu identifikaciju vrijedi $\mathbb{N} = i(\mathbb{N}) \subset \mathbb{Z}$. U daljnjem tekstu uvijek ćemo implicitno koristiti opisanu identifikaciju.

[35] Injekcije koje čuvaju strukturu obično zovemo ULAGANJIMA. U ovom slučaju struktura su operacije zbrajanje i množenja, te uređaj. Ubrzo ćemo dokazati da i zaista čuva strukturu.

Definicija 4.31 (Suprotni element)**.** *Neka je* $[(a,b)] \in \mathbb{Z}$*. Tada definiramo:* $-[(a,b)] := [(b,a)]$[36].

[36] Intuicija: $-(a-b) = b-a$.

Propozicija 4.32 (Trihotomija cijelih brojeva)**.** *Neka je* $z \in \mathbb{Z}$*. Tada vrijedi točno jedna od sljedeće tri tvrdnje:* $z \in \mathbb{N}$[37]*,* $z = 0$[38]*,* $-z \in \mathbb{N}$[39]*.*

[37] $z = [(n,0)],\ n \in \mathbb{N}$
[38] $z = [(n,n)],\ n \in \mathbb{N}$
[39] $z = [(0,n)],\ n \in \mathbb{N}$

Dokaz. Neka je $z = [(a,b)] \in \mathbb{Z}$. Tada po Propoziciji 4.13 vrijedi točno jedna od sljedećih tvrdnji:

1. $a > b$. Tada postoji $n \in \mathbb{N}$ takav da $b+n = a$, pa vrijedi $z = [(n,0)] \in \mathbb{N}$.
2. $a = b$. Tada je $z = 0$.
3. $a < b$. Tada postoji $n \in \mathbb{N}$ takav da $a+n = b$, pa vrijedi $z = [(0,n)]$ tj. $-z = [(n,0)] \in \mathbb{N}$.

□

Navedimo sada svojstva zbrajanja i množenja cijelih brojeva u sljedećoj propoziciji:

Propozicija 4.33. *Neka su $x, y, z \in \mathbb{Z}$. Tada vrijedi:*

(1) $x + y = y + x$ *(komutativnost zbrajanja),*

(2) $(x + y) + z = x + (y + z)$ *(asocijativnost zbrajanja),*

(3) $x + 0 = 0 + x = x$ *(0 je neutralni element za zbrajanje),*

(4) $x + (-x) = (-x) + x = 0$ *(inverzni element za zbrajanje),*

(5) $xy = yx$ *(komutativnost množenja),*

(6) $(xy)z = x(yz)$ *(asocijativnost množenja),*

(7) $x \cdot 1 = 1 \cdot x = x$ *(1 je neutralni element za množenje),*

(8) $x(y + z) = xy + xz$ *(distributivnost množenja prema zbrajanju),*

(9) $(y + z)x = yx + zx$ *(distributivnost množenja prema zbrajanju).*

Dokaz. Dokaz propozicije slijedi direktno iz definicije operacija na cijelim brojevima i svojstava operacija na prirodnim brojevima. Radi ilustracije dokažimo npr. svojstva (1), (4) i (7)[40]. Neka su $x = [(a, b)]$, $y = [(c, d)] \in \mathbb{Z}$, $a, b, c, d \in \mathbb{N}_0$. Tada:

[40] Vidi zadatak 4.6

$$\begin{aligned} x + y &= (def.\ 4.25) = [(a + c, b + d)] = (Prop.\ 4.5) = [(c + a, d + b)] \\ &= (def.\ 4.25) = y + x. \\ x + (-x) &= (def.\ 4.31) = [(a, b)] + [(b, a)] = (def.\ 4.25) = [(a + b, b + a)] \\ &= (Prop.\ 4.5) = [(a + b, a + b)] = (def.\ 4.22) = [(0, 0)] = 0. \\ x \cdot 1 &= [(a, b)] \cdot [(1, 0)] = (def.\ 4.28) = [(a, b)] = x. \end{aligned}$$

□

Napomena 4.34. *Propozicija 4.33 kaže da je $(\mathbb{Z}, +)$ komutativna grupa[41] (svojstva $(1) - (4)$), $(\mathbb{Z}, \cdot)$ komutativna polugrupa[42] (svojstva $(5) - (6)$), a $(\mathbb{Z}, +, \cdot)$ komutativni prsten[43] sa jedinicom.*

[41] Neka je G skup i $+ : G \times G \to G$ binarna operacija. Kažemo da je $(G, +)$ GRUPA ako vrijede svojstva $(2) - (4)$ iz Propozicije 4.33.

[42] Neka je G skup i $+ : G \times G \to G$ binarna operacija. Kažemo da je $(G, \cdot)$ POLUGRUPA ako je $\cdot$ asocijativna.

[43] Neka je G skup i $+, \cdot : G \times G \to G$ binarne operacije. Kažemo da je $(G, +, \cdot)$ PRSTEN ako vrijede svojstva $(1) - (4)$, (6), $(8) - (9)$ iz Propozicije 4.33.

U apstraktnoj teoriji prstena mogu postojati djelitelji nule, tj. elementi $a \neq 0$, $b \neq 0$ takvi da vrijedi $ab = 0$. Dokazat ćemo da u prstenu cijelih brojeva ne postoje djelitelji nule:

Propozicija 4.35. *Neka su $a, b \in \mathbb{Z}$ takvi da vrijedi $ab = 0$. Tada je $a = 0$ ili $b = 0$.*

Dokaz. Pretpostavimo suprotno, tj. $a \neq 0$ i $b \neq 0$. Tada po Propoziciji 4.32 postoje $n, m \in \mathbb{N}$ takvi da vrijedi $(a = [(n, 0)] \vee a = [(0, n)]) \wedge (b = [(m, 0)] \vee b = [(0, m)])$. Dakle, imamo 4 mogućnosti za provjeriti i po Definiciji 4.28 u svakoj dobivamo $ab \neq 0$[44] što je kontradikcija. □

[44] Npr. $[(n, 0)] \cdot [(0, m)] = [(0, mn)] \neq 0$.

Korolar 4.36. *Neka su $a, b, c \in \mathbb{Z}$, $c \neq 0$ takvi da $ac = bc$. Tada je $a = b$.*

Dokaz. Neka je $ac = bc$. Dodajmo sada s obje strane $-(bc)$ i koristimo svojstva zbrajanja i množenja iz Propozicije 4.33. Imamo $0 = ac - bc = (a - b)c$[45]. Pošto je $c \neq 0$ iz Propozicije 4.35 imamo $a - b = 0$, tj. $a = b$. □

[45] $a - b := a + (-b)$.

Ostaje nam proširiti definiciju uređaja na cijele brojeve i dokazati da je tako definiran uređaj kompatibilan s operacijama.

Definicija 4.37 (Uređaj na $\mathbb{Z}$)**.** *Neka su $n, m \in \mathbb{Z}$. Kažemo da je n* MANJI ILI JEDNAK *m, pišemo $n \leq m$, ako postoji $x \in \mathbb{N}_0$ takav da $m = n + x$.*[46]

[46] n je manji od m, $n < m$, akko $n \leq m$ i $n \neq m$.

Propozicija 4.38 (Svojstva uređaja na $\mathbb{Z}$)**.** *Neka su $a, b, c \in \mathbb{Z}$. Tada vrijedi:*

(1) $a < b$ ako i samo ako $b - a \in \mathbb{N}$.

(2) Ako $a < b$, tada $a + c < b + c$.

(3) Ako $a < b$ i $c \in \mathbb{N}$, tada $ac < bc$.

(4) Ako $a < b$, tada $-a > -b$[47].

[47] $x > y \Leftrightarrow \neg x \leq y$, $x, y \in \mathbb{Z}$

(5) Ako $a < b$ i $b < c$, tada $a < c$.

(6) Točno jedna od sljedećih tvrdnji je istinita: $a < b$, $a = b$, $a > b$.

4.3 *Racionalni brojevi*

Intuitivno, želimo definirati skup:

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\}.$$

Slično kao ranije, osnovna motivacija nam je što u cijelim brojevima ne možemo rješavati jednadžbe tipa $5x = 2$. Kao što je kod jednadžbe $n + 4 = 2$ i uvođenja cijelih brojeva bio problem što nismo imali operaciju oduzimanja, tako je sada problem što još nismo definirali operaciju dijeljenja. Zbog toga racionalne brojeve ne možemo definirati koristeći razlomke kao u gornjoj neformalnoj definiciji. Umjesto toga, koristimo ideju analognu ideji koju smo koristili kod definicije cijelih brojeva, tj. racionalne brojeve ćemo definirati kao klase ekvivalencije uređenih parova cijelih brojeva. Preciznije, definiramo relaciju na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

Definicija 4.39.

$$(a, b) \sim (c, d) :\Leftrightarrow ad = bc,\ (a, b),\ (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}).$$

Propozicija 4.40. *Relacija $\sim$ je relacija ekvivalencije na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

Dokaz. Refleksivnost i simetričnost slijede direktno iz definicije i Propozicije 4.33, tvrdnja (1). Dokažimo tranzitivnost. Neka su (a, b), (c, d), $(e, f) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ takvi da $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$. Pretpostavimo $c \neq 0$[48]. Iz definicije relacije $\sim$ imamo $ad = bc$. Množenjem te jednakosti sa cf[49] i korištenjem Propozicija 4.33 i 4.36 imamo:

[48] Ukoliko $c = 0$, tada je i $a = 0 = e$ (Prop. 4.35) pa tvrdnja vrijedi.

[49] $cf = de$

$$(ad)(cf) = (bc)(cf) \Rightarrow\ (af)(cd) = (be)(cd) \Rightarrow\ af = be.$$

Dakle, po Definiciji 4.39, slijedi $(a, b) \sim (e, f)$. □

Definicija 4.41. SKUP RACIONALNIH BROJEVA *definiramo kao*[50]

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / _{\sim}.$$

[50] Intuitivno,
$$\frac{1}{2} = [(1,2)] = \{(1,2), (-1,-2), (2,4), \dots\}.$$

Definicija 4.42 (Operacija nad $\mathbb{Q}$). *Neka su* $[(a,b)], [(c,d)] \in \mathbb{Q}$. *Tada definiramo zbrajanje i množenje racionalnih brojeva, te suprotni element:*[51]

$$\begin{aligned} [(a,b)] + [(c,d)] &:= [(ad+cb, bd)], \\ [(a,b)] \cdot [(c,d)] &:= [(ac, bd)], \\ -[(a,b)] &:= [(-a, b)]. \end{aligned}$$

[51] s obzirom na zbrajanje

Napomena 4.43. *Intuicija iza Definicije 4.41 je:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad -\frac{a}{b} = \frac{-a}{b}.$$

Kako su operacije opet definirane pomoću reprezentanata, moramo dokazati da je definicija dobra, tj. da ne ovisi o izboru reprezentanta.

Propozicija 4.44. *Operacije nad* $\mathbb{Q}$ *su dobro definirane.*

Dokaz. Dokazat ćemo tvrdnju samo za množenje, a ostatak ostaviti za vježbu[52]. Neka su $(a,b), (a',b'), (c,d), (c',d') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ takvi da $(a,b) \sim (a',b')$ i $(c,d) \sim (c',d')$. Tvrdimo da $(ac, bd) \sim (a'c', b'd')$. Zaista, koristeći Propoziciju 4.33 imamo

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (a'c')(bd).$$

□

[52] Zadatak 4.8.

Napomena 4.45. *Preslikavanje* $i : \mathbb{Z} \to \mathbb{Q}$ *definirano sa* $i(z) = [(z,1)]$ *je ulaganje*[53]. *U daljnjem tekstu uvijek ćemo identificirati* $\mathbb{Z}$ *sa* $i(\mathbb{Z})$. *Uz tu identifikaciju imamo* $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

[53] Injekcija koja čuva strukturu

Definicija 4.46 (Multiplikativni inverz). *Neka je* $q = [(a,b)] \in \mathbb{Q}$, $a \neq 0$[54]. *Tada definiramo* INVERZ*:*[55]

$$q^{-1} := [(b,a)].$$

[54] $q \neq 0$

[55] $q \cdot q^{-1} = [(a,b)] \cdot [(b,a)] = [(ab, ba)] = [(1,1)] = 1$

Propozicija 4.47. $(\mathbb{Q}, +, .)$ *je komutativni prsten s jedinicom, te vrijedi* $qq^{-1} = q^{-1}q = 1$, $q \neq 0$[56].

Dokaz. Direktno iz Definicija 4.46 i 4.42 te Propozicije 4.33. □

[56] $(\mathbb{Q}, +, \cdot)$ je polje

Neka je G skup i $+, \cdot : G \times G \to G$ binarne operacije. Kažemo da je $(G, +, \cdot)$ POLJE ako je $(G, +, \cdot)$ komutativni prsten sa jedinicom i vrijedi da za svaki $x \in G$, $x \neq 0$, postoji $x^{-1} \in G$ takav da $xx^{-1} = 1$.

Napomena 4.48. *Za* $x, y \in \mathbb{Q}$, *uvodimo oznaku* $\frac{x}{y} := xy^{-1}$.

Definicija 4.49 (Uređaj na $\mathbb{Q}$). *Neka je* $q \in \mathbb{Q}$. *Kažemo da je* q POZITIVAN *ako i samo ako postoje* $a, b \in \mathbb{N}$ *takvi da* $q = [(a,b)]$.

Neka su $q, r \in \mathbb{Q}$. *Kažemo da je* q MANJI *od* r, *pišemo* $q < r$, *ako je* $r - q$ *pozitivan. Kažemo da je* q MANJI ILI JEDNAK r, *pišemo* $q \leq r$, *ako je* $q < r$ *ili* $q = r$.

Uređaj na $\mathbb{Q}$ zadovoljava ista svojstva kao i uređaj na $\mathbb{Z}$, tj. vrijede analogoni Propozicija 4.32 i 4.38. Formulaciju i dokaz tih rezultata ostavljamo čitatelju za vježbu.

4.4 Realni brojevi

Rezimirajmo što smo do sada napravili u ovom poglavlju. Krenuvši od Peanovih aksioma, konstruirali smo prirodne, cijele i racionalne brojeve $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Dokazali smo da su racionalni brojevi uređeno polje, tj. na njemu možemo već raditi dosta matematike. Na primjer, sve operacije na računalima su zapravo operacije na racionalnim brojevima. Usprkos tome, racionalni brojevi nisu dovoljni za mnoga bazična područja matematike, npr. analizu i geometriju. Recimo, duljina hipotenuze pravokutnog trokuta čije katete imaju duljinu 1 je $\sqrt{2}$ koji nije racionalan[57]. Također, javlja se i broj π koji je u nekom smislu još dalje od racionalnih brojeva[58] od $\sqrt{2}$. S analitičke strane to možemo promatrati na sljedeći način. Ako racionalne brojeve poredamo na brojevni pravac, taj pravac će imati "rupe"[59]. Zaista, promotrimo skupove $A = \{p \in \mathbb{Q} : p^2 < 2\}$ i $B = \{q \in \mathbb{Q} : q^2 > 2\}$. Tada je $\{A, B\}$ particija skupa $\mathbb{Q}$, tj. $A \cup B = \mathbb{Q}$ i $A \cap B = \emptyset$. Dakle, postoji "rupa" tamo gdje bi trebao biti $\sqrt{2}$. Uočimo da je skup A ograničen odozgo, ali nema supremum pa prema definiciji **??** nije potpun. Intuitivno, skup $\mathbb{R}$ ćemo konstruirati popunjavanjem svih "rupa" u $\mathbb{Q}$, tj. konstruirat ćemo upotpunjenje od $\mathbb{Q}$. Nažalost, ta konstrukcija će biti bitno kompliciranija od konstrukcija $\mathbb{Z}$ i $\mathbb{Q}$. Naime, kod konstrukcija $\mathbb{Z}$ i $\mathbb{Q}$ uvodili smo nove algebarske operacije oduzimanja i dijeljenja, dok kod konstrukcije realnih brojeva popunjavamo "rupe" kojih ima bitno više nego racionalnih brojeva[60] te sama konstrukcija uključuje kompliciranije koncepte poput limesa ili supremuma.

Konstrukciju ćemo provesti pomoću Dedekindovih rezova. Ideja konstrukcije je sadržana u gornjem primjeru kada smo napravili particiju skupa $\mathbb{Q}$ pridruženu broju $\sqrt{2}$. Naime, broj $\sqrt{2}$ ćemo definirati kao skup $\{p \in \mathbb{Q} : p^2 < 2\}$.

Definicija 4.50. *Skup* REALNIH BROJEVA $\mathbb{R}$ *je skup svih podskupova* $A \subset \mathbb{Q}$ *sa sljedećim svojstvima:*

1. $A \neq \emptyset$, $A \neq \mathbb{Q}$,
2. *A je zatvoren odozdo, tj.* $(\forall x, y \in \mathbb{Q})\ (x < y \ \wedge \ y \in A) \Rightarrow x \in A$,
3. *A nema najveći element, tj.* $(\forall x \in A)(\exists y \in A)\ x < y$.

Uočimo da strogo formalno gledajući $\mathbb{Q} \not\subset \mathbb{R}$. Međutim, slično kao i u slučaju cijelih i racionalnih brojeva, možemo definirati ulaganje $i : \mathbb{Q} \to \mathbb{R}$ sa[61]

$$i(q) = \{p \in \mathbb{Q} : p < q\}.$$

Uz identifikaciju $\mathbb{Q}$ sa $i(\mathbb{Q})$ imamo $\mathbb{Q} \subset \mathbb{R}$[62].

Definicija 4.51 (Uređaj na $\mathbb{R}$)**.** *Neka su $x, y \in \mathbb{R}$. Kažemo da je x* MANJI ILI JEDNAK *y ako vrijedi $x \subset y$.*

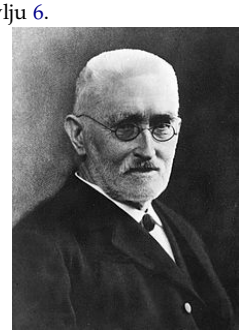
Uočimo da je definicija uređaja prirodna i jednostavna te da je dokaz činjenice da je $(\mathbb{R}, \leq)$ totalno uređen skup trivijalan[63]. Dokaz potpunosti će također biti jednostavan:

[57] Dokažite tu tvrdnju!

[58] π je transcendentan, vidi Def. 7.40

[59] Skup racionalnih brojeva nije potpun, tj. svaki Cauchy-ev niz nije konvergentan. Na "rupe" možemo neformalno gledati kao limese nizeva racionalnih brojeva koji više nisu racionalni brojevi.

[60] Racionalnih brojeva ima prebrojivo mnogo (kao i prirodnih), dok "rupa" ima neprebrojivo mnogo. Pojmove prebrojivo i neprebrojivo obradit ćemo u Poglavlju 6.



Richard Dedekind (1831.–1916.), njemački matematičar

[61] Dokažite da $i(p) \in \mathbb{R}$, $p \in \mathbb{Q}$ i da je i injekcija.

[62] Intuitivno $x \in \mathbb{R}$ idetificiramo sa skupom $\langle -\infty, x \rangle \cap \mathbb{Q}$.

[63] Pošto je općenito $(\mathcal{P}(\Omega), \subset)$ parcijalno uređen skup treba samo pokazati da za svaki $x, y \in \mathbb{R}$ vrijedi $x \subset y$ ili $y \subset x$. Međutim to je direktna posljedica zatvorenosti odozdo iz Def. 4.50.

Teorem 4.52. *Neka je $\emptyset \neq A \subset \mathbb{R}$ odozgo (odozdo) omeđen skup. Tada postoji* sup A (inf A).

Dokaz. Neka je $A \subset \mathbb{R}$ odozgo omeđen, tj. postoji $r \in \mathbb{R}$ takav da $a \leq r$, $a \in A$. Definirajmo skup:

$$s = \bigcup_{a \in A} a.$$

Očito vrijedi $a \subset s$, $a \in A$. Tvrdimo da je S supremum skupa A. Dokažimo najprije $s \in \mathbb{R}$, za što je potrebno provjeriti tri svojstva iz Definicije 4.50:

1. Kako je $A \neq \emptyset$, tada je i $s \neq \emptyset$[64]. Također, $s \subset r \neq \mathbb{Q}$, pa i $s \neq \mathbb{Q}$.
2. Neka su $x, y \in \mathbb{Q}$, $x < y$ i $y \in s$. Po definiciji od s postoji $a \in A$ takav da $y \in a$. Kako vrijedi $a \in \mathbb{R}$, iz zatvorenosti odozdo od a imamo $x \in a \subset s$.
3. Pretpostavimo suprotno, tj. da postoji $q \in \mathbb{Q}$ takav da $q \in s$ i $(\forall p \in s)\ p \leq q$. Tada postoji $a \in A$ takav da $q \in A$. Međutim, pošto je $a \subset s$, tada je q najveći element od a, što je u kontradikciji sa $a \in \mathbb{R}$.

Kako je s očito gornja međa od A, ostaje dokazati da je s najmanja gornja međa od A. Neka je $z \in \mathbb{R}$ neka gornja međa od A, tj. vrijedi $a \subset z$, $a \in A$. Dakle, $s = \cup_{a \in A} a \subset z$, čime je tvrdnja dokazana. □

[64] $(\exists a \in A \subset \mathbb{R})$, $a \subset s$.

Definicija 4.53 (Operacije nad $\mathbb{R}$). *Neka su $a, b \in \mathbb{R}$. Tada definiramo:*

$$a + b := \{x + y : x \in A,\ y \in B\},$$
$$-a := \{x - y : x < 0,\ y \in \mathbb{Q} \setminus a\}$$

$$a \cdot b := \begin{cases} \{xy : x, y \geq 0,\ x \in a,\ y \in b\} \cup \{x \in \mathbb{Q} : x < 0\}, & a, b \geq 0, \\ -(-a) \cdot b, & a < 0,\ b \geq 0, \\ -a \cdot (-b), & a \geq 0,\ b < 0, \\ (-a) \cdot (-b), & a < 0,\ b < 0. \end{cases}$$

Uočite da defincija $-a := \{-x : x \in \mathbb{Q} \setminus a\}$ nije dobra jer taj skup ima najveći element za $a \in \mathbb{Q}$.

$$a^{-1} := \begin{cases} = \left\{\frac{x}{y} : x < 1,\ y \in \mathbb{Q} \setminus a\right\}, & a > 0, \\ -(-a)^{-1}, & a < 0. \end{cases}$$

Lako se vidi da je definicija dobra u smislu da vrijedi $a + b$, $-a$, ab, $a^{-1} \in \mathbb{R}$. Za tako konstruirane realne brojeve vrijedi sljedeći teorem:

Teorem 4.54. *$(\mathbb{R}, +, \cdot, \leq)$ je potpuno uređeno polje, tj. za svaki $x, y, z \in \mathbb{R}$ vrijede sljedeća svojstva:*

$$\left.\begin{array}{l} (R1)\ (x+y)+z = x+(y+z), \\ (R2)\ 0+x = x+0 = x, \\ (R3)\ x+(-x) = (-x)+x = 0, \\ (R4)\ x+y = y+x, \end{array}\right\} (\mathbb{R}, +) \text{ je Abelova grupa.}$$
$$\left.\begin{array}{l} (R5)\ (xy)z = x(yz), \\ (R6)\ x \cdot 1 = 1 \cdot x = x, \\ (R7)\ xx^{-1} = x^{-1}x = 1, \\ (R8)\ xy = yx, \\ (R9)\ (x+y)z = xz+yz, \end{array}\right\} (\mathbb{R}, +, \cdot) \text{ je polje.}$$

$$\left.\begin{array}{l}(R10)\ x \le x,\\ (R11)\ (x \le y)\ \wedge\ (y \le x) \Rightarrow x = y,\\ (R12)\ (x \le y)\ \wedge\ (y \le z) \Rightarrow x \le z,\\ (R13)\ (x \le y)\ \vee\ (y \le x),\end{array}\right\}\ (\mathbb{R}, \le)\ \textit{je totalno uređen skup.}$$

$$\left.\begin{array}{l}(R14)\ x \le y \Rightarrow x + z \le y + z,\\ (R15)\ (0 \le x)\ \wedge\ (0 \le y) \Rightarrow 0 \le xy,\end{array}\right\}\ (\mathbb{R}, \le)\ \textit{je uređeno polje.}$$

$(R16)$ Vrijedi Teorem 4.52 $-$ potpunost.

Svojstva (R1)-(R16) obično se uzimaju za aksiome realnih brojeva. Dakle, dokazali smo da skup realnih brojeva, koje smo konstruirali Dedekindovim rezovima,[65] zadovoljava uobičajene aksiome realnih brojeva. Može se pokazati da aksiomi (R1)-(R16) jedinstveno određuju realne brojeve[66].

[65] Uočite da smo od aksioma koristili samo Peanove aksiome za prirodne brojeve. Skupovi cijelih, racionalnih i realnih brojeva su konstruirani iz prirodnih brojeva bez uvođenja dodatnih aksioma.

[66] U smislu da je svako uređeno potpuno polje izomorfno $\mathbb{R}$.

4.5 Kompleksni brojevi

Definicija 4.55. SKUP KOMPLEKSNIH BROJEVA *je dan sa*

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

Za $(x_1, y_1), (x_2, y_2) \in \mathbb{C}$ *definiramo operacije* $+$ *i* $\cdot$*:*

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2,\ y_1 + y_2),$$
$$(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2,\ x_1 y_2 + y_1 x_2).$$

Navedimo sada neka svojstva kompleksnih brojeva (bez dokaza) te par napomena:

- $(\mathbb{C}, +, \cdot)$ je polje. Neutralni element za zbrajanje je $0 = (0, 0)$, a za množenje $1 = (1, 0)$. Suprotni element je dan formulom $-(x, y) = (-x, -y)$, a inverz $(x, y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$.
- Ulaganje $j : \mathbb{R} \to \mathbb{C}$ definiramo sa $j(x) = (x, 0)$. Uz poistovjećivanje $\mathbb{R}$ i $j(\mathbb{R})$ imamo $\mathbb{R} \subset \mathbb{C}$.
- Jednadžba $x^2 + 1 = 0$ nema rješenje u $\mathbb{R}$. Međutim,

$$(0, 1) \cdot (0, 1) + 1 = (-1, 0) + (1, 0) = 0.$$

- Uvedimo oznaku $i := (0, 1)$. Kompleksan broj i nazivamo IMAGINARNA JEDINICA. Koristeći imaginarnu jedinicu i identifikaciju $\mathbb{R}$ i $j(\mathbb{R})$ svaki kompleksan broj $z = (x, y) \in \mathbb{C}$ možemo zapisati u obliku:

$$z = (x, y) = (x, 0) \cdot (1, 0) + (y, 0) \cdot (0, 1) = x + iy.$$

  x zovemo REALNI DIO broja z, pišemo $x = \mathrm{Re}(z)$, a y IMAGINARNI DIO, $y = \mathrm{Im}(z)$.
- Kompleksne brojeve možemo promatrati kao točke u kompleksnoj ravnini. Naime, broju $z = (x, y) \in \mathbb{C}$ pridružimo točku s koordinatama (x, y) u $\mathbb{R}^2$ s koordinatnim sustavom $(0, (1, 0), (0, 1))$[67].

[67] 0 je ishodište, a osi su određene vektorima $(1, 0)$ i $(0, 1)$.

Tada x-os zovemo REALNA OS, a y-os IMAGINARNA OS.

Zrcaljenje s obzirom na realnu os zovemo KONJUGIRANJE kompleksnih brojeva. To je funkcija $z \mapsto \overline{z}$ definirana formulom $\overline{z} = x - iy$, $z = x + iy$. Konačno, definiramo MODUL kompleksnog broja sa:

$$|z| := \sqrt{x^2 + y^2}, \quad z = x + iy.$$

Geometrijski, modul $|z|$ je udaljenost točke z od ishodišta 0. Uočite da vrijedi[68] $|z|^2 = z\overline{z}$.

[68] $z\overline{z} \in \mathbb{R}$.

- Neka je φ kut kojeg dužina $\overline{0z}$ zatvara s pozitivnim dijelom realne osi. φ zovemo ARGUMENT od z, pišemo $\varphi = \arg(z)$. Tada vrijedi

$$z = |z|(\cos(\arg(z)) + i\sin(\arg(z)). \tag{4.2}$$

Jednakost (4.2) zovemo TRIGONOMETRIJSKI ZAPIS kompleksnog broja. Uz definiciju[69] $e^{i\varphi} := \cos(\varphi) + i\sin(\varphi)$, trigonometrijski zapis se može kreće zapisati $z = |z|e^{i\varphi}$. Trigonometrijski zapis je pogodan za množenje kompleksnih brojeva. Zaista, neka su $z = |z|e^{i\varphi}$ i $w = |w|e^{i\psi}$. Tada se može pokazati[70]:

$$z \cdot w = |z||w|e^{i(\varphi+\psi)} = |z||w|\big(\cos(\varphi + \psi) + i\sin(\varphi + \psi)\big).$$

[69] Eksponencijalna funkcija se može definirati nad $\mathbb{C}$ i tada se dokaže da ova formula zaista vrijedi.

[70] Koristeći adicijske formule za trigonometrijske funkcije.

Nadalje, indukcijom se lako pokaže da vrijedi:

$$z^n = |z|^n e^{in\varphi} = |z|^n\big(\cos(n\varphi) + i\sin(n\varphi)\big).$$

4.6 Zadaci

Zadatak 4.1. *Dokažite da je zbrajanje prirodnih brojeva dobro definirano, tj. da je za svaki $n, m \in \mathbb{N}$ vrijednost $n + m$ jedinstveno određena Definicijom 4.2.*

Zadatak 4.2. *Dokažite Propoziciju 4.10.*

Zadatak 4.3. *Dokažite Propoziciju 4.15.*

Zadatak 4.4. *Dokažite da je relacija $\sim$ iz Definicije 4.22 relacija ekvivalencije.*

Zadatak 4.5. *Dokažite lemu 4.30.*

Zadatak 4.6. *Dokažite Propoziciju 4.6.*

Zadatak 4.7. *Dokažite Propoziciju 4.38.*

Zadatak 4.8. *Završite dokaz Propozicije 4.44.*

Zadatak 4.9. *Dokažite Propoziciju 4.47.*

Zadatak 4.10. *Formulirajte i dokažite analogone Propozicija 4.32 i 4.38 za skup racionalnih brojeva.*

Zadatak 4.11. *Dokažite da kompleksno konjugiranje ima sljedeća svojstva:*

$$\overline{a + b} = \overline{a} + \overline{b},\ \overline{a \cdot b} = \overline{a} \cdot \overline{b},\ \overline{a^n} = \overline{a}^n,\ a, b \in \mathbb{C},\ n \in \mathbb{N}.$$

5
Djeljivost i kongruencije

Nakon što smo u prethodnom poglavlju aksiomatski izgradili skupove prirodnih, cijelih, racionalnih, realnih i kompleksnih brojeva, u ovom ćemo se u potpunosti posvetiti skupu cijelih brojeva. Pri tome ćemo naglasak staviti na proučavanje djeljivosti, te promatrati klase cijelih brojeva koje daju isti ostatak pri dijeljenju nekih fiksnim brojem. Rezultati koje ćemo dobiti predstavljaju osnovu područja matematike koje zovemo "Teorija brojeva"[1] , a koje je od iznimne važnosti za suvremenu kriptografiju i računalnu sigurnost[2]. Osim ovog praktičnog aspekta, ovo poglavlje daje mali uvid i u tipičnu metodologiju razvoja matematičkih teorija: nakon što smo u prethodnom poglavlju definirali aksiome i vidjeli neka elementarna svojstva prirodnih i cijelih brojeva, u ovom dajemo nešto "jače" rezultate, teoreme i algoritme koji opravdavaju korisnost aksiomatski razvijene teorije.

[1] Istoimeni kolegij obavezan je na drugoj godini preddiplomskog studija matematike.

[2] Kolegij "Kriptografija i sigurnost mreža" je obavezni kolegij na Diplomskom studiju Računarstvo i matematika.

5.1 Djeljivost

Započinjemo s definicijom pojma djeljivosti. Ono će se oslanjati na operaciju množenja koju smo uveli u Poglavlju 4.

Definicija 5.1. *Kažemo da broj $a \in \mathbb{N}$* DIJELI *broj $b \in \mathbb{N}$ ako postoji prirodni broj $k \in \mathbb{N}$ takav da vrijedi $b = k \cdot a$.*
Tada kažemo da je a DJELITELJ *od b, a da je b* VIŠEKRATNIK *od a.*
Pišemo: $a \mid b$.

Ponekad je prirodniji pojam "biti djeljiv sa". Ovu definiciju možemo proširiti i tim pojmom: $b \in \mathbb{N}$ JE DJELJIV SA $a \in \mathbb{N}$ ako a dijeli b. Dakle, 18 je djeljiv sa 6, a 6 dijeli 18.

Na primjer,

$2 \mid 28$, jer u gornjoj definiciji za $a = 2$ i $b = 28$ možemo uzeti $k = 14$.

S druge strane,

$$2 \nmid 5, \text{ jer ne postoji } k \in \mathbb{N} \text{ takav da je } 5 = 2 \cdot k.$$

Ako 2 dijeli neki prirodni broj n, kažemo da je n PARAN. U protivnom, kažemo da je n NEPARAN.

Primijetimo da pojam "dijeli" možemo promatrati i kao binarnu relaciju na skupu prirodnih brojeva: brojevi $a, b \in \mathbb{N}$ su u relaciji ako $a \mid b$. Ova relacija će imati neka od svojstava koja smo proučavali u Poglavlju 3.

Propozicija 5.2. *Relacija "dijeli" je relacija parcijalnog[3] uređaja na skupu $\mathbb{N}$.*

[3] Uočimo da relacija "dijeli" nije totalni uređaj na skupu $\mathbb{N}$: na primjer, $3 \nmid 5$ niti $5 \nmid 3$.

Dokaz.

Refleksivnost: Neka je $a \in \mathbb{N}$ proizvoljan. Tada $a \mid a$ jer $a = a \cdot 1$, pa u Definiciji 5.1 možemo uzeti $k = 1$.

Antisimetričnost: Neka su $a \in \mathbb{N}$ i $b \in \mathbb{N}$ takvi da $a \mid b$ i $b \mid a$. Tada, po Definiciji 5.1 postoje $k, \ell \in \mathbb{N}$ takvi da $b = k \cdot a$ i $a = \ell \cdot b$. Uvrstimo li drugu jednakost u prvu, slijedi $b = (k\ell)b$, odnosno, prema Korolaru 4.17, $k\ell = 1$. Kako su k i ℓ prirodni brojevi, ovo je moguće jedino za $k = \ell = 1$, pa je $b = k \cdot a = a$.

Tranzitivnost: Neka su $a, b, c \in \mathbb{N}$ takvi da je $a \mid b$ i $b \mid c$. Tada, po Definiciji 5.1 postoje $k, \ell \in \mathbb{N}$ takvi da $b = k \cdot a$ i $c = \ell \cdot b$. Slijedi $c = (\ell k) \cdot a = m \cdot a$, za prirodni broj $m = \ell k \in \mathbb{N}$. Stoga, po definiciji relacije "dijeli", slijedi $a \mid c$. □

Relaciju "dijeli" možemo proširiti na skup cijelih brojeva: kažemo da broj $a \in \mathbb{Z}$ dijeli broj $b \in \mathbb{Z}$ ako postoji broj $k \in \mathbb{Z}$ takav da je $b = k \cdot a$; ponovno koristimo oznaku $a \mid b$. Iako se čini da je ovako proširena relacija zadržala sva svojstva kao i relacija nad skupom prirodnih brojeva, to nije tako: relacija $\mid$ nad skupom $\mathbb{Z}$ je refleksivna i tranzitivna, ali *nije* antisimetrična![4] Gdje nastaje problem u gornjem dokazu antisimetričnosti? Ako su $a, b \in \mathbb{Z}$ takvi da $a \mid b$ i $b \mid a$, onda postoje *cijeli* brojevi $k, \ell \in \mathbb{Z}$ takvi da je $b = k \cdot a$ i $a = \ell \cdot b$, pa je $b = (k\ell)b$, odnosno $k\ell = 1$. Iz ovog *ne slijedi* da je $k = \ell = 1$ jer uz tu, imamo još jednu mogućnost: $k = \ell = -1$, odnosno, $a = -b$.

[4] Na primjer, $2 \mid -2$ i $-2 \mid 2$, no naravno, $2 \neq -2$.

Unatoč ovom nedostatku relacije "dijeli" nad skupom cijelih brojeva, u nastavku ćemo promatrati upravo nju. Pogledajmo prvo neka njezina jednostavnija svojstva.

Propozicija 5.3. *Neka su $a, b, c \in \mathbb{Z}$ takvi da $a \mid b$ i $a \mid c$, te neka je broj $x \in \mathbb{Z}$ proizvoljan. Tada:*

(a) $a \mid b + c$.

(b) $a \mid b - c$.

(c) $a \mid b \cdot x$.

Drugim riječima, ako su dva broja (b i c) djeljivi istim brojem (a), onda je i njihov zbroj i razlika također djeljiv tim istim brojem.
Nadalje, ako je neki broj (b) djeljiv sa a, onda je i svaki njegov višekratnik ($b \cdot x$) također djeljiv sa a.

Dokaz. Neka su $a, b, c, x \in \mathbb{Z}$ takvi da $a \mid b$ i $a \mid c$. Tada postoje $k, \ell \in \mathbb{Z}$ za koje vrijedi $b = k \cdot a$ i $c = \ell \cdot a$. Sada lako imamo:

$$b + c = \underbrace{(k + \ell)}_{\in \mathbb{Z}} \cdot a, \text{ pa je } a \mid b + c;$$
$$b - c = \underbrace{(k - \ell)}_{\in \mathbb{Z}} \cdot a, \text{ pa je } a \mid b - c;$$
$$b \cdot x = \underbrace{(k \cdot x)}_{\in \mathbb{Z}} \cdot a, \text{ pa je } a \mid b \cdot x.$$

□

Što možemo reći u slučaju kada broj a nije djeljiv brojem b? Jedan jednostavan, ali vrlo važan rezultat daje nam sljedeći teorem.

Teorem 5.4 (o dijeljenju s ostatkom). *Neka su $a, b \in \mathbb{Z}$ cijeli brojevi takvi da je $b > 0$. Tada postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je*

$$a = q \cdot b + r, \text{ pri čemu je } 0 \leq r < b.$$

Broj q zovemo KVOCIJENT, *a broj r* OSTATAK *pri dijeljenju broja a brojem b.*

Na primjer, ostatak pri dijeljenju broja 23 brojem 5 je 3, a kvocijent je 4:

$$23 = 4 \cdot 5 + 3.$$

Uočite da možemo pisati i $23 = 3 \cdot 5 + 8$, no tada je "ostatak" veći od broja kojim dijelimo (5). Uz zahtjev $0 \leq r < b$ zapis iz iskaza teorema je *jedinstven*.

Dokaz. Trebamo dokazati da brojevi q, r iz iskaza teorema postoje, te da su jedinstveni.

Egzistencija. Označimo sa S skup svih brojeva oblika $a - x \cdot b$, pri čemu je $x \in \mathbb{Z}$ proizvoljan broj[5]:

$$S := \{a - x \cdot b \ : \ x \in \mathbb{Z}\} = \{\ldots,\ a - 2b,\ a - b,\ a,\ a + b,\ a + 2b,\ \ldots\}.$$

[5] Zašto baš ovako definiramo S? Uočite da $r = a - q \cdot b$ ima isti oblik kao brojevi iz S. Broj q ne znamo unaprijed, pa zato promatramo skup svih mogućih kandidata za broj r. Pokazat ćemo da među njima postoji broj koji ima traženo svojstvo ($0 \leq r < b$) iz teorema. Pripadni "x" će biti q.

Primijetimo da se u skupu S mora nalaziti bar jedan nenegativan broj, tj. skup $S \cap \mathbb{N}_0$ je neprazan: ako je $a \geq 0$, onda je

$$a - 0 \cdot b = a \geq 0 \text{ nenegativan broj iz skupa } S,$$

a ako je $a < 0$, onda je

$$a - a \cdot b = \underbrace{a}_{<0} \cdot \underbrace{(1 - b)}_{\leq 0} \geq 0 \text{ nenegativan broj iz skupa } S.$$

Dakle, skup $S \cap \mathbb{N}_0$ je neprazan. Kako je skup $\mathbb{N}_0$ dobro uređen (Propozicija 4.12), u $S \cap \mathbb{N}_0$ postoji najmanji element; nazovimo taj element r:

$$r := \min S \cap \mathbb{N}_0. \tag{5.1}$$

Kako je $r \in S$, po definiciji skupa S postoji $q \in \mathbb{Z}$ takav da je $r = a - q \cdot b$. Tvrdimo da je $0 \leq r < b$. Jasno, kako je $r \in \mathbb{N}_0$, vrijedi $r \geq 0$. S druge strane, pretpostavimo da je $r \geq b$, odnosno

$$b \leq r = a - q \cdot b.$$

Prebacimo b s lijeve na desnu stranu gornje nejednakosti:

$$0 \leq a - q \cdot b - b = a - \underbrace{(q + 1)}_{\in \mathbb{Z}} \cdot b = r - b < r.$$

Broj $a - (q + 1) \cdot b$ je, dakle, element od $S \cap \mathbb{N}_0$, a manji je od r, što je kontradikcija sa (5.1). Dakle, pretpostavka $r \geq b$ je pogrešna, pa mora vrijediti $r < b$, a od ranije već imamo $0 \leq r$. Ovim smo dokazali da brojevi $q, r \in \mathbb{Z}$ iz tvrdnje teorema postoje.

Jedinstvenost. Pretpostavimo da postoje dva para brojeva $q_1, r_1 \in \mathbb{Z}$ i $q_2, r_2 \in \mathbb{Z}$ za koje vrijedi

$$\begin{aligned} a &= q_1 \cdot b + r_1, \quad 0 \leq r_1 < b; \\ a &= q_2 \cdot b + r_2, \quad 0 \leq r_2 < b. \end{aligned}$$

Uočimo da je tada

$$\begin{aligned} r_1 - r_2 &= q_2 \cdot b - q_1 \cdot b = (q_2 - q_1) \cdot b \\ &\in \{\ldots,\ -2b,\ -b,\ 0,\ b\ , 2b\ \ldots\}. \end{aligned} \tag{5.2}$$

Međutim, zbrajanjem nejednakosti

$$\begin{aligned} 0 \leq r_1 &< b, \\ -b < -r_2 &\leq 0 \end{aligned}$$

koje vrijede za ostatke, dobivamo

$$-b < r_1 - r_2 < b.$$

Jedini broj iz skupa (5.2) koji ovo zadovoljava je 0, pa mora biti $r_1 - r_2 = 0$, odnosno, $r_1 = r_2$. Uvrštavanjem u $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ slijedi $q_1 \cdot b = q_2 \cdot b$, a iz toga imamo $q_1 = q_2$. Drugim riječima, postoje jedinstveni q, r sa svojstvima iz iskaza teorema. □

Primjer 5.5. *Promotrimo slučaj $b = 3$, uz proizvoljni broj $a \in \mathbb{Z}$. Gornji teorem kaže da postoji broj $q \in \mathbb{Z}$, te broj r takav da je $0 \leq r < 3$ za koji vrijedi $a = q \cdot 3 + r$. Drugim riječima, svaki cijeli broj a je ili oblika $a = 3 \cdot q$ ili oblika $a = 3 \cdot q + 1$ ili oblika $a = 3 \cdot q + 2$.*

Slično, svi parni brojevi su oblika $a = 2 \cdot q$, za neki $q \in \mathbb{Z}$, a svi neparni su oblika $a = 2 \cdot q + 1$, za neki $q \in \mathbb{Z}$.

5.2 *Prosti brojevi*

Kada promatramo operaciju zbrajanja, svaki prirodni broj možemo dobiti uzastopnim zbrajanjem broja 1; na primjer, $5 = 1+1+1+1+1$. Kada promatramo operaciju množenja, situacija je složenija: tada nam treba puno više "građevnih jedinica" da bismo mogli "sagraditi" sve prirodne brojeve; na primjer, $90 = 2 \cdot 3 \cdot 3 \cdot 5$. Kao što ćemo pokazati u Osnovnom teoremu aritmetike (Teorem 5.16), "građevne jedinice" će u ovom slučaju biti prosti brojevi.

Definicija 5.6. *Prirodan broj $p > 1$ koji je djeljiv samo brojem 1 i samim sobom zovemo* PROSTI *ili* PRIM *broj. Za ostale brojeve veće od 1 kažemo da su* SLOŽENI. *Broj 1 nije niti prost niti složen.*

Skup svih prostih brojeva (nestandardno) označavamo simbolom $\mathbb{P}$:

$$\mathbb{P} = \{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ \ldots\}.$$

Testiranje je li neki broj prost te pronalaženje što većih[6] prostih brojeva vrlo je važno za područje kriptografije. U tu svrhu razvijeni su sofisticirani i vrlo složeni algoritmi. Mi ćemo ovdje opisati jedan jednostavan i relativno efikasan algoritam za pronalaženje svih prostih brojeva manjih od nekog, unaprijed zadanog, prirodnog broja N.

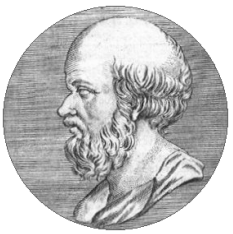
Algoritam 5.7 (Eratostenovo sito)**.** *Algoritam se sastoji od dva koraka:*

(1) Napišemo redom, jedan do drugog, sve prirodne brojeve od 2 do N. Na početku, niti jedan broj nije niti prekrižen niti zaokružen.

(2) Ponavljamo sve dok svaki broj nije ili prekrižen ili zaokružen:

(2a) Pronađemo prvi broj koji nije niti prekrižen niti zaokružen. Zaokružimo ga!

[6] U trenutku pisanja ovog teksta, najveći poznati prosti broj je $2^{74207281} - 1$. Taj broj ima 22338618 znamenki i pripada u skupinu tzv. Mersenneovih prostih brojevi. Mersenneovi prosti brojevi su prosti brojevi oblika $2^n - 1$, za neki prirodan broj n, a do sada ih je pronađeno 49. Za vježbu, pokažite da je kod svakog Mersenneovog prostog broja eksponent n nužno također prost!



Eratosten iz Kirene
(276. pr.Kr.–194. pr.Kr.), starogrčki matematičar

(2b) Prekrižimo sve brojeve koji su djeljivi brojem zaokruženim u koraku (2a) i koji su veći od njega.

Brojevi su koji su zaokruženi predstavljaju sve proste brojeve između 2 *i* N.

Pogledajmo nekoliko koraka Eratostenovog sita za $N = 20$. Prvo napišemo sve prirodne brojeve od 2 do 20:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Prvi broj koji nije niti prekrižen niti zaokružen je 2—on je prost. Zakružimo ga i prekrižimo sve njegove višekratnike.

(2) 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

Idući broj koji nije niti prekrižen niti zaokružen je 3—on je prost. Zakružimo ga i prekrižimo sve njegove višekratnike.

(2) (3) ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

Idući broj koji nije niti prekrižen niti zaokružen je 5—on je prost. Zakružimo ga i prekrižimo sve njegove višekratnike.

(2) (3) ~~4~~ (5) ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

Nastavljanjem ovog postupka, pronalazimo sve proste brojeve manje od 20, a niz na kraju izgleda ovako:

(2) (3) ~~4~~ (5) ~~6~~ (7) ~~8~~ ~~9~~ ~~10~~ (11) ~~12~~ (13) ~~14~~ ~~15~~ ~~16~~ (17) ~~18~~ (19) ~~20~~

Uz proste brojeve vezano je mnogo neriješenih matematičkih problema. Jedan vrlo poznati takav problem je tzv. Goldbachova[7] slutnja. Ona kaže da se svaki parni prirodan broj n veći od 2 može prikazati kao suma točno dva prosta broja. Na primjer, $8 = 3 + 5$, $12 = 5 + 7$. Slutnja je provjerena (pomoću računala) za sve $n < 4 \cdot 10^{18}$, ali svejedno još nije pronađen dokaz[8] za sve n.

Za razliku od Goldbachove slutnje koja promatra sume prostih brojeva, mnogo je jednostavnije proučavati njihove umnoške.

[7] Slutnju je iznio njemački matematičar Christian Goldbach 7. lipnja 1742. godine u pismu Leonhardu Euleru.

[8] Za sada je pokazano da se svaki parni prirodni broj veći od 2 može prikazati kao suma od 6 ili manje prostih brojeva (Olivier Ramaré, 1995. godine).

Lema 5.8. *Svaki prirodni broj* $n > 1$ *može se prikazati kao produkt jednog ili više prostih brojeva.*

Dokaz. Tvrdnju leme dokazujemo potpunom matematičkom indukcijom po broju n.

Baza. Broj $n = 2$ može se prikazati kao "produkt" jednog prostog broja (2).

Korak. Pretpostavimo da se, za neko $n > 1$, svaki od prirodnih brojeva $2, 3, \ldots, n$ može prikazati kao produkt jednog ili više prostih brojeva. Trebamo dokazati da se tada i broj $n + 1$ može prikazati na isti način. Ako je $n + 1$ sam prost, onda tvrdnja vrijedi ("produkt" jednog prostog broja). Pretpostavimo, dakle, da je $n + 1$ složen broj. Tada, po definiciji, postoji neki djelitelj p broja $n + 1$ koji je različit i od 1 i od $n + 1$, odnosno, $n + 1 = p \cdot q$, za neko $q \in \mathbb{N}$. Uočimo da je i broj q također različit i od 1 i od $n + 1$, odnosno, vrijedi $2 \leq p, q \leq n$.

Za brojeve p i q možemo primijeniti pretpostavku indukcije: postoje $k, \ell \in \mathbb{N}$ i neki prosti brojevi $\alpha_1, \ldots, \alpha_k$, te $\beta_1, \beta_2, \ldots, \beta_\ell$ takvi da je

$$p = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_k,$$
$$q = \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_\ell.$$

Tada je

$$n + 1 = p \cdot q = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_k \cdot \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_\ell$$

također prikazan kao umnožak prostih brojeva. Po principu (potpune) matematičke indukcije, pokazali smo tvrdnju za sve prirodne brojeve $n > 1$. □

Tvrdnju leme možemo zapisati i ovako: za svaki prirodan broj $n > 1$, postoji $k \in \mathbb{N}$, različiti[9] prosti brojevi $p_1, p_2, \ldots, p_k$, te prirodni brojevi $\alpha_1, \alpha_2, \ldots, \alpha_k$ takvi da je

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

Nešto kasnije ćemo dokazati Osnovni teorem aritmetike, koji dodatno tvrdi da je ovakav prikaz broja n jedinstven. Za sada ćemo iskoristiti lemu kako bismo pokazali da prostih brojeva ima beskonačno mnogo.

[9] Lema daje prikaz $n = q_1 \cdot q_2 \cdot \ldots q_\ell$, gdje su brojevi $q_1, q_2, \ldots q_\ell$ prosti, no oni se mogu ponavljati. Ako grupiramo sve q-ove koji su isti, dobivamo donji prikaz.

Na primjer, $36203200 = 2^6 \cdot 5^2 \cdot 11^3 \cdot 17^1$.

Teorem 5.9 (Euklid)**.** *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Pretpostavimo suprotno, odnosno, da prostih brojeva ima ukupno m, za neko $m \in \mathbb{N}$. Neka su, dakle, $p_1 < p_2 < \ldots < p_m$ svi prosti brojevi. Promotrimo broj

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1. \tag{5.3}$$

Očito, $n > 1$, pa se prema Lemi 5.8 broj n može prikazati kao produkt prostih brojeva; neka je p_j jedan od prostih brojeva koji sudjeluju u tom produktu[10]. Specijalno, to znači da je n djeljiv s p_j, odnosno, $p_j \mid n$. Zapišimo (5.3) malo drugačije:

$$1 = n - p_j \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_m).$$

Sa desne strane gornje jednakosti je razlika dva broja. Oba ta broja su djeljiva sa p_j, pa je po Propoziciji 5.3 i njihova razlika djeljiva s p_j. No to znači i da je lijeva strana jednakosti (broj 1) djeljiva sa p_j, a to je nemoguće jer je $p_j \geq 2$. Dobili smo kontradikciju, dakle, prostih brojeva ima beskonačno mnogo. □

Euklid (4. st.pr.Kr.), starogrčki matematičar, autor knjige *Elementi* koja je po prvi put na jednom mjestu objedinila svo znanje o matematici.

[10] Uočimo da svaki prosti broj koji sudjeluje u tom produktu mora biti jedan od $p_1, p_2, \ldots, p_m$ jer su to svi prosti brojevi, nema drugih.

5.3 *Najveća zajednička mjera*

Ako su zadana dva cijela broja a i b, često puta je potrebno odrediti najveći broj kojim su djeljivi i a i b—na primjer, tim brojem ćemo pokratiti razlomak a/b. Slično, svođenje određivanje zajedničkog nazivnika dvaju razlomaka svodi se na određivanje najmanjeg prirodnog broja koji je djeljiv i s nazivnikom prvog i s nazivnikom drugog razlomka. Postoje i brojne druge situacije u kojima su nam pojmovi iz sljedeće definicije vrlo korisni.

Definicija 5.10. NAJVEĆA ZAJEDNIČKA MJERA *brojeva $a, b \in \mathbb{N}$ je najveći prirodni broj koji dijeli i broj a i broj b. Taj broj označavamo sa $M(a,b)$.* NAJMANJI ZAJEDNIČKI VIŠEKRATNIK *brojeva $a, b \in \mathbb{N}$ je najmanji prirodni broj koji je djeljiv i brojem a i brojem b. Taj broj označavamo sa $V(a,b)$.*

Na primjer:

$$M(24,18) = 6, \qquad M(3,5) = 1;$$
$$V(24,18) = 72, \qquad V(3,5) = 15.$$

Pojam najveće zajedničke mjere možemo definirati i za cijele brojeve: ako su $a, b \in \mathbb{Z}$, onda

$$M(a,b) := \begin{cases} 0, & \text{za } a = b = 0; \\ |a|, & \text{za } a \neq 0,\ b = 0; \\ |b|, & \text{za } a = 0,\ b \neq 0; \\ M(|a|,|b|), & \text{za } a \neq 0,\ b \neq 0. \end{cases}$$

Tako je $M(-24,18) = M(-24,-18) = 6$, a $M(5,0) = M(0,-5) = 5$. Primijetimo da za sve cijele brojeve $a, b \in \mathbb{Z}$ vrijedi $M(a,b) \in \mathbb{N}_0$.

Posebno ističemo brojeve čija je mjera jednaka 1.

Étienne Bézout (1730.–1783.), francuski matematičar

Definicija 5.11. *Kažemo da su brojevi $a, b \in \mathbb{N}$* RELATIVNO PROSTI *ako je $M(a,b) = 1$.*

Sljedeću tvrdnju možemo lakše zapamtiti ovako: mjeru dvaju prirodnih brojeva možemo zapisati kao njihovu "linearnu kombinaciju".

Propozicija 5.12 (Bézoutov identitet)**.** *Neka su $a, b \in \mathbb{N}$. Tada postoje cijeli brojevi $x, y \in \mathbb{Z}$ takvi da je*

$$M(a,b) = x \cdot a + y \cdot b.$$

Dodatno, $M(a,b)$ je najmanji prirodni broj koji se koji se može zapisati u gornjem obliku.

Na primjer, $M(24,18) = 6$, pa nam Bézoutov identitet kaže da postoje brojevi $x, y \in \mathbb{Z}$ takvi da je $6 = x \cdot 24 + y \cdot 18$.

Kako pronaći te x, y? Dokaz teorema ne daje postupak pomoću kojeg bi se to moglo napraviti! Za takve dokaze kažemo da *nisu konstruktivni*.

Brojevi x i y mogu se odrediti pomoću (proširenog) Euklidovog algoritma—vidi Zadatak 5.6. No, u ovom slučaju, lako je pogoditi $x = 1$ i $y = -1$.

Dokaz. Promotrimo sljedeći skup[11] :

$$S := \{x \cdot a + y \cdot b \ : \ x, y \in \mathbb{Z}\}.$$

Uočimo da je presjek $S \cap \mathbb{N}$ neprazan, jer se u S nalazi, na primjer, broj $1 \cdot a + 0 \cdot b = a \in \mathbb{N}$. Promotrimo najmanji element skupa $S \cap \mathbb{N}$, te ga označimo sa d:

$$d := \min S \cap \mathbb{N}. \tag{5.4}$$

Kako je $d \in S$, postoje neki $x, y \in \mathbb{Z}$ takvi da je $d = x \cdot a + y \cdot b$. Tvrdimo da je broj d upravo mjera brojeva a, b. Da bismo to dokazali, moramo utvrditi da d zadovoljava svojstva navedena u Definiciji 5.10:

(1) Trebamo pokazati da $d \mid a$ i $d \mid b$. Primijenimo teorem o dijeljenju s ostatkom na brojeve a i d: postoje q i r takvi da je

$$a = q \cdot d + r, \qquad \text{pri čemu je } 0 \leq r < d.$$

Izračunajmo r tako da uvrstimo izraz za d:

$$\begin{aligned} r &= a - q \cdot d \\ &= a - q \cdot (x \cdot a + y \cdot b) \\ &= \underbrace{(1 - q \cdot x)}_{\in \mathbb{Z}} \cdot a + \underbrace{(-q \cdot y)}_{\in \mathbb{Z}} \cdot b. \end{aligned}$$

[11] Usporedite s dokazom teorema o dijeljenju s ostatkom (Teorem 5.4).
U skupu S nalaze se, na primjer:

$$-2a + 3b, \ -5a, \ 0, \ 2b, \ 123a + 456b, \ \ldots$$

Slijedi da je $r \in S$. Znamo da je $0 \leq r < d$, tvrdimo da je $r = 0$. Naime, ako bi bilo $0 < r < d$, onda bi bilo $r \in S \cap \mathbb{N}$ i $r < d$, što je kontradikcija s definicijom (5.4) broja d, koji je najmanji broj u skupu $S \cap \mathbb{N}$! Dakle, $r = 0$, pa je $a = q \cdot d$, odnosno, $d \mid a$. Posve analogno se dokaže $d \mid b$. Dakle, i broj a i broj b su djeljivi sa d.

(2) U (1) smo pokazali da je d djelitelj brojeva a i b; sada treba dokazati da je najveći od svih djelitelja. Neka je $q \in \mathbb{N}$ bilo koji djeljitelj brojeva a i b, odnosno, neka je $q \mid a$ i $q \mid b$. Iskoristimo sada Propoziciju 5.3 tri puta: prvo, prema (c) dijelu slijedi da je tada $q \mid x \cdot a$ i $q \mid y \cdot b$, a zatim, prema (a) dijelu Propozicije 5.3 imamo da $q \mid x \cdot a + y \cdot b$. Dakle, $q \mid d$, a kako je svaki djelitelj nekog prirodnog broja manji ili jednak tome broju, imamo $q \leq d$.

Ovim smo pokazali da je $d = x \cdot a + y \cdot b$ najveći od svih djelitelja brojeva a i b, pa je $d = M(a, b)$. Iz definicije skupa S i (5.4) slijedi da je $M(a, b)$ najmanji prirodni broj oblika *nešto*$\cdot a+$*nešto*$\cdot b$. □

U dokazu gornjeg teorema pokazali i sljedeću činjenicu: za $d \in \mathbb{N}$ vrijedi

$$d \mid a \quad \& \quad d \mid b \quad \Rightarrow \quad d \mid M(a, b), \tag{5.5}$$

odnosno, svaki djelitelj brojeva a i b je ujedno djelitelj njihove mjere. Ova činjenicu ćemo koristiti za dokaze nekih teorema koje ćemo iskazati nešto kasnije.

Promotrimo ponovno iskaz Propozicije 5.3(c):

$$a \mid b \quad \Rightarrow \quad a \mid bc,$$

za sve brojeve $a, b, c \in \mathbb{Z}$. U kojem slučaju vrijedi suprotna implikacija? Sljedeća propozicija nam pokazuje da je dovoljno da vrijedi $M(a, c) = 1$.

Primijetimo da suprotna implikacija ne vrijedi uvijek:

$10 \mid 14 \cdot 15$, ali ne vrijedi $10 \mid 14$.

Međutim,

$10 \mid 30 \cdot 7$ i $M(10, 7) = 1 \Rightarrow 10 \mid 30$.

Propozicija 5.13. *Neka su $a, b, c \in \mathbb{N}$.*

(a) Ako $a \mid b \cdot c$ i $M(a, c) = 1$, onda $a \mid b$.

(b) Ako je p prost broj i $p \mid b \cdot c$, onda $p \mid b$ ili $p \mid c$.

Dokaz. (a) Kako $a \mid b \cdot c$, postoji $k \in \mathbb{N}$ takav da je $b \cdot c = k \cdot a$. Iskoristimo Bézoutov identitet za mjeru brojeva a i c: postoje $x, y \in \mathbb{Z}$ takvi da je

$$1 = x \cdot a + y \cdot c.$$

Množenjem ove jednakosti sa b imamo:

$$\begin{aligned} b &= b \cdot x \cdot a + b \cdot y \cdot c \\ &= b \cdot x \cdot a + k \cdot y \cdot a \\ &= \underbrace{(b \cdot x + k \cdot y)}_{\in \mathbb{Z}} \cdot a, \end{aligned}$$

što povlači $a \mid b$.

(b) Uočimo da $M(p, b)$ može biti ili 1 ili p, jer $M(p, b)$ mora biti djelitelj od prostog broja p. Dakle, moguća su samo sljedeća dva slučaja:

(1) Ako je $M(p,b) = 1$, iz tvrdnje (a) slijedi $p \mid c$.

(2) Ako je $M(p,b) = p$, slijedi $p \mid b$, jer $M(p,b)$ mora biti djelitelj od b.

□

Kako možemo izračunati mjeru dvaju prirodnih brojeva a i b? Najjednostavnija metoda bi izravno koristila definiciju mjere: redom za svaki broj $d = 1, 2, \ldots, \min\{a,b\}$ provjerimo je li djelitelj i od a i od b, pa je mjera najveći od svih d koji jesu djelitelji. No čak i uz pomoć računala, ova metoda postaje izuzetno spora već kad su a i b nekoliko milijardi ili veći. Korištenjem Euklidovog algoritma moguće je (uz pomoć računala, naravno) izuzetno brzo nalaziti mjeru brojeva koji imaju nekoliko tisuća znamenki. Osnovna ideja za taj algoritam je dana u sljedećem rezultatu.

Propozicija 5.14. *Neka su $a, b \in \mathbb{N}$, te $q, r \in \mathbb{N}_0$ takvi da je $a = q \cdot b + r$. Tada je*

$$M(a,b) = M(b,r).$$

Dokaz. Prisjetimo se da je relacija "dijeli" antisimetrična na skupu prirodnih brojeva: ako za neke $x, y \in \mathbb{N}$ vrijedi $x \mid y$ i $y \mid x$, onda je $x = y$. Zbog toga[12] je dovoljno dokazati da $M(a,b) \mid M(b,r)$, te da $M(b,r) \mid M(a,b)$.

[12] Uočimo da je $M(x,y) \in \mathbb{N}$ ako je barem jedan od x, y različit od nule, pa uz pretpostavke propozicije imamo $M(a,b) \in \mathbb{N}$ i $M(b,r) \in \mathbb{N}$.

(1) Po definiciji $M(a,b)$, vrijedi $M(a,b) \mid a$, te $M(a,b) \mid b$. Prema Propoziciji 5.3(c), tada je $M(a,b) \mid q \cdot b$, a prema (b) dijelu iste propozicije je $M(a,b) \mid a - q \cdot b$. Dakle, $M(a,b) \mid r$ i $M(a,b) \mid b$, što prema (5.5) povlači da $M(a,b) \mid M(b,r)$.

(2) Po definiciji $M(b,r)$, vrijedi $M(b,r) \mid b$, te $M(b,r) \mid r$. Prema Propoziciji 5.3(c), tada je $M(b,r) \mid q \cdot b$, a prema (a) dijelu iste propozicije je $M(b,r) \mid q \cdot b + r$. Dakle, $M(b,r) \mid a$ i $M(a,b) \mid b$, što prema (5.5) povlači da $M(b,r) \mid M(a,b)$.

□

Algoritam 5.15 (Euklidov algoritam za izračunavanje mjere)**.**
Ulaz: *prirodni brojevi $a, b \in \mathbb{N}$.*
Izlaz: $d = M(a,b)$.
Sve dok je $b \neq 0$, ponavljamo korake (1) i (2):

(1) Po Teoremu o dijeljenju s ostatkom, odredimo q, r takve da je $a = q \cdot b + r$, $0 \leq r < b$.

(2) $a = b$; $b = r$ (odnosno, nastavljamo ovaj postupak kao da želimo odrediti $M(b,r)$.)

$d = a$;

Pokažimo primjerom da Euklidovim algoritmom možemo u svega nekoliko koraka odrediti mjeru relativno velikih brojeva: odredimo

$M(1317, 56)$:

$$\begin{array}{rcrcrcrl} a & = & q & \cdot & b & + & r & \\ 1317 & = & 23 & \cdot & 56 & + & 29 & \Rightarrow M(1317,56) = M(56,29) \\ 56 & = & 1 & \cdot & 29 & + & 27 & \Rightarrow M(56,29) = M(29,27) \\ 29 & = & 1 & \cdot & 27 & + & 2 & \Rightarrow M(29,27) = M(27,2) \\ 27 & = & 13 & \cdot & 2 & + & 1 & \Rightarrow M(27,2) = M(2,1) \\ 2 & = & 2 & \cdot & 1 & + & 0 & \Rightarrow M(2,1) = M(1,0) \end{array}$$

Dakle, $M(1317, 56) = M(1, 0) = 1$. Mjeru brojeva 18 i 24 možemo odrediti u samo 3 koraka:

$$\begin{array}{rcrcrcrl} a & = & q & \cdot & b & + & r & \\ 18 & = & 0 & \cdot & 24 & + & 18 & \Rightarrow M(18,24) = M(24,18) \\ 24 & = & 1 & \cdot & 18 & + & 6 & \Rightarrow M(24,18) = M(18,6) \\ 18 & = & 3 & \cdot & 6 & + & 0 & \Rightarrow M(18,6) = M(6,0) \end{array}$$

Dakle, $M(18, 24) = M(6, 0) = 6$.

Ako su nam poznati rastavi brojeva a i b na proste faktore, onda možemo vrlo lako odrediti njihovu mjeru i najmanji zajednički višekratnik. Dokažimo prvo Osnovni teorem aritmetike, koji kaže da je taj rastav jedinstven, a zatim pogledajmo kako je pomoću njega moguće izračunati mjeru i najmanji zajednički višekratnik prirodnih brojeva.

Teorem 5.16 (Osnovni teorem aritmetike)**.** *Za prirodni broj $a > 1$ postoje jedinstveni brojevi $\ell, \alpha_1, \alpha_2, \ldots, \alpha_\ell \in \mathbb{N}$, te prosti brojevi $p_1 < p_2 < \ldots < p_\ell$ takvi da je*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_\ell^{\alpha_\ell}. \tag{5.6}$$

Dokaz. U Propoziciji 5.8 smo već pokazali da se svaki $a \in \mathbb{N} \setminus \{1\}$ može prikazati u obliku (5.6). Potrebno je još dokazati samo jedinstvenost. Pretpostavimo suprotno, to jest, da postoje prirodni brojevi za koje imamo dva različita rastava; neka je a_{min} najmanji takav broj. Dakle, postoje $k, \ell \in \mathbb{N}$ i prosti brojevi $p_1, \ldots, p_\ell, q_1, \ldots, q_k$ takvi da su

$$a_{min} = p_1 \cdot p_2 \cdot \ldots \cdot p_\ell = q_1 \cdot q_2 \cdot \ldots \cdot q_k$$

dva različita rastava broja a_{min} na proste faktore. Specijalno, $p_1 \mid a_{min}$, pa prema Propoziciji 5.13 postoji[13] neki q_j takav da $p_1 \mid q_j$. Kako su brojevi p_1 i q_j prosti, to je moguće jedino u slučaju $p_1 = q_j$. Označimo sada $\tilde{a} := \frac{a_{min}}{p_1} \in \mathbb{N}$. Uočimo da je $\tilde{a} \neq 1$, jer u protivnom imamo $a_{min} = p_1$, što ima jedinstveni rastav na proste faktore. Dakle,

$$\tilde{a} = p_2 \cdot p_3 \cdot \ldots \cdot p_\ell = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_k$$

su dva različita rastava broja $\tilde{a}$, te vrijedi $1 < \tilde{a} < a_{min}$. Ovo je kontradikcija s time da je broj a_{min} najmanji broj koji nema jedinstveni rastav. Dakle, početna pretpostavka je bila pogrešna, pa za svaki prirodni broj veći od 1 postoji jedinstveni rastav na proste faktore. □

[13] Ovdje ćemo Propoziciju 5.13 zapravo primijeniti više puta uzastopno: ako $p_1 \mid q_1 \cdot (q_2 \cdot q_3 \cdot q_4)$, onda je $p_1 \mid q_1$ ili $p_1 \mid q_2 \cdot (q_3 \cdot q_4)$. U prvom slučaju smo pokazali željeno, a u drugom slučaju, prema Propoziciji 5.13, $p_1 \mid q_2$ ili $p_1 \mid q_3 \cdot q_4$. Ponovno, u prvom slučaju smo pokazali željeno, a u drugom ponovno primjenjujemo Propoziciju 5.13.

Vratimo se na problem određivanja $M(a,b)$ i $V(a,b)$. Neka je

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}, \quad \alpha_1, \alpha_2, \ldots, \alpha_\ell \geq 0,$$
$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}, \quad \beta_1, \beta_2, \ldots, \beta_\ell \geq 0,$$

za međusobno različite proste brojeve $p_1, p_2, \ldots, p_\ell$. Lako je vidjeti da je d djelitelj broja a ako i samo ako vrijedi

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\ell^{\gamma_\ell}, \quad \gamma_1 \leq \alpha_1,\ \gamma_2 \leq \alpha_2,\ \ldots,\ \gamma_\ell \leq \alpha_\ell.$$

Slično, d je djelitelj broja b ako i samo ako vrijedi

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\ell^{\gamma_\ell}, \quad \gamma_1 \leq \beta_1,\ \gamma_2 \leq \beta_2,\ \ldots,\ \gamma_\ell \leq \beta_\ell.$$

Kako je $M(a,b)$ najveći djelitelj od a i od b, slijedi da je

$$M(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_\ell^{\min\{\alpha_\ell,\beta_\ell\}}.$$

Posve analognim razmatranjem, zaključujemo da najmanji zajednički višekratnik možemo izračunati ovako:

$$V(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_\ell^{\max\{\alpha_\ell,\beta_\ell\}}.$$

U praksi se mjera dvaju brojeva izračunava Euklidovim algoritmom. Naime, za klasična[14] računala nije poznat algoritam koji bi efikasno faktorizirao zadani (veliki) broj na proste faktore—to je jedna od pretpostavki na kojima se bazira suvremena kriptografija.

Uočite da ovdje uzimamo $\alpha_i, \beta_i \geq 0$, dok je u (5.6) bilo $\alpha_i, \beta_i \geq 1$. To smo napravili kako bi se u produktu za a i b mogli javljati isti prosti brojevi $p_1, p_2, \ldots, p_\ell$. Ako je, na primjer, broj a djeljiv sa p_1, a broj b nije, onda će biti $\alpha_1 \geq 1$, ali $\beta_1 = 0$:

$$4312 = 2^3 \cdot 3^0 \cdot 7^2 \cdot 11^1,$$
$$12 = 2^2 \cdot 3^1 \cdot 7^0 \cdot 11^0.$$

Naravno, prikaz u kojem dozvoljavamo 0 u eksponentu nije jedinstven:

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 997^0.$$

$$M(4312, 12) = 2^2 \cdot 3^0 \cdot 7^0 \cdot 11^0 = 4,$$
$$V(4312, 12) = 2^3 \cdot 3^1 \cdot 7^2 \cdot 11^1 = 12936.$$

[14] Za kvantna računala je konstruiran tzv. Shorov algoritam kojim je moguće efikasno faktorizirati velike brojeve.

5.4 *Kongruencije*

U nekim situacijama nije potrebno izračunati vrijednost aritmetičkog izraza, nego je dovoljno samo odrediti ostatak kojeg on daje pri dijeljenju nekim zadanim prirodnim brojem n. Na primjer, ako nas zanimaju zadnje 3 znamenke broja

$$501^{2017} + 499^{2017},$$

dovoljno je odrediti samo ostatak koji taj broj daje pri dijeljenju s 1000, a ne i sam broj. U ovoj cjelini ćemo proučavati svojstava koja imaju ostaci pri dijeljenju zadanim brojem, te ćemo izvesti niz rezultata koji će nam bitno olakšati rješavanje problema sličnih gore navedenom.

Definicija 5.17. *Neka su $a, b \in \mathbb{Z}$, te $n \in \mathbb{N}$. Kažemo da je broj a* KONGRUENTAN *broju b* MODULO *n ako vrijedi $n \mid a - b$.*
Pišemo: $a \equiv b \pmod{n}$.

Drugim riječima, a i b su kongruentni modulo n ako daju isti ostatak pri dijeljenju sa n. Naime, po teoremu o dijeljenju s ostatkom, $a = q_1 \cdot n + r_1$ i $b = q_2 \cdot n + r_2$ za neke $0 \leq r_1, r_2 < n$. Tada je $a - b = (q_1 - q_2) \cdot n + (r_1 - r_2)$, što je djeljivo sa n ako i samo ako je $r_1 - r_2$ djeljivo sa n. Ali, $-n < r_1 - r_2 < n$, pa je $r_1 - r_2$ djeljivo sa n ako i samo ako je $r_1 - r_2 = 0$, to jest, $r_1 = r_2$.

Iz definicije lako vidimo da je, na primjer,

$$17 \equiv 2 \pmod{5} \qquad 17 \equiv -3 \pmod{5}$$
$$17 \equiv 17 \pmod{5} \qquad -3 \equiv 17 \pmod{5}$$
$$25 \equiv 0 \pmod{5} \qquad -9 \equiv -9 \pmod{5}.$$

Ako je zadan broj n, možemo uvesti relaciju "biti kongruentan modulu n": brojevi $a, b \in \mathbb{Z}$ su u relaciji ako je $a \equiv b \pmod{n}$.

Propozicija 5.18. *Relacija "biti kongruentan modulo n" je relacija ekvivalencije nad $\mathbb{Z}$, za svaki $n \in \mathbb{N}$.*

Dokaz.

Refleksivnost. Za sve $a \in \mathbb{Z}$ je $n \mid a - a$, pa je $a \equiv a \pmod{n}$.

Simetričnost. Neka su $a, b \in \mathbb{Z}$ takvi da je $a \equiv b \pmod{n}$. Tada $n \mid a - b$, pa po Propoziciji 5.3(c) vrijedi $n \mid (a - b) \cdot (-1)$, odnosno, $n \mid b - a$, iz čega slijedi $b \equiv a \pmod{n}$.

Tranzitivnost. Neka su $a, b, c \in \mathbb{Z}$ takvi da je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$. Tada $n \mid a - b$ i $n \mid b - c$, pa po Propoziciji 5.3(a) vrijedi $n \mid (a - b) + (b - c)$, odnosno, $n \mid a - c$, iz čega slijedi $a \equiv c \pmod{n}$. □

Kako je relacija "biti kongruentan modulo n" relacija ekvivalencije, prirodno je promatrati njezine klase. Za $a \in \mathbb{Z}$, čemu je jednako $[a]$? Ako je $a \equiv b \pmod{n}$, onda $n \mid a - b$, pa postoji neki cijeli broj $k \in \mathbb{Z}$ takav da je $a - b = n \cdot (-k)$. Iz ovog slijedi:

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} \,:\, a \equiv b \pmod{n}\} \\ &= \{b \in \mathbb{Z} \,:\, b = a + n \cdot k \text{ za neko } k \in \mathbb{Z}\} \\ &= \{a + n \cdot k \,:\, k \in \mathbb{Z}\} \\ &= a + n\mathbb{Z}.\end{aligned}$$

Na primjer, za $n = 5$ je

$$\begin{aligned}[3] &= 3 + 5\mathbb{Z} \\ &= 3 + \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ &= \{\ldots, -7, -2, 3, 8, 13, \ldots\}.\end{aligned}$$

Vidimo da je $[3]$ skup svih brojeva koji pri dijeljenju s 5 daju ostatak 3.

Ovdje smo koristili oznaku $n\mathbb{Z} = \{n \cdot k \,:\, k \in \mathbb{Z}\}$, te $a + S := \{a + s \,:\, s \in S\}$ za proizvoljni skup S. Dakle, u $[a]$ se nalaze svi cijeli brojevi koji se od a razlikuju za neki višekratnik od n, ili, ekvivalentno, svi cijeli brojevi koji daju isti ostatak kao broj a pri dijeljenju s n.

Svi ostaci koje možemo dobiti pri dijeljenju s n su: $0, 1, 2, \ldots, n-1$. Pokažimo da je svaka klasa u relaciji "biti kongruentan modulo n" nužno jednaka jednoj od $[0], [1], \ldots, [n-1]$, odnosno, da ta relacija definira točno n klasa.

Propozicija 5.19. *Neka je $n \in \mathbb{N}$. Tada je kvocijentni skup relacije "biti kongruentan modulo n" dan sa:*

$$\mathbb{Z}/_{\equiv \pmod{n}} = \{[0], [1], [2], \ldots, [n-1]\}.$$

Dokaz. Pokažimo prvo da su sve klase $[0], [1], [2], \ldots, [n-1]$ međusobno različite. Pretpostavimo da za neke $0 \leq \alpha, \beta < n$ vrijedi $[\alpha] = [\beta]$. Prema Teoremu 3.8, slijedi da je $\alpha \equiv \beta \pmod{n}$, odnosno, $n \mid \alpha - \beta$, pa $\alpha - \beta$ mora biti višekratnik od n. Kako je

$$\begin{aligned}0 \leq \alpha &< n, \\ -n < -\beta &\leq 0,\end{aligned}$$

zbrajanjem ovih nejednakosti dobivamo $-n < \alpha - \beta < n$. Jedini višekratnik od n koji zadovoljava ovaj uvjet je 0, pa mora biti $\alpha - \beta = 0$, odnosno, $\alpha = \beta$. Dakle, za $\alpha \neq \beta$ je $[\alpha] \neq [\beta]$.

Pokažimo još da su $[0]$, $[1]$, $[2]$, $\ldots$, $[n-1]$ sve klase koje postoje. Neka je $a \in \mathbb{Z}$ proizvoljan. Po teoremu o dijeljenju s ostatkom, postoje $q, r \in \mathbb{Z}$ takvi da je

$$a = q \cdot n + r, \quad 0 \leq r < n.$$

Tada je $a - r = q \cdot n$, pa $n \mid a - r$, iz čega imamo $a \equiv r \pmod{n}$ i $[a] = [r]$. Zbog $0 \leq r < n$, slijedi da $[a]$ mora biti jedna od klasa $[0]$, $[1]$, $[2]$, $\ldots$, $[n-1]$. □

Definicija 5.20. *Neka su $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ takvi da vrijedi*

$$\begin{aligned} a_0 &\equiv 0 \pmod{n}, \\ a_1 &\equiv 1 \pmod{n}, \\ &\vdots \\ a_{n-1} &\equiv n-1 \pmod{n}. \end{aligned}$$

Kažemo da skup $\{a_0, a_1, \ldots, a_{n-1}\}$ čini POTPUNI SUSTAV OSTATAKA MODULO n.

Na primjer, neki od potpunih sustava ostataka modulo 4 su:

$\{0, 1, 2, 3\}$, $\{4, 9, 14, -1\}$,
$\{0, 1, -2, -1\}$, $\{8, 13, 82, 63\}$.

Sada ćemo pokazati dva rezultata koji će nam omogućiti da brzo i bez previše računanja određujemo ostatke koje veliki brojevi (određenog oblika, recimo, potencije) daju pri dijeljenju.

Propozicija 5.21. *Neka je $n \in \mathbb{N}$ proizvoljan.*

(a) Ako su $a, b, c, d \in \mathbb{Z}$ takvi da vrijedi

$$\begin{aligned} a &\equiv c \pmod{n} \text{ i} \\ b &\equiv d \pmod{n}, \end{aligned}$$

onda je i

$$\begin{aligned} a + b &\equiv c + d \pmod{n}, \\ a - b &\equiv c - d \pmod{n}, \\ a \cdot b &\equiv c \cdot d \pmod{n}. \end{aligned}$$

Drugim riječima, kongruencije smijemo zbrajati, oduzimati i množiti.

(b) Ako su $a, b, c \in \mathbb{Z}$ takvi da je $M(c, n) = 1$, te $a \cdot c \equiv b \cdot c \pmod{n}$, onda je $a \equiv b \pmod{n}$.

Drugim riječima, kongruenciju smijemo pokratiti zajedničkim faktorom lijeve i desne strane *samo u slučaju* kad je taj zajednički faktor relativno prost s brojem n.

Na primjer, $3 \cdot 6 \equiv 7 \cdot 6 \pmod{8}$, ali $3 \not\equiv 7 \pmod{8}$, dakle, ne smijemo pokratiti kongruenciju brojem 6 jer $M(6, 8) \neq 1$.

Dokaz.

(a) Iz $a \equiv c \pmod{n}$ slijedi $n \mid a - c$, a iz $b \equiv d \pmod{n}$ slijedi $n \mid b - d$. Prema Propoziciji 5.3(a) vrijedi $n \mid (a - c) + (b - d)$, odnosno, $n \mid (a + b) - (c + d)$, što po definiciji kongruencije znači $a + b \equiv c + d \pmod{n}$. Posve analogno se dokaže i tvrdnja za razliku. Za produkt, iskoristimo Propoziciju 5.3(c):

$$\begin{aligned} n \mid a - c &\Rightarrow n \mid (a - c) \cdot b, \\ n \mid b - d &\Rightarrow n \mid (b - d) \cdot c, \end{aligned}$$

a zatim ponovno (a) dio iste propozicije:

$$n \mid (a - c) \cdot b + (b - d) \cdot c.$$

Kraćenjem $b \cdot c$ slijedi $n \mid a \cdot b - c \cdot d$, odnosno, $a \cdot b \equiv c \cdot d \pmod{n}$.

(b) Iz $a \cdot c \equiv b \cdot c \pmod{n}$ imamo $n \mid c \cdot (a-b)$. Kako je $M(n,c) = 1$, možemo iskoristiti Propoziciju 5.13(a) i ukloniti faktor c s desne strane. Time dobivamo $n \mid a - b$, odnosno, $a \equiv b \pmod{n}$.

□

Što nam omogućava prethodna propozicija? Primjerice, ako trebamo odrediti ostatak kojeg broj $2017 \cdot 1999$ daje pri dijeljenju s 1000, ne moramo izračunati cijeli produkt i onda tražiti ostatak. Umjesto toga, možemo bitno pojednostavniti postupak tako da prvo izračunamo ostatke koje 2017 i 1999 daju s 1000:

$$\left.\begin{array}{rl} 2017 \equiv 17 & \pmod{1000} \\ 1999 \equiv -1 & \pmod{1000} \end{array}\right\} \Rightarrow 2017 \cdot 1999 \equiv 17 \cdot (-1) \equiv -17 \equiv 983 \pmod{1000}.$$

Gornji "trik" u kojem smo iskoristili $1999 \equiv -1 \pmod{1000}$ umjesto $1999 \equiv 999 \pmod{1000}$ kako bismo imali što manje brojeve tijekom izračuna je tipičan.

Uočite da uzastopnom primjenom Propozicije 5.21(c) možemo i potencirati kongruencije: za svaki $k \in \mathbb{N}$ vrijedi[15]

[15] Dokažite ovu tvrdnju indukcijom.

$$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}. \tag{5.7}$$

Ako je broj n prost, brzo potenciranje omogućava nam i sljedeći teorem.

Teorem 5.22 (Mali Fermatov teorem)**.** *Neka je $a \in \mathbb{N}$ i neka je p prost broj takav da a nije djeljiv sa p. Tada*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Po teoremu o dijeljenju s ostatkom, za svaki $i \in \{1, 2, \ldots, p-1\}$ postoje $q_i, r_i \in \mathbb{Z}$ takvi da je

Ovdje dijelimo broj $i \cdot a$ brojem p, čime dobivamo kvocijent q_i i ostatak r_i.

$$i \cdot a = q_i \cdot p + r_i, \quad 0 \leq r_i < p.$$

Dakle, $p \mid i \cdot a - r_i$, pa je

$$i \cdot a \equiv r_i \pmod{p}. \tag{5.8}$$

Sada uočimo dvije činjenice:

(1) Niti jedan ostatak r_i nije jednak 0. U protivnom, $i \cdot a \equiv r_i \equiv 0 \pmod{p}$, pa $p \mid i \cdot a$. Kako je $M(a,p) = 1$, po Propoziciji 5.13 slijedi $p \mid i$. No to je nemoguće jer je $i \in \{1, 2, \ldots, p-1\}$.

(2) Svi ostaci $r_1, r_2, \ldots, r_{p-1}$ su međusobno različiti. U protivnom, vrijedi $r_i = r_j$ za neke indexe $i \neq j$; možemo bez smanjenja općenitosti uzeti $i < j$. Tada je, po Propoziciji 5.21,

$$\left.\begin{array}{rl} i \cdot a \equiv r_i & \pmod{p} \\ j \cdot a \equiv r_j & \pmod{p} \end{array}\right\} \Rightarrow (j-i) \cdot a \equiv r_j - r_i \equiv 0 \pmod{p},$$

što znači $p \mid (j-i) \cdot a$. Kao i u (1), zbog $M(a,p) = 1$ ovo povlači $p \mid j - i$. Međutim, zbog $0 < i < j < p$ je $0 < j - i < p$, pa je nemoguće da $p \mid j - i$. Dobili smo kontradikciju, pa svi ostaci moraju biti međusobno različiti.

Pierre de Fermat (1607.–1665.), francuski matematičar. Najpoznatiji po tzv. Velikom Fermatovom teoremu: "Ne postoje prirodni brojevi a, b, c, n, takvi da je $n > 2$ i da vrijedi $a^n + b^n = c^n$".

Pomnožimo sve kongruencije (5.8), za $i = 1, 2, \ldots, p-1$:

$$(1 \cdot a) \cdot (2 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \pmod{p}.$$

Sa desne strane gornje kongruencije se nalazi ukupno $p-1$ ostataka pri dijeljenju s p; pri tome niti jedan nije jednak nuli i nikoja dva nisu međusobno jednaka. To znači da se sa desne strane moraju nalaziti *svi* ostaci pri dijeljenju sa p osim nule! Zato gornju kongruenciju možemo zapisati kao

Na primjer, za $p = 5$ su r_1, r_2, r_3, r_4 neki ostaci pri dijeljenju s 5. Ako niti jedan nije nula i nikoja dva nisu ista, onda r_1, r_2, r_3, r_4 moraju biti $1, 2, 3, 4$ u nekom poretku, na primjer $r_1 = 3$, $r_2 = 1$, $r_3 = 4$, $r_4 = 2$. Poredak postaje nebitan kada računamo umnožak $r_1 \cdot r_2 \cdot r_3 \cdot r_4$.

$$(1 \cdot a) \cdot (2 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

odnosno,

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Kako je $M((p-1)!, p) = M(1 \cdot 2 \cdot \ldots \cdot (p-1), p) = 1$, prema Propoziciji 5.21(b) ovu kongruenciju možemo skratiti sa $(p-1)!$, čime dobivamo

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Primjer 5.23. *Pokažimo da je broj* $2^{70} + 3^{70}$ *djeljiv s* 13.

Broj 13 *je prost; zbog* $M(2, 13) = 1$ *i malog Fermatovog teorema vrijedi*

$$2^{12} \equiv 1 \pmod{13}.$$

Kako je s desne strane kongruencije broj 1, *možemo ju brzo potencirati: iskoristimo* (5.7) *uz* $k = 5$ *(želimo se što više približiti potenciji* 2^{70}*):*

$$(2^{12})^5 \equiv 1^5 \pmod{13}, \quad \textit{odnosno,} \quad 2^{60} \equiv 1 \pmod{13}.$$

Trebamo još odrediti ostatak koji daje 2^{10}*: kako je* $2^5 \equiv 32 \equiv 6 \pmod{13}$, *kvadriranjem dobivamo* $2^{10} \equiv 6^2 \equiv 36 \equiv 10 \pmod{13}$. *Sada imamo:*

$$2^{70} \equiv 2^{60} \cdot 2^{10} \equiv 1 \cdot 10 \equiv 10 \pmod{13}.$$

Na gotovo identičan način dobivamo $3^{70} \equiv 3 \pmod{13}$. *Slijedi da je*

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 0 \pmod{13},$$

pa je taj zbroj djeljiv brojem 13.

Leonhard Euler (1707.–1783.), švicarski matematičar, fizičar, logičar, astronom i inženjer

I bez upotrebe malog Fermatovog teorema zbog $3^3 \equiv 27 \equiv 1 \pmod{13}$ odmah dobivamo $3^{69} \equiv (3^3)^{23} \equiv 1^{23} \equiv 1 \pmod{13}$.

Uvjet da je broj p prost u malom Fermatovom teoremu je nužan.[16] Međutim, postoji poopćenje ovog teorema koje koristi tzv. Eulerovu funkciju.

[16] Na primjer, za $p = 10$ i $a = 3$ imamo

$$3^{11} \equiv 177147 \equiv 7 \not\equiv 1 \pmod{10}.$$

Definicija 5.24. *Neka je* $\varphi : \mathbb{N} \to \mathbb{N}$ *definirana ovako:* $\varphi(n)$ *je jednak broju elemenata skupa* $\{1, 2, \ldots, n\}$ *koji su relativno prosti sa* n. *Funkciju* φ *zovemo* EULEROVA FUNKCIJA.

Na primjer, za $n = 6$ promatramo sve brojeve iz skupa $\{1, 2, 3, 4, 5, 6\}$ koji su relativno prosti sa 6. Ima ih 2: to su 1 i 5. Zato je $\varphi(6) = 2$.
Za $n = 6 = 2^1 \cdot 3^1$ formula (5.9) daje

$$\varphi(6) = 6 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 2.$$

Ako imamo rastav broja n na proste faktore, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_\ell^{\alpha_\ell}$, može se pokazati da vrijedi

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_\ell}). \tag{5.9}$$

Dokažite da je izraz na desnoj strani jednakosti (5.9) uvijek cijeli broj!

Koristeći Eulerovu funkciju možemo iskazati poopćenje malog Fermatovog teorema.

Teorem 5.25. *Neka je $n \in \mathbb{N}$ proizvoljan, te $a \in \mathbb{Z}$ takav da je $M(a,n) = 1$. Tada vrijedi:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Na primjer, za $n = 6$ i $a = 25$ imamo $\varphi(6) = 2$, pa Teorem 5.25 daje

$$25^2 \equiv 1 \pmod{6}.$$

Ako je broj n prost, onda su svi brojevi iz skupa $\{1, 2, \ldots, n-1\}$ relativno prosti sa n, pa vrijedi $\varphi(n) = n - 1$. U tom se slučaju Teorem 5.25 svodi na Mali Fermatov teorem.

Osim Eulerove funkcije, postoji još mnogo zanimljivih funkcija vezanih uz proste brojeve. Na primjer, istaknimo funkciju π:

$$\pi : \mathbb{R} \to \mathbb{N}, \quad \pi(x) := \text{ broj prostih brojeva manjih ili jednakih } x.$$

Može se pokazati da vrijedi[17] $\pi(x) \approx \frac{x}{\ln x}$. Svi poznati dokazi ove, kao i brojnih drugih činjenica koji se tiču distribucije prostih brojeva su neelementarni i zahtijevaju vrlo napredne tehnike iz teorije brojeva!

[17] Preciznije,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Za kraj ove cjeline, recimo nešto i o linearnim jednadžbama s kongruencijama. Neka su zadani $n \in \mathbb{N}$, te $a, b \in \mathbb{Z}$. Potrebno je odrediti sve $x \in \mathbb{Z}$ za koje vrijedi

$$a \cdot x \equiv b \pmod{n}. \tag{5.10}$$

Svaki takav x zovemo rješenje kongruencije (5.10). Pogledajmo neke primjere ovakvih jednadžbi i pogodimo njihova rješenja:

$$3x \equiv 1 \pmod{4} \Rightarrow x = \ldots, -5, -1, 3, 7, 11, \ldots$$
$$4x \equiv 1 \pmod{6} \Rightarrow \text{nema rješenja}$$
$$4x \equiv 2 \pmod{6} \Rightarrow \begin{cases} x = \ldots, 2, 8, 14, \ldots \\ x = \ldots, 5, 11, 17, \ldots \end{cases}$$

Lako se vidi da, ako je x rješenje od (5.10), onda je rješenje i svaki $\tilde{x}$ takav da je $\tilde{x} \equiv x \pmod{n}$; za ovakva rješenja kažemo da su ekvivalentna. Dakle, ako (5.10) ima rješenje, onda ih ima beskonačno mnogo. Zanima nas koliko ima međusobno neekvivalentnih rješenja, te postupak njihovog nalaženja. Sljedeći rezultat nam daje odgovor na to pitanje.

U gornjim primjerima, sva rješenja prve jednadžbe su međusobno ekvivalentna. Treća jednadžba ima dva neekvivalentna rješenja, na primjer $x = 2$ i $x = 5$. Sva ostala rješenja su ekvivalentna nekom od ta dva.

Teorem 5.26. *Neka je $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, te $d = M(a,n)$.*
Kongruencija $a \cdot x \equiv b \pmod{n}$ ima rješenje ako i samo ako $d \mid b$. U tom slučaju postoji d neekvivalentnih rješenja.
Ako je x_0 jedno rješenje, onda su $x_0,\ x_0 + \tilde{n},\ x_0 + 2\cdot\tilde{n},\ \ldots, x_0 + (d-1)\cdot\tilde{n}$ sva neekvivalentna rješenja, pri čemu je $\tilde{n} = n/d$.

Dokaz. Dokažimo da $a \cdot x \equiv b \pmod{n}$ ima rješenje ako i samo ako $d \mid b$.

($\Rightarrow$) Neka je x_0 neko rješenje konguencije. Tada $n \mid a \cdot x_0 - b$, pa postoji $y \in \mathbb{Z}$ takav da je $a \cdot x_0 - b = n \cdot y$, odnosno, $b = a \cdot x_0 - n \cdot y$. S druge strane, kako je $d = M(a,n)$, pa $d \mid a$ i $d \mid n$, po Propoziciji 5.3 slijedi $d \mid a \cdot x_0 - n \cdot y$, odnosno, $d \mid b$.

($\Leftarrow$) Obratno, pretpostavimo $d \mid b$. Neka je $c = b/d \in \mathbb{Z}$. Iskoristimo Bézoutov identitet za brojeve a i n: postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$d = a \cdot x_0 + n \cdot y_0.$$

Pomnožimo ovu jednakost sa c:

$$a \cdot (c \cdot x_0) + n \cdot (y_0 \cdot c) = c \cdot d = b.$$

Označimo li $x := c \cdot x_0$, te pogledamo ostatak lijeve i desne strane pri dijeljenju sa n, dobivamo $a \cdot x \equiv b \pmod{n}$, pa je x jedno rješenje konguencije.

Drugi dio dokaza podijelimo u četiri dijela:

(1) Ako je x_0 neko rješenje, onda je i $x_0 + j \cdot \tilde{n}$ također rješenje, za svako $j \in \mathbb{Z}$. To vidimo ovako: uz oznaku $\tilde{a} = a/d \in \mathbb{Z}$, vrijedi

$$\begin{aligned} a \cdot (x_0 + j \cdot \tilde{n}) &\equiv a \cdot x_0 + j \cdot a \cdot \tilde{n} \\ &\equiv b + j \cdot \tilde{a} \cdot d \cdot \tilde{n} \\ &\equiv b + j \cdot \tilde{a} \cdot n \\ &\equiv b \pmod{n}. \end{aligned}$$

(2) Ako su x_0 i x_1 dva rješenja, onda postoji $j \in \mathbb{Z}$ takav da je $x_1 = x_0 + j \cdot \tilde{n}$. To vidimo ovako: kako je $a \cdot x_0 \equiv b \equiv a \cdot x_1 \pmod{n}$, onda $n \mid a \cdot (x_1 - x_0)$, pa postoji $k \in \mathbb{Z}$ takav da je

$$a \cdot (x_1 - x_0) = k \cdot n.$$

Podijelimo ovu jednakost sa d, čime dobivamo $\tilde{a} \cdot (x_1 - x_0) = k \cdot \tilde{n}$, gdje smo ponovno označili $\tilde{a} = a/d \in \mathbb{Z}$. Ovo možemo zapisati kao $\tilde{n} \mid \tilde{a} \cdot (x_1 - x_0)$, a kako je $M(\tilde{n}, \tilde{a}) = 1$, prema Propoziciji 5.13(a) slijedi $\tilde{n} \mid x_1 - x_0$. Dakle, postoji $j \in \mathbb{Z}$ takav da je $x_1 - x_0 = j\tilde{n}$.

(3) Svako rješenje kongruencije je ekvivalentno jednom od $x_0,\ x_0 + \tilde{n},\ \ldots,\ x_0 + (d-1) \cdot \tilde{n}$. To vidimo ovako: prema (2), svako rješenje je oblika $x = x_0 + j \cdot \tilde{n}$. Neka je $\tilde{j}$ ostatak pri dijeljenju broja j sa d: $j = q \cdot d + \tilde{j}$, gdje je $0 \leq \tilde{j} < d$. Tada je

$$\begin{aligned} x &\equiv x_0 + j \cdot \tilde{n} \equiv x_0 + (q \cdot d + \tilde{j}) \cdot \tilde{n} \\ &\equiv x_0 + q \cdot d \cdot \tilde{n} + \tilde{j} \cdot \tilde{n} \equiv x_0 + q \cdot n + \tilde{j} \cdot \tilde{n} \\ &\equiv x_0 + \tilde{j} \cdot \tilde{n} \pmod{n}, \end{aligned}$$

dakle, rješenje x je ekvivalentno rješenju $\tilde{x} = x_0 + \tilde{j} \cdot \tilde{n}$.

(4) Rješenja $x_0,\ x_0 + \tilde{n},\ \ldots,\ x_0 + (d-1) \cdot \tilde{n}$ nisu ekvivalentna. To vidimo ovako: pretpostavimo da je $x_0 + j_1 \cdot \tilde{n} \equiv x_0 + j_2 \cdot \tilde{n} \pmod{n}$ za neke $0 \leq j_1, j_2 < d$. Tada $n \mid \tilde{n} \cdot (j_1 - j_2)$, pa postoji $k \in \mathbb{Z}$ takav da $\tilde{n} \cdot (j_1 - j_2) = n \cdot k$. Podijelimo li ovu jednakost sa $\tilde{n}$, dobivamo

$$j_1 - j_2 = d \cdot k,$$

pa je $j_1 - j_2$ djeljivo sa d. No, zbog $-d < j_1 - j_2 < d$ to povlači $j_1 - j_2 = 0$, odnosno, $j_1 = j_2$.

□

Opišimo sada efektivni postupak za rješavanje linearnih kongruencija. Prema prethodnom teoremu, dovoljno je pronaći samo jedno rješenje, pa ćemo automatski moći odrediti sva. Radi jednostavnosti, promotrimo samo kongruencije oblika[18]

$$a \cdot x \equiv b \pmod{n}, \qquad \text{pri čemu je } M(a,n) = 1. \tag{5.11}$$

[18] Za opći slučaj, pogledajte Zadatak 5.5.

Pretpostavimo da uspijemo odrediti broj $\hat{a}$ takav[19] da je $\hat{a} \cdot a \equiv 1 \pmod{n}$. Pomnožimo (5.11) brojem $\hat{a}$:

[19] Broj $\hat{a}$ zovemo MULTIPLIKATIVNI INVERZ od a.

$$x \equiv (\hat{a} \cdot a) \cdot x \equiv \hat{a} \cdot b \pmod{n}.$$

Dakle, broj $x = \hat{a} \cdot b$ je jedno rješenje kongruencije. Kako odrediti $\hat{a}$? Prisjetimo se Teorema 5.25: vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$. Stoga, ako stavimo

$$\hat{a} = a^{\varphi(n)-1},$$

očito imamo $a \cdot \hat{a} \equiv 1 \pmod{n}$.

Za ilustraciju, riješimo $3x \equiv 2 \pmod{8}$. Kako je $d = M(3,8) = 1$, prema Teoremu 5.26 dovoljno je pronaći jedno rješenje i sva će biti ekvivalentna njemu. Da odredimo to rješenje, prvo trebamo izračunati $\hat{a} = 3^{\varphi(8)-1}$. Kako je $\varphi(8) = 4$, slijedi $\hat{a} \equiv 3^3 \equiv 3 \pmod{8}$, pa dobivamo rješenje kongruencije kao

$$x \equiv \hat{a} \cdot b \equiv 3 \cdot 2 \equiv 6 \pmod{8}.$$

5.5 Zadaci

Zadatak 5.1. *Dokažite da je broj koraka u Euklidovom algoritmu za određivanje $M(a,b)$ manji ili jednak $2\lceil \log_2(\min\{a,b\}) + 1 \rceil$. Ovdje je $\lceil x \rceil$ najmanji cijeli broj veći ili jednak x. Uputa: ako je $a = q_1 \cdot b + r_1$, te $b = q_2 \cdot r_1 + r_2$, dokažite da je $r_2 \leq b/2$.*

Dakle, ako a i b imaju 1000 znamenki u binarnom zapisu (otprilike 300 u dekadskom, dakle, $a, b \approx 10^{300}$), Euklidov algoritam će trebati manje od 2000 koraka! "Naivni" algoritam bi trebao 10^{300} koraka.

Zadatak 5.2. *Dokažite da za prirodne brojeve $a, b \in \mathbb{N}$ vrijedi $M(a,b) \cdot V(a,b) = a \cdot b$.*

Zadatak 5.3. *Odredite zadnje tri znamenke broja $501^{2017} + 499^{2017}$.*

Zadatak 5.4. *Dokažite Teorem 5.25. Uputa: slijedite dokaz malog Fermatovog teorema, no umjesto svih $i \in \{1, 2, \ldots, n-1\}$ promatrajte samo one za koje vrijedi $M(i,n) = 1$.*

Zadatak 5.5. *Promotrimo kongruenciju $a \cdot x \equiv b \pmod{n}$, pri čemu $d \mid b$ za $d = M(a,n)$. Neka su $k, \ell \in \mathbb{Z}$ takvi da je $d = k \cdot a + \ell \cdot n$ (ovi brojevi postoje prema Bézoutovom identitetu). Dokažite da je jedno rješenje kongruencije dano sa $x = k \cdot \tilde{b}$, pri čemu je $\tilde{b} = b/d$.*

Zadatak 5.6. *Promotrimo sljedeće proširenje Euklidovog algoritma za određivanje $M(a,b)$: neka je $r_0 = a$, $r_1 = b$, $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$. Za $i = 1, 2, \ldots$, neka u i-tom koraku algoritma primjenjujemo teorem o dijeljenju s ostatkom na brojeve r_{i-1} i r_i, te dobivamo kvocijent q_i i ostatak r_{i+1}:*

$$r_{i-1} = q_i \cdot r_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i.$$

Definirajmo

$$x_{i+1} = x_{i-1} - q_i \cdot x_i,$$
$$y_{i+1} = y_{i-1} - q_i \cdot y_i.$$

Dokažite (indukcijom) da za sve $i = 0, 1, 2, \ldots$ vrijedi

$$r_i = x_i \cdot a + y_i \cdot b.$$

Dakle, ako je $r_{\ell+1} = 0$, onda je $r_\ell = M(a, b)$, pa je

$$M(a, b) = x_\ell \cdot a + y_\ell \cdot b.$$

Ovaj algoritam zovemo PROŠIRENI EUKLIDOV ALGORITAM *i njime možemo odrediti koeficijente iz Bézoutovog identiteta.*

Na primjer odredimo x, y takve da je $M(23, 7) = 1 = x \cdot 23 + y \cdot 7$.

Priprema: $r_0 = 23$, $r_1 = 7$
$x_0 = 1$, $x_1 = 0$
$y_0 = 0$, $y_1 = 1$

Korak $i = 1$:
$23 = q_1 \cdot 7 + r_2 \Rightarrow q_1 = 3$, $r_2 = 2$
$x_2 = x_0 - q_1 \cdot x_1 = 1$
$y_2 = y_0 - q_1 \cdot y_1 = -3$

Korak $i = 2$:
$7 = q_2 \cdot 2 + r_3 \Rightarrow q_2 = 3$, $r_3 = 1$
$x_3 = x_1 - q_2 \cdot x_2 = -3$
$y_3 = y_1 - q_2 \cdot y_2 = 10$

Korak $i = 3$:
$2 = q_3 \cdot 1 + r_4 \Rightarrow q_3 = 2$, $r_4 = 0$

Dakle, $r_3 = M(23, 7) = 1$, pa je

$$M(23, 7) = x_3 \cdot 23 + y_3 \cdot 7.$$

I zaista, $1 = -3 \cdot 23 + 10 \cdot 7$.

6
Funkcije

Definicija 6.1. *Neka su A, B neprazni skupovi. Relacija $\rho \subseteq A \times B$ je* FUNKCIJSKA *ako*

$$(\forall a \in A)(\exists! b \in B)\ a\rho b.$$

Funkcijsku relaciju zovemo i FUNKCIJA (PRESLIKAVANJE)*.*

Uočimo da funkcijska relacija jednoznačno određuje pridruživanje

$$A \ni a \mapsto b \in B,$$

odnosno, svakom elementu skupa A jednoznačno je pridružen točno jedan element skupa B.

Primjer 6.2. *Neka su $A = \{1, 2, 3\}$, $B = \{a, b\}$. Definiramo relacije:*

$$f_1 = \{(1, a), (2, b), (3, a)\}, \quad f_2 = \{(1, a), (2, a), (2, b), (3, c)\}.$$

Relacija f_1 je funkcijska, a relacija f_2 nije funkcijska.[1] *Relacija f_1 definira pridruživanje $1 \mapsto a$, $2 \mapsto b$ i $3 \mapsto a$, što obično zapisujemo na sljedeći način: $f_1(1) = a$, $f_1(2) = b$, $f_1(3) = a$.*

[1] Zaista, za element $2 \in A$ postoje dva elementa skupa B koja su s njim u relaciji f_2: $2 f_2 a$ i $2 f_2 b$.

Definicija 6.3. *Neka su A, B neprazni skupovi i $f \subseteq A \times B$ funkcijska relacija. Skup A zovemo* DOMENA*, a skup B* KODOMENA *funkcije f. Neka je $x \in A$. Tada jedinstveni element $y \in B$ takav da xfy označavamo sa $y = f(x)$.*[2] *Pišemo $f : A \to B$.*

[2] Alternativno, funkciju možemo definirati bez korištenja relacija kao uređenu trojku (A, B, f), gdje je f pravilo koje svakom elementu skupa A pridružuje točno jedan element skupa B.

Navedimo sada nekoliko osnovnih primjera funkcija:

(a) Neka su $A \subseteq B$ neprazni skupovi. Funkciju

$$i : A \to B,\ i(x) = x,\ x \in A,$$

zovemo INKLUZIJA.

(b) Neka je $f : A \to B$ i $D \subseteq A$. Funkciju

$$f|_D : D \to B,\ f|_D(x) = f(x),\ x \in D,$$

zovemo RESTRIKCIJA funkcije f na D.[3]

[3] Uočite da funkcije f i $f|_D$ nisu jednake usprkos tome što imaju jednako pravilo pridruživanja jer im domene nisu jednake.

(c) Funkciju $id_A : A \to A$, $id_A(x) = x$, $x \in A$, zovemo IDENTITETA na skupu A.

(d) Neka su A, B neprazni skupovi. Definiramo funkcije p_A i p_B na sljedeći način:

$$p_A : A \times B \to A,\ p_A(a,b) = a,\ (a,b) \in A \times B,$$

$$p_B : A \times B \to B,\ p_B(a,b) = b,\ (a,b) \in A \times B.$$

Funkciju p_A zovemo PROJEKCIJA na skup A duž skupa B, a funkciju p_B zovemo PROJEKCIJA na skup B duž skupa A.

(e) Neka je A neprazan skup te $\sim$ relacija ekvivalencije na A. Tada definiramo:

$$q : A \to A/_{\sim},\ q(x) = [x].$$

Preslikavanje q zovemo KVOCIJENTNO PRESLIKAVANJE.[4]

(f) BINARNA OPERACIJA na G je preslikavanje sa domenom $G \times G$ i kodomenom G.[5]

(g) Neka je $f : \mathbb{R} \to \mathbb{R}$. Tada kažemo da je f REALNA FUNKCIJA REALNE VARIJABLE. Primjer takve funkcije je:

$$h(x) = \begin{cases} x^2 + 1 & , \quad x > 0, \\ 0 & , \quad x = 0, \\ e^x & , \quad x < 0. \end{cases}$$

[4] Npr. neka je $A = \mathbb{Z}$, a relacija $\sim = \equiv \pmod 5$. Tada je preslikavanje $q : \mathbb{Z} \to \mathbb{Z}_5$ zadano sa $q(n) = [n]$ primjer jednog kvocijentnog preslikavanja. Na primjer, $q(17) = [17] = [2]$.

[5] Primjerice, zbrajanje je binarna operacija na $\mathbb{N}$, tj. $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Definicija 6.4. *Funkcije $f : A \to B$ i $g : C \to D$ su* JEDNAKE *ako vrijedi $A = B$, $C = D$ i $(\forall x \in A)\ f(x) = g(x)$. Tada pišemo $f = g$.*

Primjer 6.5. *(a)*

$$\left.\begin{array}{l} f : \mathbb{R} \to \mathbb{R},\ f(x) = |x| \\ g : \mathbb{R} \to \mathbb{R},\ g(x) = \sqrt{x^2} \end{array}\right\}\ f = g.$$

(b)

$$\left.\begin{array}{l} f : \mathbb{R} \to \mathbb{R},\ f(x) = |x| \\ g : \mathbb{R} \to [0, \infty\rangle,\ g(x) = |x| \end{array}\right\}\ f \neq g.$$

Definicija 6.6. *Neka je $f : A \to B$ funkcija. Kažemo da je f*

(a) INJEKCIJA *ako* $(\forall x, y \in A)\ x \neq y \Rightarrow f(x) \neq f(y)$.

(b) SURJEKCIJA *ako* $(\forall y \in B)(\exists x \in A)\ f(x) = y$.

(c) BIJEKCIJA *ako je f i injekcija i surjekcija.*

Promotrimo sada četiri funkcije, koje ilustriraju da svojstva injektivnosti i surjektivnosti mogu doći u bilo kojoj kombinaciji.

(a) $A = \{a, b, c\}$, $B = \{1, 2, 3\}$. Preslikavanje $f_1 : A \to B$ zadamo sa $a \mapsto 2,\ b \mapsto 1,\ c \mapsto 3$. Tada je f_1 injekcija i surjekcija, tj. f_1 je bijekcija.

(b) $A = \{a, b, c\}$, $B = \{1, 2\}$. Preslikavanje $f_2 : A \to B$ zadamo sa $a \mapsto 2,\ b \mapsto 1,\ c \mapsto 2$. Tada je f_2 surjekcija, ali nije injekcija.

(c) $A = \{a, b\}$, $B = \{1, 2, 3\}$. Preslikavanje $f_3 : A \to B$ zadamo sa $a \mapsto 2,\ b \mapsto 1$. Tada je f_3 injekcija, ali nije surjekcija.

(d) $A = \{a, b, c\}$, $B = \{1, 2, 3\}$. Preslikavanje $f_4 : A \to B$ zadamo sa $a \mapsto 2$, $b \mapsto 2$, $c \mapsto 1$. Tada f_4 nije ni injekcija ni surjekcija.

Gornji primjer nam pokazuje da općenito iz činjenice da je neka funkcija injekcija (surjekcija) ne možemo ništa zaključiti o surjektivnosti (injektivnosti) te funkcije.[6]

[6] U nekim specijalnim slučajevima su pojmovi injektivnosti i surjektivnosti povezani. Recimo, neka je A konačan skup. Tada je $f : A \to A$ injekcija ako i samo ako je i surjekcija. Vidi Zadatak 6.1.

Napomena 6.7. *Obrat po kontrapoziciji daje:*

$$f : A \to B \text{ je injekcija } \Leftrightarrow (\forall x, y \in A)\ f(x) = f(y) \Rightarrow x = y.$$

Definicija 6.8. KOMPOZICIJA *funkcija $f : A \to B$ i $g : B \to C$ je funkcija $g \circ f : A \to C$ definirana*[7] *sa:*

$$(g \circ f)(x) = g(f(x)),\ x \in A.$$

[7] Uočite da domene moraju biti ulančane da bi kompozicija bila dobro definirana, tj. kodomena funkcije f mora biti jednaka domeni funkcije g.

Primjer 6.9. *Promotrimo funkcije $f, g : \mathbb{R} \to \mathbb{R}$ zadane sa $f(x) = x + 1$, $g(x) = x^2 + 1$, $x \in \mathbb{R}$. Tada su i obje kompozicije $g \circ f, f \circ g : \mathbb{R} \to \mathbb{R}$ dobro definirane i vrijedi:*

$$(g \circ f)(x) = g(f(x)) = f(x+1) = (x+1)^2 + 1 = x^2 + 2x + 2,$$

$$(f \circ g)(x) = f(g(x)) = f(x^2+1) = (x^2+1) + 1 = x^2 + 2.$$

Dakle, $g \circ f \neq f \circ g$.

Gornji primjer nam pokazuje da operacija kompozicije funkcija nije komutativna.[8] Dokažimo sada neka svojstva kompozicije funkcija.

[8] Općenito, obje kompozicije $f \circ g$ i $g \circ f$ ne moraju istovremeno biti ni definirane jer domene nisu nužno ulančane.

Propozicija 6.10. *Neka su $f : A \to B$, $g : B \to C$ i $h : C \to D$ funkcije. Tada vrijedi:*

(a) Kompozicija funkcija je asocijativna, tj. $(h \circ g) \circ f = h \circ (g \circ f)$.

(b) Ako su f i g injekcije, tada je i $g \circ f$ injekcija.

(c) Ako su f i g surjekcije, tada je i $g \circ f$ surjekcija.

Dokaz.

(a) Najprije uočimo da su obje kompozicije $(h \circ g) \circ f$ i $h \circ (g \circ f)$ definirane sa domenom A i kodomenom D. Računamo:

$$\big((h \circ g) \circ f\big)(x) = (h \circ g)(f(x)) = h\big(g(f(x))\big) = h\big((g \circ f)(x)\big)$$

$$= \big(h \circ (g \circ f)\big)(x), \quad x \in A.$$

Dakle, $(h \circ g) \circ f = h \circ (g \circ f)$.

(b) Koristit ćemo karakterizaciju injekcije iz Napomene 6.7. Neka su $x, y \in A$ takvi da $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Tada zbog injektivnosti funkcije g vrijedi $f(x) = f(y)$ pa zbog injektivnosti funkcije f vrijedi $x = y$. Po Napomeni 6.7 dokazali smo da je $g \circ f$ injekcija.

(c) Neka je $c \in C$ proizvoljan. Po pretpostavci, funkcija g je surjekcija, pa postoji $b \in B$ takav da $g(b) = c$. Kako je i f surjekcija, postoji $a \in A$ takav da $f(a) = b$. Tada vrijedi:

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

Kako je bio $c \in C$ proizvoljan, dokazali smo da je $g \circ f$ surjekcija.

□

Propozicija 6.11. *Neka su $f : A \to B$ i $g : B \to C$ funkcije. Tada vrijedi:*

(a) Ako je $g \circ f$ injekcija, onda je f injekcija.

(b) Ako je $g \circ f$ surjekcija, onda je g surjekcija.

Dokaz.

(a) Neka su $x_1, x_2 \in A$ takvi da $f(x_1) = f(x_2)$. Tada vrijedi

$$(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2).$$

Kako je $g \circ f$ injekcija, po Napomeni 6.7 vrijedi $x_1 = x_2$. Ponovno koristeći Napomenu 6.7 zaključujemo da je i f injekcija.

(b) Neka je $c \in C$. Tvrdimo da postoji $b \in B$ takav da $g(b) = c$.

Kako je $g \circ f$ surjekcija, postoji $a \in A$ takav da $(g \circ f)(a) = c$. Definiramo $b := f(a)$. Tada direktno iz Definicije 6.8 slijedi $g(b) = c$.

□

Propozicija 6.12. *Funkcija $f : A \to B$ je bijekcija ako i samo ako vrijedi*

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

Dokaz.

[⇒] Neka je $f : A \to B$ bijekcija, te $y \in B$. Kako je f surjekcija, postoji $x \in A$ takav da $f(x) = y$.

Ako su $x_1, x_2 \in A$ takvi da $f(x_1) = y = f(x_2)$, onda vrijedi $x_1 = x_2$ pošto je f injekcija.

[⇐] Očito je f surjekcija. Pokažimo da je i injekcija.

Neka su $x_1, x_2 \in A$ takvi da $f(x_1) = f(x_2) = y$. Tada $(\exists! x \in A)$ takav da $f(x) = y$. Dakle, $x_1 = x = x_2$.

□

Neka je $f : A \to B$ bijekcija. Iz Propozicije 6.12 slijedi da možemo definirati preslikavanje $f^{-1} : B \to A$ na sljedeći način:

$$f^{-1}(y) = x \ \Leftrightarrow f(x) = y, \quad y \in B. \tag{6.1}$$

Funkciju f^{-1} zovemo INVERZNA FUNKCIJA funkcije f.

Propozicija 6.13. *Neka je $f : A \to B$ bijekcija i $f^{-1} : B \to A$ njoj inverzna funkcija. Tada:*

(a) $f \circ f^{-1} = id_B$, $f^{-1} \circ f = id_A$.

(b) f^{-1} *je jedinstvena funkcija za koju vrijedi svojstvo (a).*

Dokaz.

(a) Obje tvrdnje se dokazuju analogno pa ćemo dokazati samo $f^{-1} \circ f = id_A$. Po definiciji kompozicije, vrijedi $f^{-1} \circ f : A \to A$ i

$$(f^{-1} \circ f)(x) = f^{-1}(\underbrace{f(x)}_{y}) = f^{-1}(y) = x.$$

Zadnja jednakost slijedi iz definicije inverzne funkcije (6.1).

(b) Pretpostavimo da je $g : B \to A$ neka funkcija za koju vrijedi $f \circ g = id_B$ i $g \circ f = id_A$. Tada:

$$\begin{aligned} f \circ g = id_B \quad &\Rightarrow \quad f^{-1} \circ (f \circ g) = f^{-1} \circ id_B \\ &\Rightarrow \quad (f^{-1} \circ f) \circ g = f^{-1} \\ &\Rightarrow \quad id_A \circ g = f^{-1} \\ &\Rightarrow \quad g = f^{-1}. \end{aligned}$$

□

Korolar 6.14. *Neka je $f : A \to B$ funkcija. Pretpostavimo da postoji funkcija $g : B \to A$ takva da $f \circ g = id_B$ i $g \circ f = id_A$. Tada je f bijekcija i vrijedi $f^{-1} = g$.*

Dokaz. Kako je $g \circ f = id_A$ injekcija, po Propoziciji 6.11 (a) slijedi da je f injekcija. Nadalje, pošto je $f \circ g = id_B$ surjekcija, po Propoziciji 6.11 (b) slijedi da je f surjekcija. Dakle, f je bijekcija. Sada $f^{-1} = g$ slijedi iz Propozicije 6.13 (b). □

Ako je $f : A \to B$ bijekcija, tada je po Korolaru 6.14 i f^{-1} bijekcija te vrijedi $(f^{-1})^{-1} = f$.

Definicija 6.15. *Neka je $f : A \to B$ funkcija. Za $C \subseteq A$ definiramo* SLIKU SKUPA *C sa:*

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

Za $D \subseteq B$ definiramo PRASLIKU SKUPA *D sa*[9]*:*

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

Skup $\mathcal{R}_f := f(A)$ zovemo SLIKA FUNKCIJE *f.*

[9] f nije nužno bijekcija pa f^{-1} u ovom slučaju ne označava inverz funkcije f. Međutim, u slučaju da f jest bijekcija, onda je praslika skupa D za funkciju f jednaka slici skupa D za funkciju f^{-1}, tj. oznaka je konzistentna.

Primjer 6.16. *Neka je $f : \mathbb{Z} \to \mathbb{Z}$ zadana sa $f(z) = |z|$. Tada:*

$$\mathcal{R}_f = f(\mathbb{Z}) = \mathbb{N}_0, \quad f^{-1}(\{2,4,6,8\}) = \{2,-2,4,-4,6,-6,8,-8\}.$$

Ako je $f : A \to B$ injekcija, onda je $f : A \to f(A)$ bijekcija[10] pa možemo definirati $f^{-1} : f(A) \to A$. Pogledajmo sada u kakvom su odnosu slika i praslika funkcije sa skupovnim operacijama unije i presjeka.

[10] Npr. $f(x) = x^2$ je bijekcija $\mathbb{R}_+ \to \mathbb{R}_+$, a njen inverz $f^{-1} : \mathbb{R}_+ \to \mathbb{R}_+$ dan je sa $f^{-1}(x) = \sqrt{x}$.

Propozicija 6.17. *Neka je $f : S \to T$, te $A, B \subseteq S$, $C, D \subseteq T$. Tada:*

(a) $f(A \cup B) = f(A) \cup f(B)$,

(b) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,

(c) $f(A \cap B) \subseteq f(A) \cap f(B)$,

(d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$,

(e) $A \subseteq f^{-1}(f(A))$.

Dokaz. Dokaz ostavljamo kao Zadatak 6.2. □

Uočite da u tvrdnjama (c) i (e) Propozicije 6.17 općenito ne vrijede jednakosti.[11] Uzmimo npr. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $A = [0,1]$, $B = [-1,0]$. Tada

$$f(A \cap B) = f(\{0\}) = \{0\},\ f(A) \cap f(B) = [0,1] \cap [0,1] = [0,1].$$

Također, $f^{-1}(f(A)) = f^{-1}([0,1]) = [-1,1]$.

U ostatku ovog poglavlja bavit ćemo se "veličinom" skupova u određenom smislu. U slučaju konačnih skupova elemente skupa možemo jednostavno prebrojiti pa skupove možemo uspoređivati po broju elemenata. Recimo skup $\{a,b,c\}$ ima 3 elementa pa je "veći" od skupa $\{\heartsuit, \diamondsuit\}$ koji ima dva elementa. Međutim, u slučaju beskonačnih skupova situcija je bitno složenija.

Definicija 6.18. *Neprazni skupovi A i B su* EKVIPOTENTNI *ako postoji bijekcija $f : A \to B$. Pišemo $|A| = |B|$ ili* $\operatorname{card} A = \operatorname{card} B$.

Promotrimo par primjera koji će ilustrirati Definiciju 6.18:

(a) Neka je $A = \{1,2\}$, $B = \{\heartsuit, \diamondsuit\}$. Tada je preslikavanje zadano sa $1 \mapsto \heartsuit$, $2 \mapsto \diamondsuit$ bijekcija pa su skupovi A i B ekvipotentni. Uočite da ova bijekcija odgovara upravo onome što intuitivno zovemo brojenje elemenata skupa. Naime, elemente skupa B smo prebrojali tako da smo mu pridružili brojeve 1 i 2. Dakle, za konačne skupove Definicija 6.18 odgovara intuitivnom pojmu "broj elemenata skupa".

David Hilbert (1862.–1943.), njemački matematičar

(b) Definiramo funkciju $f : \mathbb{Z} \to \mathbb{N}$ sa

$$f(z) = \begin{cases} 2z+1 & , \quad z \geq 0, \\ -2z & , \quad z < 0. \end{cases}$$

Lako se vidi da je f bijekcija.[12] Dakle, skupovi $\mathbb{N}$ i $\mathbb{Z}$ su ekvipotentni iako vrijedi[13] $\mathbb{N} \subsetneq \mathbb{Z}$.

(c) Funkcija $f : \langle 0,1 \rangle \to \mathbb{R}$ zadana sa $f(x) = \frac{2x-1}{1-|2x-1|}$ je bijekcija.[14] Dakle, $\operatorname{card} \langle 0,1 \rangle = \operatorname{card} \mathbb{R}$.

Uočite da "biti ekvipotentan" ima sljedeća svojstva:

1. $|A| = |A|$. Naime, $id_A : A \to A$ je bijekcija.
2. $|A| = |B| \ \Rightarrow \ |B| = |A|$. Ako je $f : A \to B$ bijekcija, onda je $f^{-1} : B \to A$ bijekcija.

[11] Međutim, jednakosti vrijedi ako je f injekcija. Dokažite!

[12] Zadatak 6.3.

[13] Ovu na prvi pogled neintuitivnu činjenicu o beskonačnim skupovima Hilbert je pokušao ilustrirati pričom o "Hilbertovom hotelu". Zgodnu ilustraciju te priče možete vidjeti u sljedećem linku.

[14] Zadatak 6.4

3. $(|A| = |B| \wedge |B| = |C|) \Rightarrow |A| = |C|$. Neka su $f : A \to B$ i $g : B \to C$ bijekcija. Tada je $g \circ f : A \to C$ bijekcija.

Međutim, ne kažemo da je "biti ekvipotentan" relacija ekvivalencije. Naime, ne postoji skup na kojem bi definirali tu relaciju[15].

[15] "Skup svih skupova" nije skup, vidi Primjer 2.24

Definicija 6.19. *Neka je $A \neq \emptyset$. Kažemo da je A:*

(a) KONAČAN, *ako je ekvipotentan sa skupom $\{1, 2, \ldots, n\}$ za neko $n \in \mathbb{N}$. Pišemo $|A| = n$ ili $\operatorname{card} A = n$. U protivnom, kažemo da je A* BESKONAČAN.

(b) PREBROJIV, *ako je A ekvipotentan sa skupom $\mathbb{N}$. Pišemo*[16] *$|A| = \aleph_0$ ili $\operatorname{card} A = \aleph_0$.*

[16] $\aleph_0$ čitamo "aleph nula", $\aleph$ je prvo slovo hebrejskog alfabeta.

(c) NEPREBROJIV, *ako nije konačan niti prebrojiv.*

Također, dogovorno pišemo $|\emptyset| = 0$.

Promotrimo ponovno par primjera:

(a) Po Definiciji 6.19 vrijedi $\operatorname{card}\{1, 2, \ldots, n\} = n$.

(b) Po Zadatku 6.3 vrijedi $\operatorname{card} \mathbb{Z} = \aleph_0$.

(c) Tvrdimo $\operatorname{card} \mathbb{N} \times \mathbb{N} = \aleph_0$. Zaista, definirajmo funkciju $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ formulom

$$f(m, n) = \frac{(m + n - 1)(m + n - 2)}{2} + m, \quad (m, n) \in \mathbb{N} \times \mathbb{N}.$$

Funkcija f je bijekcija. Definiciju funkcije f najlakše ćemo ilustrirati pomoću sljedeće tablice:

~~$(1,1)^1$~~	~~$(1,2)^2$~~	~~$(1,3)^4$~~	~~$(1,4)^7$~~	~~$(1,5)^{11}$~~ $\ldots$
~~$(2,1)^3$~~	~~$(2,2)^5$~~	~~$(2,3)^8$~~	~~$(2,4)^{12}$~~	$(1,5)\ldots$
~~$(3,1)^6$~~	~~$(3,2)^9$~~	~~$(3,3)^{13}$~~	$(3,4)$	$(3,5)\ldots$
~~$(4,1)^{10}$~~	~~$(4,2)^{14}$~~	$(4,3)$	$(4,4)$	$(4,5)\ldots$
~~$(5,1)^{15}$~~	$(5,2)$	$(5,3)$	$(5,4)$	$(5,5)\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Sljedeći cilj nam je odrediti $\operatorname{card} \mathbb{Q}$. U tu svrhu najprije dokažimo sljedeću propoziciju.

Propozicija 6.20. *Neka su A, B, C, D neprazni skupovi takvi da $\operatorname{card} A = \operatorname{card} B$ i $\operatorname{card} C = \operatorname{card} D$. Tada $\operatorname{card} A \times C = \operatorname{card} B \times D$.*

Dokaz. Neka su $f : A \to B$ i $g : C \to D$ bijekcija. Sada definiramo $h : A \times C \to B \times D$ sa

$$h(a, c) = (f(a), g(c)), \quad (a, c) \in A \times C.$$

Očito[17] je h bijekcija i time je tvrdnja propozicije dokazana. □

[17] Neka je $(b, d) \in B \times D$ proizvoljan. Tada postoje $a \in A$ i $c \in C$ takvi da $f(a) = b$, $g(c) = d$, pa tada vrijedi $h(a, c) = (b, d)$.
Neka su $(a_1, c_1), (a_2, c_2) \in A \times C$ takvi da $h(a_1, c_1) = h(a_2, c_2)$. Tada $f(a_1) = f(a_2)$ i $g(c_1) = g(c_2)$, pa zbog injektivnosti f i g vrijedi $a_1 = a_2$ i $c_1 = c_2$, tj. $(a_1, c_1) = (a_2, c_2)$.

Iz Propozicije 6.20 direktno slijedi $\operatorname{card} \mathbb{Z} \times \mathbb{N} = \aleph_0$. Intuitivno, elemenata iz $\mathbb{Q}$ ima "manje ili jednako" od elemenata u $\mathbb{Z} \times \mathbb{N}$. Zbog toga očekujemo da je $\mathbb{Q}$ prebrojiv. Međutim, najprije je potrebno precizno definirati pojam "ima manje ili jednako elemenata".

Definicija 6.21. *Neka su A, B skupovi. Kažemo da je kardinalnost skupa A* MANJA OD KARDINALNOSTI SKUPA *B, pišemo* $\operatorname{card} A \leq \operatorname{card} B$, *ako postoji injekcija $f : A \to B$.*

Sljedeći teorem ćemo samo iskazati bez dokaza. Dokaz tog teorema radit će se u kolegiju "Teorija skupova", a može se naći u svakom udžbeniku iz teorije skupova, vidi npr. [18].

[18] M Vuković. Teorija skupova, skripta. *PMF-Matematički odsjek*, 2015

Teorem 6.22 (Cantor-Bernstein-Schröder)**.** *Neka su A, B skupovi takvi da postoje injekcije $f : A \to B$ i $g : B \to A$. Tada su A i B ekvipotentni. Ekvivalentno,* $\operatorname{card} A \leq \operatorname{card} B \wedge \operatorname{card} B \leq \operatorname{card} A \Rightarrow \operatorname{card} A = \operatorname{card} B$.

Propozicija 6.23. *Skup $\mathbb{Q}$ je prebrojiv, tj.* $\operatorname{card} \mathbb{Q} = \aleph_0$.

Dokaz. Definiramo funkciju $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ formulom

$$f(q) = (m, n),\ q = \frac{m}{n} \in Q,\ M(m, n) = 1,\ m \in \mathbb{Z},\ n \in \mathbb{N}.$$

Funkcija f je injekcija. Pošto vrijedi $\operatorname{card} \mathbb{Z} \times \mathbb{N} = \operatorname{card} \mathbb{N}$, postoji bijekcija $g : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$. Dakle, $g \circ f : \mathbb{Q} \to \mathbb{N}$ je injekcija. S druge strane, $\mathbb{N} \subset \mathbb{Q}$ pa je inkluzija $i : \mathbb{N} \to \mathbb{Q}$ injekcija. Po Teoremu 6.22 vrijedi $\operatorname{card} \mathbb{Q} = \aleph_0$. □

Propozicija 6.24. *Neka je $A \subseteq \mathbb{N}$ beskonačan. Tada je A prebrojiv.*

Dokaz. Dokaz ćemo provesti koristeći Teorem 6.22 tako što ćemo dokazati $\operatorname{card} A \leq \operatorname{card} \mathbb{N}$ i $\operatorname{card} \mathbb{N} \leq \operatorname{card} A$.

Tvrdnja $\operatorname{card} A \leq \operatorname{card} \mathbb{N}$ je trivijalna. Naime, inkluzija $i : A \to \mathbb{N}$, $i(n) = n$, $n \in \mathbb{N}$, je očito injekcija.

Dokažimo sada obratnu nejednakost, tj. $\operatorname{card} \mathbb{N} \leq \operatorname{card} A$. Funkciju $g : \mathbb{N} \to A$ definiramo na sljedeći način:

$$\begin{aligned}
&g(1) = \min A,\\
&g(2) = \min A \setminus \{g(1)\},\\
&g(3) = \min A \setminus \{g(1), g(2)\},\\
&\vdots\\
&g(n) = \min A \setminus \{g(1), g(2, \ldots, g(n-1)\},\\
&\vdots
\end{aligned}$$

Definicija od g je dobra zbog dobre uređenosti skupa $\mathbb{N}$, Propozicija 4.12. Također, uočimo da vrijedi $g(1) < g(2) < \cdots < g(n) < \ldots$, pa je g injekcija. □

Korolar 6.25. *Neka je A skup takav da postoji injekcija $f : A \to \mathbb{N}$. Tada je A konačan ili prebrojiv.*

Dokaz. Najprije uočimo da je $f : A \to f(A)$ bijekcija pa vrijedi $\operatorname{card} A = \operatorname{card} f(A)$. Dakle, ako je $f(A)$ konačan, onda je i A konačan. S druge strane, ako je $f(A)$ beskonačan, onda je po Propoziciji 6.24 $f(A)$ prebrojiv, pa je i A prebrojiv. □

Propozicija 6.26. *Neka je A_n, $n \in \mathbb{N}$, familija prebrojivih skupova. Tada je $\bigcup_{n \in \mathbb{N}} A_n$ prebrojiv.*

Dokaz. Uočite da skupovi A_n nisu nužno disjunktni. Definiramo[19]:

$$B_1 := A_1,\ B_2 := A_2 \setminus A_1,\ B_3 := A_3 \setminus (A_1 \cup A_2), \ldots,$$

$$B_n := A_n \setminus \bigcup_{i=1}^{n-1} A_i, \ldots$$

Tada su B_n, $n \in \mathbb{N}$, međusobno disjunktni i vrijedi

$$\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} B_n.$$

Zbog $B_n \subseteq A_n$ slijedi da je B_n konačan ili prebrojiv, pa postoji injekcija $f_n : B_n \to \mathbb{N}$. Definiramo funkciju

$$f : \bigcup_{n\in\mathbb{N}} B_n \to \mathbb{N} \times \mathbb{N}, \quad f(x) := (n, f_n(x)),\ x \in B_n.$$

Uočite da je f dobro definiran jer se svaki $x \in \bigcup_{n\in\mathbb{N}} B_n$ nalazi u točno jednom skupu B_n zbog međusobne disjunktnosti skupova B_n, $n \in \mathbb{N}$. Također, očito[20] je f injekcija. Dakle,

$$\operatorname{card} \bigcup_{n\in\mathbb{N}} A_n = \operatorname{card} \bigcup_{n\in\mathbb{N}} B_n \leq \operatorname{card}\mathbb{N} \times \mathbb{N} = \aleph_0.$$

S druge strane, zbog $A_1 \subseteq \bigcup_{n\in\mathbb{N}} A_n$ vrijedi

$$\aleph_0 = \operatorname{card} A_1 \leq \operatorname{card} \bigcup_{n\in\mathbb{N}} A_n.$$

Dakle, skup $\bigcup_{n\in\mathbb{N}} A_n$ je prebrojiv po Teoremu 6.22. □

Rezimirajmo što smo do sada dokazali. Korolar 6.25 nam govori da je $\aleph_0$ najmanji beskonačni kardinalitet, tj. da ne postoje beskonačni skupovi "s manje elemenata" od $\mathbb{N}$. S druge strane, Propozicije 6.23 i 6.26 nam govore da su i iznenađujuće veliki skupovi prebrojivi. Prirodno pitanje je da li postoje skupovi koji su neprebrojivi. Sljedeći slavan Cantorov rezultat daje nam potvrdan odgovor na to pitanje.

Teorem 6.27 (Cantor). *Skup realnih brojeva je neprebrojiv.*

Dokaz. Pretpostavimo suprotno, tj. da je $\mathbb{R}$ prebrojiv. Tada $\operatorname{card}\mathbb{N} = \operatorname{card}\mathbb{R} = \operatorname{card}\langle 0,1\rangle$. Dakle, postoji bijekcija $f : \mathbb{N} \to \langle 0,1\rangle$. Po Teoremu o decimalnom zapisu realnog broja, svaki $x \in \langle 0,1\rangle$ može se zapisati u obliku:

$$x = 0.x_1x_2x_3 \ldots x_n \ldots,$$

pri čemu zapis ne završava s beskonačno mnogo znamenki[21] 9. Kako je po pretpostavci $f(\mathbb{N}) = \langle 0,1\rangle$, sve elemente skupa $\langle 0,1\rangle$ možemo poredati u niz:

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13} \ldots a_{1n} \ldots \\
f(2) &= 0.a_{21}a_{22}a_{23} \ldots a_{2n} \ldots \\
f(3) &= 0.a_{31}a_{32}a_{33} \ldots a_{3n} \ldots \\
&\vdots \\
f(n) &= 0.a_{n1}a_{n2}a_{n3} \ldots a_{nn} \ldots \\
&\vdots
\end{aligned}$$

[19] Intuitivno govoreći, izbacit ćemo elemente iz presjeka jer su oni višak u smislu da ne pridonose uniji.

[20] Neka su x, y takvi da $(n, f_n(x)) = f(x) = f(y) = (m, f_m(y))$. Tada vrijedi $m = n$ i $f_n(x) = f_m(y)$. Dakle, $x, y \in B_n$ i $f_n(x) = f_n(y)$. Zbog injektivnosti od f_n vrijedi $x = y$.

[21] Broj $0.12999\ldots$ zapisat ćemo kao $0.13000\ldots$

Tvrdimo da postoji $g \in \langle 0,1\rangle$ takav da $g \neq f(n)$, $n \in \mathbb{N}$.[22] Definiramo:

$$g := 0.b_1b_2b_3\ldots, \text{ gdje je } b_i := \begin{cases} a_{ii}+1 & , \quad a_{ii} \neq 8,9, \\ 5 & , \quad a_{ii} = 8, \\ 3 & , \quad a_{ii} = 9. \end{cases}$$

Vrijedi $g \neq f(n)$, $n \in \mathbb{N}$. Naime, u protivnom $g = f(m)$, pa $b_m = a_{mm}$, što je u suprotnosti s definicijom b_m. Dakle, f nije surjekcija, što je u kontradikciji s pretpostavkom da je $\mathbb{R}$ prebrojiv. □

[22] Ideja je da broj g konstruiramo tako da promatramo dijagonalu gornje tablice i svaki broj dijagonale promijenimo. Taj postupak se zove "Cantorov dijagonalni postupak".

Pišemo[23] $\operatorname{card}\mathbb{R} = \mathfrak{c}$. Koristeći tu oznaku, Teorem 6.27 može se kraće iskazati na sljedeći način: $\aleph_0 < \mathfrak{c}$. Prirodno pitanje je da li postoje skupovi "sa više elemenata" od $\mathbb{R}$. Odgovor je opet potvrdan.

[23] Oznaka $\mathfrak{c}$ dolazi od engleske riječi "continuum".

Propozicija 6.28. *Neka je $A \neq \emptyset$. Tada* $\operatorname{card} A < \operatorname{card}\mathcal{P}(A)$.

Dokaz. Pretpostavimo suprotno, tj. da postoji surjekcija $g : A \to \mathcal{P}(A)$. Definiramo skup:

$$B := \{x \in A : x \notin g(x)\} \subseteq A.$$

Kako je g surjekcija, postoji $b \in A$ takav da $g(b) = B$. Imamo dvije mogućnosti:

1. $b \in B$. Međutim, tada po definiciji skupa B vrijedi $b \notin g(b) = B$, što je kontradikcija.
2. $b \notin B$. Međutim, tada po definiciji skupa B vrijedi $b \in g(b) = B$, što je opet kontradikcija.

Dakle, obje mogućnosti vode na kontradikciju čime smo dovršili dokaz. □

Kardinalni broj partitivnog skupa od A označavamo sa $2^{\operatorname{card} A}$. Dakle,

$$\operatorname{card}\mathcal{P}(A) = 2^{\operatorname{card} A} > \operatorname{card} A.$$

Kurt Gödel (1906.–1978.), austrijski i američki matematičar i logičar

Propozicija 6.29. $\operatorname{card}\mathcal{P}(\mathbb{N}) = \mathfrak{c}$.

Dokaz. Ideja je kodirati podskupove od $\mathbb{N}$ pomoću nizova 0 i 1. Preciznije, za $A \subseteq \mathbb{N}$ definiramo:

$$f(A) = (0.a_1a_2a_3\ldots)_3, \quad a_i := \begin{cases} 1 & , \quad i \in A, \\ 0 & , \quad i \notin A, \end{cases}$$

pri čemu $(0.a_1a_2a_3\ldots)_3$ označava zapis realnog broja u bazi 3. Funkcija $f : \mathcal{P}(\mathbb{N}) \to \langle 0,1\rangle$ je injekcija.

S druge strane, neka je $x = (0.x_1x_2x_3\ldots)_2 \in \langle 0,1\rangle$ binarni zapis realnog broja s beskonačno decimala različitih od 0. Tada definiramo

$$g(x) = \{i : x_i = 1\}.$$

Funkcija $g : \langle 0,1\rangle \to \mathcal{P}(\mathbb{N})$ je injekcija. Sada tvrdnja slijedi iz Teorema 6.22. □

Paul Cohen (1934.–2007.), američki matematičar

Dakle, dokazali smo da vrijedi $2^{\aleph_0} = \mathfrak{c}$. Sljedeće pitanje koje se postavlja je da li postoji neki skup A takav da $\aleph_0 < \operatorname{card} A < \mathfrak{c}$. Negativan odgovor na to pitanje je tzv. "hipoteza kontinuuma" koja je jedan od najpoznatijih matematičkih problema[24]. Hipoteza kontinuuma je djelomično riješena tako što je dokazano[25] da se hipoteza kontinuuma ne može ni dokazati ni opovrgnuti unutar Zermelo–Frankelove teorije skupova sa aksiomom izbora.[26]

[24] Hipoteza kontinuuma je Prvi Hilbertov problem.

[25] Gödel 1940. i Cohen 1963.

[26] Vidi Poglavlje 2.6.

6.1 Zadaci

Zadatak 6.1. *Neka je $A = \{1, \ldots, n\}$, $n \in \mathbb{N}$, te $f : A \to A$. Dokažite da je f injekcija ako i samo ako je f surjekcija.*

Zadatak 6.2. *Dokažite Propoziciju 6.17.*

Zadatak 6.3. *Neka je funkcija $f : \mathbb{Z} \to \mathbb{N}$ zadana sa:*

$$f(z) = \begin{cases} 2z+1 & , \quad z \geq 0, \\ -2z & , \quad z < 0. \end{cases}$$

Dokažite da je f bijekcija.

Zadatak 6.4. *Neka je funkcija $f : \langle 0, 1\rangle \to \mathbb{R}$ zadana sa $f(x) = \frac{2x-1}{1-|2x-1|}$. Dokažite da je f bijekcija.*

7
Polinomi u jednoj varijabli

7.1 Uvod

Definicija 7.1. POLINOM n-TOG STUPNJA *(nad $\mathbb{R}$) je funkcija $f : \mathbb{R} \to \mathbb{R}$ dana sa*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i, \qquad (7.1)$$

gdje su $n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$. Brojeve $a_0, \ldots, a_n$ zovemo KOEFICIJENTI POLINOMA, *a_n* VODEĆI KOEFICIJENT, *a a_0* SLOBODNI KOEFICIJENT[1].

Ako je $f \neq 0$, broj n zovemo STUPANJ POLINOMA *i pišemo*[2] $\deg f = n$. *Ako je $f(x) = 0$ za sve $x \in \mathbb{R}$, onda polinom f zovemo* NUL-POLINOM, *pišemo $f = 0$. Stupanj nul-polinoma se ne definira*[3].

Ako je $a_n = 1$, kažemo da je polinom NORMIRAN. *Ako postoji $a \in \mathbb{R} \setminus \{0\}$ takav da $f(x) = a$ za sve $x \in \mathbb{R}$, tada polinom f zovemo* KONSTANTNI POLINOM *i pišemo $f = a$.*

Skup svih polinoma $f : \mathbb{R} \to \mathbb{R}$ označavamo sa $\mathbb{R}[x]$.

[1] Nekada kažemo i "vodeći član", "slobodni član".

[2] Nekada pišemo i $\operatorname{st} f = n$.

[3] Nekada je iz formalnih razloga pogodno staviti $\deg f = -\infty$.

Operacije zbrajanja i množenja na polinomima definiramo kao pripadne operacije na funkcijama, tj. po točkama: za $x \in \mathbb{R}$ definiramo vrijednost funkcija $f + g$ i fg u točki x ovako:

$$(f+g)(x) := f(x) + g(x),$$
$$(fg)(x) := f(x)g(x).$$

Pokažimo da su $f + g$ i fg opet polinomi. Po Definiciji 7.1, polinomi f i g mogu se zapisati u obliku:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$
$$g(x) = b_m x^m + a_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum_{i=0}^{m} b_i x^i.$$

Bez smanjenja općenitosti možemo pretpostaviti $n \geq m$[4]. Tada:

[4] U protivnom zamijenimo uloge f i g.

$$\begin{aligned}(f+g)(x) &= a_n x^n + \cdots + a_{m+1}x^{m+1} + (a_n + b_n)x^m + \cdots + \\ &\quad + (a_1 + b_1)x + (a_0 + b_0) \\ &= \sum_{i=m+1}^{n} a_i x^i + \sum_{i=0}^{m} (a_i + b_i)x^i.\end{aligned}$$

Ukoliko je $m = n$ tada nema prve sume.

$$\begin{aligned}(fg)(x) &= \Big(\sum_{i=0}^{n} a_i x^i\Big)\Big(\sum_{i=0}^{m} b_i x^i\Big) \\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + \\ &\quad + (a_1 b_0 + a_0 b_1) x + a_0 b_0 \\ &= \sum_{i=0}^{n+m} \Big(\sum_{\substack{p,q\geq 0,\\ p+q=i}} a_p b_q \Big) x^i = \sum_{i=0}^{n+m} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) x^i.\end{aligned}$$

Dakle, $f+g,\ fg \in \mathbb{R}[x]$. Nadalje, koristeći osnovna svojstva operacija zbrajanja i množenja funkcija lako se dokažu sljedeće tvrdnje:

Propozicija 7.2. *$(\mathbb{R}[x], +, \cdot)$ je komutativni prsten[5] s jedinicom $e(x) = 1$.*

[5] Neutralni element za zbrajanje je nul-polinom.

Propozicija 7.3. *Funkcija* $\deg : \mathbb{R}[x] \setminus \{0\} \to \mathbb{N}_0$ *zadovoljava sljedeća svojstva[6]:*

[6] Uočite da sva svojstva vrijede i za nul-polinome uz konvenciju $\deg(0) = -\infty$.

1. $\deg(fg) = \deg f + \deg g$,
2. $\deg(f+g) \leq \max\{\deg f, \deg g\}$,[7]
3. $\deg(f \circ g) = \deg f \cdot \deg g$.

[7] Jednakost općenito ne vrijedi, npr. $f(x) = x+1$, $g(x) = -x$.

Dokaz. Prve dvije jednakosti su direktna posljedica izraza za $f+g$ i fg. Dokažimo tvrdnju 3:

$$(f \circ g)(x) = \sum_{i=0}^{n} \Big(a_i \big(\sum_{j=0}^{m} b_j x^j \big)^i \Big).$$

Koristeći binomnu formulu vidimo da je vodeći član od $f \circ g$ jednak $a_n (b_m)^n x^{nm}$ iz čega slijedi tvrdnja. □

Napomena 7.4. *Uočimo da u Definiciji 7.1 i Propoziciji 7.2 nigdje nismo koristili činjenicu da je f realna funkcija realne varijable, te da Definicija 7.1 ima smisla ako $\mathbb{R}$ zamijenimo općenitim komutativnim prstenom s jedinicom[8]. Preciznije, ako je $\mathbb{K}$ komutativni prsten s jedinicom, onda se skup funkcija $f : \mathbb{K} \to \mathbb{K}$ dani sa (7.1), gdje su $a_0, \ldots, a_n \in \mathbb{K}$, $a_n \neq 0$, zajedno s operacijama množenja i zbrajanja zove* PRSTEN POLINOMA NAD $\mathbb{K}$ U VARIJABLI x. *Oznaka: $\mathbb{K}[x]$. Specijalno, za $\mathbb{K} = \mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ imamo prstene polinoma $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ i $\mathbb{C}[x]$.*

[8] Npr. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$

Definicija 7.5 (Jednakost polinoma)**.** *Polinomi $f, g \in \mathbb{R}[x]$ su* JEDNAKI *ako su jednaki kao funkcije, tj. $f(x) = g(x)$, $x \in \mathbb{R}$.*

Teorem 7.6 (Teorem o nul-polinomu)**.** *Polinom $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_0, \ldots, a_n \in \mathbb{R}$, jednak je nul-polinomu ako i samo ako $a_i = 0$, $i = 0, \ldots, n$.*

Dokaz.

($\Leftarrow$): Ako su $a_0 = \cdots = a_n = 0$, tada za svaki $x \in \mathbb{R}$ vrijedi $f(x) = 0$, što slijedi direktno iz (7.1).

($\Rightarrow$): Neka je $f(x) = 0$, $x \in \mathbb{R}$. Dokaz ćemo provesti svođenjem na kontradikciju. Pretpostavimo suprotno, tj. da postoji koeficijent polinoma f različit od 0, te neka je a_m najmanji takav. Dakle,

$a_m \neq 0$ i $a_0 = a_1 = \cdots = a_{m-1} = 0$, pa f možemo zapisati u sljedećem obliku:

$$f(x) = b_0 x^m + b_1 x^{m+1} + \cdots + b_p x^n = 0, \quad x \in \mathbb{R}, \tag{7.2}$$

gdje je $p = n - m$ i $b_0 = a_m, b_1 = a_{m+1}, \ldots, b_p = a_n$. Dijeljenjem (7.2) sa x^m dobivamo:

$$b_0 + b_1 x + \cdots + b_p x^p = 0, \quad x \in \mathbb{R}. \tag{7.3}$$

Ideja dokaza je da koristimo (7.3) kako bi ocijenili koeficijent $|b_0|$ i pokazali da je b_0 manji od proizvoljnog pozitivnog realnog broja što će voditi na kontradikciju[9]. U tu svrhu najprije definiramo

[9] Ovo je primjer analitičkog dokaza.

$$M := \max\{|b_0|, |b_1|, \ldots, |b_p|\} > 0.$$

Za $0 < x < 1/2$ vrijedi

Nejednakost trokuta $|a+b| \leq |a+b|$, $|ab| = |a||b|$, $|x| = x$, $x > 0$

$$\begin{aligned} |b_0| &= |-b_1 x - \cdots - b_p x^p| = |b_1 x + \cdots + b_p x^p| \\ &\leq \underbrace{|b_1|}_{\leq M} |x| + \cdots + \underbrace{|b_p|}_{\leq M} |x|^p \leq Mx(1 + x + \cdots + x^{p-1}) \\ &< Mx(1 + \frac{1}{2} + \cdots + (\frac{1}{2})^{p-1}) = Mx\frac{1 - 1/2^p}{1 - 1/2} \\ &< 2Mx. \end{aligned}$$

Dakle, dokazali smo da za svaki $0 < x < 1/2$ vrijedi $b_0 < 2Mx$. Sada ostaje samo dokazati da iz gornje ocjene slijedi $b_0 = 0$, što je u kontradikciji s pretpostavkom. Zaista, iz $|b_0| \leq M$ imamo $\frac{|b_0|}{4M} \leq \frac{1}{4} < \frac{1}{2}$. Dakle, gornja nejednakost specijalno vrijedi za $x = \frac{|b_0|}{4M}$. Sada uvrštavanjem dobivamo $|b_0| < \frac{1}{2}|b_0|$ iz čega zaključujemo $b_0 = 0$.

□

Napomena 7.7. *Teorem o nul-polinomu vrijedi i na $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ i $\mathbb{C}[x]$. Međutim, dokaz koji smo prezentirali ne možemo provesti*[10] *na $\mathbb{Z}[x]$. Srećom, dokaz na $\mathbb{Z}[x]$ je još jednostavniji:*

[10] Ne postoje $z \in \mathbb{Z}$, $0 < z < \frac{1}{2}$.

$$|b_0| = |b_1 x + \cdots + b_p x^p| = |x| \underbrace{|b_1 + \cdots + b_p x^{p-1}|}_{\in \mathbb{Z}}, \ x \in \mathbb{Z}.$$

Dakle, za svaki $x \in \mathbb{Z}$ vrijedi $|x| \mid |b_0|$ iz čega slijedi $b_0 = 0$.

Napomenimo da Teorem o nul-polinomu ne vrijedi općenito za komutativne prstene s jedinicom. Promotrimo, na primjer, prsten polinoma $\mathbb{Z}_2[x]$[11] *i polinom $f(x) = x^2 + x$. Tada vrijedi $f(x) = 0$*[12]*, $x \in \mathbb{Z}_2 = \{0, 1\}$, ali $a_2 = a_1 = 1 \neq 0$.*

[11] $\mathbb{Z}_2 = \mathbb{Z}/_{\equiv \pmod 2}$

[12] $f(1) = 1 + 1 \equiv 0 \pmod 2$

Koristeći Teorem o nul-polinomu lako ćemo dokazati teorem koji nam daje karakterizaciju jednakosti polinoma:

Teorem 7.8 (O jednakosti polinoma)**.** *Polinomi $f(x) = \sum_{i=0}^{n} a_i x^i$ i $g(x) = \sum_{i=0}^{m} b_i x^i$, $m, n \in \mathbb{N}_0$, $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{R}$, $a_n \neq 0$, $b_m \neq 0$, su jednaki ako i samo ako vrijedi $m = n$ i $a_i = b_i$, $i = 0, \ldots, n$.*

Dokaz.

($\Leftarrow$): Očito.

($\Rightarrow$): Neka je $f = g$. Tada je $f - g$ nul-polinom.

Dokažimo najprije $n = m$. Pretpostavimo suprotno, tj. $n \neq m$. Bez smanjenja općenitosti možemo pretpostaviti $m < n$.

$$(f-g)(x) = a_n x^n + \cdots + a_{m+1}x^{m+1} + (a_m - b_m)x^m + \cdots + (a_0 - b_0) = 0,\ x \in \mathbb{R}.$$

Po Teoremu o nul-polinomu vrijedi $a_n = 0$, što je u kontradikciji s pretpostavkama teorema. Dakle, dokazali smo $m = n$. Sada imamo:

$$(f-g)(x) = \sum_{i=0}^{n}(a_i - b_i)x^i,\ x \in \mathbb{R}.$$

Po Teoremu o nul-polinomu imamo $a_i - b_i = 0$, $i = 0, \ldots, n$.

□

Primjer 7.9. *Odredite sve $f \in \mathbb{R}[x]$ takve da vrijedi $f(x-1) = x^3 - 2x^2 + 2x$.*

Iz Propozicije 7.3 slijedi $\deg f = 3$ pa vrijedi:

$$\begin{aligned} f(x) &= ax^3 + bx^2 + cx + d, \\ f(x-1) &= a(x-1)^3 + b(x-1)^2 + c(x-1) + d \\ &= ax^3 + (-3a+b)x^2 + (3a-2b+c)x + (-a+b-c+d). \end{aligned}$$

Po Teoremu o jednakosti polinoma slijedi:

$$\left.\begin{aligned} a &= 1 \\ -3a + b &= -1 \\ 3a - 2b + c &= 2 \\ -a + b - c + d &= 0 \end{aligned}\right\} \begin{aligned} &\Rightarrow a = b = c = d = 1 \\ &\Rightarrow f(x) = x^3 + x^2 + x + 1. \end{aligned}$$

7.2 *Dijeljenje polinoma. Mjera*

Definicija 7.10. *Polinom $f \in \mathbb{R}[x]$ je* DJELJIV *polinomom $g \in \mathbb{R}[x] \setminus \{0\}$ ako postoji polinom $h \in \mathbb{R}[x]$ takav da $f = gh$.*[13]

[13] Uočite da tada $\deg f = \deg g + \deg h$.

Teorem 7.11 (O dijeljenju s ostatkom)**.** *Neka su $f, g \in \mathbb{R}[x]$, $g \neq 0$. Tada postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ takvi da $f = gq + r$, pri čemu je $r = 0$ ili $0 \leq \deg r < \deg g$.*

Polinom q iz iskaza Teorema 7.11 zovemo KVOCIJENT pri dijeljenju f sa g, a r OSTATAK pri dijeljenju f sa g. Ukoliko je $r = 0$, kažemo da je f DJELJIV sa g i pišemo $g \mid f$.

Dokaz Teorema 7.11 je konstruktivan, tj. daje nam algoritam za određivanje polinoma q i r. Prisjetimo[14] se algoritma na konkretnom

[14] Algoritam za dijeljenje polinoma sa ostatkom se obično obrađuje u srednjoj školi.

primjeru: $f(x) = 5x^4 + 7x^3 + x^2 + 10$, $g(x) = 2x^2 + 2x + 4$.

$$(5x^4 + 7x^3 + x^2 + 10) : (2x^2 + 2x + 4) = \underbrace{\frac{5}{2}x^2 + x - \frac{11}{2}}_{q(x)}$$

$$\begin{array}{rl} & 5x^4 + 5x^2 + 10x^2 \\ \hline & 2x^3 - 9x^2 + 10 \\ - & 2x^3 + 2x^2 + 4x \\ \hline & -11x^2 - 4x + 10 \\ - & -11x^2 - 11x - 22 \\ \hline & 7x + 32 = r(x) \end{array}$$

Dokaz. Teorem 7.11 sadrži dvije tvrdnje: egzistenciju polinoma q i r s traženim svojstvima i njihovu jedinstvenost. Te dvije tvrdnje dokazat ćemo odvojeno.

[egzistencija]

Uočimo da je slučaj $\deg f < \deg g$ trivijalan[15], pa stoga promotrimo preostali slučaj $\deg f \geq \deg g$. Neka je $m = \deg g \in \mathbb{N}_0$ i

$$g(x) = \sum_{i=0}^{m} b_i x^i,\ b_m \neq 0.$$

[15] Ako je $f = 0$, tada uzmimo $q = r = 0$. Ako je $0 \leq \deg f < \deg g$ tada uzmimo $q = 0$ i $f = r$.

Dokaz ćemo provesti indukcijom po $\deg f$.

[baza]: Neka je $\deg f = m$ i $f(x) = \sum_{i=0}^{m} a_i x^i,\ a_m \neq 0$. Tada definiramo $q := \frac{a_m}{b_m}$ i

$$\begin{aligned} r(x) &:= f(x) - \frac{a_m}{b_m} g(x) \\ &= (\cancel{a_m x^m} + \cdots + a_0) - \frac{a_m}{\cancel{b_m}}(\cancel{b_m} x^m + \cdots + b_0) \\ &= \left(a_{m-1} - \frac{a_m}{b_m} b_{m-1}\right) x^{m-1} + \cdots + \left(a_0 - \frac{a_m}{b_m} b_0\right). \end{aligned}$$

Dakle, $\deg r < m = \deg g$ i $f = gq + r$ čime smo dokazali bazu indukcije.

[korak]: Pretpostavimo da tvrdnja vrijedi za sve $f \in \mathbb{R}[x]$ takve da $m \leq \deg f \leq n - 1$ za neko $n \in \mathbb{N}$.

Neka je $f \in \mathbb{R}[x]$, $\deg f = n$, $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$. Definiramo

$$\begin{aligned} F(x) &:= f(x) - \frac{a_n}{b_m} g(x) x^{n-m} \\ &= (\cancel{a_n x^n} + \cdots + a_0) - \frac{a_m}{\cancel{b_m}} x^{n-m}(\cancel{b_m} x^m + \cdots + b_0) \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \cdots + \\ &\quad + \left(a_{n-m} - \frac{a_n}{b_m} b_0\right) + a_{n-m-1} x^{n-m-1} + \cdots + a_0. \end{aligned}$$

Dakle, vrijedi $F = 0$ ili $\deg F < n$. Po pretpostavci indukcije[16]

[16] Ili po već dokazanome u slučaju $F = 0$

postoje $Q, R \in \mathbb{R}[x]$, $\deg R < \deg g$ ili $R = 0$ takvi da vrijedi

$$F = gQ + R.$$

Međutim, iz definicije od R imamo:

$$\begin{aligned} f(x) &= F(x) + \frac{a_n}{b_m} x^{n-m} g(x) \\ &= g(x)Q(x) + R(x) + \frac{a_n}{b_m} x^{n-m} g(x) \\ &= g(x) \underbrace{\left(Q(x) + \frac{a_n}{b_m} x^{n-m}\right)}_{:=q(x)} + \underbrace{R(x)}_{:=r(x)}. \end{aligned}$$

Po principu matematičke indukcije, tvrdnja vrijedi za sve $f, g \in \mathbb{R}[x]$, $g \neq 0$.

[jedinstvenost] Pretpostavimo da $f = gq_1 + r_1 = gq_2 + r_2$, pri čemu vrijedi $r_i = 0$ ili $0 \leq \deg r_i < \deg g$, $i = 1, 2$. Tada vrijedi

$$g(q_1 - q_2) = r_2 - r_1. \tag{7.4}$$

Tvrdimo da (7.4) povlači $q_1 = q_2$. Pretpostavimo suprotno, tj. $q_1 - q_2 \neq 0$. Tada po Propoziciji 7.3 imamo

$$\begin{aligned} \deg g &\leq \deg g + \deg(q_1 - q_2) = \deg g(q_1 - q_2) = \deg(r_2 - r_1) \\ &\leq \max\{\deg r_1, \deg r_2) < \deg g. \end{aligned}$$

Dakle, $\deg g < \deg g$, što je kontradikcija, pa smo dokazali $q_1 = q_2$. Tvrdnja $r_2 = r_1$ sada slijedi direktno iz (7.4). □

Napomena 7.12. *Uočite da Teorem 7.18 vrijedi i za $\mathbb{Q}[x]$ i $\mathbb{C}[x]$, uz potpuno isti dokaz.*[17]

[17] Zašto ne vrijedi za $\mathbb{Z}[x]$?

Primjer 7.13. *Odredimo ostatak pri dijeljenju $f(x) = x^{2017} + x + 1$ sa $g(x) = x^2 - 1$.*

Iz Teorema 7.11 slijedi

$$f(x) = g(x)q(x) + Ax + B = (x^2 - 1)q(x) + Ax + B.$$

Uvrštavanjem[18] *$x = 1$ i $x = -1$ dobivamo linearan sustav za A i B:*

[18] Uočite da ne trebamo računati $q(x)$.

$$\left.\begin{aligned} x = 1 &\Rightarrow 3 = A + B \\ x = -1 &\Rightarrow -1 = -A + B \end{aligned}\right\} A = 2,\ B = 1,\ r(x) = 2x + 1.$$

Algoritam 7.14 (Hornerov algoritam)**.** *Hornerov algoritam je efikasan algoritam za računanje $f(\alpha)$ za zadani $\alpha \in \mathbb{R}$. Neka je*

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ x \in \mathbb{R}.$$

Definiramo $g(x) = x - \alpha$. Po Teoremu 7.11 postoje jedinstveni $q \in \mathbb{R}[x]$ i $r \in \mathbb{R}$[19] *takvi da:*

[19] $r = 0$ ili $\deg r = 0$.

$$f(x) = (x - \alpha)q(x) + r,\ x \in \mathbb{R}.$$

Uvrštavanjem $x = \alpha$ dobivamo $r = f(\alpha)$. Dakle, dovoljno je izračunati ostatak pri dijeljenju sa $g(x) = x - \alpha$. Imamo:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x-\alpha)(b_{n-1}x^{n-1} + \cdots + b_0) + r$$

$$= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + \cdots + (b_0 - \alpha b_1)x + (r - \alpha b_0).$$

Po Teoremu o jednakosti polinoma, vrijedi:

$$\begin{array}{ll} a_n = b_{n-1} & b_{n-1} = a_n \\ a_{n-1} = (b_{n-2} - \alpha b_{n-1}) & b_{n-2} = a_{n-1} + \alpha b_{n-1} \\ \vdots & \Rightarrow \quad \vdots \\ a_1 = b_0 - \alpha b_1 & b_0 = a_1 + \alpha b_1 \\ a_0 = r - \alpha b_0 & r = a_0 + \alpha b_0 \end{array}$$

Hornerov algoritam se može zapisati i tablično, što ćemo ilustrirati sljedećim primjerom:

Primjer 7.15. *Podijelimo $f(x) = 3x^5 - x^4 + 7x^2 + 2x - 6$ sa $g(x) = x - 2$ i izračunajmo $f(2)$.*

U prvi redak tablice upišemo koeficijente polinoma f, a drugi popunjavamo s lijeva na desno koristeći formule za b_i i r iz Hornerovog algoritma 7.14.

	3	-1	0	7	2	-6
2	3	5	10	27	56	106

Dakle, iz tablice možemo iščitati:

$$f(x) = (x-2)\underbrace{(3x^4 + 5x^3 + 10x^2 + 27x + 56)}_{q(x)} + \underbrace{106}_{r}, \quad f(2) = 106.$$

Definicija 7.16. *Neka su $f, g \in \mathbb{R}[x] \setminus \{0\}$ polinomi.* NAJVEĆA ZAJEDNIČKA MJERA *polinoma f i g je normirani[20] polinom $h \in \mathbb{R}[x] \setminus \{0\}$ takav da su i f i g djeljivi sa h. Pišemo[21] $h = M(f, g)$.*

[20] Normiranost zahtijevamo radi jedinstvenosti najveće zajedničke mjere.

[21] Stogo govoreći, oznaku možemo uvesti tek nakon što dokažemo da je mjera jedinstvena. Međutim, to je dio sljedećeg teorema.

Primjer 7.17.

$$\left.\begin{array}{l} f(x) = 2x^3 + x^2 + x - 1 = (2x-1)(x^2+x+1) \\ g(x) = 6x^2 + 7x - 5 = (2x-1)(3x+5) \end{array}\right\} M(f,g) = x - \frac{1}{2}.$$

Teorem 7.18. *Za sve polinome $f, g \in \mathbb{R}[x] \setminus \{0\}$ postoji jedinstvena najveća zajednička mjera.*

Dokaz. [**egzistencija**]: Bez smanjenja općenitosti možemo pretpostaviti $\deg f \geq \deg g$[22]. Uzastopnom primjerom Teorema od dijeljenju

[22] Inače zamijenimo $f \leftrightarrow g$.

s ostatkom dobivamo:

$$\begin{array}{lcl}
f = gq_1 + r_1,\ \deg r_1 < \deg g & & r_n|f \\
 & & \Uparrow \\
g = r_1q_2 + r_2\ ,\deg r_2 < \deg r_1 & & r_n|g \\
 & & \Uparrow \\
r_1 = r_2q_3 + r_3\ ,\deg r_3 < \deg r_2 & & r_n|r_1 \\
 & & \Uparrow \\
\vdots & & \vdots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}\ ,\deg r_{n-1} < \deg r_{n-2} & & r_n|r_{n-3} \\
 & & \Uparrow \\
r_{n-2} = r_{n-1}q_n + r_n\ ,\deg r_n < \deg r_{n-1} & & r_n|r_{n-2} = r_{n-1}q_n + r_n \\
 & & \Uparrow \\
r_{n-1} = r_nq_{n+1} + 0 & \Rightarrow & r_n|r_{n-1}
\end{array}$$

Uočite da gornja tablica mora biti konačna jer $\deg r_i$ u svakom koraku pada, pa je maksimalan broj redaka jednak $\deg g$.

Dakle, iz gornje tablice zaključujemo da $r_n \mid f$ i $r_n \mid g$. Normiranjem[23] polinoma r_n dobivamo normiran polinom $d \in \mathbb{R}[x]$ takav da $d \mid f$ i $d \mid g$.

[23] Neka je a_k vodeći koeficijent od r_n. Tada je $a_k \neq 0$ i $d = \frac{1}{a_k} r_n$.

Dokažimo da je d normirani polinom najvećeg stupnja sa svojstvom da $d \mid f$ i $d \mid g$. Neka je $h \in \mathbb{R}[x]$ takav da $h \mid f$ i $h \mid g$. Tada:

$$\begin{array}{c}
h \mid f - gq_1 \Rightarrow h|r_1 \\
h \mid g - r_1q_2 \Rightarrow h|r_2 \\
\vdots \\
h \mid r_{n-2} - r_{n-1}q_n \Rightarrow h|r_n.
\end{array}$$

Iz $h \mid r_n$ slijedi $\deg h \leq \deg r_n = \deg d$. Kako je h bio proizvoljan polinom sa svojstvom da dijeli polinome f i g, zaključujemo da je d najveća zajednička mjera.

[**jedinstvenost**]: Neka je $h \in \mathbb{R}[x]$ najveća zajednička mjera. Tada $\deg h = \deg d$ po Definiciji 7.16. U prvom dijelu dokaza pokazali smo da $h \mid d$. Dakle, postoji $a \in \mathbb{R}$ takav da $d = ah$. Međutim, kako su i d i h normirani, po Teoremu o jednakosti polinoma vrijedi $a = 1$, tj. $d = h$. □

Uočimo da je dokaz Teorema 7.18 također konstruktivan i da nam daje algoritam[24] za računanje najveće zajedničke mjere dva polinoma.

[24] To je upravo Euklidov algoritam, tj. u potpunosti je analogan Euklidovom algoritmu 5.15.

Primjer 7.19. *Neka su $f, g \in \mathbb{R}[x]$ polinomi zadani sa $f(x) = x^4 + x^3 + 2x^2 + x + 1$ i $g(x) = x^3 - 2x^2 + x - 2$. Odredite $M(f, g)$.*

Uzastopnom primjenom Teorema o dijeljenju s ostatkom kao u dokazu Teorema 7.18 dobivamo:

$$f = gq_1 + r_1,\ q_1(x) = x + 3,\ r_1(x) = 7x^2 + 7,$$

$$g = r_1q_2 + r_2,\ q_2(x) = \frac{1}{7}(x - 2),\ r_2(x) = 0.$$

Dakle[25], $M(f, g) = \frac{1}{7}(7x^2 + 7) = x^2 + 1$.

[25] $M(f, g)$ je normirani r_1.

Napomena 7.20. [26] *Iz dokaza Teorema o mjeri 7.18 slijedi da za* $f, g \in \mathbb{R}[x] \setminus \{0\}$ *postoje polinomi* $u, v \in \mathbb{R}[x] \setminus \{0\}$ *takvi da* $fu + gv = M(f, g)$.

[26] Usporedite ovu napomenu s Bézoutovim identitetom, tj. sPropozicijom 5.12.

Koristimo oznake iz dokaza Teorema 7.18 i bez smanjenja općenitosti pretpostavimo[27] $M(f, g) = r_n$. Tada imamo:

[27] U protivnom cijeli račun podijelimo sa vodećim koeficijentom polinoma r_n.

$$\begin{aligned} M(f,g) = r_n &= r_{n-2} - q_n r_{n-1} = r_{n-1} - q_n(r_{n-3} - r_{n-2}q_{n-1}) \\ &= -q_n r_{n-3} + (1 + q_{n-1}q_n) \underbrace{r_{n-2}}_{=r_{n-4} - r_{n-3}q_{n-2}} \\ &\vdots \\ &= u_1 r_1 + u_2 r_2 = u_1 r_1 + u_2(g - q_2 r_1) \\ &= u_2 g + r_1 \underbrace{(u_1 - u_2 q_2)}_{:=u} = u_2 g + u r_1 \\ &= u_2 g + u(f - q_1 g) = uf + \underbrace{(u_2 - u q_1)}_{:=v} g \end{aligned}$$

Specijalno, ako je $M(f, g) = 1$, tj. f i g su RELATIVNO PROSTI, onda postoje $u, v \in \mathbb{R}[x] \setminus \{0\}$ takvi da $fu + gv = 1$.

7.3 Nultočke polinoma i algebarske jednadžbe

Definicija 7.21. NULTOČKA POLINOMA $f \in \mathbb{C}[x]$ *je kompleksni broj*[28] $\alpha \in \mathbb{C}$ *takav da* $f(\alpha) = 0$.

[28] Ako je $\alpha \in \mathbb{R}$, tada kažemo da je α REALNA NULTOČKA, inače kažemo da je α KOMPLEKSNA NULTOČKA.

Teorem 7.22 (Bézoutov teorem za polinome)**.** $\alpha \in \mathbb{C}$ *je nultočka polinoma* $f \in \mathbb{C}[x]$ *ako i samo ako* $(x - \alpha) \mid f$.

Dokaz.

($\Rightarrow$): Neka je $\alpha \in \mathbb{C}$ nultočka polinoma f. Po Teoremu o dijeljenju s ostatkom postoje $q \in \mathbb{C}[x]$ i $r \in \mathbb{C}$ takvi da

$$f(x) = (x - \alpha)q(x) + r.$$

Uvrštavanjem $x = \alpha$ u gornju jednakost dobivamo $r = 0$, tj. $(x - \alpha) \mid f$.

($\Leftarrow$): Pretpostavimo $(x - \alpha) \mid f$, tj. postoji $q \in \mathbb{C}[x]$ takav da $f(x) = (x - \alpha)q(x)$. Uvrštavanjem $x = \alpha$ dobivamo $f(\alpha) = 0$, tj. α je nultočka polinoma f.

□

Definicija 7.23. *Ako je* $f \in \mathbb{C}[x]$ *djeljiv polinomom* $(x - \alpha)^k$*, ali nije djeljiv sa* $(x - \alpha)^{k+1}$*, za neko* $\alpha \in \mathbb{C}$ *i* $k \in \mathbb{N}$[29]*, onda kažemo da je* α k-STRUKA NULTOČKA *od* f *ili nultočka* KRATNOSTI k.

[29] $(x - \alpha)^k \mid f$ i $(x - \alpha)^{k+1} \nmid f$.

Primjer 7.24. *Odredimo kratnost nultočke* $\alpha = 1$ *polinoma* $f(x) = x^5 - 2x^4 + x^3 + x^2 - 2x + 1$.

Koristeći Hornerov algoritam podijelimo f *sa* $(x - 1)$*:*

	1	-2	1	1	-2	1
1	1	-1	0	1	-1	0

Dakle, $f(x) = (x-1)(x^4 - x^3 + x - 1)$. *Ponovno koristimo Hornerov algoritam:*

	1	-1	0	1	-1
1	1	0	0	1	0

Sada imamo $f(x) = (x-1)^2(x^3+1) = (x-1)^2 q(x)$. *Kako* $q(1) = 1 \neq 0$, *po Teoremu 7.22 vrijedi* $(x-1)^3 \nmid f$, *pa je 1 dvostruka nultočka od* f.

Sljedeći teorem nećemo dokazivati pošto njegov dokaz izlazi iz okvira ovog kolegija[30].

[30] Postoji mnogo različitih dokaza ovog teorema. Na kolegiju Kompleksna analiza na trećoj godini napravit će se jedan kratak i elegantan dokaz koji koristi rezultate kompleksne analize.

Teorem 7.25 (Osnovni teorem algebre)**.** *Neka je* $f \in \mathbb{C}[x]$, $\deg f \geq 1$. *Tada postoji* $\alpha \in \mathbb{C}$ *takav da* $f(\alpha) = 0$, *tj.* α *je nultočka polinoma* f.

Uočite da analogan teorem ne vrijedi na $\mathbb{R}[x]$. Naime, polinom $f(x) = x^2 + 1$ nema realnu nultočku[31]. Kombinirajući Teoreme 7.20 i 7.25 možemo dokazati teorem o faktorizaciji polinoma nad $\mathbb{C}$:

[31] Ima dvije kompleksne nultočke: $z = \pm i$.

Korolar 7.26. *Svaki polinom* $f \in \mathbb{C}[x]$ *n-tog stupnja može se na jedinstven način prikazati kao produkt n polinoma prvog stupnja. Preciznije, ako je* $a \in \mathbb{C}$ *vodeći koeficijent od* f, *onda postoje* $\alpha_i \in \mathbb{C}$, $i = 1, \ldots, n$ *takvi da*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n). \tag{7.5}$$

Dokaz.
[**egzistencija**]: Egzistenciju ćemo dokazati indukcijom po stupnju polinoma f:

[baza]: $n = 1$. Tada $f(x) = a_1 x + a_0 = a_1(x + \frac{a_0}{a_1})$.

[korak]: Pretpostavimo da se za neko $n \in \mathbb{N}$ svaki polinom stupnja n može zapisati u obliku (7.5). Neka je f polinom stupnja $n+1$. Tada po Osnovnom teoremu algebre 7.25 postoji $\alpha_{n+1} \in \mathbb{C}$ takva da $f(\alpha_{n+1}) = 0$. Po Teoremu 7.20 slijedi da $(x - \alpha_{n+1}) \mid f$, tj. postoji $g \in \mathbb{C}[x]$ takva da

$$f(x) = (x - \alpha_{n+1})g(x),\ x \in \mathbb{C}.$$

Kako po Propoziciji 7.3 vrijedi $\deg g = n$, iz pretpostavke indukcije slijedi da postoje $\alpha_i \in \mathbb{C}$, $i = 1, \ldots, n$ takvi da

$$g(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

Dakle,

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)(x-\alpha_{n+1}).$$

[**jedinstvenost**]: Pretpostavimo da

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n) = b(x-\beta_1)\cdots(x-\beta_n),$$

za $\alpha_i, \beta_i, a, b \in \mathbb{C}$, $i = 1, \ldots, n$. Po Teoremu o jednakosti polinoma imamo $a = b$. Također, uočimo da $\{\alpha_1, \ldots, \alpha_n\} = \{\beta_1, \ldots, \beta_n\}$. U protivnom, postoji α_k takav da $\alpha_k \neq \beta_i$, $i = 1, \ldots, n$ (ili obratno,

postoji β_k takav da $\beta_k \neq \alpha_i$, $i = 1, \ldots, n$). Međutim, tada odmah dolazimo do kontradikcije:

$$0 = f(\alpha_k) = b(\alpha_k - \beta_1) \cdots (\alpha_k - \beta_n) \neq 0 \; \lightning$$

Ostaje nam samo još dokazati da se i kratnosti nultočaka podudaraju. Pretpostavimo suprotno, tj. da vrijedi $\alpha_k = \beta_j$, ali kratnost od α_k je p, a kratnost od β_j je $q < p$. No tada,

$$\left.\begin{array}{l} (x-\alpha_k)^p \mid a(x-\alpha_1)\cdots(x-\alpha_n) = f \\ (x-\beta_j)^p \nmid b(x-\beta_1)\cdots(x-\beta_n) = f \end{array}\right\}$$

što je kontradikcija. Dakle, dokazali smo da se kratnosti podudaraju, čime je dokaz jedinstvenosti završen. □

Iz Korolara 7.26 slijedi da se svaki polinom $f \in \mathbb{C}[x]$ može zapisati u obliku:

$$f(x) = a_n(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_p)^{k_p}, \tag{7.6}$$

gdje su $\alpha_1, \ldots, \alpha_p$ međusobno različite nultočke od f, a k_j kratnost nultočke α_j, $j = 1, \ldots, p$. Također, vrijedi $\sum_{j=1}^{p} k_p = n$.

Korolar 7.27.

(1) Svaki polinom $f \in \mathbb{C}[x]$ stupnja $n \geq 1$ ima točno n nultočaka, pri čemu svaku nultočku brojimo onoliko puta kolika joj je kratnost.

(2) Ako se polinomi $f, g \in \mathbb{C}[x]$ stupnja najviše n podudaraju u barem $n+1$ točaka, onda je $f = g$.

Dokaz. Prva tvrdnja je direktna posljedica (7.6). Dokažimo tvrdnju (2). Neka su $f, g \in \mathbb{C}[x]$, $\deg f, \deg g \leq n$ i $\alpha_1, \ldots, \alpha_{n+1} \in \mathbb{C}$ takvi da $f(\alpha_i) = g(\alpha_i)$, $i = 1, \ldots, n+1$. Definiramo $h := f - g$. Tada $\deg h \leq n$ i h ima $n+1$ nultočku. Međutim, tada po tvrdnji (1) slijedi[32] da $\deg h < 1$. Dakle, polinom je konstantan, a pošto ima nultočku, mora biti nul-polinom. □

[32] U protivnom bi imamo točno $\deg g < n+1$ nultočaka.

Teorem 7.28 (Viéte). *Neka je $f(x) = \sum_{i=0}^{n} a_i x^n$, $a_i \in \mathbb{C}$, $a_n \neq 0$, te neka su $x_1, \ldots, x_n \in \mathbb{C}$ njegove nultočke. Tada vrijede* VIÉTEOVE FORMULE*:*

$$\begin{aligned} \sum_{i=1}^{n} x_i &= -\frac{a_{n-1}}{a_n}, \\ \sum_{1\leq i<j\leq n} x_i x_j &= \frac{a_{n-2}}{a_n}, \\ \sum_{1\leq i<j<k\leq n} x_i x_j x_k &= -\frac{a_{n-2}}{a_n}, \\ &\vdots \\ \prod_{i=1}^{n} x_i &= (-1)^n \frac{a_0}{a_n}. \end{aligned} \tag{7.7}$$

Dokaz. Po Korolaru 7.26 imamo

$$\begin{aligned} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \\ &= f(x) = a_n(x-x_1)(x-x_2)\cdots(x-x_n) \\ &= a_n x^n \\ &\quad - a_n(x_1+x_2+\cdots+x_n)x^{n-1} \\ &\quad + a_n(x_1x_2+x_1x_3+\cdots+x_1x_n+\cdots+x_{n-1}x_n)x^{n-2} \\ &\quad +\ldots+ \\ &\quad + a_n(-1)^n x_1x_2\cdots x_n. \end{aligned}$$

Tvrdnja teorema sada slijedi iz Teorema o jednakosti polinoma. □

Primjer 7.29.

1. *Neka su x_1, x_2 rješenja jednadžbe ax^2+bx+c. Tada po Teoremu 7.28 za $n=2$ vrijedi:*

$$x_1+x_2 = -\frac{b}{a}, \quad x_1x_2 = \frac{c}{a}.$$

2. *Neka su x_1, x_2, x_3 rješenja jednadžbe $2x^3-x^2+2x-5=0$. Odredimo $\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}$ bez rješavanja jednadžbe:*

$$\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3} = \frac{x_2x_3+x_1x_3+x_1x_2}{x_1x_2x_3} = (Tm.7.28,\ n=3) = \frac{\frac{2}{2}}{\frac{5}{2}} = \frac{2}{5}.$$

Definicija 7.30. *Jednadžba oblika*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \tag{7.8}$$

gdje su $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, zove se ALGEBARSKA JEDNADŽBA *n-TOG STUPNJA.*

Ako je $a_n = 1$ kažemo da je jednadžba NORMIRANA.

Broj $x_0 \in \mathbb{C}$ je KORIJEN *ili* RJEŠENJE *jednadžbe (7.8) ako vrijedi*

$$a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1x_0 + a_0 = 0.$$

Jednadžbi (7.8) pridružujemo polinom $f(x) = \sum_{i=0}^{n} a_i x^i$. Kažemo da je x_0 k-STRUKI KORIJEN od (7.8) ako je x_0 k-struka nultočka od f.

Proučavanjem algebarskih jednadžbi tipa (7.8) matematičari se bave od samih početaka[33]. Iz Korolara 7.27 slijedi da jednadžba (7.8) ima točno n korijena, pri čemu svaki brojimo onoliko puta kolika mu je kratnost. Međutim, Korolar 7.27 nam ne daje način za efektivno rješavanje jednadžbe, tj. ne sadrži formulu ili metodu za određivanje korijena jednadžbe (7.8). Rješenje jednadžbe prvog reda (linearne jednadžbe) je trivijalno[34], a formula za rješenja jednadžbe drugog reda (kvadratne jednadžbe) poznata nam je iz srednješkolskog obrazovanja[35]. Za rješenja jednadžba stupnja 3 i 4 također postoje formule koje su poznate od 16. stoljeća (formulu za rješenje opće jednadžbe stupnja 3 otkrio je Gerolamo Cardano (1501.–1576.), a za jednadžbe stupnja 4 njegov učenik Lodovico de Ferrari (1522.–1565.)),

[33] Već su babilonski matematičari (oko 2000. pr. Kr.) znali rješavati neke kvadratne jednadžbe.

[34] Rješenje jednadžbe $ax+b=0$ je dano sa $x_0 = -b/a$.

[35] Rješenja jednadžbe $ax^2+bx+c=0$ su dana formulom $x_{1,2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

ali su prekomplicirane da bi bile od praktične koristi. Međutim, za odgovor da li je moguće riješiti opću jednadžbu reda 5 trebalo je proći još 250 godina. Naime, 1824. Abel je dokazao[36] da za opću jednadžbu stupnja 5 ili više ne postoji algebarsko rješenje, tj. rješenje koje koristi samo algebarske operacije (zbrajanje, oduzimanje, množenje i dijeljenje) i potencije s racionalnim eksponentima (n-te korijene). Naravno, neke jednadžbe stupnja 5, npr. $x^5 - 1 = 0$, su rješive. Évariste Galois je razvio teoriju koja karakterizira jednadžbe koje su rješive. Primjer nerješive jednadžbe (u smislu algebarskog rješenja) je $x^5 - x + 1 = 0$. Naravno, danu jednadžbu možemo riješiti numerički s proizvoljnom točnošću. Na primjer, približno realno rješenje gornje jednažbe je 1.1673039782614186843.

[36] Abel-Ruffinijev teorem. Paolo Ruffini (1765.–1822.) je 1799. dao dokaz koji je imao rupe.

U nastavku ovog poglavlja dat ćemo neke rezultate o korijenima specijalnog oblika za neke algebarske jednadžbe.

Niels Henrik Abel (1802.–1829.), norveški matematičar

Évariste Galois (1811.–1832.), francuski matematičar

Propozicija 7.31. *Neka su $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, te $\alpha \in \mathbb{Z} \setminus \{0\}$ korijen jednadžbe (7.8). Tada $\alpha \mid a_0$.*

Dokaz. Iz (7.8) dobivamo:

$$a_0 = -\alpha \underbrace{\left(a_n \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_2\alpha + a_1\right)}_{\in \mathbb{Z}}.$$

Dakle, $\alpha \mid a_0$. □

Rezultati ovog tipa nam olakšavaju "pogađanje" korijena ukoliko imamo neku dodatnu informaciju, na primjer, da postoji cjelobrojni korijen.

Primjer 7.32. *Riješimo jednadžbu $2x^3 - 3x^2 - x - 2 = 0$.*

Neka je $f(x) = 2x^3 - 3x^2 - x - 2$ polinom pridružen jednadžbi. Ako jednadžba ima cjelobrojni korijen α, onda po Propoziciji 7.31 vrijedi $\alpha \mid -2$. Dakle, jedino brojevi $\pm 1, \pm 2$ mogu biti cjelobrojni korijeni. Provjerimo ih sve: $f(1) = -4, f(-1) = -6, f(2) = 0, f(-2) = -28$. Dakle, $\alpha = 2$ je jedina cjelobrojna nultočka polinoma f, te po Teoremu 7.20 slijedi $x - 2 \mid f$. Koristimo Horenerov algoritam za računanje kvocijenta:

	2	-3	-1	-2
2	2	1	1	0

Dakle, $f(x) = (x-2)(\underbrace{2x^2 + x + 1}_{q(x)})$ pa su preostali korijeni nultočke od q: $x_{1,2} = \frac{-1 \pm \sqrt{1-8}}{4} = \frac{-1 \pm i\sqrt{7}}{2}$.

Primjer 7.33. *Jednadžba $\underbrace{x^3 + x^2 + x + 3}_{f(x)} = 0$ nema cjelobrojnih korijena!*

Zaista, ako je $\alpha \in \mathbb{Z}$ korijen jednadžbe, tada $\alpha \mid 3$. Dakle, $\alpha \in \{\pm 1, \pm 3\}$. Međutim, direktnim računom vidimo da $f(1), f(-1), f(3), f(-3) \neq 0$.

Teorem 7.34. *Neka su $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$. Ako je $\alpha = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $M(p,q) = 1$, korijen jedanžbe (7.8), onda $p \mid a_0$ i $q \mid a_n$.*

Dokaz. Kako je $\alpha = \frac{p}{q}$ korijen jednadžbe (7.8) vrijedi:

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0.$$

Množenjem sa q^n dobivamo:

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0. \tag{7.9}$$

Dakle, $a_0 q^n = -p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_2 p q^{n-2} + a_1 q^{n-1})$, tj. $p \mid a_0 q^n$. Po pretpostavci teorema vrijedi $M(p,q) = 1$ te stoga $M(p, q^n) = 1$. Sada iz Propozicije 5.13 slijedi $p \mid a_0$.

S druge strane, iz (7.9) također slijedi:

$$a_n p^n = -q(a_0 q^{n-1} + a_1 q^{n-2} p + \cdots + a_{n-2} q p^{n-2} + a_{n-1} p^{n-1}).$$

Analognim zaključivanjem kao i ranije[37], dobivamo $q \mid a_n$. □

[37] $(q \mid a_n p^n \ \wedge \ M(q,p) = 1) \Rightarrow q \mid a_n$

Korolar 7.35. *Za $a, n \in \mathbb{N}$ broj $\sqrt[n]{a}$ je ili cijeli ili iracionalan.*

Dokaz. $\sqrt[n]{a}$ je korijen jednadžbe $x^n - a = 0$. Pretpostavimo $\sqrt[n]{a} \in \mathbb{Q}$. Tada postoje $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $M(p,q) = 1$, takvi da je $\sqrt[n]{a} = \frac{p}{q}$ korijen navedene jednadžbe. Po Teoremu 7.34, slijedi $q \mid 1$, tj. $q = 1$, pa $\sqrt[n]{a} \in \mathbb{Z}$.

Dakle, ili $\sqrt[n]{a} \in \mathbb{Z}$ ili $\sqrt[n]{a} \notin \mathbb{Q}$. □

Primjer 7.36. *Dokažimo $\sqrt{2 - \sqrt{3}} \notin \mathbb{Q}$.*

Neka je $\alpha = \sqrt{2 - \sqrt{3}}$. Tada vrijedi:

$$\alpha^2 = 2 - \sqrt{3} \ \Rightarrow \ \sqrt{3} = \alpha^2 - 2 \ \Rightarrow \ 3 = (\alpha^2 - 2)^2.$$

Dakle, α je korijen jednadžbe:

$$x^4 - 4x^2 - 1 = 0.$$

Ukoliko je $\mathbb{Q} \ni \alpha = \frac{p}{q}$, tada po Teoremu 7.34 slijedi $q \mid 1$ i $p \mid 1$, tj. $\alpha \in \{-1, 1\}$. Međutim, očito ni 1 ni -1 nisu korijeni gornje jednadžbe. Dakle, $\alpha \notin \mathbb{Q}$.

Lema 7.37. *Neka su $a_i \in \mathbb{R}$, $i = 0, 1, \ldots, n$ te neka je $x_0 = a + bi \in \mathbb{C}$ korijen jednadžbe (7.8). Tada je i $\overline{x_0} = a - bi$ također korijen jednadžbe (7.8).*

Dokaz. Koristimo svojstva kompleksnog konjugiranja iz Zadatka 4.11. Neka je f polinom pridružen jednadžbi (7.8). Tada imamo:

$$\begin{aligned} f(\overline{x_0}) &= a_n \overline{x_0}^n + a_{n-1} \overline{x_0}^{n-1} + \cdots + a_1 \overline{x_0} + a_0 \\ &= a_n \overline{x_0^n} + a_{n-1} \overline{x_0^{n-1}} + \cdots + a_1 \overline{x_0} + a_0 = (a_k = \overline{a_k}) \\ &= \overline{a_n x_0^n} + \overline{a_{n-1} x_0^{n-1}} + \cdots + \overline{a_1 x_0} + \overline{a_0} \\ &= \overline{a_n x_0^n + a_{n-1} x_0^{n-1} + \cdots + a_1 x_0 + a_0} = \overline{f(x_0)} = 0. \end{aligned}$$

□

Teorem 7.38. *Neka su $a_i \in \mathbb{Z}$, $i = 0, 1, \ldots, n$, te neka je $\alpha + \beta i$ korijen jednadžbe (7.8), pri čemu su $\alpha, \beta \in \mathbb{Z}$. Tada vrijedi $\alpha^2 + \beta^2 \mid a_0$.*

Dokaz. Neka je f polinom pridružen jednadžbi (7.8). Po Lemi 7.37 iz $f(\alpha + \beta i) = 0$ slijedi $f(\alpha - \beta i) = 0$. Sada po Teoremu 7.22 slijedi da je f djeljiv polinomom g koji je dan formulom

$$g(x) = (x - (\alpha + \beta i))(x - (\alpha - \beta i)) = x^2 - 2\alpha x + \alpha^2 + \beta^2.$$

Dakle,

$$f(x) = g(x)q(x) = (x^2 - 2\alpha x + \alpha^2 + \beta^2)(b_{n-2}x^{n-2} + \cdots + b_0).$$

Po Teoremu o jednakosti polinoma imamo:

$$\begin{aligned} a_n = b_{n-2} &\Rightarrow b_{n-2} \in \mathbb{Z}, \\ a_{n-1} = b_{n-3} - 2\alpha b_{n-2} &\Rightarrow b_{n-3} \in \mathbb{Z}, \\ a_{n-2} = b_{n-4} - 2\alpha b_{n-3} + (\alpha^2 + \beta^2)b_{n-2} &\Rightarrow b_{n-4} \in \mathbb{Z}, \\ &\vdots \\ a_2 = b_0 - 2\alpha b_1 + (\alpha^2 + \beta^2)b_2 &\Rightarrow b_0 \in \mathbb{Z}, \\ a_0 = (\alpha^2 + \beta^2)b_0 &\Rightarrow \alpha^2 + \beta^2 \mid a_0. \end{aligned}$$

□

Primjer 7.39. *Riješimo jednadžbu* $\underbrace{x^4 - 4x^3 + 2x^2 + 12x - 15}_{f(x)} = 0$.

Provjerom djelitelja od 15 *vidimo da nema cjelobrojnih korijena. Tražimo korijene oblika* $\alpha + \beta i$, $\alpha, \beta \in \mathbb{Z}$. *Tada po Teoremu 7.38 slijedi* $\alpha^2 + \beta^2 \mid 15$, *tj.* $\alpha^2 + \beta^2 \in \{1, 3, 5, 15\}$.

Dakle, vrijedi[38] $\alpha + \beta i \in \{\pm 1 \pm 2i, \pm 2 \pm i\}$. *Uvrštavanjem svih* 8 *kombinacija dobijemo dvije nultočke* $x_{1,2} = 2 \pm i$. *Stoga je* f *djeljiv sa* $(x - (2 - i))(x - (2 + i)) = x^2 - 4x + 5$, *pa dijeljenjem* f *sa* g *dobivamo:*

$$f(x) = (x^2 - 4x + 5)(x^2 - 3).$$

Dakle, preostali korijeni su $x_{3,4} = \pm\sqrt{3}$.

[38] Uočite da se 1, 3 i 15 ne mogu napisati kao zbroj kvadarata prirodnih brojeva, a 5 se može na dva načina: $5 = 1^2 + 2^2 = 2^2 + 1^2$.

Definicija 7.40. *Kažemo da je broj* $\alpha \in \mathbb{R}$ ALGEBARSKI *ako postoje* $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ *takvi da je* α *korijen jednadžbe* $a_n x^n + \cdots + a_1 x + a_0 = 0$[39]. *U protivnom kažemo da je* α TRANSCENDENTAN.

[39] Uočite da je ekvivalentno zahtijevati $a_i \in \mathbb{Z}$. Naime, množenjem jednadžbe najvećim zajedničkim nazivnikom brojeva a_i dobivamo jednadžbu s cjelobrojnim koeficijentima.

Na primjer, broj $\sqrt[n]{a}$ je algebarski za $n \in \mathbb{N}$ i $a \in \mathbb{Q}$, $a > 0$. Naime, $\sqrt[n]{a}$ je rješenje jednadžbe $x^n - a = 0$ sa racionalnim koeficijentima.

Međutim, algebarskih brojeva ima prebrojivo mnogo jer polinoma s racionalnim koeficijentima ima prebrojivo mnogo, a svaki polinom ima najviše konačno mnogo realnih nultočaka. Dakle, po Teoremu 6.27, transcendentnih brojeva ima neprebrojivo mnogo. Primjeri[40] transcendentnih brojeva su π, e, $\sin 1$.

[40] Iako smo jednostavnim argumentom pokazali da transcendentni brojevi postoje i da ih ima mnogo više od algebarskih, dokazati da je konkretan broj transcendentan nije jednostavno. Charles Hermite (1822.–1901.) je prvi dokazao da je e transcendentan 1873., a Ferdinand von Lindemann (1852.–1939.) je prvi dokazao da je π transcendentan 1882.

7.4 *Reducibilni i ireducibilni polinomi*

U ovom poglavlju $\mathbb{F}$ će označavati jedno od polja $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$.

Definicija 7.41. *Polinom* $f \in \mathbb{F}[x]$ *je* REDUCIBILAN *nad* $\mathbb{F}$ *ako postoje polinomi* $g, h \in \mathbb{F}[x]$, $\deg g \geq 1$, $\deg h \geq 1$, *takvi da* $f = gh$. *Ako* f *nije reducibilan nad* f, *kažemo da je* IREDUCIBILAN.

Uočite da reducibilnost ovisi o polju $\mathbb{F}$. Na primjer, polinom $f(x) = x^2 + 1$ je reducibilan[41] nad $\mathbb{C}$, ali je ireducibilan nad $\mathbb{R}$. Naime, f nema realnu nultočku pa po Teoremu 7.22 nije djeljiv nijednim polinomom stupnja 1.

[41] $x^2 + 1 = (x - i)(x + i)$

Dokazat ćemo teoreme koji karakteriziraju ireducibilnost nad $\mathbb{R}$ i $\mathbb{C}$.

Teorem 7.42. *Neka je $f \in \mathbb{C}[x]$ ireducibilan. Tada je* $\deg f \leq 1$.[42]

[42] Dakle, svi normirani ireducibilni polinomi su oblika $f(x) = 1$ ili $f(x) = x - \alpha$, $\alpha \in \mathbb{C}$.

Dokaz. Neka je $f \in \mathbb{C}[x]$ ireducibilan i pretpostavimo da je $\deg f \geq 2$. Tada po Osnovnom teoremu algebre postoji $x_0 \in \mathbb{C}$ takav da $f(x_0) = 0$. Sada iz Teorema 7.22 slijedi $x - x_0 \mid f$, tj. postoji $q \in \mathbb{C}[x]$, $\deg q \geq 1$ takav da $f(x) = (x - x_0)q(x)$. Međutim, to je u kontradikciji s ireducibilnošću od f, pa smo dokazali da $\deg f \leq 1$. □

Promotrimo sada kvadratnu jednadžbu nad $\mathbb{R}$:

$$ax^2 + bx + c = 0,\ a, b, c \in \mathbb{R},\ a \neq 0.$$

Tada:

$$0 = x^2 + \frac{b}{a}x + \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}.$$

Dakle,

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \ \Rightarrow\ x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Po Teoremu 7.22, zaključujemo da je polinom $ax^2 + bx + c$ ireducibilan nad $\mathbb{R}$ ako i samo ako vrijedi $\underbrace{b^2 - 4ac}_{\text{diskriminanta}} < 0$.

Teorem 7.43. *Ako je $f \in \mathbb{R}[x]$ ireducibilan, onda je* $\deg f \leq 2$. *Svi normirani ireducibilni polinomi su oblika* 1, $x - \alpha$, *za* $\alpha \in \mathbb{R}$, $x^2 + \beta x + \gamma$, *za* $\beta, \gamma \in \mathbb{R}$ *takve da* $\beta^2 < 4\gamma$.

Dokaz. Iz prethodnog razmatranja znamo da su navedeni polinomi ireducibilni. Ostaje dokazati da su svi ireducibilni tog oblika.

Neka je $f \in \mathbb{R}[x]$, $\deg f \geq 3$. Kako je $f \in \mathbb{C}[x]$ po Osnovnom teoremu algebre postoji $x_0 \in \mathbb{C}$ takav da $f(x_0) = 0$. Postoje dvije mogućnosti:

1. $x_0 \in \mathbb{R}$. Tada po Teoremu 7.22 slijedi $f(x) = (x - x_0)q(x)$, $q \in \mathbb{R}[x]$ i $\deg q \geq 2$. Dakle, f je reducibilan.

2. $x_0 \in \mathbb{C} \setminus \mathbb{R}$, tj. $x_0 = \alpha + i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$. Tada po Lemi 7.37 vrijedi $f(\overline{x_0}) = 0$, pa po Teoremu 7.22 postoji $q \in \mathbb{C}[x]$, $\deg q \geq 1$ takav da

$$\begin{aligned} f(x) &= (x - x_0)(x - \overline{x_0})q(x) \\ &= \underbrace{(x^2 - 2\alpha x + \alpha^2 + \beta^2)}_{\in \mathbb{R}[x]}\, q(x). \end{aligned}$$

Stoga je i $q \in \mathbb{R}[x]$, pa je f reducibilan.

Dakle, dokazali smo da su ireducibilni polinomi stupnja manjeg ili jednako 2. Polinomi stupnja manjeg ili jednako 1 su ireducibilni po definiciji, a polinomi stupnja 2 oblika $x^2 + \beta x + \gamma$ su ireducibilni ako i samo ako $\beta^2 < 4\gamma$ po razmatranjima koja su prethodila ovom teoremu. □

8
Bibliografija

[1] Boris Pavković and Darko Veljan. *Elementarna matematika 1*. Tehnička knjiga, 1992.

[2] Boris Pavković and Darko Veljan. *Elementarna matematika II: trigonometrija, stereometrija-geometrija prostora, analitička geometrija, elementarna teorija brojeva*. Školska knjiga, 1995.

[3] Terence Tao. *Analysis. I*, volume 37 of *Texts and Readings in Mathematics*. Hindustan Book Agency, New Delhi, third edition, 2014.

[4] M Vuković. Teorija skupova, skripta. *PMF-Matematički odsjek*, 2015.