UVOD U MATEMATIKU -REVIZIJA SIJEČANJ 2023.

DIJANA ILIŠEVIĆ I GORAN MUIĆ

Sadržaj

1. Osnove logike predikata i sudova

Sud (ili izjava) je svaka smislena izjavna rečenica koja je ili istinita ili lažna, ali ne istovremeno i istinita i lažna.

Primjer 1.1. (a) *"$2+2=4$" je sud (istina).*
(b) *"$2+3=7$" je sud (laž).*
(c) *"Koliko je sati?" nije sud.*
(d) *"$x+2=8$" nije sud.*
(e) *"Broj* 0.00001 *je mali broj." nije sud.*

U ovom poglavlju ćemo sudove označavati velikim slovima $A, B, C, \ldots$ Prema gornjoj definiciji svaki sud je ili istinit ili lažan. Kratko istinitost suda označavamo sa 1, a lažnost suda sa 0. Dakle, svaki sud ima vrijednost ili 0 ili 1, ali ne istovremeno i 0 i 1. Kada radimo s dva suda, onda uvijek imamo ove četiri mogućnosti:

A	B
0	0
0	1
1	0
1	1

Iz zadanih sudova gradimo nove sudove koristeći **logičke veznike**:

oznaka	naziv	čita se	piše se
$\&$ $(\wedge)$	konjunkcija	i	$A\&B$ $(A\wedge B)$
$\vee$	disjunkcija	ili	$A\vee B$
—	negacija	ne	$\overline{A}$
$\Longrightarrow$	implikacija	... povlači ...	$A \Longrightarrow B$
		... implicira ...	
		ako ... onda ...	
		iz ... slijedi ...	
$\Longleftrightarrow$	ekvivalencija	... je ekvivalentno sa ...	$A \Longleftrightarrow B$
		... ako i samo ako ...	
		... onda i samo onda ...	

Operacije konjunkcije, disjunkcije, implikacije i ekvivalencije su binarne (djeluju na dva suda), a negacija je unarna operacija (djeluje na samo jedan sud).

Definicija logičkih veznika dana je ovom **semantičkom tablicom ili tablicom istinitosti** (redom za konjunkciju, disjunkciju, implikaciju i ekvivalenciju te posebno za negaciju):

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

A	$\overline{A}$
0	1
1	0

Izjave X i Y su **semantički jednake** ako im se semantičke tablice podudaraju. Tada pišemo

$$X \equiv Y.$$

Prvi važan primjer je **negacija implikacije**:

$$\overline{A \implies B} \quad \equiv \quad A\&\overline{B}.$$

Riječima: negacija izjave "A povlači B" je izjava "vrijedi A i vrijedi negacija od B". To će se tijekom studija često koristiti u ovom obliku. Konkretno: želimo provjeriti istinitost neke izjave koja je oblika $A \implies B$. Ako to ne možemo učiniti direktno, tada napišemo negaciju te izjave i dokažemo da je ona lažna. Ova metoda dokazivanja naziva se **metoda suprotnog**, a često govorimo i o dokazivanju **kontradikcijom**.

Uvjerimo se sada u semantičku jednakost izjava $\overline{A \implies B}$ i $A\&\overline{B}$. Formiramo tablicu:

A	B	$A \implies B$	$\overline{A \implies B}$	$\overline{B}$	$A\&\overline{B}$
0	0	1	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	1	1	0	0	0

Najprije uočimo da su prva tri stupca ista kao u definiciji logičkih veznika. Preostala tri stupca su dobivena primjenom logičkih veznika (negacije i konjunkcije) na neke od prethodnih stupaca. Uočimo da su stupci koji odgovaraju izjavama $\overline{A \implies B}$ i $A\&\overline{B}$ jednaki:

$\overline{A \implies B}$	$A\&\overline{B}$
0	0
0	0
1	1
0	0

To je upravo definicija semantičke jednakosti.

Drugi važan primjer je **obrat po kontrapoziciji**:

$$A \implies B \quad \equiv \quad \overline{B} \implies \overline{A}.$$

Riječima: uvjeriti se u istinitost izjave “A povlači B” je isto kao i uvjeriti se u istinitost izjave “negacija izjave B povlači negaciju izjave A”. Kao i ranije opisana metoda suprotnog, obrat po kontrapoziciji se također redovito koristi u dokazivanju tvrdnji u matematici.

Istinitost obrata po kontrapoziciji pokazuje nam ova semantička tablica:

A	B	$A \implies B$	$\overline{A}$	$\overline{B}$	$\overline{B} \implies \overline{A}$
0	0	1	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	1	1	0	0	1

Vidimo da su stupci koji odgovaraju izjavama $A \implies B$ i $\overline{B} \implies \overline{A}$ jednaki:

$A \implies B$	$\overline{B} \implies \overline{A}$
1	1
1	1
0	0
1	1

To je upravo definicija semantičke jednakosti.

Evo standardnog primjera za obrat po kontrapoziciji:

izjava

$$\text{kiša pada} \implies \text{ulice su mokre}$$

ima obrat po kontrapoziciji

$$\text{ulice nisu mokre} \implies \text{kiša ne pada.}$$

U matematici, **obrat izjave**

$$A \implies B$$

je izjava

$$B \implies A.$$

Uočimo da izjave $A \implies B$ i $B \implies A$ nisu semantički jednake:

A	B	$A \implies B$	$B \implies A$
0	0	1	1
0	1	1	0
1	0	0	1
1	1	1	1

Naime, stupci koji odgovaraju izjavama $A \implies B$ i $B \implies A$ nisu jednaki.

Zadatak 1.2. *Napišite odgovarajuće semantičke tablice i uvjerite se u odgovarajuće semantičke jednakosti:*

(a) $\overline{A\&B} \quad\equiv\quad \overline{A} \vee \overline{B}$,
(b) $\overline{A \vee B} \quad\equiv\quad \overline{A}\&\overline{B}$,
(c) $A \iff B \quad\equiv\quad (A \implies B)\&(B \implies A)$.

Za izjavu kažemo da je **tautologija** ako je uvijek istinita bez obzira na istinitost njezinih sastavnih sudova.

Najjednostavniji primjer tautologije je izjava $A \vee \overline{A}$. To pokazuje sljedeća tablica:

A	$\overline{A}$	$A \vee \overline{A}$
0	1	1
1	0	1

Vidimo da su u zadnjem stupcu same jedinice, što i treba biti za tautologiju.

Zadatak 1.3. *Uvjerite se da su sljedeći sudovi tautologije:*

(a) $A \implies (B \implies A)$,
(b) $A \implies A \vee B$,
(c) $A\&B \implies B$,
(d) $(\overline{B} \implies \overline{A}) \implies (A \implies B)$.

Promotrimo sljedeće rečenice:

- $P(x) =$ "Prirodan broj x nije djeljiv s 3."
- $Q(x,y) =$ "x i y zadovoljavaju $y^2 < 3x$."
- $R(x) =$ "x zadovoljava $x+1=0$."

Takve rečenice nisu sudovi. Nazivamo ih **predikatima**.

Damo li neku konkretnu vrijednost varijabli x u prvom i trećem primjeru, odnosno x i y u drugom primjeru, dolazimo do sudova. Predikati $P(x)$ i $R(x)$ su **jednomjesni** jer ovise samo o jednoj varijabli x, dok je predikat $Q(x,y)$ **dvomjesni** jer ovisi o varijablama x i y. Ovdje je važno istaknuti da x i y nisu u potpunosti određeni i zato o gornjim rečenicama ne možemo govoriti kao o sudovima. Ponekad se takve rečenice nazivaju **izjavne funkcije** jer ovise o varijablama koje nisu određene (nemaju konkretnu vrijednost), a za odnos koji definiraju kaže se da je **predikat.** No, mi ćemo kratko govoriti samo o predikatima.

Primjer 1.4. (1) *Za $x = 2$, rečenica $P(x)$ glasi*

$$P(2) = \text{“}\textit{Prirodan broj } 2 \textit{ nije djeljiv s } 3.\text{”}$$

*Tu rečenicu smo dobili zamjenom (ili supstitucijom) varijable x sa 2 i to je **sud** koji je očigledno istinit.*

(2) *Za $x = 6$, rečenica $P(x)$ glasi*

$$P(6) = \text{“}\textit{Prirodan broj } 6 \textit{ nije djeljiv s } 3.\text{”}$$

*To je **sud** koji je očigledno lažan.*

(3) *Za $x = 1$ i $y = 2$, rečenica $Q(x, y)$ glasi*

$$Q(1,2) = \text{“ } 1 \text{ i } 2 \text{ zadovoljavaju } 2^2 < 3 \cdot 1.\text{”}$$

*Tu rečenicu smo dobili zamjenom x sa 1 i y sa 2. To je **sud** koji je očigledno lažan.*

(4) *Za $x = 2$ i $y = 1$, rečenica $Q(x, y)$ glasi*

$$Q(2,1) = \text{“ } 2 \text{ i } 1 \text{ zadovoljavaju } 1^2 < 3 \cdot 2.\text{”}$$

*To je **sud** koji je očigledno istinit.*

(5) *Za $x = 2$, rečenica $R(x)$ glasi*

$$R(2) = \text{“ } 2 \text{ zadovoljava } 2 + 1 = 0.\text{”}$$

*Nju smo dobili zamjenom x sa 2. To je **sud** koji je očigledno lažan.*

(6) *Za $x = -1$, rečenica $R(x)$ glasi*

$$R(-1) = \text{“ } -1 \text{ zadovoljava } -1 + 1 = 0.\text{”}$$

*To je **sud** koji je očigledno istinit.*

Iz ovih primjera i iz dosadašnjeg matematičkog iskustva jasno je da predikati igraju važnu ulogu u matematici. Međutim, nije moguće sve razumne sudove dobiti iz predikata samo jednostavnom supstitucijom varijabli koje ulaze u opis predikata kao u gornjim primjerima. Promotrimo sljedeći primjer:

$$\text{“Za svaki prirodan broj } x \text{ vrijedi } x + 1 \neq 0.\text{”}$$

U ovom slučaju rečenica nije predikat, već sud koji je očigledno istinit. Razabiremo dalje da takav sud ne dolazi od predikata supstitucijom neke konkretne vrijednosti za x jer gornja rečenica govori o svim mogućim vrijednostima $x = 1, 2, 3, 4, \ldots$

Međutim, promotrimo sljedeću rečenicu:

$$T(x) = \text{“}x \text{ je prirodan broj i zadovoljava } x + 1 \neq 0.\text{”}$$

Ova rečenica nije sud već predikat iz kojeg se dobiju sudovi

$$T(1),\ T(2),\ T(3),\ T(4), \ldots,$$

tj. za svaki prirodan broj $x = 1, 2, 3, 4, \ldots$ dobivamo konkretan sud kao u ranijim primjerima.

Naš sud *“Za svaki prirodan broj x vrijedi $x + 1 \neq 0$.”* nije niti jedan konkretan od sudova $T(1)$, $T(2)$, $T(3)$, $T(4), \ldots$, već je on dobiven spajanjem svih tih sudova logičkim veznikom “&”. Dakle,

$$\text{“Za svaki prirodan broj } x \text{ vrijedi } x + 1 \neq 0.\text{”}$$

može se napisati kao

$$T(1) \,\&\, T(2) \,\&\, T(3) \,\&\, T(4) \,\&\, \ldots$$

Jasno je da je ovaj zapis nepraktičan, ali koristeći

univerzalni kvantifikator $\forall$ (koji se čita: za sve ili za svaki),

naš sud

$$\text{“Za svaki prirodan broj } x \text{ vrijedi } x + 1 \neq 0.\text{”}$$

može se elegantno zapisati u obliku

$$(\forall x)T(x)$$

ili raspisano

$$(\forall x)(\text{“}x \text{ je prirodan broj i zadovoljava } x+1 \neq 0.\text{”}).$$

Dakle, drugi način građenja sudova iz predikata je dodavanje kvantifikatora na sve varijable koje se pojavljuju u predikatu. Kvantifikatori su:

- **univerzalni kvantifikator** $\forall$ (koji se čita: za sve ili za svaki)
- **egzistencijalni kvantifikator** $\exists$ (koji se čita: postoji).

Postoji još jedan egzistencijalni kvantifikator: $\exists!$ (koji se čita: postoji jedinstven ili postoji točno jedan).

Studij matematike se sastoji od provjere istinitosti sudova koji se grade od predikata dodavanjem kvantifikatora (najčešće) ili supstitucijom varijabli.

Primjer 1.5. (a) $(\exists x)$ *(x je prirodan broj,* $x+1=2$*).*
Ovaj sud, koji se čita

$$\text{“}\textit{Postoji prirodan broj } x \textit{ takav da je } x+1=2.\text{”}$$

dobiven je iz predikata

$$P(x) = \text{“}x \textit{ je prirodan broj, } x+1=2\text{”}$$

dodavajući egzistencijalni kvantifikator $\exists$.

(b) $(\forall x)$ $(\exists n)$ *(x je realan broj, n je prirodan broj,* $n > x$*).*
Ovaj sud, koji se čita

$$\text{“}\textit{Za svaki realan broj } x \textit{ postoji prirodan broj } n \textit{ takav da je } n > x.\text{”}$$

dobiven je iz dvomjesnog predikata

$$P(x,n) = \text{“}x \textit{ je realan broj, } n \textit{ je prirodan broj, } n > x\text{”}$$

dodavajući univerzalni kvantifikator $\forall$ *i egzistencijalni kvantifikator* $\exists$. *Ako, kao što je uobičajeno u matematici, sa* $\mathbb{R}$ *odnosno* $\mathbb{N}$ *označimo skup svih realnih brojeva odnosno skup svih prirodnih brojeva, onda se gornji sud može napisati i na ovaj uobičajeniji način*

$$(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(n > x).$$

(c) *Iz osnovne škole znamo da je množenje realnih brojeva asocijativno:*

$$(ab)c = a(bc).$$

Ovdje se radi o tromjesnom predikatu

$$Q(a,b,c) = \text{“}(ab)c = a(bc)\text{”},$$

a sama asocijativnost je sud

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})Q(a,b,c)$$

ili

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})\big((ab)c = a(bc)\big).$$

Ponekad ćemo radi jednostavnosti kratko pisati

$$(ab)c = a(bc), \quad \forall a, b, c \in \mathbb{R}$$

ili sasvim kratko, ne pišući kvantifikator $\forall$*, ali ga podrazumijevajući:*

$$(ab)c = a(bc), \quad a, b, c \in \mathbb{R}.$$

U predikatima mogu sudjelovati i logički veznici kao što pokazuje sljedeći primjer:

Primjer 1.6. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x > 0 \;\&\; y > 0 \implies xy > 0)$.

U ovom slučaju govorimo da je sud zadan formulom koja se sastoji od logičkih veznika, kvantifikatora i predikata. Većina sudova s kojima ćemo se sretati u ovom kolegiju moći će se zapisati na ovaj način.

Znamo da svaki sud možemo negirati. Prilikom dokazivanja raznih tvrdnji će nam posebno važna biti negacija sudova zadanih formulom. Kod negiranja suda zadanog formulom, kvantifikator $\exists$ prelazi u $\forall$, dok $\forall$ prelazi u $\exists$. Kvantifikator $\exists!$ izveden je od $\exists$ and $\forall$, pa se njegova negacija svodi na opisane negacije. Detalje negacije kvantifikatora $\exists!$ nećemo iznositi.

Primjerice, promotrimo sud (istinit)

$$(\forall x \in \mathbb{R})(x^2 \geq 0).$$

Njegova negacija je sud (lažan)

$$(\exists x \in \mathbb{R})(x^2 < 0).$$

Ovdje je negiranjem kvantifikator $\forall$ prešao u $\exists$, dok je predikat $x^2 \geq 0$ prešao u suprotnu tvrdnju $x^2 < 0$.

Zadatak 1.7. *Napišite negaciju sljedećih sudova zadanih formulom:*

(a) $(\forall x \in \mathbb{R})(x < x + 1)$,
(b) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x < y)$,
(c) $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(xy < 0)$.

Ponovo se sjetimo negacije implikacije:

$$\overline{A \implies B} \quad \equiv \quad A\&\overline{B}.$$

Rekli smo da se na semantičkoj jednakosti sudova $\overline{A \implies B}$ i $A\&\overline{B}$ zasniva metoda suprotnog: sud $A \implies B$ dokazujemo (utvrđujemo njegovu istinitost) tako da pretpostavimo suprotno (tj. negiramo ga) i njegovu negaciju, koja je semantički jednaka sudu $A\&\overline{B}$, dovedemo u kontradikciju s nekom već ustanovljenom istinom. Tako zaključujemo da je negacija suda $A \implies B$ laž, pa je $A \implies B$ istina.

Negiranjem suda oblika

$$(\forall x)(\forall y)(P(x, y) \implies Q(x, y))$$

dobije se sud

$$(\exists x)(\exists y)(P(x,y) \ \& \text{ negacija od } Q(x,y)).$$

Primjerice, promotrimo sud

$$(\forall x)(\forall y)(x > 0 \ \& \ y > 0 \implies xy < 1),$$

u kojem je

$$P(x,y) = \text{“}x > 0 \ \& \ y > 0\text{”}$$

i

$$Q(x,y) = \text{“}xy < 1\text{”}.$$

Kod negacije $(\forall x)$ prelazi u $(\exists x)$, $(\forall y)$ prelazi u $(\exists y)$, predikat $P(x,y)$ ostaje isti, $\implies$ prelazi u &, a $Q(x,y)$ se zamjenjuje svojom negacijom, tj. sa $xy \geq 1$. Dakle, negacija danog suda je

$$(\exists x)(\exists y)(x > 0 \ \& \ y > 0 \ \& \ xy \geq 1).$$

Sjetimo se sada i obrata po kontrapoziciji:

$$A \implies B \quad \equiv \quad \overline{B} \implies \overline{A}.$$

Metoda dokazivanja koja se zasniva na ovoj semantičkoj jednakosti se koristi kada je istinitost suda $\overline{B} \implies \overline{A}$ jednostavnije provjeriti negoli istinitost suda $A \implies B$. Kod obrata po kontrapoziciji kvantifikatori ostaju isti. Tipičan primjer je sljedeći sud:

$$(\forall x)(\forall y)(P(x,y) \implies Q(x,y))$$

čiji je obrat po kontrapoziciji:

$$(\forall x)(\forall y)(\text{negacija od } Q(x,y) \implies \text{negacija od } P(x,y)).$$

Konkretno, sud

$$(\forall x)(\forall y)(x \neq y \implies 2x \neq 2y)$$

ima obrat po kontrapoziciji

$$(\forall x)(\forall y)(2x = 2y \implies x = y),$$

čiju istinitost jednostavno vidimo: naime, ako je $2x = 2y$, onda dijeljenjem s 2 odmah dobivamo $x = y$. Tako smo jednostavno dokazali istinitost polaznog suda (s tim u vezi vidite definiciju 5.1 i komentar iza nje).

Još jednom naglasimo, obrat po kontrapoziciji daje tvrdnju koja je semantički jednaka originalnoj, što znači da su istovremeno ili istinite ili lažne, dok metoda suprotnog daje tvrdnju čija je istinitost suprotna od one u originalnoj tvrdnji.

2. Skupovi

U matematici se pojmovi precizno definiraju uvodeći novi pojam preko do tada definiranih (matematičkih) pojmova. Međutim, taj proces svođenja pojma na jednostavniji mora završiti u konačnom broju koraka. Na taj način dolazimo do pojmova koji se ne definiraju preko jednostavnijih. Pojmovi koji dolaze "na početku" moraju biti toliko jednostavni da ih intutivno dobro razumijemo i nemamo problema s njihovim prihvaćanjem. U geometriji su takvi pojmovi točka, pravac i ravnina; oni se u geometriji ne definiraju, već geometrija polazi od tih pojmova kao pojmova o kojima imamo jasnu intuitivnu predodžbu te gradi teoriju i ostale definicije polazeći od njih.

U matematici je jedan od najfundamentalnijih pojmova **skup**. Skup se u matematici ne definira, ali svatko ima sasvim jasnu predodžbu o tome što je skup (skup svih studenata PMF-a, skup rješenja jednadžbe $x^3 + 1 = 0$, skup prirodnih brojeva itd.).

Skupove najčešće označavamo velikim slovima $A, B, C, \ldots, X, Y, Z$. Intuitivno nam je jasno da se skup sastoji od svojih elemenata te razumijemo što znači:

$$x \text{ pripada skupu } S \quad (\text{pišemo: } x \in S),$$
$$y \text{ ne pripada skupu } S \quad (\text{pišemo: } y \notin S).$$

Skupove najčešće opisujemo (kažemo: definiramo) preko nekog predikata $P(x)$ (vidite 1. poglavlje):

$$S = \{x \mid x \text{ zadovoljava svojstvo } P(x)\}.$$

Primjer 2.1. (1) $S = \{x \mid x$ *je student PMF-a*$\}$,
(2) $S = \{x \mid x$ *je realan broj,* $x > 3\}$.

Međutim, nekada jednostavno možemo popisati sve elemente danog skupa. Primjerice, skup S sastavljen od elemenata a, b, c, d pišemo kao

$$S = \{a, b, c, d\}.$$

Smatramo također da postoji jedan i samo jedan skup koji nema niti jedan element. Takav skup nazivamo **prazan skup** i označavamo sa $\emptyset$.

U razvoju naše male matematičke teorije imali smo kao osnovne pojmove: pojam skupa, elementa skupa te pripadanja skupu. Sada ćemo pomoću njih izgraditi složen pojam sastavljen od ovih pojmova kao osnovnih elemenata. Evo kako izgleda jedna stroga matematička definicija:

Definicija 2.2. *Neka su S i T skupovi. Kažemo da je S* ***podskup*** *skupa T ako vrijedi*

$$(\forall x)(x \in S \implies x \in T).$$

U tom slučaju pišemo $S \subseteq T$. Također kažemo da je T ***nadskup*** *skupa S.*

Iz ove definicije razabiremo da je pojam "biti podskup" definiran preko ranije uvedenih matematičkih pojmova.

U matematici ne bismo daleko stigli da imamo samo definicije. Matematika također iskazuje tvrdnje koje su sudovi (izjave) o uvedenim pojmovima u kojima opisuje njihovu strukturu ili međusobni odnos. Izjave u matematici se dokazuju strogom logičkom dedukcijom iz prije dokazanih sudova (koristeći logička pravila iz 1. poglavlja). Kao i kod definiranja pojmova, tako i ovdje imamo tvrdnje koje dolaze "na početku teorije" i koje se ne dokazuju već ih smatramo točnim i izvan svake sumnje te koristimo kao temelj izgradnje matematičke teorije. Takve tvrdnje nazivaju se **aksiomi**. Primjerice, u geometriji Euklidov peti aksiom (aksiom o paralelama) kaže da zadanom točkom izvan zadanog pravca prolazi točno jedan pravac paralelan danom pravcu. To je tvrdnja koja se ne dokazuje, već je prihvaćamo kao istinitu iako ju je teško eksperimentalno provjeriti.

Kada se odrede aksiomi neke matematičke teorije, onda se ostale tvrdnje dokazuju logičkom dedukcijom. Ostale tvrdnje u matematici nazivaju se **lema**, **propozicija**, **teorem** i **korolar**. Lema je obično pomoćni tehnički korak u dokazivanju složenijih tvrdnji propozicija i teorema. Propozicijom se naziva tvrdnja u nekoj cjelini koja je po važnosti između leme i teorema. Teorem je najvažnija tvrdnja neke cjeline. Korolar je posljedica, najčešće direktna, neke leme, propozicije ili teorema. Često je vrlo individualno što autor naziva lemom, propozicijom, teoremom ili korolarom.

Svaki teorem / propozicija / lema / korolar ima pretpostavke (uvjete koji se moraju provjeriti prije primjene teorema) i zaključke.

Prisjetimo se, Pitagorin teorem glasi:

> Ako je trokut ABC pravokutan s pravim kutom pri vrhu C,
>
> tada za duljine a, b, c njegovih stranica vrijedi $a^2 + b^2 = c^2$.

U ovom teoremu je pretpostavka: "trokut je pravokutan", a zaključak: "za duljine a, b, c njegovih stranica vrijedi $a^2 + b^2 = c^2$". Jasno je da Pitagorin teorem ne smijemo primjenjivati na trokute koji nisu pravokutni (jer za njih nije ispunjena pretpostavka teorema).

Dakle, svaki teorem / propozicija / lema / korolar je izjava oblika

$$A \implies B,$$

pri čemu je sud A pretpostavka, a sud B zaključak.

Obrat tog teorema je izjava

$$B \implies A$$

i ovdje je B pretpostavka, a A zaključak.

Konkretno, obrat Pitagorinog teorema je teorem:

> Ako za duljine stranica a, b, c trokuta ABC vrijedi $a^2 + b^2 = c^2$,
>
> tada je trokut ABC pravokutan s pravim kutom pri vrhu C.

Ovdje je pretpostavka: "za duljine stranica a, b, c trokuta ABC vrijedi $a^2 + b^2 = c^2$", a zaključak: "tada je trokut ABC pravokutan s pravim kutom pri vrhu C".

Jasno, ako je $A \implies B$ istina, ne mora biti istina i $B \implies A$ (usporedite semantičke tablice). Drugim riječima, postoje teoremi čiji obrat ne vrijedi (pronađite primjere).

Teoremi u kojima se pojavljuje fraza "ako i samo ako" (ili kraće: "akko") su oblika $A \iff B$ i u sebi zapravo sadrže dvije tvrdnje: $A \implies B$ i $B \implies A$ jer je

$$A \iff B \quad \equiv \quad (A \implies B) \,\&\, (B \implies A)$$

(provjerite).

Sada ćemo iskazati i dokazati našu prvu tvrdnju.

Propozicija 2.3. *Neka je T skup. Tada je $\emptyset \subseteq T$ tj. prazan skup je podskup svakog skupa.*

Dokaz. Primjenjujući definiciju 2.2 na slučaj $S = \emptyset$, nalazimo da treba dokazati:

$$(\forall x)(x \in \emptyset \implies x \in T).$$

Međutim, ne postoji niti jedan $x \in \emptyset$ te je stoga implikacija trivijalno ispunjena (jer nema elementa za provjeriti pripadnost skupu T). □

Definicija 2.4. *Kažemo da su skupovi S i T* ***jednaki*** *ako je $S \subseteq T$ i $T \subseteq S$.*

Kod provjere jednakosti skupova S i T treba provjeriti da je S podskup od T i T podskup od S. Po definiciji 2.2, za provjeru izjave "S je podskup od T" moramo vidjeti da vrijedi

$$(\forall x)(x \in S \implies x \in T),$$

dok za provjeru izjave "T je podskup od S" moramo vidjeti da vrijedi

$$(\forall x)(x \in T \implies x \in S).$$

Kombinirajući jedno i drugo, zaključujemo da kod provjere jednakosti skupova S i T moramo provjeriti da vrijedi

$$(\forall x)(x \in S \iff x \in T).$$

Definicija 2.5. *Kažemo da je skup S* ***pravi podskup*** *skupa T ako je $S \subseteq T$, ali $S \neq T$. Pišemo $S \subset T$ ili $S \subsetneq T$.*

Primjer 2.6. (a) $\{1,2,3\} = \{2,3,1\}$,
(b) $\{1,2\} \neq \{1,2,3\}$,
(c) $\{1,2,3\} \subset \{1,2,3,4,5\}$,
(d) $\{1,1\} = \{1\}$.

Vezano uz (d) u primjeru 2.6, naglasimo da na skup nema utjecaja ako neki element ponovimo u popisu elemenata skupa.

Primjer 2.7. *Uočimo da je $\emptyset \neq \{\emptyset\}$ jer s lijeve strane imamo skup $\emptyset$ koji nema niti jedan element, ali s desne strane imamo skup $\{\emptyset\}$ koji nije prazan već ima kao svoj jedini element prazan skup.*

Zadatak 2.8. *Dokažite $\{\emptyset\} \neq \{\{\emptyset\}\}$.*

Neka je S skup. **Partitivni skup** skupa S, u oznaci $\mathcal{P}(S)$, je skup svih podskupova skupa S. Ponekad se partitivni skup skupa S označava i sa 2^S.

Svaki skup S ima dva očigledna podskupa, a to su $\emptyset$ i S. Zato je uvijek

$$\emptyset, S \in \mathcal{P}(S).$$

Ti podskupovi su različiti ako i samo ako je $S \neq \emptyset$. Dakle, ako je S neprazan skup, skup $\mathcal{P}(S)$ ima barem dva elementa.

Primjer 2.9. (a) $S = \emptyset \implies \mathcal{P}(S) = \{\emptyset\}$,
(b) $S = \{1\} \implies \mathcal{P}(S) = \{\emptyset, \{1\}\}$,
(c) $S = \{1,2,3\} \implies \mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Zadatak 2.10. *Odredite partitivni skup skupa S ako je:*

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

U određenom matematičkom razmatranju potrebno je gledati samo podskupove nekog skupa. U tom slučaju takav skup nazivamo **univerzalni skup**. Primjerice, u planimetriji je univerzalni skup ravnina, a u stereometriji je univerzalni skup prostor.

Važno je naglasiti da kolekcija svih skupova nije skup. Sljedeći paradoks, tzv. Russelov paradoks, to objašnjava. Ako bi svi skupovi tvorili skup, recimo S, onda bismo pomoću predikata mogli opisati skup

$$T = \{A \mid A \text{ je skup, ali } A \notin A\}.$$

Dakle, skup T se sastoji od svih skupova koji nisu svoji elementi. Primjerice, $\{1\} \in T$ jer $\{1\} \notin \{1\}$ (jasno je da $1 \in \{1\}$ vrijedi!). U sljedećem koraku možemo se zapitati je li skup T svoj element. Tada imamo:

(1) Ako je $T \in T$, onda T mora zadovoljavati predikat koji definira skup T, a to je:

$$A \text{ je skup, ali } A \notin A.$$

Dakle, za $A = T$, dobili bismo $T \notin T$. Dakle, polazeći od $T \in T$ dobili smo $T \notin T$.

(2) Ako $T \notin T$, onda T ne zadovoljava predikat koji definira T. Dakle, za $A = T$, dobili bismo $T \in T$.

Prema tome, za skup T ne vrijedi niti jedna od izjava $T \in T$ i $T \notin T$. Ovo je paradoks i takve mogućnosti isključujemo. Dakle, svi skupovi ne tvore skup, radije govorimo o kolekciji svih skupova.

Sada definiramo **Boolove operacije na skupovima**. Smatramo da radimo s podskupovima univerzalnog skupa U.

(1) *Unija skupova A i B:*

$$A \cup B \stackrel{def}{=} \{x \in U \mid x \in A \text{ ili } x \in B\}.$$

(2) *Presjek skupova A i B:*

$$A \cap B \stackrel{def}{=} \{x \in U \mid x \in A \text{ i } x \in B\}.$$

(3) *Razlika (ili diferencija) skupova A i B:*

$$A \setminus B \stackrel{def}{=} \{x \in U \mid x \in A \text{ i } x \notin B\}.$$

(4) *Simetrična razlika (ili simetrična diferencija) skupova A i B:*

$$A \Delta B \stackrel{def}{=} (A \setminus B) \cup (B \setminus A).$$

(5) *Komplement skupa A (u skupu U):*

$$A^c \stackrel{def}{=} \{x \in U \mid x \notin A\}.$$

Naglasimo sljedeće:

(1) $x \in A \cup B$ ako i samo ako je $x \in A$ ili $x \in B$,
(2) $x \notin A \cup B$ ako i samo ako je $x \notin A$ i $x \notin B$,
(3) $x \in A \cap B$ ako i samo ako je $x \in A$ i $x \in B$,
(4) $x \notin A \cap B$ ako i samo ako je $x \notin A$ ili $x \notin B$.

Za skupove A i B kažemo da su **disjunktni** ako je $A \cap B = \emptyset$.

Uočimo: $A \cap B \subseteq A$. Naime,

$$(\forall x)(x \in A \cap B) \implies (x \in A \text{ i } x \in B) \implies x \in A.$$

Analogno, $A \cap B \subseteq B$.

Nadalje, $A \subseteq A \cup B$ jer

$$(\forall x)(x \in A) \implies (x \in A \text{ ili } x \in B) \implies x \in A \cup B.$$

Analogno je $B \subseteq A \cup B$.

Zadatak 2.11. *Dokažite sljedeće tvrdnje:*

(i) $A \subseteq A$, $\forall A$,
(ii) $A \subseteq B$ *i* $B \subseteq C \implies A \subseteq C$,
(iii) $A = B$ *i* $B = C \implies A = C$.

Propozicija 2.12. *Neka su A i B podskupovi skupa U. Neka su A^c i B^c redom komplementi skupova A i B u skupu U. Tada vrijedi:*

$$A \setminus B = A \cap B^c.$$

Dokaz. Treba dokazati da je $A \setminus B$ podskup od $A \cap B^c$ i da je $A \cap B^c$ podskup od $A \setminus B$.

Najprije dokažimo da je $A \setminus B$ podskup od $A \cap B^c$. Treba dokazati

$$(\forall x)(x \in A \setminus B) \implies x \in A \cap B^c.$$

Zaista,

$$x \in A \setminus B \implies x \in A \text{ i } x \notin B \implies x \in A \text{ i } x \in B^c \implies x \in A \cap B^c.$$

Sada dokažimo da je $A \cap B^c$ podskup od $A \setminus B$. Treba dokazati

$$(\forall x)(x \in A \cap B^c) \implies x \in A \setminus B.$$

Zaista,

$$x \in A \setminus B^c \implies x \in A \text{ i } x \in B^c \implies x \in A \text{ i } x \notin B \implies x \in A \setminus B.$$

Ovim je propozicija dokazana. □

Sada ćemo iskazati glavni rezultat ovog predavanja. Prisjetimo se, takve rezultate nazivamo teoremi.

Teorem 2.13. *Neka su A, B, C podskupovi skupa U. Neka su A^c, B^c i C^c redom komplementi skupova A, B i C u skupu U. Tada vrijede sljedeće tvrdnje:*

(i) *(asocijativnost)* $(A \cup B) \cup C = A \cup (B \cup C)$ *i* $(A \cap B) \cap C = A \cap (B \cap C)$,
(ii) *(komutativnost)* $A \cup B = B \cup A$ *i* $A \cap B = B \cap A$,
(iii) *(distributivnost)* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *i* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
(iv) $A \cup A^c = U$ *i* $A \cap A^c = \emptyset$,
(v) $A \cup \emptyset = A$ *i* $A \cap U = A$,
(vi) $A \cup U = U$ *i* $A \cap \emptyset = \emptyset$,
(vii) *(de Morganove formule:)* $(A \cup B)^c = A^c \cap B^c$ *i* $(A \cap B)^c = A^c \cup B^c$,
(viii) $U^c = \emptyset$ *i* $\emptyset^c = U$,
(ix) *(idempotentnost)* $A \cup A = A$ *i* $A \cap A = A$,
(x) $(A^c)^c = A$,

(xi) $A \cup (A \cap B) = A$ *i* $A \cap (A \cup B) = A$.

Dokaz. Dokazi ovih tvrdnji slični su onima u propoziciji 2.12. Dokazat ćemo (vii), a ostalo ostavljamo za zadaću.

Dokažimo prvo $(A \cup B)^c = A^c \cap B^c$. Treba dokazati da je lijeva strana podskup desne i obratno.

Najprije, ako je $x \in (A \cup B)^c$, onda vrijedi $x \notin A \cup B$. Po definiciji unije, to znači da vrijedi $x \notin A$ i $x \notin B$. Dakle, $x \in A^c$ i $x \in B^c$. Stoga, po definiciji presjeka, $x \in A^c \cap B^c$. Dakle, $(A \cup B)^c \subseteq A^c \cap B^c$.

Obratno, ako je $x \in A^c \cap B^c$, onda, po definiciji presjeka, nalazimo $x \in A^c$ i $x \in B^c$. Dakle, $x \notin A$ i $x \notin B$. Stoga, po definiciji unije, $x \notin A \cup B$. Dakle, $x \in (A \cup B)^c$. Ovim je dokazano $A^c \cap B^c \subseteq (A \cup B)^c$.

Druga jednakost $(A \cap B)^c = A^c \cup B^c$ dokazuje se slično. U ovim dokazima je bilo ključno sjetiti se da kod negacije "**i**" prelazi u "**ili**" i obratno. □

Definicija 2.14. *Neka su A i B neprazni skupovi. Neka je $a \in A$ i $b \in B$.* ***Uređen par*** *(a, b) je skup $\{\{a\}, \{a, b\}\}$. Nadalje, a se naziva prva koordinata, a b druga koordinata u uređenom paru. Skup svih uređenih parova (a, b), pri čemu a prolazi skupom A a b prolazi skupom B, nazivamo* ***Kartezijev produkt*** *skupova A i B, tj.*

$$A \times B \overset{def}{=} \{(a, b) \mid a \in A,\ b \in B\}.$$

Iz osnovne škole poznat nam je pojam uređenog para, ali tek sada imamo strogu definiciju. Također nam je poznata i tvrdnja sljedećeg teorema, ali tek sada dajemo strogi dokaz.

Teorem 2.15. *Neka su A i B neprazni skupovi. Neka su $a, a' \in A$ i $b, b' \in B$. Tada vrijedi:*

$$(a, b) = (a', b') \iff a = a' \text{ i } b = b'. \tag{2.16}$$

Dokaz. Ovaj dokaz koristi semantičko pravilo uvedeno zadatkom 1.2 (3). Preciznije, zbog " $\iff$ " u (2.16) moramo dokazati "dva smjera":

$\boxed{\Longrightarrow}$: U ovom smjeru treba dokazati da $(a, b) = (a', b')$ povlači $a = a'$ i $b = b'$. Zaista, ako je $(a, b) = (a', b')$, onda prema definiciji 2.14 imamo sljedeću jednakost skupova:

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}. \tag{2.17}$$

Najprije, ako je $a = b$, onda lijeva strana u (2.17) postaje (vidite komentar iza primjera 2.6)

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

Dakle, u ovom slučaju lijeva strana u (2.17) ima samo jedan element. Stoga i desna strana u (2.17) mora imati samo jedan element. Dakle, mora biti $a' = b'$. Sada, slično kao gore, desna strana postaje $\{\{a'\}\}$.

Stoga je (2.17) u ovom slučaju oblika

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

Primjenjući definiciju jednakosti skupova dolazimo do

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

Primjenjući definiciju jednakosti skupova još jednom, zaključujemo

$$a = a'.$$

Dakle, ako je $a = b$, tada je $a = b = a' = b'$. Ovo završava analizu slučaja $a = b$ i u tom slučaju je željena tvrdnja dokazana.

Neka je sada $a \neq b$. Sada se lijeva strana u (2.17) sastoji od skupa koji ima dva elementa (koji su po svojoj prirodi opet skupovi): $\{a\}$ i $\{a, b\}$. Zbog jednakosti skupova, svaki od elemenata desne strane u (2.17), a to su $\{a'\}$ i $\{a', b'\}$, mora biti jedan od onih na lijevoj strani, a to su $\{a\}$ i $\{a, b\}$. Očito je $\{a'\} = \{a\}$, jer $\{a'\} = \{a, b\}$ zbog $a \neq b$ nije moguće. Sada, iz $\{a'\} = \{a\}$ slijedi $a = a'$. Također, $\{a, b\}$ se mora pojaviti na desnoj strani, ali kako već imamo $\{a'\} = \{a\}$, mora biti

$$\{a, b\} = \{a', b'\}. \tag{2.18}$$

Kako smo već dokazali $a = a'$, to (2.18) pišemo u obliku

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

Konačno, kako je $a \neq b$, iz jednakosti skupova zaključujemo $b = b'$. Ovim je "$\Longrightarrow$" provjereno.

Ostaje još dokazati obratan smjer:

$\boxed{\Longleftarrow}$: Treba dokazati da $a = a'$ i $b = b'$ povlači $(a, b) = (a', b')$. Međutim, to je očigledna tvrdnja. $\square$

Primjer 2.19. *Neka je $A = \{1, 2\}$ i $B = \{1, 2, 3\}$. Tada imamo:*

$$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\},$$

$$B \times A = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,2)\}.$$

Jasno je da $A \times B$ i $B \times A$ uvijek imaju isti broj elemenata (jednak produktu broja elemenata skupa A i broja elemenata skupa B). Međutim, kao što pokazuje primjer 2.19, općenito je $A \times B \neq B \times A$.

Definicija 2.20. *Neka je A neprazan skup.* ***Kartezijev kvadrat*** *(ili samo kvadrat) skupa A je skup*

$$A^2 \overset{def}{=} A \times A.$$

Dijagonala skupa *A je skup $\{(a, a) \mid a \in A\}$. Očito je dijagonala skupa A podskup skupa A^2.*

Mi smo do sada definirali uređene parove, ali možemo definirati redom i uređene trojke, četvorke itd. Primjerice, neka su A, B i C neprazni skupovi. Neka su $a \in A$, $b \in B$ i $c \in C$. Tada možemo definirati uređenu trojku na ovaj način:

$$(a, b, c) \stackrel{def}{=} (a, (b, c)),$$

odnosno kao uređen par kojemu je prva koordinata a, a druga koordinata uređen par (b, c). Vrijedi ova posljedica (korolar) teorema 2.15:

Korolar 2.21. *Neka su A, B i C neprazni skupovi. Neka su $a, a' \in A$, $b, b' \in B$ i $c, c' \in C$. Tada vrijedi:*

$$(a, b, c) = (a', b', c') \iff a = a' \text{ i } b = b' \text{ i } c = c'.$$

Dokaz. Smjer "$\Longleftarrow$" je trivijalan. Dokažimo "$\Longrightarrow$". Iz $(a, b, c) = (a', b', c')$, koristeći definiciju uređene trojke, dobivamo

$$(a, (b, c)) = (a', (b', c')).$$

Primjenjujući teorem 2.15, zaključujemo da ovi uređeni parovi imaju jednake prve koordinate tj.

$$a = a'$$

i jednake druge koordinate:

$$(b, c) = (b', c'). \tag{2.22}$$

Konačno, primjenjujući još jednom teorem 2.15, ali sada na (2.22), zaključujemo $b = b'$ i $c = c'$. □

Sada kada smo definirali uređenu trojku, spremni smo definirati Kartezijev produkt skupova A B i C:

$$A \times B \times C \stackrel{def}{=} \{(a, b, c) \mid a \in A,\ b \in B,\ c \in C\}.$$

Analogno definiramo i uređenu n-torku (za bilo koji prirodni broj n), a pomoću nje i Kartezijev produkt n skupova $A_1, A_2, \dots, A_n$.

3. Relacije

Neka su A i B dva skupa. **Relacija** je svaki podskup ρ Kartezijevog produkta $A \times B$.

Za element $a \in A$ kažemo da je u relaciji ρ s elementom $b \in B$ ako je $(a, b) \in \rho$. Kraće pišemo: $a \, \rho \, b$.

Pojam "relacija" se često rabi u svakodnevnom životu označavajući neki odnos ili vezu. Kao što vidimo, slično značenje ovaj pojam ima i u matematici: $a \, \rho \, b$ znači da su a i b u izvjesnoj vezi, a ta veza je $(a, b) \in \rho$.

Primjer 3.1. (a) *Prazan skup je relacija koju nazivamo prazna relacija. Vrijedi: $\emptyset \subseteq A \times B$ za sve skupove A i B (vidite propoziciju 2.3).*

(b) *Ako je $A = \{1, 3, 5\}$ i $B = \{a, b\}$, tada je*

$$A \times B = \{(1, a), (1, b), (3, a), (3, b), (5, a), (5, b)\}.$$

Neka je $\rho_1 = \{(1, a), (5, a), (3, b)\}$ i $\rho_2 = \{(3, a)\}$. Tada primjerice imamo: $(1, b) \notin \rho_1$, $(1, a) \in \rho_1$, $(3, b) \notin \rho_2$.

Binarna relacija na skupu A je svaki podskup $\rho \subseteq A \times A$.

Evo nekoliko primjera binarnih relacija na skupu $\mathbb{R}$ s pripadnim geometrijskim značenjima.

Primjer 3.2. $\rho = \{(x, y) \in \mathbb{R}^2 \,|\, y < 3x - 2\}$ *poluravnina.*

Primjer 3.3. $\rho = \{(x, y) \in \mathbb{R}^2 \,|\, x^2 + y^2 < 1\}$ *otvoreni krug $K(0, 1)$.*

Primjer 3.4. $\rho = \{(x, y) \in \mathbb{R}^2 \,|\, \frac{x^2}{25} + \frac{y^2}{9} = 1, xy = 1\}$ *četiri točke ravnine.*

Sljedeći primjer binarne relacije smo već susreli (definicija 2.20).

Primjer 3.5. *Dijagonala $\Delta = \{(x, x) \,|\, x \in A\} \subseteq A \times A$ je binarna relacija na skupu A.*

Sada istaknimo neka važna svojstva koja binarna relacija može imati.

Definicija 3.6. *Neka je ρ binarna relacija na skupu A. Kažemo da je relacija ρ :*

(i) ***refleksivna*** *ako je*

$$(x, x) \in \rho, \quad \forall x \in A;$$

(ii) ***simetrična*** *ako*

$$\forall (x, y) \in A \times A, \quad (x, y) \in \rho \implies (y, x) \in \rho;$$

(iii) ***antisimetrična*** *ako*

$$\forall (x,y) \in A \times A, \quad (x,y) \in \rho \ \& \ (y,x) \in \rho \implies x = y;$$

(iv) ***tranzitivna*** *ako*

$$\forall (x,y),(y,z) \in A \times A, \quad (x,y) \in \rho \ \& \ (y,z) \in \rho \implies (x,z) \in \rho.$$

Uočimo da je binarna relacija ρ na skupu A refleksivna ako i samo ako sadrži dijagonalu Δ od A tj. ako i samo ako je $\Delta \subseteq \rho$.

Primjer 3.7. *(a) Neka je binarna relacija $\rho \subseteq \mathbb{R}^2$ definirana sa*

$$\rho = \{(x,y) \in \mathbb{R}^2 \,\big|\, x \leq y\}, \text{ tj. } x \, \rho \, y \Longleftrightarrow x \leq y.$$

Ova relacija ima sljedeća svojstva:

(i) *refleksivnost:*

$$x \leq x \implies x \, \rho \, x,$$

(ii) *antisimetričnost:*

$$x \, \rho \, y \ \& \ y \, \rho \, x \implies x \leq y \ \& \ y \leq x \implies x = y,$$

(iii) *tranzitivnost:*

$$x \, \rho \, y \ \& \ y \, \rho \, z \implies x \leq y \ \& \ y \leq z \implies x \leq z \implies x \, \rho \, z.$$

(b) Neka je binarna relacija $\rho \subseteq \mathbb{N}^2$ definirana sa

$$\rho = \{(m,n) \in \mathbb{N}^2 \mid m \mid n\}.$$

Uočimo:

$$m \mid n \Longleftrightarrow (\exists k \in \mathbb{N})(n = m \cdot k).$$

Dakle,

$$m \, \rho \, n \Longleftrightarrow (\exists k \in \mathbb{N})(n = m \cdot k).$$

Ova relacija ima sljedeća svojstva:

(i) *refleksivnost:*

$$m = m \cdot 1 \implies m \, \rho \, m;$$

(ii) *antisimetričnost:*

$$m \, \rho \, n \ \& \ n \, \rho \, m$$

povlači

$$(\exists k \in \mathbb{N})(n = m \cdot k) \ \& \ (\exists l \in \mathbb{N})(m = n \cdot l);$$

sada imamo

$$n = m \cdot k = (n \cdot l) \cdot k = n \cdot (l \cdot k) \implies l \cdot k = 1,$$

a kako su $k, l \in \mathbb{N}$, zaključujemo $k = l = 1$, odakle slijedi $m = n$;

(iii) *tranzitivnost:*

$$m \,\rho\, n \;\&\; n \,\rho\, p$$

povlači

$$(\exists k \in \mathbb{N})(n = m \cdot k) \;\&\; (\exists l \in \mathbb{N})(p = n \cdot l);$$

slijedi

$$p = n \cdot l = (m \cdot k) \cdot l = m \cdot (k \cdot l),$$

a kako su $k, l \in \mathbb{N}$, *to je i* $k \cdot l \in \mathbb{N}$, *pa je* $m \,\rho\, p$.

Vidimo da binarna relacija "$\leq$" ("manje ili jednako") na skupu $\mathbb{R}$ i binarna relacija "$|$" ("biti djelitelj") na skupu $\mathbb{N}$ formalno zadovoljavaju ista svojstva: refleksivnost, antisimetričnost i tranzitivnost.

Definicija 3.8. ***Relacija parcijalnog uređaja*** *"$\leq$" na skupu X je binarna relacija na X koja ima sljedeća svojstva:*

(i) *refleksivnost tj.* $(\forall x \in X)(x \leq x)$,
(ii) *antisimetričnost tj.* $(\forall x, y \in X)((x \leq y \;\&\; y \leq x) \implies x = y)$,
(iii) *tranzitivnost tj.* $(\forall x, y, z \in X)((x \leq y \;\&\; y \leq z) \implies x \leq z)$.

Dakle, binarne relacije "$\leq$" ("manje ili jednako") na skupu $\mathbb{R}$ i "$|$" ("biti djelitelj") na skupu $\mathbb{N}$ su relacije parcijalnog uređaja.

Uočimo da se u definiciji relacije parcijalnog uređaja ne zahtijeva

$$(\forall x, y \in X)(x \leq y \text{ ili } y \leq x),$$

što znači da je moguće da postoje "neusporedivi" $x, y \in X$, tj. oni za koje nije niti $x \leq y$ ili $y \leq x$.

Primjer 3.9. (a) *Parcijalni uređaj "$\leq$" na skupu $\mathbb{R}$ je parcijalni uređaj u kojem su svaka dva elementa od $\mathbb{R}$ usporediva, tj.* $(\forall x, y \in \mathbb{R})(x \leq y \text{ ili } y \leq x)$.
(b) *Parcijalni uređaj "$|$" na skupu $\mathbb{N}$ je parcijalni uređaj u kojem postoje neusporedivi elementi od $\mathbb{N}$: primjerice, nije niti $2 \mid 3$ niti $3 \mid 2$.*

Definicija 3.10. *Parcijalni uređaj "$\leq$" na skupu X je* **uređaj ili totalni uređaj** *ako* $(\forall x, y \in X)(x \leq y \text{ ili } y \leq x)$.

Dakle, binarna relacija "$\leq$" na skupu $\mathbb{R}$ je totalni uređaj, a binarna relacija "$|$" na skupu $\mathbb{N}$ nije totalni uređaj.

Ako je "$\leq$" totalni uređaj, tada za različite $x, y \in X$ vrijedi ili $x \leq y$ ili $y \leq x$, ali ne i jedno i drugo (zbog antisimetričnosti).

Propozicija 3.11. *Neka je S bilo koji skup. Binarna relacija "$\leq$" na skupu $\mathcal{P}(S)$ definirana sa*

$$(\forall A, B \in \mathcal{P}(S))(A \leq B \iff A \subseteq B)$$

je relacija parcijalnog uređaja.

Dokaz. (i) Refleksivnost:

$$A \subseteq A, \forall A \in \mathcal{P}(S) \implies A \leq A.$$

(ii) Antisimetričnost:

$$(\forall A, B \in \mathcal{P}(S))(A \subseteq B \;\&\; B \subseteq A) \implies A = B$$

(sjetimo se da je upravo to definicija jednakosti među skupovima).

(iii) Tranzitivnost:

$$\begin{aligned}
&(\forall A, B, C \in \mathcal{P}(S))(A \subseteq B \,\&\, B \subseteq C)\\
\implies &(\forall x)(x \in A \implies x \in B) \quad \& \quad (\forall y)(y \in B \implies y \in C)\\
\implies &(\forall x)(x \in A \implies x \in B \implies x \in C)\\
\implies &(\forall x)(x \in A \implies x \in C) \implies A \subseteq C.
\end{aligned}$$

□

Primjer 3.12. *Ako je $S = \{1, 2\}$, tada je $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Promotrimo binarnu relaciju "$\leq$" na $\mathcal{P}(S)$ definiranu kao u propoziciji 3.11, tj. sa*

$$(\forall A, B \in \mathcal{P}(S))\,(A \leq B \iff A \subseteq B).$$

Uočimo da nije niti $\{1\} \leq \{2\}$ niti $\{2\} \leq \{1\}$, dakle $\{1\}$ i $\{2\}$ su neusporedivi! Prema tome, parcijalni uređaj "$\leq$" na skupu $\mathcal{P}(S)$ nije totalni uređaj. No, primijetimo da je $\emptyset \leq \{1\} \leq \{1, 2\}$ i $\emptyset \leq \{2\} \leq \{1, 2\}$.

Definicija 3.13. *Neka je $(X, \leq)$ parcijalno uređen skup te neka je $S \subseteq X$ neprazan.*

*Kažemo da je $m \in X$ **donja među** skupa S ako je $m \leq x$ za svaki $x \in S$.*

*Za skup S kažemo da je **odozdo omeđen** ako postoji barem jedna donja međa skupa S.*

*Kažemo da je $\inf S \in X$ **infimum ili najveća donja međa** skupa S ako ima sljedeća svojstva:*

(i) $\inf S$ *je donja međa skupa S,*
(ii) *za svaku donju među m skupa S vrijedi $m \leq \inf S$.*

*Za element $\min S \in S$ kažemo da je **minimum ili najmanji element** skupa S ako je $\min S$ donja međa skupa S.*

Ako infimum i minimum postoje, tada su jedinstveni, što dokazujemo u sljedećoj propoziciji. Time opravdavamo oznaku $\inf S$ za infimum skupa S i $\min S$ za minimum skupa S.

Propozicija 3.14. *Neka je $(X, \leq)$ parcijalno uređen skup te neka je $S \subseteq X$ neprazan skup. Tada vrijede sljedeće tvrdnje:*

(i) *Ako postoji infimum skupa S, tada je on jedinstven.*

(ii) *Ako postoji minimum skupa S, tada je on jednak infimumu, pa je jedinstven.*

Dokaz. (i) Neka su m_1 i m_2 infimumi skupa S. Tada vrijedi:

(1) m_1 i m_2 su donje međe skupa S,
(2) za svaku donju među m skupa S vrijedi $m \leq m_1$ i $m \leq m_2$.

Ukoliko u (2) stavimo $m = m_2$, zaključujemo $m_2 \leq m_1$, a stavimo li $m = m_1$, zaključujemo $m_1 \leq m_2$. Sada iz $m_2 \leq m_1$ i $m_1 \leq m_2$ slijedi $m_1 = m_2$ zbog antisimetričnosti. Dakle, infimum skupa S je jedinstven.

(ii) Kako je $\inf S$ donja međa skupa S, to je $\inf S \leq x$ za svaki $x \in S$. Obzirom da skup S ima minimum $\min S$, to za $x = \min S$ dobivamo $\inf S \leq \min S$. Međutim, $\inf S$ je najveća donja međa skupa S, a $\min S$ donja međa od S, pa je $\min S \leq \inf S$. Antisimetričnost konačno povlači $\min S = \inf S$. $\square$

Zadatak 3.15. *Neka je $(X, \leq)$ parcijalno uređen skup te neka je $S \subseteq X$ neprazan.*

Definirajte pojam gornje međe skupa S, pojam odozgo omeđenog skupa, pojam supremuma ili najmanje gornje međe skupa S (oznaka: $\sup S$) te maksimuma skupa S (oznaka: $\max S$).

Dokažite jedinstvenost supremuma, ukoliko postoji.

Dokažite da je $\max S = \sup S$ ako skup S ima maksimum.

Sada se opet vratimo na binarne relacije.

Definicija 3.16. *Binarnu relaciju ρ na skupu S nazivamo **relacija ekvivalencije (ili relacija klasifikacije)** ako ima sljedeća svojstva:*

(i) *refleksivnost tj.* $(\forall x \in X)(x \,\rho\, x)$,
(ii) *simetričnost tj.* $(\forall x, y \in X)(x \,\rho\, y \implies y \,\rho\, x)$,
(iii) *tranzitivnost tj.* $(\forall x, y, z \in X)((x \,\rho\, y \;\&\; y \,\rho\, z) \implies x \,\rho\, z)$.

Primjer 3.17. *Neka je $X = \{$skup studenata u ovoj predavaonici$\}$.*
Na X definiramo relaciju ρ sa:

$$A \,\rho\, B \iff A \text{ i } B \text{ imaju istu boju očiju.}$$

Uočimo da je ρ relacija ekvivalencije na X. Ona prirodno daje particiju (podjelu) studenata u klase i svaki student pripada točno jednoj klasi. Ovo opravdava naziv "relacija klasifikacije". Dakle, relacija ρ dijeli skup X na disjunktne podskupove.

Primjer 3.18. *Neka je $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ skup svih cijelih brojeva te neka je n zadani prirodni broj (o prirodnim i cijelim brojevima se govori u 8. poglavlju). Tada*

$$(\forall m \in \mathbb{Z})((\exists! q \in \mathbb{Z}) \;\&\; (\exists! r \in \{0, 1, \dots, n-1\}))(m = n \cdot q + r);$$

kažemo da je q kvocijent pri dijeljenju m sa n, a r ostatak pri dijeljenju m sa n. Primjerice, za $n = 5$ je:

$$38 = 5 \cdot 7 + 3, \text{ tj. } q = 7 \text{ i } r = 3,$$

odnosno

$$-38 = 5 \cdot (-8) + 2, \text{ tj. } q = -8 \text{ i } r = 2.$$

Kako smo došli do ovih prikaza?

$$5 \cdot 7 \leq 38 < 5 \cdot 8 \text{ daje } q = 7, \text{ a } r = m - n \cdot q = 38 - 5 \cdot 7 = 3,$$

odnosno

$$5 \cdot (-8) \leq -38 < 5 \cdot (-7) \text{ daje } q = -8, \text{ a } r = m - n \cdot q = -38 - 5 \cdot (-8) = 2.$$

Dakle, najprije nađemo $q \in \mathbb{Z}$ takav da vrijedi

$$n \cdot q \leq m < n \cdot (q + 1).$$

Egzistenciju takvog $q \in \mathbb{Z}$ nije jednostavno dokazati i to ostavljamo za kasnije (vidite teorem 8.16 i njegov dokaz). Sada je

$$0 \leq m - n \cdot q < n.$$

Stavimo li $r = m - n \cdot q$, imamo

$$0 \leq r < n.$$

Kako je $r \in \mathbb{Z}$, to je $r \in \{0, 1, \ldots, n-1\}$. Dakle, $m = n \cdot q + r$, gdje je $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, n-1\}$.

Sada dokažimo jedinstvenost takvog prikaza. Neka su $q_1, q_2 \in \mathbb{Z}$ i $r_1, r_2 \in \{0, 1, \ldots, n-1\}$ takvi da je $m = n \cdot q_1 + r_1$ i $m = n \cdot q_2 + r_2$. Tada je

$$n \cdot q_1 + r_1 = n \cdot q_2 + r_2,$$

odakle slijedi

$$n \cdot (q_1 - q_2) = r_2 - r_1.$$

Pretpostavimo $q_1 \neq q_2$. Bez smanjenja općenitosti smijemo uzeti $q_1 > q_2$. Kako su $q_1, q_2 \in \mathbb{Z}$, to je $q_1 - q_2 \geq 1$. Slijedi $n \cdot (q_1 - q_2) \geq n$. Međutim, kako vrijedi $0 \leq r_1, r_2 < n$, to je $r_2 - r_1 \leq r_2 < n$. Prema tome, $n \cdot (q_1 - q_2) \neq r_2 - r_1$. Obratom po kontrapoziciji zaključujemo da $n \cdot (q_1 - q_2) = r_2 - r_1$ povlači $q_1 = q_2$ i stoga $r_1 = r_2$.

Ako je ostatak pri dijeljenju m sa n jednak nuli, tada je $m = n \cdot q$; u tom slučaju kažemo da je m djeljiv sa n i pišemo $n \mid m$. Posebno, ako $2 \mid m$, kažemo da je m paran, inače je neparan. Navedimo neka svojstva djeljivosti. Očigledno je nula djeljiva svakim prirodnim brojem jer je $0 = n \cdot 0$. Dalje, ako $n \mid m$, tada je $m = n \cdot q$ za neki $q \in \mathbb{Z}$, pa je $-m = n \cdot (-q)$ i stoga $n \mid -m$. Ako $n \mid m$ i $n \mid p$, tada je $m = n \cdot q$ i $p = n \cdot r$ za neke $q, r \in \mathbb{Z}$, pa je $m + p = n \cdot (q + r)$, odakle zaključujemo $n \mid m + p$.

Na skupu $\mathbb{Z}$ definiramo relaciju "$\equiv \pmod{n}$" sa:

$$a \equiv b \pmod{n} \Longleftrightarrow n \mid a - b.$$

Relacija "$\equiv \pmod{n}$" je relacija ekvivalencije na skupu $\mathbb{Z}$:

(1) *refleksivnost: za svaki* $a \in \mathbb{Z}$ *vrijedi*

$$n \mid 0 = a - a, \text{ pa je } a \equiv a \pmod{n},$$

(2) *simetričnost: za sve* $a, b \in \mathbb{Z}$ *imamo*

$$a \equiv b \pmod{n} \implies n \mid a - b \implies n \mid b - a \implies b \equiv a \pmod{n},$$

(3) *tranzitivnost: za sve* $a, b, c \in \mathbb{Z}$ *imamo*

$$a \equiv b \pmod{n} \;\&\; b \equiv c \pmod{n} \implies n \mid a - b \;\&\; n \mid b - c,$$

odakle slijedi

$$n \mid (a-b) + (b-c) = a - c \implies a \equiv c \pmod{n}.$$

Neka $n \mid a - b$*. Zapišimo*

$$a = n \cdot q + r \text{ i } b = n \cdot s + t, \text{ gdje su } r, t \in \{0, 1, \ldots, n-1\}.$$

Tada je

$$a - b = (n \cdot q + r) - (n \cdot s + t) = (n \cdot q - n \cdot s) + (r - t) = n \cdot (q - s) + (r - t)$$

odnosno

$$r - t = a - b - n \cdot (q - s).$$

Obzirom da $n \mid a - b$*, to* $n \mid r - t$*. Kako je* $r - t \in \{-(n-1), \ldots, 0, \ldots, n-1\}$*, to je* $r - t = 0$*, tj.* $r = t$*. Drugim riječima,* a *i* b *imaju isti ostatak pri dijeljenju sa* n*.*

Prema tome,

$$n \mid a - b \implies a \text{ i } b \text{ imaju isti ostatak pri dijeljenju sa } n.$$

Obratno, ako je $a = n \cdot q + r$ *i* $b = n \cdot s + r$*, tada je* $a - b = n \cdot (q - s)$ *djeljiv sa* n*, pa vrijedi i obrat, tj.*

$$a \text{ i } b \text{ imaju isti ostatak pri dijeljenju sa } n \implies n \mid a - b.$$

Dakle, dokazali smo

$$n \mid a - b \iff a \text{ i } b \text{ imaju isti ostatak pri dijeljenju sa } n.$$

Za zadani $n \in \mathbb{N}$, relacija "$\equiv \pmod{n}$" dijeli skup $\mathbb{Z}$ na n disjunktnih podskupova obzirom na ostatak pri dijeljenju sa n, koji može biti $0, 1, \ldots, n-1$.

Sada se vratimo na opći slučaj:

Teorem 3.19. *Neka je* $\sim$ *relacija ekvivalencije na skupu* X*. Za* $x \in X$ *neka je* $[x] = \{y \in X \mid y \sim x\}$*. Tada vrijede sljedeće tvrdnje:*

(i) $x \in [x]$ *tj.* $[x] \neq \emptyset$,
(ii) $x \sim y \implies [x] = [y]$,
(iii) $x \nsim y \implies [x] \cap [y] = \emptyset$.

Dokaz. (i) Kako je $\sim$ refleksivna, to je $x \sim x$, pa je $x \in [x]$.

(ii) Neka je $x \sim y$. Dokažimo da su skupovi $[x]$ i $[y]$ jednaki.

Neka je $z \in [x]$. Tada je $z \sim x$. Iz $z \sim x$ i $x \sim y$ zbog tranzitivnosti slijedi $z \sim y$ tj. $z \in [y]$. Dakle, $[x] \subseteq [y]$.

Obratno, neka je $z \in [y]$. Tada je $z \sim y$. Međutim, simetričnost iz $x \sim y$ povlači $y \sim x$, pa imamo $z \sim y$ i $y \sim x$. Konačno, tranzitivnost daje $z \sim x$ tj. $z \in [x]$. Dakle, $[y] \subseteq [x]$.

(iii) Dokaz provodimo obratom po kontrapoziciji, tj. dokazujemo:

$$[x] \cap [y] \neq \emptyset \implies x \sim y.$$

Kako je $[x] \cap [y] \neq \emptyset$, to postoji $z \in [x] \cap [y]$. Znači da je $z \sim x$ i $z \sim y$. Zbog simetričnosti imamo $x \sim z$, pa tranzitivnost iz $x \sim z$ i $z \sim y$ povlači $x \sim y$. $\square$

Definicija 3.20. *Neka je $\sim$ relacija ekvivalencije na skupu X. Za $x \in X$, skup $[x] = \{y \in X \,|\, y \sim x\}$ se naziva* ***klasa ekvivalencije*** *određena elementom x. Skup $X/_\sim = \{[x] \,|\, x \in X\}$ se naziva* ***kvocijentni skup*** *skupa X obzirom na relaciju $\sim$.*

Ako u primjeru 3.17 izaberemo jednog studenta smeđih očiju, tada on predstavlja svoju klasu tj. skup studenata smeđih očiju. Znači da taj student svojom bojom očiju određuje svoju klasu.

U primjeru 3.18, za zadani $n \in \mathbb{N}$, relacija "$\equiv \pmod{n}$", dijeli skup $\mathbb{Z}$ na n klasa ekvivalencije: $[0], [1], \ldots, [n-1]$, pa je kvocijentni skup skupa $\mathbb{Z}$ obzirom na relaciju "$\equiv \pmod{n}$" jednak $\{[0], [1], \ldots, [n-1]\}$. Broj 0 predstavlja brojeve djeljive sa n, broj 1 predstavlja brojeve koji pri dijeljenju sa n daju ostatak 1 itd.

Zadatak 3.21. *Neka je E zadana ravnina, a $X = \{p \,|\, p \subset E \text{ pravac}\}$. Na E definirajmo relaciju $\sim$ sa:*

$$p \sim q \Longleftrightarrow p || q.$$

Ova relacija se naziva "paralelnost pravca". Prisjetimo se,

$$p || q \Longleftrightarrow p = q \text{ ili } p \cap q = \emptyset.$$

Dokazati da je $\sim$ relacija ekvivalencije na X. Skup $X/_\sim$ se naziva smjer određen pravcem p.

Zadatak 3.22. *Neka je T skup svih trokuta u ravnini. Na skupu T definiramo relacije $\sim_1$, $\sim_2$ i $\sim_3$ sa:*

$$\Delta \sim_1 \Delta' \Longleftrightarrow \text{površina}(\Delta) = \text{površina}(\Delta'),$$

$$\Delta \sim_2 \Delta' \Longleftrightarrow \text{trokuti } \Delta \text{ i } \Delta' \text{su sukladni},$$

$$\Delta \sim_3 \Delta' \Longleftrightarrow \text{trokuti } \Delta \text{ i } \Delta' \text{su slični}.$$

Dokazati da su relacije $\sim_1$, $\sim_2$ i $\sim_3$ relacije ekvivalencije. Također dokazati da je $\sim_2 \subseteq \sim_1$ i $\sim_2 \subseteq \sim_3$ te da obratne inkluzije ne vrijede, ali da vrijedi $\sim_1 \cap \sim_3 = \sim_2$.

4. Funkcije

Definicija 4.1. *Neka su D i K neprazni skupovi.* ***Funkcija ili preslikavanje*** *$f : D \to K$ (čita se: "funkcija f sa D u K") je svaka relacija $f \subseteq D \times K$ sa svojstvom da za svaki $x \in D$ postoji jedinstven $y \in K$ takav da je $(x, y) \in f$.*

Dakle, funkcija je poseban slučaj relacije. Preciznije, relacija $f \subseteq D \times K$ koja ima svojstvo

$$(\forall x \in D)(\exists! y \in K)((x, y) \in f)$$

naziva se funkcija.

Uočimo da se svaki $x \in D$ pojavljuje kao prva koordinata jednog i samo jednog uređenog para $(x, y) \in f$. Znači da je druga koordinata jedinstveno određena prvom te zato o funkciji f sa D u K govorimo kao o "pravilu" koje svakom $x \in D$ pridružuje točno jedan $y \in K$. Pišemo

$$y = f(x),$$

a sâmo pridruživanje označavamo sa

$$x \mapsto y = f(x), \quad \text{ili} \quad x \mapsto f(x).$$

Prema tome,

$$y = f(x) \quad \Longleftrightarrow \quad (x, y) \in f.$$

Kratko, ali matematički manje precizno, o funkciji govorimo kao o uređenoj trojci (D, K, f) koja se sastoji od:

(1) nepraznog skupa D koji se naziva **domena** funkcije
(2) nepraznog skupa K koji se naziva **kodomena** funkcije
(3) pravila f koje svakom elementu skupa D pridružuje točno jedan element skupa K: $x \mapsto y = f(x)$.

Relaciju koja strogo definira pojam funkcije označavamo sa Γ_f umjesto sa f i nazivamo **graf funkcije:**

$$\Gamma_f = \{(x, f(x)) \mid x \in D\}.$$

Primjer 4.2. *Neka je D skup svih studenata u ovoj predavaonici, a K neka je skup svih prirodnih brojeva. Funkciju $f : D \to K$ definiramo sa*

$$f(\mathit{student}) = \mathit{starost}.$$

Radi jednostavnosti pretpostavimo da je

$$D = \{\mathit{Anita}, \mathit{Pero}, \mathit{Ivo}, \mathit{Ana}, \mathit{Maja}\}$$

te da vrijedi

$$\begin{aligned} f(Anita) &= 18, \\ f(Pero) &= 18, \\ f(Ivo) &= 19, \\ f(Ana) &= 18, \\ f(Maja) &= 20. \end{aligned}$$

Tada je graf funkcije dan sa

$$\Gamma_f = \{(Anita, 18), (Pero, 18), (Ivo, 19), (Ana, 18), (Maja, 20)\}.$$

Definicija 4.3. *Kažemo da su preslikavanja $f : D \to K$ i $g : D' \to K'$* ***jednaka*** *ako vrijedi:*

- *domene su jednake: $D = D'$,*
- *kodomene su jednake: $K = K'$,*
- *pravila su jednaka: $f(x) = g(x)$ za svaki $x \in D = D'$.*

Primjer 4.4. *Preslikavanja*

$$\begin{cases} f : \mathbb{R} \to \mathbb{R}, & f(x) = x \\ g : \mathbb{R} \to \mathbb{R}, & g(x) = x^2 \end{cases}$$

imaju iste domene i kodomene, ali različita pravila jer je $f(2) = 2 \neq 4 = g(2)$.

Primjer 4.5. *Neka je $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Znamo da je $x^2 \geq 0$ za svaki $x \in \mathbb{R}$. Zato je preslikavanje*

$$g : \mathbb{R} \to [0, +\infty >, \quad g(x) = x^2$$

dobro definirano. Preslikavanja f i g imaju iste domene i pravila, ali je kodomena funkcije f jednaka $\mathbb{R}$, a kodomena funkcije g je jednaka $[0, +\infty >$. Dakle, ove funkcije nisu jednake.

Primjer 4.6. *Neka su dana preslikavanja:*

$$\begin{cases} f : \mathbb{N} \to \mathbb{R}, & f(x) = x^2 \\ g : \mathbb{R} \to \mathbb{R}, & g(x) = x^2. \end{cases}$$

U ovom slučaju su kodomene i pravila ista, ali su domene različite. Dakle, ove funkcije nisu jednake.

Iako su preslikavanja iz primjera 4.6 različita, ona ipak nisu posve nevezana. Uočimo da je domena funkcije f podskup domene funkcije g dok su pravila i kodomene iste! U tom slučaju kažemo da je f restrikcija funkcije g na skup $\mathbb{N}$. Općenito imamo ovakvu definiciju.

Definicija 4.7. *Neka su D_1, D_2 i K neprazni skupovi. Pretpostavimo da vrijedi $D_1 \subseteq D_2$. Kažemo da je preslikavanje $f_1 : D_1 \to K$* ***restrikcija preslikavanja*** *$f_2 : D_2 \to K$ na skup D_1 ako vrijedi*

$$f_1(x) = f_2(x), \quad \forall x \in D_1.$$

Ponekad se govori da je f_2 ***proširenje (ili ekstenzija) preslikavanja*** *f_1 na skup D_2.*

Primjer 4.8. *Neka je $x \in \mathbb{R}$. Označimo sa $\lfloor x \rfloor$ najveći cijeli broj koji je manji ili jednak x. Primjerice, $\lfloor 4.567 \rfloor = 4$, jer je $4 \leq 4.567 < 5$, $\lfloor -4.567 \rfloor = -5$ jer je $-5 \leq -4.567 < 4$, dok je $\lfloor x \rfloor = x$ za svaki cijeli broj x: $\lfloor 0 \rfloor = 0, \lfloor 1 \rfloor = 1, \lfloor -1 \rfloor = -1, \ldots$*

Dakle, $\lfloor \quad \rfloor$ je funkcija sa $\mathbb{R}$ u $\mathbb{R}$ čija je restrikcija na $\mathbb{Z}$ dana sa $x \mapsto x$.

Ponekad se u literaturi koristi i oznaka $[x]$ za $\lfloor x \rfloor$.

Zadatak 4.9. *Neka je $x \in \mathbb{R}$. Označimo sa $\lceil x \rceil$ najmanji cijeli broj koji je veći ili jednak x. Koja je veza između $\lfloor x \rfloor$ i $\lceil x \rceil$? Razmotrite funkciju $\lceil \quad \rceil$ u svjetlu primjera 4.8.*

Definicija 4.10. *Neka je U (univerzalan) skup i $A \subseteq U$ njegov podskup.* ***Karakteristična funkcija*** *skupa A u skupu U je funkcija $\chi_A : U \to \{0, 1\}$ zadana sa*

$$\chi_A(x) = \begin{cases} 1; & x \in A, \\ 0; & x \in U \setminus A. \end{cases}$$

Zadatak 4.11. *Odredite $\chi_\emptyset$ i χ_U.*

Zadatak 4.12. *Neka je U (univerzalan) skup i $A, B \subseteq U$ njegovi podskupovi. Dokažite sljedeće tvrdnje:*

(i) *$A = B$ ako i samo ako su funkcije χ_A i χ_B jednake,*
(ii) *$\chi_A(x) + \chi_{A^c}(x) = 1$ za svaki $x \in U$,*
(iii) *$\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ za svaki $x \in U$,*
(iv) *$\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x)$ za svaki $x \in U$,*
(v) *$\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x)$ za svaki $x \in U$ ako i samo ako su A i B disjunktni (tj. $A \cap B = \emptyset$).*

Definicija 4.13. *Neka su dana preslikavanja $f : D \to K$ i $g : K \to L$ takva da je kodomena preslikavanja f jednaka domeni preslikavanja g. Kompozicija preslikavanja f i g je preslikavanje h čija je domena jednaka domeni preslikavanja f, a kodomena je kodomena preslikavanja g (dakle, $h : D \to L$) i čije je pravilo dano sa*

$$h(x) = g(f(x)), \quad \forall x \in D.$$

Takvo preslikavanje h se označava sa $g \circ f$.

U praksi je uvjet da je kodomena preslikavanja f jednaka domeni preslikavanja g previše restriktivan. Zapravo je za definiciju kompozicije dovoljno da za svaki $x \in D$ vrijednost $f(x)$ pripada domeni preslikavanja g. Zato dajemo sljedeću definiciju:

Definicija 4.14. *Neka je dano preslikavanje $f : D \to K$.* ***Slika preslikavanja*** *f, u oznaci $f(D)$, je skup svih vrijednosti funkcije f tj.*

$$f(D) = \{f(x) \mid x \in D\}.$$

Odmah vidimo da je slika funkcije f sadržana u kodomeni K te funkcije. Nadalje, vidimo da se, za dane funkcije $f : D \to K$ i $g : M \to L$, funkcija $h : D \to L$ može zadati pravilom

$$h(x) = g(f(x)), \quad \forall x \in D$$

ukoliko

$$(\forall x)(x \in D \implies f(x) \in M)$$

tj.

$$f(D) \subseteq M.$$

Opet takvu funkciju označavamo sa $h = g \circ f$ i nazivamo kompozicijom funkcija f i g.

U sljedećim primjerima ćemo raditi s kompozicijom funkcija danom definicijom 4.13, ali čitatelj će lako utvrditi da sva svojstva vrijede i za ovu općenitiju definiciju.

Primjer 4.15. *Neka su $f : \mathbb{R} \to \mathbb{R}$ i $g : \mathbb{R} \to \mathbb{R}$ zadane sa $f(x) = 2x + 1$ i $g(x) = x^2$ za svaki $x \in \mathbb{R}$. Tada je kompozicija $g \circ f : \mathbb{R} \to \mathbb{R}$ dana sa*

$$(g \circ f)(x) = g(f(x)) = (2x + 1)^2 = 4x^2 + 4x + 1.$$

Nadalje, nalazimo da je i kompozicija $f \circ g : \mathbb{R} \to \mathbb{R}$ također definirana te da vrijedi

$$(f \circ g)(x) = f(g(x)) = 2x^2 + 1.$$

Iako su im domene i kodomene jednake, preslikavanja $f \circ g$ i $g \circ f$ nisu jednaka jer im pravilo nije isto jer je, primjerice,

$$(f \circ g)(1) = 3, \quad (g \circ f)(1) = 9.$$

Ovaj primjer pokazuje da kompozicija preslikavanja općenito nije komutativna tj. nije $f \circ g = g \circ f$. Međutim, u sljedećoj propoziciji dokazujemo da je kompozicija preslikavanja asocijativna (ukoliko su sve kompozicije definirane).

Propozicija 4.16. *Neka su dana preslikavanja $f : D \to K$, $g : K \to L$ i $h : L \to M$. Tada su sve kompozicije $g \circ f : D \to L$, $h \circ (g \circ f) : D \to M$, $h \circ g : K \to M$ i $(h \circ g) \circ f : D \to M$ dobro definirane. Nadalje, funkcije $h \circ (g \circ f) : D \to M$ i $(h \circ g) \circ f : D \to M$ su jednake.*

Dokaz. Da su sve navedene kompozicije dobro definirane slijedi odmah iz definicije 4.13. Kako preslikavanja $h \circ (g \circ f) : D \to M$ i $(h \circ g) \circ f : D \to M$ imaju iste domene i kodomene, za njihovu jednakost treba utvrditi da im je pravilo isto: za svaki $x \in D$ imamo

$$\begin{aligned}((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x))) \\ &= h((g \circ f)(x)) = (h \circ (g \circ f))(x).\end{aligned}$$

□

Definicija 4.17. *Neka je D neprazan skup.* ***Identiteta*** *na D, u oznaci 1_D, je preslikavanje $1_D : D \to D$ zadano sa $1_D(x) = x$ za svaki $x \in D$.*

Identiteta je, dakle, preslikavanje koje svakom elementu domene pridruži njega samog, pa je pravilo preslikavanja uvijek isto (neovisno o domeni). Međutim, preslikavanja 1_D i 1_K su jednaka ako i samo ako je $D = K$.

Propozicija 4.18. *Neka su D i K i neprazni skupovi i neka je $f : D \to K$ preslikavanje. Tada su kompozicije $f \circ 1_D : D \to K$ i $1_K \circ f : D \to K$ dobro definirane i vrijedi da su oba preslikavanja jednaka preslikavanju $f : D \to K$.*

Dokaz. Da su sve navedene kompozicije dobro definirane slijedi odmah iz definicije 4.13. Nadalje, za svaki $x \in D$ je

$$(f \circ 1_D)(x) = f(1_D(x)) = f(x),$$

$$(1_K \circ f)(x) = 1_D(f(x)) = f(x).$$

Dakle, propozicija slijedi iz definicije jednakosti dva preslikavanja. □

U sljedećoj definiciji proširujemo definiciju 4.14.

Definicija 4.19. *Neka su D i K neprazni skupovi i neka je $f : D \to K$ preslikavanje.* ***Slika skupa*** *$X \subseteq D$ je skup svih vrijednosti koje f poprima na skupu X, tj.*

$$f(X) = \{f(x) \mid x \in X\}.$$

Inverzna slika (ili praslika) skupa *$Y \subseteq K$ je skup svih vrijednosti u domeni koji f preslikava u Y, tj.*

$$f^{-1}(Y) = \{x \in D \mid f(x) \in Y\}.$$

Oznaka f^{-1} koristi se i za oznaku inverzne funkcije kojom ćemo se baviti u 7. poglavlju. Zato moramo paziti u kojem kontekstu se ta oznaka koristi. U okviru prethodne definicije oznaka $f^{-1}(Y)$ nije u vezi s inverznom funkcijom f^{-1}.

Uočimo da je za $X = D$ skup

$$f(D)$$

slika funkcije f definirana u definiciji 4.14.

Nadalje, za $X = \emptyset$ imamo

$$f(\emptyset) = \emptyset,$$

jer je po definiciji $f(\emptyset) = \{f(x) \mid x \in \emptyset\}$, a taj skup je prazan jer uvjet $x \in \emptyset$ nije ispunjen niti za jedan $x \in D$.

Isto tako, za $Y = K$ nalazimo da je

$$f^{-1}(K) = D,$$

jer je po definiciji funkcije

$$f^{-1}(K) = \{x \in D \mid f(x) \in K\} = D.$$

Nadalje, za $Y = \emptyset$ imamo

$$f^{-1}(\emptyset) = \emptyset,$$

jer je po definiciji

$$f^{-1}(\emptyset) = \{x \in D \mid f(x) \in \emptyset\} = \emptyset.$$

Primjer 4.20. *Neka je* $f : \{1,2,3,4\} \to \{0,1,2\}$ *preslikavanje zadano sa* $f(1) = f(2) = 0$, $f(3) = f(4) = 1$. *Neka je* $A = \{1,2,3\}$ *i* $B = \{3,4\}$, *te* $E = \{0,1\}$, $F = \{2\}$ *i* $G = \{0\}$. *Tada imamo*

$$D = \{1,2,3,4\}, \quad K = \{0,1,2\}$$

i vrijedi

$$\begin{aligned}
&f(A) = \{f(x) \mid x \in A\} = \{f(1), f(2), f(3)\} = \{0,1\},\\
&f(B) = \{f(x) \mid x \in B\} = \{f(3), f(4)\} = \{1,1\} = \{1\},\\
&f^{-1}(E) = \{x \in D \mid f(x) \in E\} = \{x \in D \mid f(x) = 0 \text{ ili } f(x) = 1\} = \{1,2,3,4\},\\
&f^{-1}(F) = \{x \in D \mid f(x) \in F\} = \{x \in D \mid f(x) = 2\} = \emptyset,\\
&f^{-1}(G) = \{x \in D \mid f(x) \in G\} = \{x \in D \mid f(x) = 0\} = \{1,2\}.
\end{aligned}$$

Zadatak 4.21. *Neka je* $f : \{1,2,3,4,5\} \to \{0,1,2,3\}$ *preslikavanje zadano sa* $f(1) = f(2) = 0$, $f(3) = f(4) = 1$ *i* $f(5) = 2$. *Odredite slike skupova* $\{1,2\}$, $\{1,2,3,5\}$ *i* $\{1,2,4,5\}$. *Odredite inverzne slike skupova* $\{1,2\}, \{0,1,2\}, \{0,3\}$ *i* $\{3\}$.

Sljedeći teorem daje daljnja svojstva slike i inverzne slike. Njih ćemo često sretati tijekom studija.

Teorem 4.22. *Neka su D i K neprazni skupovi i neka je $f : D \to K$ preslikavanje. Neka su $A, B \subseteq D$ i $E, F \subseteq K$ bilo koji skupovi. Tada vrijedi:*

$$\begin{aligned}
&f(A \cup B) = f(A) \cup f(B),\\
&f(A \cap B) \subseteq f(A) \cap f(B),\\
&f(A) \setminus f(B) \subseteq f(A \setminus B),\\
&f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F),\\
&f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F),\\
&f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F),\\
&A \subseteq f^{-1}(f(A)),\\
&f(f^{-1}(E)) = E \cap f(D).
\end{aligned}$$

Dokaz. Dokažimo najprije $f(A \cup B) = f(A) \cup f(B)$. Ovdje se radi o jednakosti skupova

$$f(A \cup B) \quad \text{i} \quad f(A) \cup f(B).$$

Jednakost ovih skupova dokazujemo tako da dokažemo sljedeće dvije tvrdnje

$$f(A \cup B) \subseteq f(A) \cup f(B), \tag{4.23}$$

$$f(A) \cup f(B) \subseteq f(A \cup B). \tag{4.24}$$

Imamo redom:

$$\begin{aligned}
y \in f(A \cup B) &\iff (\exists x \in A \cup B)\ (y = f(x))\\
&\iff (\exists x \in A \text{ ili } \exists x \in B)\ (y = f(x))\\
&\iff (\exists x \in A)\ (y = f(x)) \text{ ili } (\exists x \in B)\ (y = f(x))\\
&\iff y \in f(A) \text{ ili } y \in f(B)\\
&\iff y \in f(A) \cup f(B).
\end{aligned}$$

Implikacije " $\Longrightarrow$ " dokazuju (4.23), dok implikacije "$\Longleftarrow$" dokazuju (4.24).

Dokažimo sada $f(A \cap B) \subseteq f(A) \cap f(B)$. Imamo redom:

$$\begin{aligned}
y \in f(A \cap B) &\Longrightarrow (\exists x \in A \cap B)\ (y = f(x))\\
&\Longrightarrow (\exists x)(x \in A \text{ i } x \in B)\ (y = f(x))\\
&\Longrightarrow (\exists x \in A)\ (y = f(x)) \text{ i } (\exists x \in B)\ (y = f(x))\\
&\Longrightarrow y \in f(A) \text{ i } y \in f(B)\\
&\Longrightarrow y \in f(A) \cap f(B).
\end{aligned}$$

Dokažimo sada $f(A) \setminus f(B) \subseteq f(A \setminus B)$. Ako je $y \in f(A) \setminus f(B)$, tada imamo $y \in f(A)$ i $y \notin f(B)$. Sada po definiciji slike skupa zaključujemo da postoji $x \in A$ takav da je $y = f(x)$. Ako je $x \in B$, tada je $f(x) \in f(B)$ tj. $y \in f(B)$. Obratom po kontrapoziciji zaključujemo da $y \notin f(B)$ povlači $x \notin B$. Dakle, imamo $y = f(x)$, gdje je $x \in A$ i $x \notin B$. To znači $y = f(x)$ za neki $x \in A \setminus B$, tj. $y \in f(A \setminus B)$.

Dokažimo $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$. Imamo redom:

$$\begin{aligned} x \in f^{-1}(E \cup F) &\iff f(x) \in E \cup F \\ &\iff f(x) \in E \text{ ili } f(x) \in F \\ &\iff x \in f^{-1}(E) \text{ ili } x \in f^{-1}(F) \\ &\iff x \in f^{-1}(E) \cup f^{-1}(F). \end{aligned}$$

Sličan argument dokazuje i tvrdnje

$$f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F),$$

$$f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F).$$

Tvrdnja $A \subseteq f^{-1}(f(A))$ se dokazuje ovako:

$$x \in A \implies f(x) \in f(A) \implies x \in f^{-1}(f(A)).$$

Konačno, tvrdnja $f(f^{-1}(E)) = E \cap f(D)$ se dokazuje na sljedeći način:

$$\begin{aligned} y \in f(f^{-1}(E)) &\iff (\exists x \in f^{-1}(E))\ (y = f(x)) \\ &\iff y \in E \text{ i } y \in f(D) \iff y \in E \cap f(D). \end{aligned}$$

(Netko može pomisliti da u predzadnjoj ekvivalenciji imamo samo $y \in E$, ali kako je $y = f(x)$ to mora biti i $y \in f(D)$!) $\square$

Primjerom pokazujemo da jednakosti u $f(A \cap B) \subseteq f(A) \cap f(B)$ i $f(A) \setminus f(B) \subseteq f(A \setminus B)$ ne vrijede općenito.

Primjer 4.25. *Neka je $f : \{1, 2, 3\} \to \{0, 1\}$ preslikavanje zadano sa $f(1) = f(2) = f(3) = 0$. Neka je $A = \{1, 2\}$ i $B = \{3\}$. Tada je*

$$f(A) = \{f(x) \mid x \in A\} = \{f(1), f(2)\} = \{0, 0\} = \{0\},$$

$$f(B) = \{f(x) \mid x \in B\} = \{f(3)\} = \{0\}.$$

Dakle, imamo

$$f(A) \cap f(B) = \{0\} \cap \{0\} = \{0\}.$$

S druge strane, $A \cap B = \emptyset$ i stoga

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

Dakle,

$$f(A \cap B) \subsetneq f(A) \cap f(B).$$

Također, imamo $A \setminus B = A = \{1, 2\}$, pa je

$$f(A \setminus B) = f(A) = \{0\}.$$

Nadalje,

$$f(A) \setminus f(B) = \{0\} \setminus \{0\} = \emptyset.$$

Dakle,

$$f(A) \setminus f(B) \subsetneq f(A \setminus B).$$

Teorem 4.26. *Neka su dana preslikavanja* $f : D \to K$ *i* $g : K \to L$*. Tada za svaki podskup* $E \subseteq L$ *vrijedi slijedeća jednakost inverznih slika*

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

Dokaz. Imamo redom:

$$\begin{aligned} x \in (g \circ f)^{-1}(E) &\iff (g \circ f)(x) \in E \\ \iff g(f(x)) \in E &\iff f(x) \in g^{-1}(E) \iff x \in f^{-1}(g^{-1}(E)). \end{aligned}$$

$\square$

5. Neke elementarne funkcije; jednadžbe i nejednadžbe (prvi dio)

U 4. poglavlju smo se bavili općenitom definicijom funkcija. Ovdje ćemo se podsjetiti nekih elementarnih funkcija koje smo učili u srednjoj školi. Kasnije, u 10. poglavlju, sustavno ćemo uvesti funkcije poput "drugog korijena" i općenito "n–tog korijena". Nadalje, potpun prikaz teorije polinoma sadržaj je 12., 13. i 14. poglavlja, dok je sustavan prikaz teorije racionalnih funkcija sadržaj 15. poglavlja.

Definicija 5.1. *Neka je $f : D \to K$ funkcija. Kažemo da je f funkcija realne varijable ako je domena D podskup skupa realnih brojeva $\mathbb{R}$. Kažemo da je f realna funkcija ako je kodomena K podskup skupa realnih brojeva. Na kraju, f je realna funkcija realne varijable ako je i njena domena podskup skupa realnih brojeva i njena kodomena podskup skupa realnih brojeva.*

U ovom poglavlju su sve funkcije s kojima radimo realne funkcije realne varijable, pa to nećemo uvijek iznova naglašavati.

Dakle, domene i kodomene funkcija koje proučavamo su podskupovi skupa realnih brojeva $\mathbb{R}$. Realne brojeve ćemo detaljno proučavati u 10. poglavlju. Za sada navedimo neke istaknute podskupove skupa $\mathbb{R}$.

Neka su $a, b \in \mathbb{R}$, $a \leq b$.

- $[a, b] \stackrel{def}{=} \{x \in \mathbb{R} \,|\, a \leq x \leq b\}$,
- $\langle a, b] \stackrel{def}{=} \{x \in \mathbb{R} \,|\, a < x \leq b\}$,
- $[a, b\rangle \stackrel{def}{=} \{x \in \mathbb{R} \,|\, a \leq x < b\}$,
- $\langle a, b\rangle \stackrel{def}{=} \{x \in \mathbb{R} \,|\, a < x < b\}$,
- $\langle a, +\infty\rangle \stackrel{def}{=} \{x \in \mathbb{R} \,|\, x > a\}$,
- $\langle -\infty, a\rangle \stackrel{def}{=} \{x \in \mathbb{R} \,|\, x < a\}$,
- $[a, +\infty\rangle \stackrel{def}{=} \{x \in \mathbb{R} \,|\, x \geq a\}$,
- $\langle -\infty, a] \stackrel{def}{=} \{x \in \mathbb{R} \,|\, x \leq a\}$.

Skup $[a, b]$ zovemo **zatvoreni interval ili segment**, skup $\langle a, b\rangle$ se naziva **otvoreni interval**, a skupovi $\langle a, b]$ i $[a, b\rangle$ **poluotvoreni intervali**.

Definicija 5.2. *Kažemo da f **raste** na skupu $S \subseteq D$ ako vrijedi*

$$\forall x_1, x_2 \in S,\ x_1 < x_2 \implies f(x_1) \leq f(x_2).$$

*Isto tako, kažemo da f **strogo raste** na skupu $S \subseteq D$ ako vrijedi*

$$\forall x_1, x_2 \in S,\ x_1 < x_2 \implies f(x_1) < f(x_2).$$

*Kažemo da f **pada** na skupu $S \subseteq D$ ako vrijedi*

$$\forall x_1, x_2 \in S,\ x_1 < x_2 \implies f(x_1) \geq f(x_2).$$

*Isto tako, kažemo da f **strogo pada** na skupu $S \subseteq D$ ako vrijedi*

$$\forall x_1, x_2 \in S,\ x_1 < x_2 \implies f(x_1) > f(x_2).$$

Nadalje, ako funkcija raste ili pada, kažemo da je ***monotona****, a ako strogo raste ili strogo pada, kažemo da je* ***strogo monotona****.*

Funkcija f ima ***minimum*** *na skupu S u točki $c \in S$ i on iznosi $f(c)$ ako vrijedi*

$$f(x) \geq f(c), \quad \forall x \in S.$$

Funkcija f ima ***strogi minimum*** *na skupu S u točki $c \in S$ i on oznosi $f(c)$ ako vrijedi*

$$f(x) > f(c), \quad \forall x \in S, \ x \neq c.$$

Funkcija f ima ***maksimum*** *na skupu S u točki $c \in S$ i on iznosi $f(c)$ ako vrijedi*

$$f(x) \leq f(c), \quad \forall x \in S.$$

Funkcija f ima ***strogi maksimum*** *na skupu S u točki $c \in S$ i on iznosi $f(c)$ ako vrijedi*

$$f(x) < f(c), \quad \forall x \in S, \ x \neq c.$$

Kažemo da funkcija f ima ***ekstrem*** *na skupu S u točki $c \in S$ ako u c ima minimum ili maksimum.*

Ukoliko je u bilo kojoj od gornjih definicija $S = D$, onda govorimo o rastu, padu, strogom rastu, strogom padu, minimumu, maksimumu, strogom minimumu te strogom maksimumu funkcije f.

U kolegijima iz diferencijalnog računa će se uvedeni pojmovi sustavno proučavati, a mi ćemo o njima govoriti samo za neke klase elementarnih funkcija.

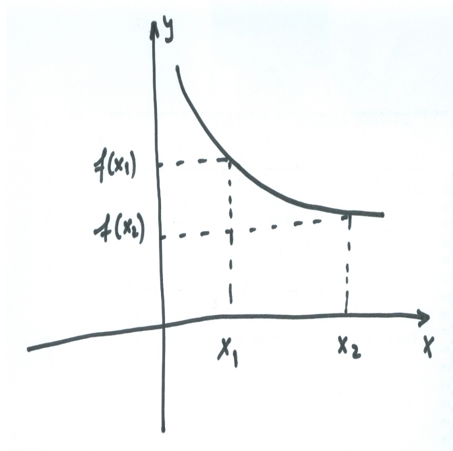
Zadatak 5.3. *Dokažite da funkcija f (strogo) pada na nekom skupu S ako i samo ako $-f$ (strogo) raste S, te da minimum funkcije f na S postaje maksimum funkcije $-f$ na S i obratno.*

Graf realne funkcije realne varijable prikazujemo u Kartezijevom koordinatnom sustavu $\mathbb{R}^2$ u ravnini. Po definiciji, graf takve funkcije je skup

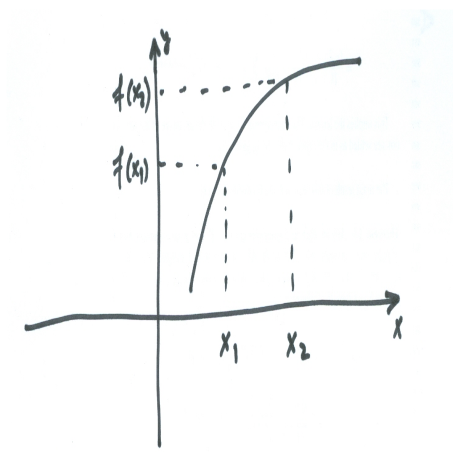
$$\Gamma_f = \{(x, y) \,|\, x \in D, \quad y = f(x)\}.$$

Graf nam omogućuje predočiti mnoge informacije vezane za funkcije.

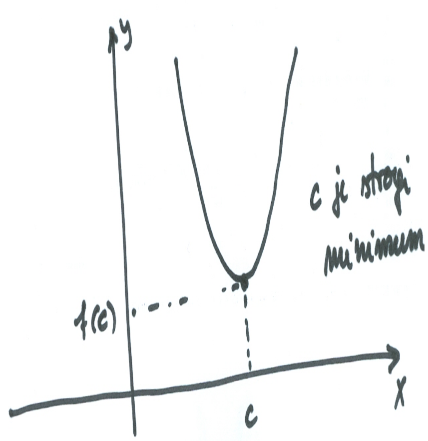
Slijedi ilustracija strogog pada funkcije.

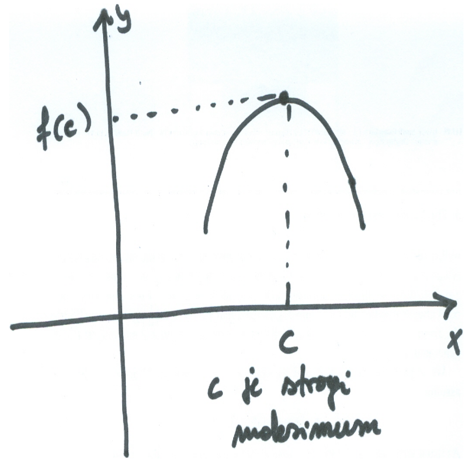


Evo i ilustracije strogog rasta funkcije.



Dalje slijede ilustracije pojmova strogog minimuma i strogog maksimuma funkcije.





Sljedeća definicija je poseban slučaj općih definicija iz 4. poglavlja.

Definicija 5.4. *Za svaki $S \subseteq D$,* ***slika skupa*** *S pri preslikavanju f je skup*

$$f(S) = \{f(x) \,|\, x \in S\}.$$

Slika funkcije f je skup $f(D)$. Za svaki $T \subseteq K$, ***inverzna slika (ili praslika) skupa*** *T pri preslikavanju f je skup*

$$f^{-1}(T) = \{x \in D \,|\, f(x) \in T\}.$$

Očigledno je $f^{-1}(K) = D$.

Definicija 5.5. *Nultočka funkcije f je realan broj $x \in D$ takav da je $f(x) = 0$.*

Definicija 5.6. *Kažemo da je f* ***injekcija (injektivno preslikavanje)*** *ako*

$$(\forall x_1, x_2 \in D)(x_1 \neq x_2 \implies f(x_1) \neq f(x_2)).$$

Za f kažemo da je ***surjekcija (surjektivno preslikavanje)*** *ako*

$$(\forall y \in K)(\exists x \in D)(y = f(x)).$$

Za f kažemo da je ***bijekcija (bijektivno preslikavanje)*** *ako je i injekcija i surjekcija.*

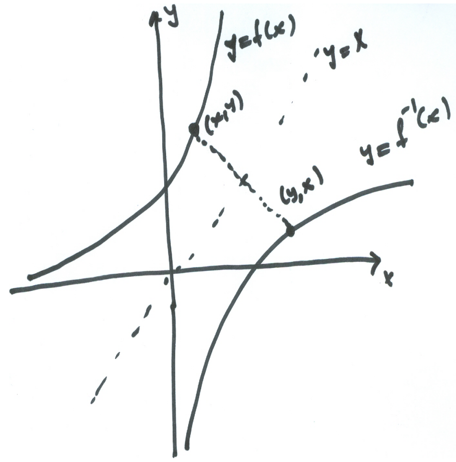
Ukoliko je funkcija $f : D \to K$ bijekcija, onda čitamo "f je sa D **na** K bijekcija". Nadalje, iz gornje definicije je očito da je f bijekcija ako i samo ako za svaki $y \in K$ postoji jedan i samo jedan $x \in D$ takav da je

$$y = f(x).$$

Stoga možemo definirati novu funkciju $g : K \to D$ koristeći

$$\forall y \in K, \quad g(y) = x \iff y = f(x).$$

Funkcija g naziva se inverzna funkcija funkcije f i označava sa f^{-1}. Na ovom mjestu napominjemo da čitatelj ne smije pomiješati oznaku za inverznu funkciju s oznakom za prasliku skupa (vidite definiciju 5.4). Funkcija f^{-1} također je bijekcija. Napomenimo da se graf inverzne funkcije dobije zrcaljenjem oko pravca $y = x$ grafa funkcije f.



Propozicija 5.7. *Neka je $f : D \to K$ bijekcija. Tada vrijede sljedeće tvrdnje:*

(i) *ako je f strogo rastuća, onda je f^{-1} također strogo rastuća;*
(ii) *ako je f strogo padajuća, onda je f^{-1} također strogo padajuća.*

Dokaz. Dokažimo (i) jer se (ii) dokazuje slično. Sjetimo se da je

$$x = f^{-1}(y) \iff y = f(x).$$

Obzirom da želimo dokazati da f^{-1} strogo raste, moramo dokazati

$$\forall y_1, y_2 \in K, \quad y_1 < y_2 \implies x_1 < x_2,$$

gdje je $y_1 = f(x_1)$ i $y_2 = f(x_2)$. Ako nije tako, tada postoje $y_1, y_2 \in K$, $y_1 < y_2$, takvi da je

$$x_2 \leq x_1.$$

No, tada je

$$y_2 = f(x_2) \leq f(x_1) = y_1,$$

jer f raste. Dobivamo

$$y_2 \leq y_1,$$

što je u kontradikciji s pretpostavkom $y_1 < y_2$. □

U ovoj točki ćemo proučavati konkretne primjere funkcija iz definicije 5.6. U 7. poglavlju ćemo prikazati opću teoriju ovih funkcija.

Sada prelazimo na pregled nekih elementarnih funkcija.

1. **Konstantna funkcija.** Neka je $b \in \mathbb{R}$ zadan. Tada definiramo konstantnu funkciju $f : \mathbb{R} \to \mathbb{R}$ formulom:

$$f(x) = b, \quad \forall x \in \mathbb{R}.$$

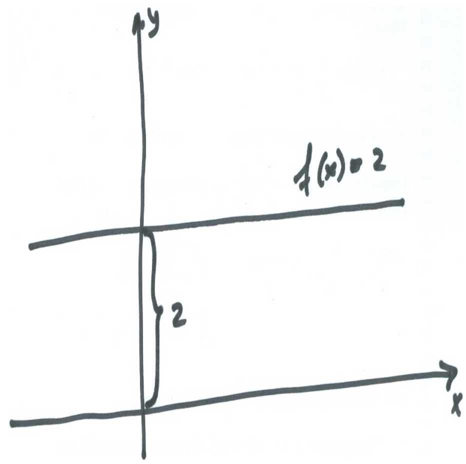
Ova funkcija je rastuća jer imamo

$$\forall x_1, x_2 \in \mathbb{R}, x_1 < x_2 \implies f(x_1) = f(x_2) = b \implies f(x_1) \leq f(x_2).$$

Ona je također padajuća jer vrijedi

$$\forall x_1, x_2 \in \mathbb{R}, x_1 < x_2 \implies f(x_1) = f(x_2) = b \implies f(x_1) \geq f(x_2).$$

Konstantna funkcija nije strogo rastuća niti strogo padajuća. Slično se vidi da konstantna funkcija ima minimum i maksimum u svakom $c \in \mathbb{R}$, ali nema strogog minimuma niti strogog maksimuma. Graf konstantne funkcije za $b = 2$ prikazan je na sljedećoj slici.



Odredimo slike, praslike i nultočke konstantne funkcije. Neka je $S \subseteq \mathbb{R}$. Po definiciji računamo

$$f(S) = \{f(x) \mid x \in S\} = \{b\}.$$

Posebno, slika funkcije je

$$f(\mathbb{R}) = \{b\}.$$

Za svaki $T \subseteq \mathbb{R}$, inverzna slika (ili praslika) skupa T pri preslikavanju f je skup

$$\begin{aligned} f^{-1}(T) &= \{x \in \mathbb{R} \mid f(x) \in T\} \quad (\text{jer je uvijek } f(x) = b) \\ &= \{x \in \mathbb{R} \mid b \in T\} = \begin{cases} \emptyset & \text{ako } \ b \notin T \\ \mathbb{R} & \text{ako } \ b \in T. \end{cases} \end{aligned}$$

Konstantna funkcija nije injekcija jer sve elemente domene $D = \mathbb{R}$ prevodi u b. Isto tako nije surjekcija jer niti jedan element kodomene $K = \mathbb{R}$, osim b, nije u slici konstantne funkcije. Konstantna funkcija stoga nije ni bijekcija.

2. **Linearna funkcija.** Neka su $a, b \in \mathbb{R}$, $a \neq 0$. Linearna funkcija je funkcija $f : \mathbb{R} \to \mathbb{R}$ zadana formulom

$$f(x) = ax + b, \quad \forall x \in \mathbb{R}.$$

Ovdje smo isključili slučaj $a = 0$, jer se tada funkcija svodi na konstantnu funkciju iz prethodne točke. Ponekad se u literaturi ovakva funkcija naziva afina funkcija, a poseban slučaj $b = 0$ naziva se linearna funkcija. Mi ćemo je radi jednostavnosti zvati linearna funkcija u oba slučaja. Dokazujemo sljedeću propoziciju:

Propozicija 5.8. *Neka je $f : \mathbb{R} \to \mathbb{R}$ zadana sa $f(x) = ax + b$, $a \neq 0$. Tada vrijede sljedeće tvrdnje:*

(i) *funkcija f strogo raste ako je $a > 0$;*

(ii) *funkcija f strogo pada ako je $a < 0$;*
(iii) *funkcija f nema niti minimuma niti maksimuma.*

Dokaz. Dokažimo (i). Treba dokazati da, uz pretpostavku $a > 0$, funkcija f strogo raste tj. treba dokazati

$$\forall x_1, x_2 \in \mathbb{R}, x_1 < x_2 \implies f(x_1) < f(x_2).$$

Uzmimo bilo koje $x_1, x_2 \in \mathbb{R}$ takve da je $x_1 < x_2$. Tada imamo

$$f(x_2) - f(x_1) = (ax_2 + b) - (ax_1 + b) = a(x_2 - x_1) > 0.$$

Naime, $x_2 > x_1$ povlači $x_2 - x_1 > 0$ i konačno imamo

$$a > 0 \ \text{ i } \ x_2 - x_1 > 0 \implies a(x_2 - x_1) > 0.$$

Ovim smo (i) dokazali. Dokaz tvrdnje (ii) je analogan. Uz pretpostavku $a < 0$, moramo dokazati

$$\forall x_1, x_2 \in \mathbb{R}, x_1 < x_2 \implies f(x_1) > f(x_2).$$

Uzmimo bilo koje $x_1, x_2 \in \mathbb{R}$ takve da je $x_1 < x_2$. Tada imamo

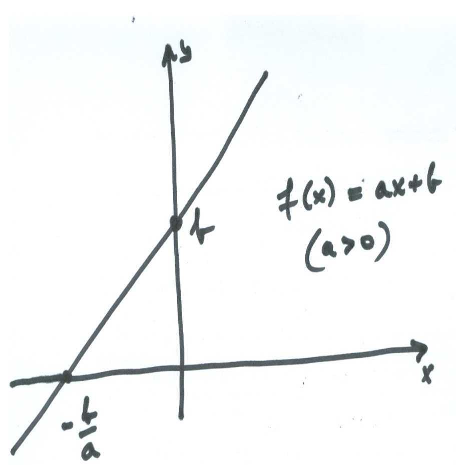
$$f(x_2) - f(x_1) = (ax_2 + b) - (ax_1 + b) = a(x_2 - x_1) < 0,$$

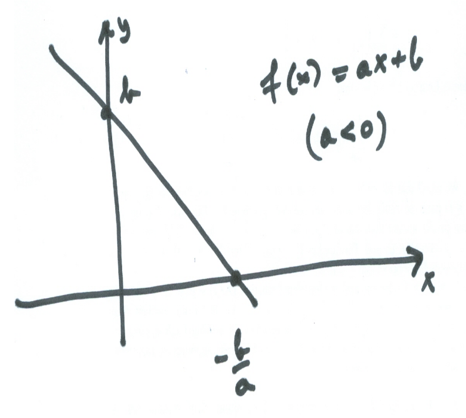
obzirom da je $x_2 > x_1$ te je stoga $x_2 - x_1 > 0$ i konačno

$$a < 0 \ \text{ i } \ x_2 - x_1 > 0 \implies a(x_2 - x_1) < 0.$$

Ovim smo (ii) dokazali. Zadnja tvrdnja propozicije kaže da f nema niti minimuma niti maksimuma. Ta tvrdnja je posljedica činjenice da f strogo raste ili strogo pada i ostavljamo je čitatelju za vježbu. □

Graf linearne funkcije je pravac $y = ax + b$ čiji je koeficijent smjera jednak a, a odsječak na osi y jednak b. Sljedeće slike pokazuju dvije mogućnosti: $a > 0$ i $a < 0$.





Jedina nultočka linearne funkcije je broj $-\frac{b}{a}$ jer je

$$f(x)=0 \iff ax+b=0 \iff x=-\frac{b}{a}.$$

Propozicija 5.9. *Neka su $a, b \in \mathbb{R}$, $a \neq 0$. Funkcija $f : \mathbb{R} \to \mathbb{R}$ zadana sa $f(x) = ax + b$ je bijekcija. Njena inverzna funkcija dana je formulom*

$$f^{-1}(x)=\frac{1}{a}x-\frac{b}{a}.$$

Dokaz. Dokažimo da je f injekcija. Treba dokazati da za sve $x_1, x_2 \in D = \mathbb{R}$ vrijedi

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Općenito, tvrdnju ovakvog tipa jednostavnije je dokazati obratom po kontrapoziciji (vidite 1. poglavlje):

$$\forall x_1, x_2 \in D, f(x_1)=f(x_2) \implies x_1=x_2.$$

Dakle, ako je $f(x_1) = f(x_2)$, onda nalazimo

$$f(x_1)=f(x_2) \implies ax_1+b=ax_2+b \implies ax_1=ax_2 \overset{\text{jer je } a\neq 0}{\implies} x_1=x_2.$$

Ovim smo dokazali da je linearna funkcija injekcija.

Dokažimo da je f surjekcija. Treba dokazati da za svaki $y \in K$ postoji $x \in D$ takav da je $y = f(x)$. Neka je $y \in K$. Jednadžbu $f(x) = y$ rješavamo po x:

$$f(x)=y \implies ax+b=y \implies x=\frac{1}{a}y-\frac{b}{a}.$$

Moramo na kraju provjeriti da je dobiveno rješenje u domeni funkcije f, međutim to je očigledno jer je $D = \mathbb{R}$. Dakle, $x \in D$. Ovim smo dokazali da je f surjekcija.

Ostaje izračunati inverznu funkciju. Prisjetimo se definicije inverzne funkcije koju smo dali nakon definicije 5.6:

$$\forall y \in K, \quad f^{-1}(y)=x \iff y=f(x).$$

Imamo

$$y=f(x) \implies y=ax+b \implies x=\frac{1}{a}y-\frac{b}{a} \implies f^{-1}(y)=x=\frac{1}{a}y-\frac{b}{a}.$$

Dakle,

$$f^{-1}(y) = \frac{1}{a}y - \frac{b}{a}.$$

Konačno, zamjenjujući y sa x, dobivamo formulu

$$f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}.$$

□

Propozicija 5.10. *Neka su* $[\alpha,\beta],[\gamma,\delta]\subset\mathbb{R}$ *segmenti. Tada vrijedi:*

(i) *Slika segmenta* $[\alpha,\beta]$ *pri preslikavanju* f *je segment*

$$f\left([\alpha,\beta]\right) = \begin{cases} [a\alpha+b, a\beta+b] & \textit{ako je } \ a>0 \\ [a\beta+b, a\alpha+b] & \textit{ako je } \ a<0. \end{cases}$$

(ii) *Inverzna slika segmenta* $[\gamma,\delta]$ *pri preslikavanju* f *je segment*

$$f^{-1}\left([\gamma,\delta]\right) = \begin{cases} [(\gamma-b)/a, (\delta-b)/a] & \textit{ako je } \ a>0 \\ [(\delta-b)/a, (\gamma-b)/a] & \textit{ako je } \ a<0. \end{cases}$$

Dokaz. Razmotrimo u (i) slučaj $a<0$. Slučaj $a>0$ tretira se analogno. Po definiciji, vrijedi

$$f\left([\alpha,\beta]\right) = \{f(x)\,|\,x\in[\alpha,\beta]\}.$$

Međutim, za $x\in[\alpha,\beta]$ vrijedi

$$\alpha\le x\le\beta.$$

Kako funkcija f pada za $a<0$ (vidite propoziciju 5.8), to imamo

$$\begin{aligned} &\alpha\le x\le\beta \implies f(\beta)\le f(x)\le f(\alpha) \\ &\implies a\beta+b\le f(x)\le a\alpha+b \implies f(x)\in[a\beta+b, a\alpha+b]. \end{aligned}$$

Drugim riječima, dokazali smo

$$f\left([\alpha,\beta]\right)\subseteq[a\beta+b, a\alpha+b].$$

Dokažimo i obratnu inkluziju, tj.

$$[a\beta+b, a\alpha+b]\subseteq f\left([\alpha,\beta]\right).$$

Te dvije inkluzije dokazivat će tvrdnju (i) u slučaju $a<0$. Neka je

$$y\in[a\beta+b, a\alpha+b].$$

Stavimo li

$$x=\frac{y-b}{a},$$

vrijedi

$$y=ax+b=f(x).$$

Ostaje nam dokazati

$$x\in[\alpha,\beta]$$

jer je tada $y\in f\left([\alpha,\beta]\right)$. Imamo:

$$\begin{aligned} &y\in[a\beta+b, a\alpha+b] \implies a\beta+b\le y\le a\alpha+b \\ &\implies a\beta\le y-b\le a\alpha \overset{\text{zbog } a<0}{\implies} \alpha\le\frac{y-b}{a}\le\beta, \end{aligned}$$

pa je

$$x = \frac{y-b}{a} \in [\alpha, \beta].$$

Dokažimo sada (ii). Po definiciji je

$$x \in f^{-1}\left([\gamma, \delta]\right) \iff f(x) \in [\gamma, \delta].$$

Međutim, vrijedi

$$f(x) \in [\gamma, \delta] \iff \gamma \leq f(x) \leq \delta \iff \gamma \leq ax + b \leq \delta.$$

Nadalje,

$$\gamma \leq ax + b \leq \delta \iff \begin{cases} (\gamma - b)/a \leq x \leq (\delta - b)/a & \text{ako je } \ a > 0 \\ (\delta - b)/a \leq x \leq (\gamma - b)/a & \text{ako je } \ a < 0. \end{cases}$$

Sve skupa imamo

$$x \in f^{-1}\left([\gamma, \delta]\right) \iff \begin{cases} (\gamma - b)/a \leq x \leq (\delta - b)/a & \text{ako je } \ a > 0 \\ (\delta - b)/a \leq x \leq (\gamma - b)/a & \text{ako je } \ a < 0, \end{cases}$$

a to je tvrdnja (ii). □

Zadatak 5.11. *Odredite:*

(i) *sliku segmenta* $[-1, 2]$ *pri preslikavanju* f *zadanom formulom* $f(x) = 2x - 1/2$,
(ii) *sliku segmenta* $[0, 3]$ *pri preslikavanju* f *zadanom formulom* $f(x) = -3x - 1$,
(iii) *inverznu sliku skupa* $[1, 4]$ *pri preslikavanju* f *zadanom formulom* $f(x) = 2x - 2$,
(iv) *inverznu sliku skupa* $[-2, 1]$ *pri preslikavanju* f *zadanom formulom* $f(x) = -3x + 1$.

Zadatak riješite bez uporabe zaključka prethodne propozicije, ali koristeći metode uporabljene u njenom dokazu.

3. **Kvadratna funkcija.** Neka su $a, b, c \in \mathbb{R}$, $a \neq 0$. Kvadratna funkcija je funkcija $f : \mathbb{R} \to \mathbb{R}$ zadana formulom $f(x) = ax^2 + bx + c$.

Nadopunjavanjem do potpunog kvadrata dolazimo do formule koja određuje nultočke kvadratne funkcije:

$$\begin{aligned} f(x) &= ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x\right) + c \\ &= a\left(x^2 + 2 \cdot \frac{b}{2a}x + \left(\frac{b}{2a}\right)^2\right) + c - a\left(\frac{b}{2a}\right)^2 \\ &= a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a}. \end{aligned} \tag{5.12}$$

Odatle nalazimo poznatu formulu za nultočke:[1]

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Imamo tri slučaja ovisno o tome kakva je diskriminanta $D \overset{def}{=} b^2 - 4ac$ kvadratne jednadžbe:

$$\begin{aligned} D > 0 &\implies x_1, x_2 \text{ su realni i različiti} \\ D = 0 &\implies x_1 = x_2 = -\frac{b}{2a} \text{ realan broj} \\ D < 0 &\implies x_1, x_2 \text{ su kompleksno konjugirani.} \end{aligned}$$

Sada se bavimo rastom, padom i ekstremima kvadratnih funkcija.

Propozicija 5.13. *Neka je kvadratna funkcija dana formulom $f(x) = ax^2 + bx + c$, gdje su $a, b, c \in \mathbb{R}$, $a \neq 0$. Tada vrijedi:*

(i) *Ako je $a > 0$, onda funkcija f strogo pada na $\langle -\infty,\ -\frac{b}{2a}]$ i strogo raste na $[-\frac{b}{2a},\ +\infty\rangle$. U točki $x = -\frac{b}{2a}$ funkcija f ima minimum jednak $-\frac{b^2-4ac}{4a}$.*

(ii) *Ako je $a < 0$, onda funkcija f strogo raste na $\langle -\infty,\ -\frac{b}{2a}]$ i strogo pada na $[-\frac{b}{2a},\ +\infty\rangle$. U točki $x = -\frac{b}{2a}$ ima maksimum jednak $-\frac{b^2-4ac}{4a}$.*

Dokaz. Dokažimo (i). Tvrdnja (ii) se dokazuje analogno, a može se dobiti i iz (i) promatranjem funkcije $-f$ (vidite zadatak 5.3).

Neka je $a > 0$. Dokažimo da f strogo pada na $\langle -\infty,\ -\frac{b}{2a}]$. Treba dokazati

$$\forall x_1, x_2 \in \left\langle -\infty,\ -\frac{b}{2a}\right],\ x_1 < x_2 \implies f(x_1) > f(x_2).$$

Zaista, imamo

$$\begin{aligned} f(x_2) - f(x_1) &= \left(ax_2^2 + bx_2 + c\right) - \left(ax_1^2 + bx_1 + c\right) \\ &= a\left(x_2^2 - x_1^2\right) + b\left(x_2 - x_1\right) \\ &= a\left(x_2 - x_1\right)\left(x_2 + x_1\right) + b\left(x_2 - x_1\right) \\ &= \left(x_2 - x_1\right)\left(a\left(x_2 + x_1\right) + b\right). \end{aligned} \tag{5.14}$$

Vrijedi

$$\begin{aligned} x_1 < x_2 \leq -\frac{b}{2a} &\implies x_1 + x_2 < \left(-\frac{b}{2a}\right) + \left(-\frac{b}{2a}\right) = -\frac{b}{a} \\ &\implies x_1 + x_2 + \frac{b}{a} < 0 \overset{\text{jer je } a > 0}{\implies} \left(a\left(x_2 + x_1\right) + b\right) < 0. \end{aligned}$$

Isto tako

$$x_1 < x_2 \implies x_2 - x_1 > 0.$$

Sve skupa daje:

$$\left(x_2 - x_1\right)\left(a\left(x_2 + x_1\right) + b\right) < 0.$$

Dakle, (5.14) povlači

$$f(x_2) - f(x_1) < 0$$

odnosno

$$f(x_1) > f(x_2).$$

[1]Egzistencija drugog korijena iz nenegativnog realnog broja biti će dokazana u teoremu 10.4

Ovim smo dokazali da f strogo pada na $\langle -\infty,\ -\frac{b}{2a}]$. Slično se vidi da f strogo raste na $[-\frac{b}{2a}, \infty\rangle$ ako je $a > 0$.

Za završetak dokaza tvrdnje (i) treba vidjeti da se u $-\frac{b}{2a}$ postiže minimum funkcije f i da je taj minimum upravo

$$f\left(-\frac{b}{2a}\right) = -\frac{b^2 - 4ac}{4a}.$$

U tu svrhu koristimo prikaz funkcije f iz (5.12):

$$f(x) = a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a}.$$

Zbog $a > 0$ za svaki $x \in \mathbb{R}$ vrijedi

$$f(x) = a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a} \geq -\frac{b^2 - 4ac}{4a} = f\left(-\frac{b}{2a}\right).$$

Ovim je (i) dokazano. $\square$

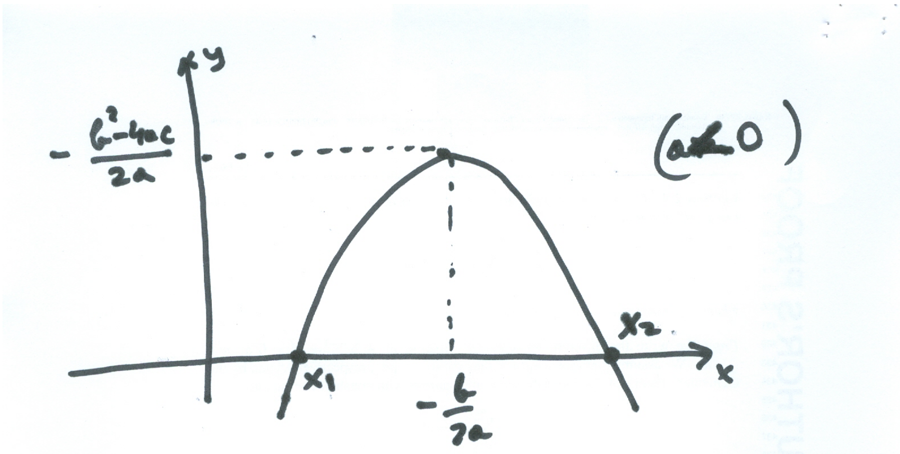
Graf kvadratne funkcije je parabola čije je tjeme u točki

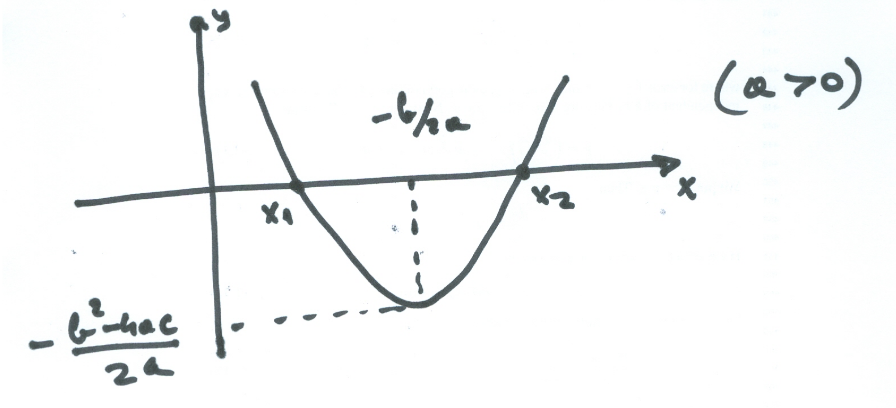
$$\left(-\frac{b}{2a},\ -\frac{b^2 - 4ac}{4a}\right).$$

Os simetrije ove parabole je pravac

$$x = -\frac{b}{2a},$$

a parabola je otvorena prema gore ako je $a > 0$, a dolje ako je $a < 0$. Sljedeća slika ilustrira grafove kvadratnih funkcija.





Iz grafova ovih funkcija vidljivo je da kvadratna funkcija nikada nije injekcija niti surjekcija. Ipak njezina restrikcija na $\langle -\infty,\ -\frac{b}{2a}]$ ili $[-\frac{b}{2a},\ +\infty\rangle$ je bijekcija na $< -\infty, -\frac{b^2-4ac}{4a}]$ ako je $a < 0$ odnosno na $[-\frac{b^2-4ac}{4a}, \infty >$ ako je $a > 0$, kao što iz slike možemo naslutiti.

Zadatak 5.15. *Neka je dana kvadratna funkcija* $f(x) = x^2 - 3x + 2$*. Nacrtajte graf te funkcije i odredite:*

(i) $f([-2, -1])$,
(ii) $f([0, 3/2])$,
(iii) $f(\langle 1/2, 3])$,
(iv) $f([4, 6])$,
(v) $f^{-1}[-1/4, 2])$,
(vi) $f^{-1}[-1, 2])$.

Zadatak 5.16. *Odredite (ako postoje) minimum i maksimum danih kvadratnih funkcija te odredite u kojim točkama se postižu. Nacrtajte grafove tih funkcija.*

(i) $f(x) = -2x^2 + 5x + 7$,
(ii) $f(x) = x^2 - 2x + 3$.

Zadatak 5.17. *Riješite nejednadžbe:*

(i) $-x^2+7x-10>0$,
(ii) $x^2-2x+3>0$,
(iii) $(x+4)(x+5)>x+5$,
(iv) $\frac{x-11}{x^2-2x-15}<0$.

4. **Opća potencija.** Neka je n prirodan broj. Funkcija $f:\mathbb{R}\to\mathbb{R}$ zadana sa $f(x)=x^n$ naziva se opća potencija.

Propozicija 5.18. *Neka je n neparan prirodan broj tj. $n\in\{1,3,5,7,\ldots\}$. Tada je funkcija $f:\mathbb{R}\to\mathbb{R}$ zadana sa $f(x)=x^n$ strogo rastuća bijekcija. Nadalje, f je neparna funkcija tj. $f(-x)=-f(x)$ za svaki $x\in\mathbb{R}$.*

Dokaz. Najprije dokažimo da je f neparna funkcija. Kako je n neparan prirodan broj, to za svaki $x\in\mathbb{R}$ vrijedi

$$f(-x)=(-x)^n=(-1)^nx^n=-x^n=-f(x).$$

Sada dokažimo da funkcija f strogo raste na $\mathbb{R}$ tj. da vrijedi

$$x_1<x_2 \implies f(x_1)<f(x_2).$$

Razmatramo nekoliko mogućnosti:

(i) Za $0\leq x_1<x_2$ imamo

$$f(x_2)-f(x_1)=x_2^n-x_1^n=(x_2-x_1)\left(x_2^{n-1}+x_2^{n-2}x_1+\cdots+x_2x_2^{n-2}+x_1^{n-1}\right)>0,$$

jer je $x_2-x_1>0$, a drugi izraz je strogo pozitivan zbog $0\leq x_1<x_2$.

(ii) Ako je $x_1\leq 0<x_2$, tada je $f(x_2)=x_2^n>0$, ali $f(x_1)\leq 0$ jer množimo neparan broj puta $x_1\leq 0$ sa samim sobom.

(iii) Ako je $x_1<x_2\leq 0$, tada je

$$0\leq -x_2<-x_1.$$

Stoga prema (i) zaključujemo

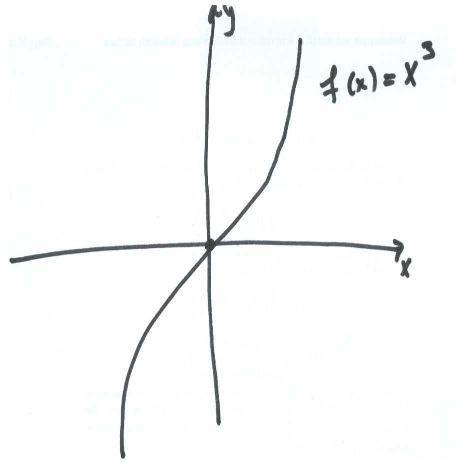
$$f(-x_2)<f(-x_1).$$

Kako je f neparna funkcija, imamo

$$f(-x_2)<f(-x_1) \implies -f(x_2)<-f(x_1) \implies f(x_1)<f(x_2).$$

Ovim je dokazano da je funkcija f strogo rastuća. Svaka strogo rastuća funkcija je injekcija (zašto?). Dakle, preostaje dokazati da je f surjekcija, tj. da za svaki $y\in\mathbb{R}$ postoji $x\in\mathbb{R}$ takav da je $y=x^n$. Ovo pitanje je suptilno i zadire u samu strukturu skupa realnih brojeva, pa to ostavljamo za 10. poglavlje (vidjeti teorem 10.5 i korolar 10.6). $\square$

Sljedeća slika ilustrira slučaj $n=3$. Graf te funkcije naziva se kubna parabola.



Dokaz sljedeće propozicije analogan je dokazu propozicije 5.18(vidjeti također teorem 10.5 i korolar 10.6) i prepuštamo ga čitatelju:

Propozicija 5.19. *Neka je n paran prirodan broj tj. $n \in \{2, 4, 6, 8, \ldots\}$. Tada je $f : \mathbb{R} \to \mathbb{R}$ zadana sa $f(x) = x^n$ parna funkcija tj. $f(-x) = f(x)$ za svaki $x \in \mathbb{R}$. Na $\langle -\infty,\ 0]$ funkcija f strogo pada, a na $[0,\ \infty\rangle$ funkcija f strogo raste. U $x = 0$ funkcija f ima minimum.*

Zbog uvjeta parnosti, funkcija f nikada nije injekcija pa zato ne može biti niti bijekcija, ali njezina restrikcija na $[0, \infty\rangle$ je strogo rastuća bijekcija sa $[0, \infty\rangle$ na $[0, \infty\rangle$.

Zaključimo:

(i) Ako je n neparan, tada funkcija $f : \mathbb{R} \to \mathbb{R}$ definirana sa $f(x) = x^n$ ima inverznu funkciju $f^{-1} : \mathbb{R} \to \mathbb{R}$.
(ii) Ako je n paran, tada funkcija $f : [0, \infty\rangle \to [0, \infty\rangle$ definirana sa $f(x) = x^n$ ima inverznu funkciju $f : [0, \infty\rangle \to [0, \infty\rangle$.

U oba slučaja funkciju f^{-1} zovemo **n-ti korijen** i označavamo sa

$$f^{-1}(x) = \sqrt[n]{x} = x^{1/n}.$$

Uočimo da propozicija 5.7 povlači da je n-ti korijen rastuća funkcija.

Za funkciju koja je zadana nekom formulom njezina prirodna domena je skup svih $x \in \mathbb{R}$ takvih da formula ima smisla i da je $f(x)$ realan. Primjerice,

$$f(x) = \frac{1}{x} + \sqrt{x} + \sqrt[3]{2x}.$$

Vidimo da je prvi sumand definiran za $x \neq 0$, drugi sumand za $x \geq 0$, a treći za sve $x \in \mathbb{R}$. Dakle domena ove funkcije je

$$D = \langle 0, \infty\rangle.$$

Zadatak 5.20. *Odredite prirodnu domenu funkcije:*

(i) $f(x) = \sqrt{\frac{2x-3}{x}} + \sqrt[4]{\frac{1}{x^2-1}}$,
(ii) $f(x) = \sqrt{\frac{3}{x-5}}$.

5. **Apsolutna vrijednost.** Apsolutna vrijednost je funkcija $f : \mathbb{R} \to \mathbb{R}$ dana sa

$$f(x) = |x| = \begin{cases} x & \text{ako je } x \geq 0 \\ -x & \text{ako je } x < 0. \end{cases}$$

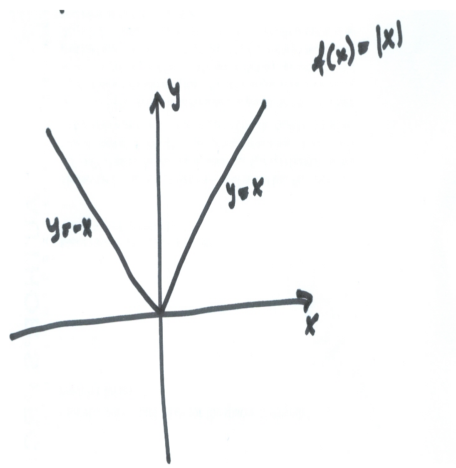
Vidimo da je

$$f(x) = |x| \geq 0, \quad \forall x \in \mathbb{R}.$$

Primjerice,

$$f(-5) = |-5| = -(-5) = 5, \quad f(0) = |0| = 0, \quad f(5) = |5| = 5.$$

Očito je funkcija f parna tj. $f(-x) = f(x)$ za svaki $x \in \mathbb{R}$. To povlači da f nije injekcija, zato f nije niti bijekcija. Slika funkcije f je skup $[0, \infty\rangle$. Graf ove funkcije dan je na sljedećoj slici.



Zadatak 5.21. *Riješite jednadžbe:*

(i) $|x| + x = 1$,
(ii) $|2x - 1| = 3$,
(iii) $|4x - 1| - |2x - 3| + |x + 2| = 0$,
(iv) $|x| + |x + 1| + |x + 2| = 9$.

Zadatak 5.22. *Riješite nejednadžbe:*

(i) $|x + 2| > |x|$,
(ii) $|x + 3| - |2x + 1| \geq 0$,
(iii) $|x + 3| + |x - 1| + |x - 3| < 10$,
(iv) $|x + 2| - |x + 1| + |x| - |x - 1| + |x - 2| > \frac{5}{2}$.

Zadatak 5.23. *Nacrtajte graf funkcije i odredite sliku funkcije*

(i) $f(x) = |x + 2|$,

(ii) $f(x) = |x+3| - |2x+1|$,
(iii) $f(x) = |x+3| + |x-1| + |x-3|$,
(iv) $f(x) = |x+2| - |x+1| + |x| - |x-1| + |x-2|$.

6. **Eksponencijalna i logaritamska funkcija.** Neka je $a \neq 0$. Tada potencije broja a imaju ova svojstva:

$$\begin{aligned} &a^0 = 1,\\ &a^1 = a,\\ &a^m a^n = a^{m+n} \quad \text{za sve cijele brojeve } m, n \in \mathbb{Z},\\ &a^{-n} = \frac{1}{a^n} \quad \text{za sve cijele brojeve } n \in \mathbb{Z}. \end{aligned}$$

Ukoliko je $a > 0$, tada imamo n–te korijene

$$a^{1/n} = \sqrt[n]{a} \qquad \text{za sve prirodne brojeve } n \in \mathbb{N}.$$

To nam omogućuje da potenciju definiramo i za sve racionalne brojeve:

$$a^{m/n} \overset{\text{def}}{=} \left(\sqrt[n]{a}\right)^m \qquad \text{za sve prirodne brojeve } n \in \mathbb{N} \text{ i sve cijele brojeve } m \in \mathbb{Z}.$$

Ovako proširena potencija ima svojstva:

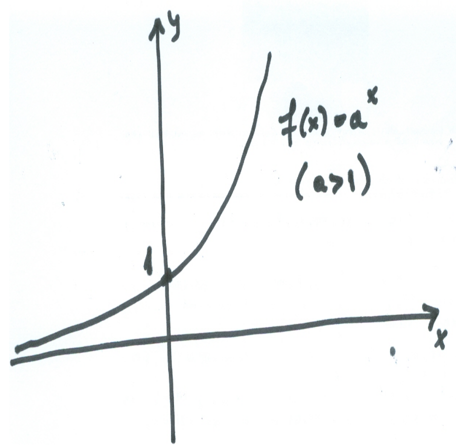
$$\begin{aligned} &a^0 = 1,\\ &a^1 = a,\\ &a^r a^q = a^{r+q} \quad \text{za sve racionalne brojeve } r, q \in \mathbb{Q},\\ &a^{-r} = \frac{1}{a^r} \quad \text{za sve racionalne brojeve } r \in \mathbb{Q}. \end{aligned}$$

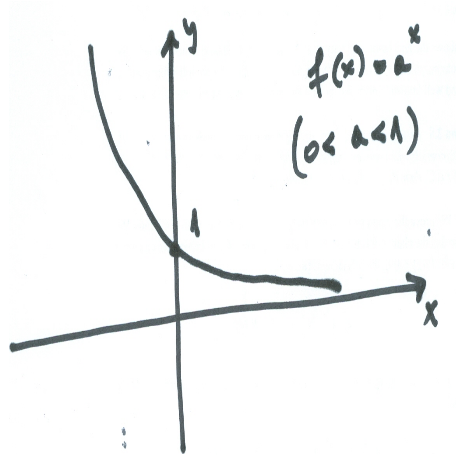
Neka je $a > 0$ i $a \neq 1$. Kao što smo ranije rekli, stroga definicija i egzistencija n–tog korijena zahtijeva dodatna razmatranja (koje ćemo provesti kasnije u 10. poglavlju). Definicija broja a^x za proizvoljni realan broj slijedi ista razmatranja, ali njih nećemo provoditi u ovom kolegiju; ona se oslanjaju na aksiom potpunosti iz 10. poglavlja.

Teorem 5.24. *Neka je $a > 0$, $a \neq 1$. Tada je funkcija $f : \mathbb{R} \to \langle 0,\ \infty\rangle$ definirana sa $f(x) = a^x$ bijekcija i to strogo rastuća ako je $a > 1$, odnosno strogo padajuća ako je $0 < a < 1$. Nadalje, funkcija f zadovoljava ova svojstva:*

$$\begin{aligned} &a^0 = 1,\\ &a^1 = a,\\ &a^x a^y = a^{x+y} \quad \forall x, y \in \mathbb{R},\\ &a^{-x} = \frac{1}{a^x} \quad \forall x \in \mathbb{R}. \end{aligned}$$

Gornji teorem opisuje svojstva eksponencijalne funkcije $x \mapsto a^x$. U izrazu a^x broj a naziva se baza, a x eksponent. Grafovi eksponencijalnih funkcija prikazani su na sljedećim slikama. Uočimo da je $f(x) > 0$ za svaki $x \in \mathbb{R}$, pa zato graf funkcije leži iznad osi x.





Inverzna funkcija eksponencijalne funkcije $f(x) = a^x$ je logaritamska funkcija $f^{-1}(y) = \log_a(y)$.

Vrijedi:

$$y = a^x \iff x = \log_a y.$$

Ukoliko je baza $a = e = 2,71828...$, onda govorimo o prirodnom logaritmu i umjesto $\log_a$ pišemo ln. Također se za bazu $a = 10$ piše log umjesto $\log_{10}$.

Iz definicije inverzne funkcije odmah dobivamo:

$$\begin{aligned} \log_a(a^x) &= x, \quad \text{za sve } x \in \mathbb{R}, \\ a^{\log_a x} &= x, \quad \text{za sve } x \in <0, \infty>. \end{aligned} \tag{5.25}$$

Teorem 5.26. *Neka je $a > 0$, $a \neq 1$. Tada je funkcija $\log_a : \langle 0, \infty\rangle \to \mathbb{R}$ bijekcija i to strogo rastuća ako je $a > 1$, odnosno strogo padajuća ako je $0 < a < 1$.*

Nadalje, funkcija $\log_a$ *ima sljedeća svojstva:*

$$\begin{aligned}
&\log_a 1 = 0,\\
&\log_a a = 1,\\
&\log_a (xy) = \log_a x + \log_a y, \quad \forall x, y \in \langle 0,\ \infty\rangle,\\
&\log_a (x^{-1}) = -\log_a (x), \quad \forall x \in \langle 0,\ \infty\rangle,\\
&\log_a (x^n) = n \log_a (x), \quad \forall x \in \langle 0,\ \infty\rangle,\ n \in \mathbb{Z}.
\end{aligned}$$

Dokaz. Teorem 5.26 dokazujemo pomoću teorema 5.24. Jasno je da je $\log_a$ bijekcija jer je inverz bijekcije (to ćemo dokazati općenito u 7. poglavlju). Funkcija $\log_a$ je strogo rastuća funkcija jer je inverz strogo rastuće funkcije (vidite propoziciju 5.7).

Identiteti iz ovog teorema posljedice su onih za eksponencijalnu funkciju i činjenice da je $\log_a$ inverzna funkcija funkcije $x \longmapsto a^x$. Kako je $a^0 = 1$ i $a^1 = a$, to odmah dobivamo $\log_a 1 = 0$ i $\log_a a = 1$. Nadalje, koristeći drugu jednakost u (5.25), nalazimo

$$a^{\log_a (xy)} = xy = a^{\log_a x} a^{\log_a y} = a^{\log_a x + \log_a y}.$$

Kako je eksponencijalna funkcija injekcija, gornja jednakost daje

$$\log_a (xy) = \log_a x + \log_a y.$$

Ovim je dokazana treća jednakost teorema. Ako u nju stavimo $y = x^{-1}$, dobivamo

$$0 = \log_a 1 = \log_a (xx^{-1}) = \log_a x + \log_a x^{-1}.$$

Odatle slijedi četvrta jednakost. Ako je $n = 0$, posljednja jednakost slijedi iz prve. Ako je $n \geq 1$, onda se posljednja jednakost dobiva uzastopnom primjenom treće jednakosti. Dakle imamo

$$\log_a (x^n) = n \log_a (x),$$

za $n = 0, 1, 2, \ldots$. Ako je $n < 0$, onda je $-n \geq 1$ i prema gore dokazanom vrijedi

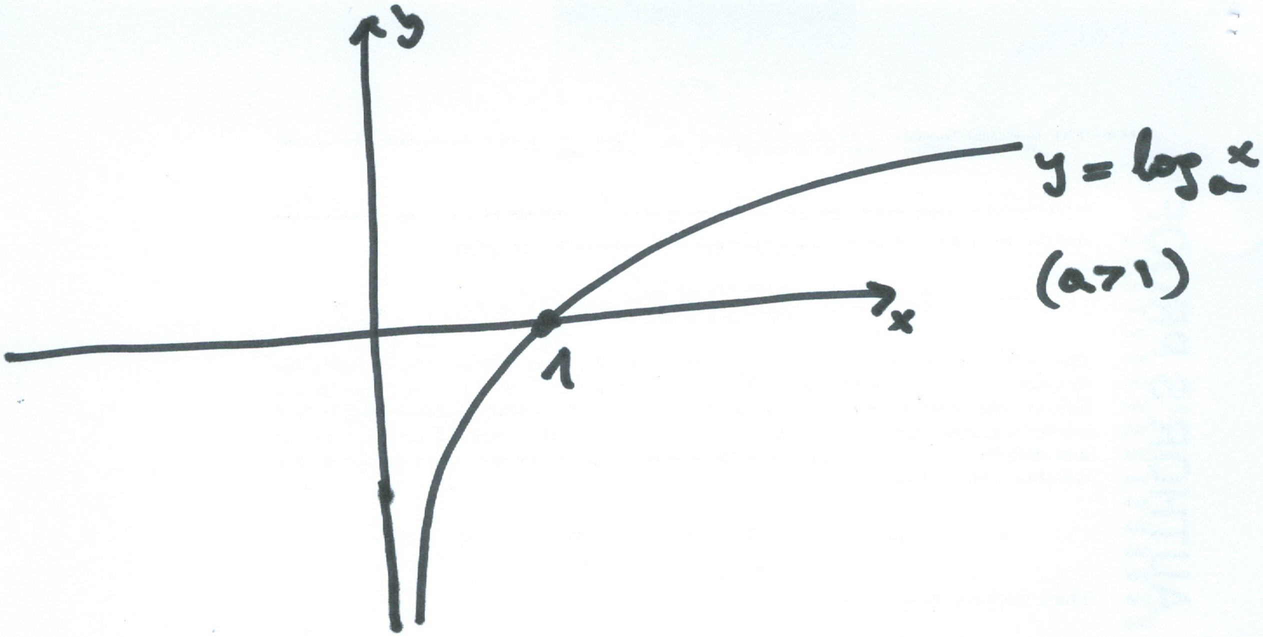
$$\log_a (x^{-n}) = -n \log_a (x).$$

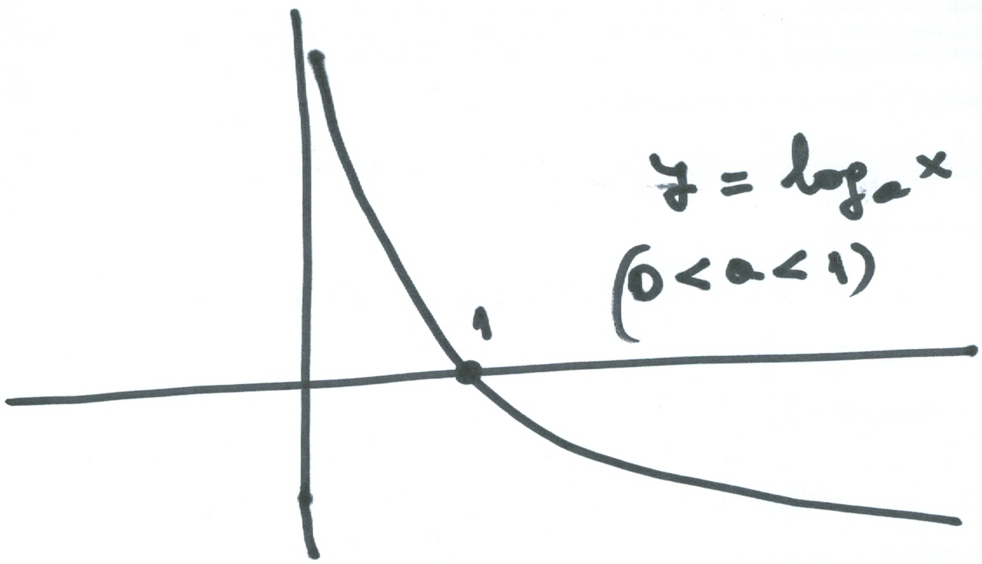
Konačno, četvrta jednakost daje

$$\log_a (x^n) = -\log_a (x^{-n}) = -\left(-n \log_a (x)\right) = n \log_a (x).$$

$\square$

Grafovi logaritamskih funkcija dobiveni su zrcaljenjem oko osi $y = x$ odgovarajućih grafova eksponencijalnih funkcija.


y
x
1
$y = \log_a x$
$(a > 1)$

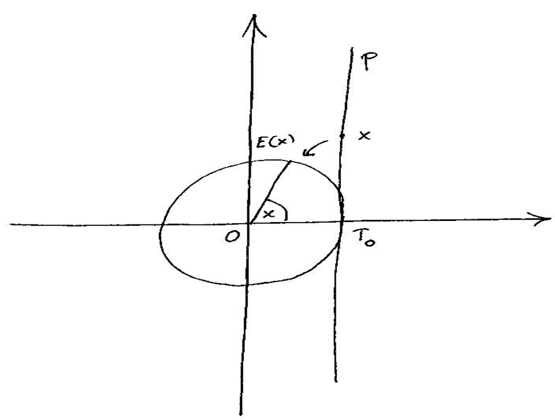

1
$y = \log_a x$
$(0 < a < 1)$

6. Neke elementarne funkcije; jednadžbe i nejednadžbe (drugi dio)

Ovo poglavlje je nastavak prethodnog poglavlja.

7. **Trigonometrijske funkcije.** Zanima nas put koji točka na obodu kotača prevali prilikom vrtnje kotača. Obod kotača predstavljamo kružnicom $K = k(O, 1)$ sa središtem u ishodištu O Kartezijevog koordinatnog sustava i polumjerom koji je jednak jediničnoj dužini koordinatnog sustava; ta kružnica se zove jedinična kružnica i njen opseg je 2π.

Uočimo da točka na obodu kotača prilikom vrtnje prevali put koji može biti mnogo veći od opsega kotača. Zato na kružnicu prislonimo pravac p koji dodiruje kružnicu K u točki $T_0(1, 0)$ tj. pravac p je tangenta na kružnicu K u $T_0(1, 0)$ i na njega smjestimo realne brojeve tako da se nula nalazi u točki T_0, a pozitivni realni brojevi na dijelu pravca koji je iznad osi x.



Pravac p sada namatamo na kružnicu (kao da se radi, primjerice, o užetu) i to tako da dio pravca (polupravac) s pozitivnim brojevima namatamo suprotno gibanju kazaljke na satu (tzv. gibanje u pozitivnom smjeru), a polupravac s negativnim brojevima u smjeru gibanja kazaljke na satu (tzv. gibanje u negativnom smjeru). Pritom na svaku točku kružnice K padne beskonačno mnogo točaka s pravca p. Konkretno, u točku T_0 padne i broj 0 i brojevi 2π, -2π, 4π, -4π, ... tj. brojevi oblika $2k\pi$, $k \in \mathbb{Z}$. Svaki realni broj x na opisani način smjestimo na kružnicu K.

Za razliku od obične kružnice, na ovu kružnicu su smješteni realni brojevi i zato se zove **brojevna ili trigonometrijska kružnica**.

Preslikavanje koje realnom broju x pridruži točku na trigonometrijskoj kružnici K označimo sa E. Dakle, $E : \mathbb{R} \to K$. Ovo preslikavanje nazivamo **namatanje pravca na kružnicu**.

Uočimo da je E surjekcija, tj. E je funkcija sa $\mathbb{R}$ na K, jer na svaku točku kružnice padne neka točka pravca p odnosno neki realni broj. Ta točka očito nije jedinstvena jer za svaki $x \in \mathbb{R}$ vrijedi

$$E(x) = E(x + 2k\pi),\ \forall k \in \mathbb{Z}.$$

Naime, ako se neki $x \in \mathbb{R}$ preslika u točku $T \in K$, tada se i brojevi $x + 2\pi$, $x - 2\pi$, $x + 4\pi$, $x - 4\pi$, $\ldots$, općenito brojevi oblika $x + 2k\pi$, $k \in \mathbb{Z}$, preslikaju u točku T. Prema tome, funkcija E sa $\mathbb{R}$ na K nije injekcija. Obzirom da se u istu točku $T = E(x)$ kružnice K preslikaju samo oni realni brojevi čija je međusobna udaljenost jednaka nekom (cjelobrojnom) višekratniku opsega kružnice K, brojevi oblika $x + 2k\pi$, $k \in \mathbb{Z}$, su jedini brojevi koji se preslikaju u T. Znači da je praslika točke $T = E(x)$ skup

$$E^{-1}(T) = \{x + 2k\pi \mid k \in \mathbb{Z}\}.$$

Prethodna razmatranja nas motiviraju uvesti pojam periodičke funkcije.

Definicija 6.1. *Za funkciju f kažemo da je* ***periodička s periodom*** $\tau \neq 0$ *ako vrijedi:*

(i) *ako je x iz domene funkcije f, tada je i $x + \tau$ iz domene funkcije f,*
(ii) *za svaki x iz domene funkcije f vrijedi $f(x + \tau) = f(x)$.*

Najmanji takav $\tau > 0$ (ako postoji) zove se ***temeljni period*** *funkcije f.*

Dakle, preslikavanje $E : \mathbb{R} \to K$, tj. namatanje pravca na kružnicu, je periodička funkcija s temeljnim periodom 2π. Preslikavanje E je surjekcija, ali nije injekcija, pa nije niti bijekcija.

No, ako promatramo restrikciju $E|_{[0,2\pi\rangle} : [0, 2\pi\rangle \to K$, tada je ona bijekcija jer prolaskom x po intervalu $[0, 2\pi\rangle$ točka $E(x)$ prolazi kroz svaku točku kružnice (u pozitivnom smjeru) samo jednom:

$$(\forall T \in K)(\exists! x \in [0, 2\pi\rangle)(E(x) = T).$$

Kao i svaka bijekcija, tako i $E|_{[0,2\pi\rangle}$ ima inverznu funkciju. To je funkcija sa K na $[0, 2\pi\rangle$ i ona služi kao mjera kuta kojeg zatvaraju pravac OT_0 i pravac $OE(x)$: kažemo da taj kut ima x radijana. Uočimo da je x duljina luka kružnice K od T_0 do $E(x)$ u pozitivnom smjeru (jer na taj luk namotamo interval $[0, x]$).

Osim u radijanima, kutovi se mjere i u stupnjevima: ako kut ima x radijana, tada ima $\frac{360^\circ}{2\pi}x$ stupnjeva, a ako ima x stupnjeva, tada ima $\frac{2\pi}{360^\circ}x$ radijana.

Trigonometrijska kružnica je, prisjetimo se, smještena u Kartezijev koordinatni sustav i to tako da joj je središte u ishodištu O, a polumjer jednak jediničnoj dužini koordinatnog sustava. Stoga svakoj točki T trigonometrijske kružnice pridružujemo uređeni par (x_T, y_T) realnih brojeva; realan broj x_T se naziva apscisa, a realan broj y_T ordinata točke T.

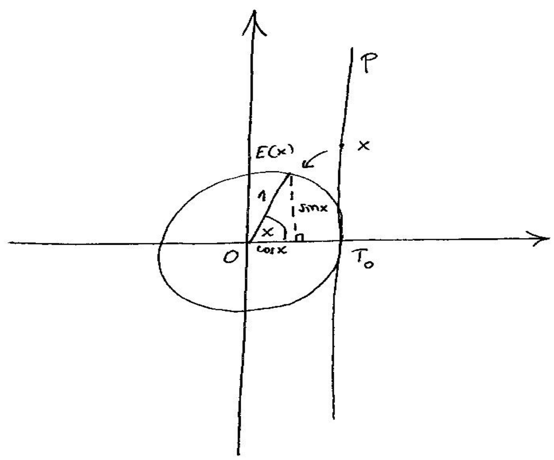
Svakom $x \in \mathbb{R}$ preslikavanje E pridružuje točku $E(x)$ na trigonometrijskoj kružnici. Primjerice,

$$E(0) = (1,0), \quad E\Big(\frac{\pi}{2}\Big) = (0,1), \quad E(\pi) = (-1,0),$$

$$E\Big(\frac{3\pi}{2}\Big) = (0,-1), \quad E(2\pi) = (1,0), \quad E(-3\pi) = (-1,0), \ldots$$

Apscisa točke $E(x)$ zove se **kosinus** broja x i označava sa $\cos x$, a ordinata točke $E(x)$ zove se **sinus** broja x i označava sa $\sin x$. Tako smo definirali funkcije

$$\cos : \mathbb{R} \to \mathbb{R}, \qquad \sin : \mathbb{R} \to \mathbb{R}.$$



Pomoću funkcija kosinus i sinus definiraju se funkcije **tangens** i **kotangens** redom sa

$$\operatorname{tg} x = \frac{\sin x}{\cos x}, \qquad \operatorname{ctg} x = \frac{\cos x}{\sin x}.$$

Funkcije sinus, kosinus, tangens i kotangens se zovu **trigonometrijske funkcije**.

Iz definicije sinusa i kosinusa, Pitagorinog teorema i činjenice da je trigonometrijska funkcija jedinična odmah zaključujemo da je

$$\sin^2 x + \cos^2 x = 1, \qquad \forall x \in \mathbb{R}.$$

Iz definicije tangensa i kotangensa imamo:

$$\operatorname{tg} x \cdot \operatorname{ctg} x = 1, \qquad \forall x \in \mathbb{R} \text{ za koje je } \sin x \neq 0,\ \cos x \neq 0.$$

Sve točke na jediničnoj kružnici sa središtem u ishodištu imaju koordinate $(\cos t, \sin t)$ za neki $t \in [0, 2\pi\rangle$, pa kažemo da je

$$x = \cos t,\ y = \sin t \qquad (t \in [0, 2\pi\rangle)$$

parametarska jednadžba kružnice.

Geometrijsko značenje tangensa i kotangensa. Neka je, kao i ranije, točka O ishodište koordinatnog sustava, a točka T_0 točka s koordinatama $(1,0)$. Neka je p tangenta na trigonometrijsku kružnicu $K = k(0,1)$ u točki T_0. Neka je x realan broj te neka je $E(x)$ točka kružnice K u koju se x preslika namatanjem na kružnicu. Sa $A(x)$ označimo točku s koordinatama $(\cos x, 0)$, a sa $B(x)$ sjecište pravca p i pravca $OE(x)$, tj. onog kraka kuta x koji ne leži na osi apscisa. Uočimo da su trokuti $OT_0B(x)$ i $OA(x)E(x)$ slični prema K-K-K teoremu o sličnosti (kut pri vrhu O im je zajednički, a sukladnost ostalih kutova slijedi iz sukladnosti kutova uz transverzalu paralelnih pravaca). Odatle slijedi

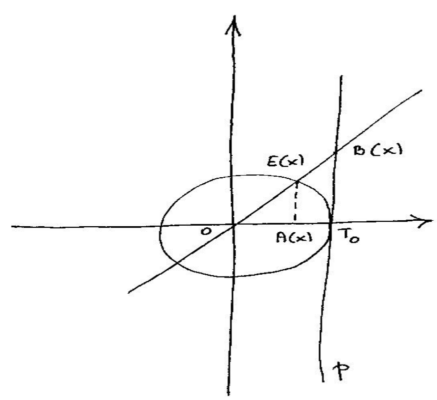
$$\frac{|T_0B(x)|}{|OT_0|} = \frac{|A(x)E(x)|}{|OA(x)|},$$

a kako je $|OT_0| = 1$ i

$$\frac{|A(x)E(x)|}{|OA(x)|} = \frac{\sin x}{\cos x} = \operatorname{tg} x,$$

to je

$$|T_0B(x)| = \operatorname{tg} x.$$

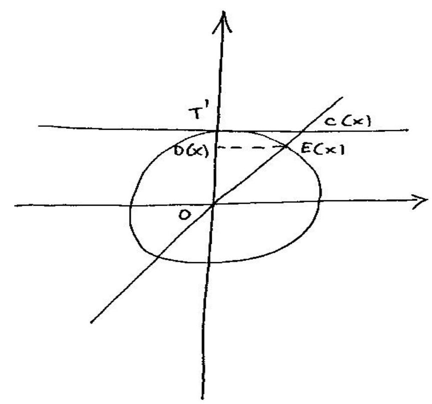


Sada sa T' označimo točku s koordinatama $(0,1)$, sa $C(x)$ označimo sjecište tangente na K u točki T' i pravca $OE(x)$, tj. onog kraka kuta x koji ne leži na osi apscisa, a sa $D(x)$ označimo sjecište one paralele s osi apscisa koja prolazi kroz $E(x)$ i osi ordinata. Trokuti $OC(x)T'$ i $OE(x)D(x)$ su slični (K-K-K teorem o sličnosti, obrazložite), pa je

$$\frac{|T'C(x)|}{|OT'|} = \frac{|D(x)E(x)|}{|OD(x)|},$$

a kako je $|OT'| = 1$, $|D(x)E(x)| = |OA(x)| = \cos x$ i $|OD(x)| = |A(x)E(x)| = \sin x$, to je

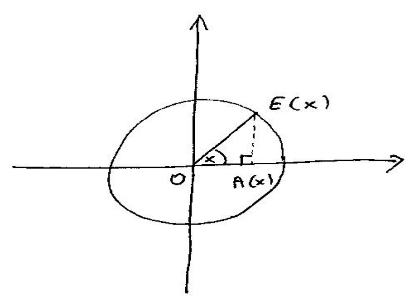
$$|T'C(x)| = \operatorname{ctg} x.$$

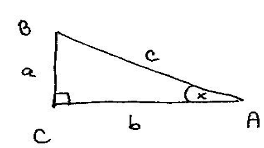


Trigonometrija pravokutnog trokuta. Neka je ABC pravokutan trokut s pravim kutom pri vrhu C te neka je mjera šiljastog kuta pri vrhu A jednaka x. Neka su a i b duljine kateta, a c duljina hipotenuze tog trokuta. Definirajmo trigonometrijske funkcije kuta x:

$$\sin x = \frac{a}{c}, \qquad \cos x = \frac{b}{c}, \qquad \operatorname{tg} x = \frac{a}{b}, \qquad \operatorname{ctg} x = \frac{b}{a}.$$

Opravdajmo uvedene oznake $\sin x$, $\cos x$, $\operatorname{tg} x$, $\operatorname{ctg} x$, tj. dokažimo da se zaista radi o ranije definiranim funkcijama sinus, kosinus, tangens i kotangens kuta x.





Rabeći iste oznake kao i ranije, uočavamo da su trokuti ABC i $OE(x)A(x)$ slični prema K-K-K teoremu o sličnosti. Odatle zaista slijede sljedeće jednakosti:

$$\frac{|BC|}{|AB|} = \frac{|E(x)A(x)|}{|OE(x)|} = \frac{\sin x}{1} = \sin x,$$

$$\frac{|AC|}{|AB|} = \frac{|OA(x)|}{|OE(x)|} = \frac{\cos x}{1} = \cos x,$$

$$\frac{|BC|}{|AC|} = \frac{|E(x)A(x)|}{|OA(x)|} = \frac{\sin x}{\cos x} = \operatorname{tg} x,$$

$$\frac{|AC|}{|BC|} = \frac{|OA(x)|}{|E(x)A(x)|} = \frac{\cos x}{\sin x} = \operatorname{ctg} x.$$

Dakle, u pravokutnom trokutu za šiljasti kut vrijedi:

Sinus kuta je omjer nasuprotne katete i hipotenuze.

Kosinus kuta je omjer priležeće katete i hipotenuze.

Tangens kuta je omjer nasuprotne i priležeće katete.

Kotangens kuta je omjer priležeće i nasuprotne katete.

Neka svojstva trigonometrijskih funkcija.

Teorem 6.2. *Trigonometrijske funkcije imaju sljedeća svojstva:*

(i) *Nultočke funkcija* sin *i* tg *su* $k\pi$, $k \in \mathbb{Z}$. *Nultočke funkcija* cos *i* ctg *su* $\frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$.
(ii) *Domena funkcija* sin *i* cos *je* $\mathbb{R}$, *a slika* $[-1, 1]$. *Domena funkcije* tg *je* $\mathbb{R} \setminus \{\frac{\pi}{2} + k\pi \,|\, k \in \mathbb{Z}\}$, *domena funkcije* ctg *je* $\mathbb{R} \setminus \{k\pi \,|\, k \in \mathbb{Z}\}$, *a slika i funkcije* tg *i funkcije* ctg *je* $\mathbb{R}$.
(iii) *Funkcija* cos *je parna, a* sin, tg *i* ctg *su neparne funkcije.*
(iv) *Funkcije* sin *i* cos *su periodičke s temeljnim periodom* 2π, *a* tg *i* ctg *su periodičke s temeljnim periodom* π.
(v) *Funkcija* sin *je strogo rastuća na* $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, cos *je strogo padajuća na* $[0, \pi]$, tg *je strogo rastuća na* $\left\langle -\frac{\pi}{2}, \frac{\pi}{2}\right\rangle$, ctg *je strogo padajuća na* $\langle 0, \pi\rangle$.

Dokaz. (i) Znamo da je $\cos x = 0$ za one $x \in \mathbb{R}$ za koje je apscisa točke $E(x)$ jednaka nuli. Znači da je $x = \frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$. Također, $\sin x = 0$ za one $x \in \mathbb{R}$ za koje je ordinata točke $E(x)$ jednaka nuli. Slijedi $x = k\pi$, $k \in \mathbb{Z}$. Uočimo da funkcija tangens ima iste nultočke kao i funkcija sinus, a funkcija kotangens ima iste nultočke kao i funkcija kosinus.

(ii) Uočimo da su funkcije sinus i kosinus definirane na čitavom skupu realnih brojeva, tj.

$$D(\sin) = \mathbb{R}, \qquad D(\cos) = \mathbb{R}.$$

Funkcija tangens je definirana za sve realne brojeve x za koje je $\cos x \neq 0$, a funkcija kotangens za sve realne brojeve x za koje je $\sin x \neq 0$. Prema tome, domene funkcija tangens i kotangens su

$$D(\operatorname{tg}) = \mathbb{R} \setminus \left\{\frac{\pi}{2} + k\pi \,|\, k \in \mathbb{Z}\right\}, \qquad D(\operatorname{ctg}) = \mathbb{R} \setminus \{k\pi \,|\, k \in \mathbb{Z}\}.$$

Kako je sinus ordinata, a kosinus apscisa točke na jediničnoj kružnici, to je slika obje funkcije segment $[-1, 1]$. Funkcije tangens i kotangens mogu poprimiti bilo koju realnu vrijednost (vidite geometrijsko značenje ovih funkcija), pa je njihova slika čitav $\mathbb{R}$.

(iii) Za svaki $x \in \mathbb{R}$, točke $E(x)$ i $E(-x)$ imaju istu apscisu, a ordinate su im suprotne. Zaključujemo da je

$$\cos(-x) = \cos x, \qquad \sin(-x) = -\sin x.$$

Odatle slijedi

$$\begin{aligned} \mathrm{tg}(-x) &= \frac{\sin(-x)}{\cos -x} = \frac{-\sin x}{\cos x} = -\,\mathrm{tg}\, x, \\ \mathrm{ctg}(-x) &= \frac{\cos(-x)}{\sin -x} = \frac{\cos x}{-\sin x} = -\,\mathrm{ctg}\, x. \end{aligned}$$

Dakle, kosinus je parna, a sinus, tangens i kotangens neparne funkcije.

(iv) Iz definicije funkcija sinus i kosinus vidimo da za svaki $x \in \mathbb{R}$ vrijedi

$$\sin(x + 2\pi) = \sin x, \qquad \cos(x + 2\pi) = \cos x.$$

Broj 2π je najmanji pozitivan broj τ za koji je $\sin(x + \tau) = \sin x$ za svaki $x \in \mathbb{R}$. Naime, za $x = 0$ dobivamo $\sin \tau = \sin 0 = 0$, pa je τ nultočka funkcije sinus i stoga oblika $k\pi$ za neki $k \in \mathbb{Z}$. Jedini takav τ sa svojstvom $0 < \tau < 2\pi$ je $\tau = \pi$. Kada bi bilo $\tau = \pi$, tada bismo za $x = \frac{\pi}{2}$ imali $\sin(\frac{\pi}{2} + \pi) = \sin \frac{\pi}{2}$ odnosno $-1 = 1$, što nije. Slično bi se dokazalo i za funkciju kosinus.

Nadalje, iz definicije funkcija tangens i kotangens vidimo da za svaki $x \in \mathbb{R}$ vrijedi

$$\mathrm{tg}(x + \pi) = \mathrm{tg}\, x, \qquad \mathrm{ctg}(x + \pi) = \mathrm{ctg}\, x.$$

Ako je τ pozitivan broj za koji je $\mathrm{tg}(x + \tau) = \mathrm{tg}\, x$ za svaki $x \in \mathbb{R}$, tada je $\mathrm{tg}\, \tau = \mathrm{tg}(0 + \tau) = \mathrm{tg}\, 0 = 0$, pa je $\tau = k\pi$ za neki $k \in \mathbb{Z}$. Najmanji takav τ je upravo π. Slično i za funkciju kotangens. Kod funkcija tangens i kotangens treba voditi računa da im domena nije čitav $\mathbb{R}$, pa treba provjeriti i zahtjev (i) iz definicije 6.1. Znamo da je

$$x \in D(\mathrm{tg}) \implies x + \pi \in D(\mathrm{tg})$$

ekvivalentno sa

$$x + \pi \notin D(\mathrm{tg}) \implies x \notin D(\mathrm{tg}).$$

To je istina jer

$$\begin{aligned} x + \pi \notin D(\mathrm{tg}) \quad &\implies (\exists k \in \mathbb{Z})(x + \pi = \frac{\pi}{2} + k\pi) \\ &\implies (\exists k \in \mathbb{Z})(x = \frac{\pi}{2} + k\pi) \implies x \notin D(\mathrm{tg}). \end{aligned}$$

Analogno za funkciju kotangens.

(v) Iz definicije trigonometrijskih funkcija. □

Periodičke funkcije nisu injekcije: ako je $\tau \neq 0$ period funkcije f, tada za svaki x iz domene funkcije f vrijedi $f(x + \tau) = f(x)$ iako je $x + \tau \neq x$. Dakle, trigonometrijske funkcije nisu injekcije. Međutim, možemo ih suziti tako da dobivena suženja budu injekcije. Sužavamo ih u skladu s tvrdnjom (v) iz teorema 6.2.

Označimo sa

$$\begin{gathered} \mathrm{Sin} : \Big[-\frac{\pi}{2}, \frac{\pi}{2}\Big] \to [-1, 1], \\ \mathrm{Cos} : [0, \pi] \to [-1, 1], \end{gathered}$$

$$\mathrm{Tg} : \left\langle -\frac{\pi}{2}, \frac{\pi}{2}\right\rangle \to \mathbb{R},$$

$$\mathrm{Ctg} : \langle 0, \pi\rangle \to \mathbb{R}$$

redom restrikcije funkcija sinus, kosinus, tangens i kotangens. Ove funkcije su bijekcije, pa svaka od njih ima inverznu funkciju.

Inverzna funkcija funkcije Sin se označava sa arcsin i naziva **arkus sinus**, inverzna funkcija funkcije Cos se označava sa arccos i naziva **arkus kosinus**, inverzna funkcija funkcije Tg se označava sa arctg i naziva **arkus tangens**, a inverzna funkcija funkcije Ctg se označava sa arcctg i naziva **arkus kotangens**. Ove četiri funkcije se jednim imenom zovu **ciklometrijske funkcije**.

Kako su Sin i Tg strogo rastuće funkcije, to su i arcsin i arctg strogo rastuće, a kako su Cos i Ctg strogo padajuće funkcije, to su i arccos i arcctg strogo padajuće. To slijedi iz propozicije 5.7 dokazane u poglavlju 5.

Naglasimo:

$$\arcsin : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right],$$

$$\arccos : [-1, 1] \to [0, \pi],$$

$$\mathrm{arctg} : \mathbb{R} \to \left\langle -\frac{\pi}{2}, \frac{\pi}{2}\right\rangle,$$

$$\mathrm{arcctg} : \mathbb{R} \to \langle 0, \pi\rangle.$$

Uočimo: $\arcsin(\sin x) = x$ za svaki $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, dok je $\sin(\arcsin x) = x$ za svaki $x \in [-1, 1]$. Drugim riječima, funkcije $\arcsin \circ \sin$ i $\sin \circ \arcsin$ su identitete, ali s različitim domenama!

Teorem 6.3. *Vrijede sljedeće adicijske formule:*

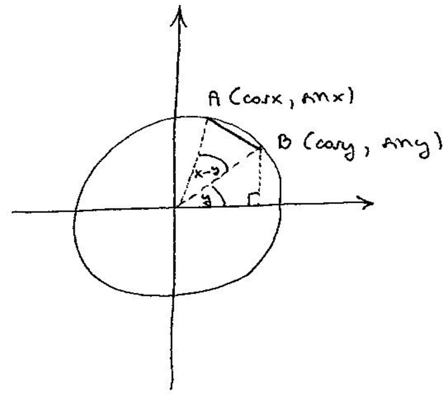
(i) $\cos(x \pm y) = \cos x \cos y \mp \sin x \sin y$,
(ii) $\sin(x \pm y) = \sin x \cos y \pm \cos x \sin y$,
(iii) $\mathrm{tg}(x \pm y) = \frac{\mathrm{tg}\, x \pm \mathrm{tg}\, y}{1 \mp \mathrm{tg}\, x\, \mathrm{tg}\, y}$,
(iv) $\mathrm{ctg}(x \pm y) = \frac{\mathrm{ctg}\, x\, \mathrm{ctg}\, y \mp 1}{\mathrm{ctg}\, y \pm \mathrm{ctg}\, x}$.

Dokaz. Zbog periodičnosti je dovoljno uzeti $x, y \in [0, 2\pi\rangle$. Pretpostavimo da je $x \geq y$. Neka je $A = (\cos x, \sin x)$ i $B = (\cos y, \sin y)$. Tada je

$$|AB|^2 = (\cos x - \cos y)^2 + (\sin x - \sin y)^2.$$

S druge strane, ukoliko zarotiramo os apscisa za kut y, u tom novom koordinatnom sustavu je $A = (\cos(x - y), \sin(x - y))$ i $B = (1, 0)$, pa je

$$|AB|^2 = (\cos(x - y) - 1)^2 + \sin^2(x - y).$$



Slijedi

$$(\cos(x-y)-1)^2+\sin^2(x-y)^2=(\cos x-\cos y)^2+(\sin x-\sin y)^2,$$

odnosno, koristeći $\sin^2 x+\cos^2 x=1$ za svaki $x\in\mathbb{R}$,

$$-2\cos(x-y)+2=2-2\cos x\cos y-2\sin x\sin y$$

odakle zaključujemo

$$\cos(x-y)=\cos x\cos y+\sin x\sin y.$$

Ukoliko umjesto y stavimo $-y$ i iskoristimo parnost funkcije kosinus i neparnost funkcije sinus, dobivamo

$$\cos(x+y)=\cos x\cos y-\sin x\sin y.$$

Slično se dokazuju i ostale formule. □

Zadatak 6.4. *Dokažite sljedeće formule za dvostruke kutove:*

(i) $\cos 2x=\cos^2 x-\sin^2 x=2\cos^2 x-1=1-2\sin^2 x$,
(ii) $\sin 2x=2\sin x\cos x$,
(iii) $\operatorname{tg} 2x=\frac{2\operatorname{tg} x}{1-\operatorname{tg}^2 x}$,
(iv) $\operatorname{ctg} 2x=\frac{\operatorname{ctg}^2 x-1}{2\operatorname{ctg} x}$.

Zadatak 6.5. *Dokažite sljedeće formule za polovične kutove:*

(i) $\cos x=\cos^2\frac{x}{2}-\sin^2\frac{x}{2}=2\cos^2\frac{x}{2}-1=1-2\sin^2\frac{x}{2}$,
(ii) $\sin x=2\sin\frac{x}{2}\cos\frac{x}{2}$,
(iii) $\operatorname{tg} x=\frac{2\operatorname{tg}\frac{x}{2}}{1-\operatorname{tg}^2\frac{x}{2}}$,
(iv) $\operatorname{ctg} x=\frac{\operatorname{ctg}^2\frac{x}{2}-1}{2\operatorname{ctg}\frac{x}{2}}$.

Zadatak 6.6. *Dokažite sljedeće formule redukcije*

$$\cos\left(\frac{\pi}{2}+x\right) = -\sin x, \qquad \sin\left(\frac{\pi}{2}+x\right) = \cos x$$

i formule komplementiranja

$$\cos\left(\frac{\pi}{2}-x\right) = \sin x, \qquad \sin\left(\frac{\pi}{2}-x\right) = \cos x$$

te ih komentirajte na trigonometrijskoj kružnici. Također, izvedite formule redukcije i komplementiranja za tangens i kotangens.

Teorem 6.7. *Vrijede sljedeće formule za pretvaranje produkta u sumu trigonometrijskih funkcija:*

(i) $\sin x \cos y = \frac{1}{2}\big(\sin(x+y)+\sin(x-y)\big)$,
(ii) $\sin x \sin y = \frac{1}{2}\big(\cos(x-y)-\cos(x+y)\big)$,
(iii) $\cos x \cos y = \frac{1}{2}\big(\cos(x-y)+\cos(x+y)\big)$.

Dokaz. Zbrajanjem obiju formula iz tvrdnje (ii) teorema 6.3 dobije se formula u (i), a analogno bi se dobile i ostale. □

Teorem 6.8. *Vrijede sljedeće formule za pretvaranje sume i razlike kosinusa odnosno sinusa u produkt:*

(i) $\cos x + \cos y = 2\cos\frac{x+y}{2}\cos\frac{x-y}{2}$,
(ii) $\cos x - \cos y = -2\sin\frac{x+y}{2}\sin\frac{x-y}{2}$,
(iii) $\sin x + \sin y = 2\sin\frac{x+y}{2}\cos\frac{x-y}{2}$,
(iv) $\sin x - \sin y = 2\sin\frac{x-y}{2}\cos\frac{x+y}{2}$.

Dokaz. Stavimo $z = \frac{x+y}{2}$ i $w = \frac{x-y}{2}$. Tada je $x = z + w$ i $y = z - w$, pa imamo

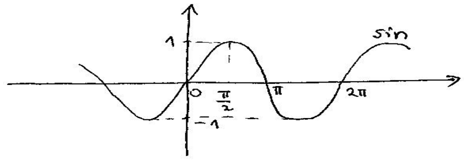
$$\begin{aligned} &\cos x + \cos y = \cos(z+w) + \cos(z-w) \\ = \;& (\cos z\cos w - \sin z \sin w) + (\cos z \cos w + \sin z \sin w) \\ = \;& 2\cos z\cos w = 2\cos\frac{x+y}{2}\cos\frac{x-y}{2}. \end{aligned}$$

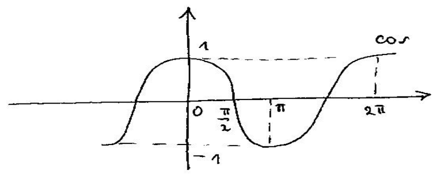
Analogno se izvode i ostale formule. □

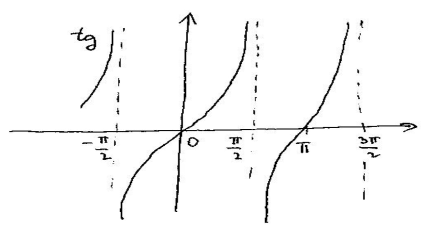
Zadatak 6.9. *Dokazati sljedeće formule za sumu i razliku tangensa i kotangensa:*

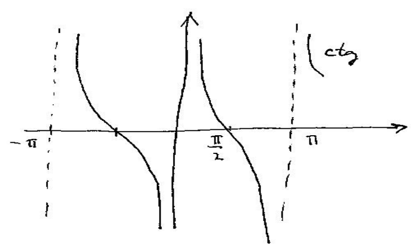
(i) $\operatorname{tg} x \pm \operatorname{tg} y = \frac{\sin(x\pm y)}{\cos x\cos y}$,
(ii) $\operatorname{ctg} x \pm \operatorname{ctg} y = \pm\frac{\sin(x\pm y)}{\sin x\sin y}$,
(iii) $\operatorname{tg} x + \operatorname{ctg} y = \frac{\cos(x-y)}{\cos x\sin y}$,
(iv) $\operatorname{ctg} x - \operatorname{tg} y = \frac{\cos(x+y)}{\sin x\cos y}$.

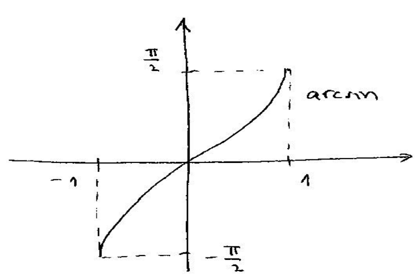
Grafovi trigonometrijskih i ciklometrijskih funkcija. Zbog periodičnosti je dovoljno znati skicirati grafove funkcija sin i cos na $[0, 2\pi]$, a tg i ctg na $[0,\pi]$. No, zahvaljujući formulama redukcije i komplementiranja, trigonometrijske funkcije je dovoljno znati skicirati na $\left[0, \frac{\pi}{2}\right]$.

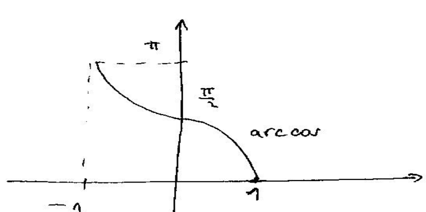

sin
1
0
$\frac{\pi}{2}$
π
2π
-1

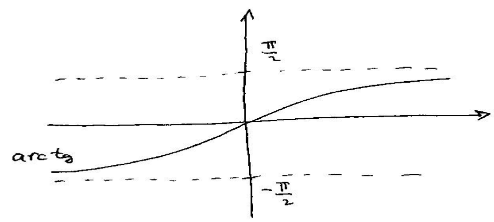

cos
1
0
$\frac{\pi}{2}$
π
2π
-1

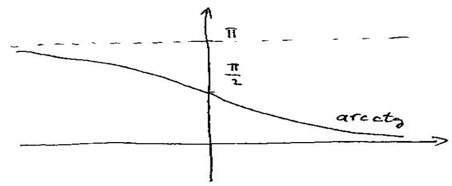

tg
$-\frac{\pi}{2}$
0
$\frac{\pi}{2}$
π
$\frac{3\pi}{2}$


ctg
$-\pi$
$\frac{\pi}{2}$
π


$\frac{\pi}{2}$
arcsin
-1
1
$-\frac{\pi}{2}$

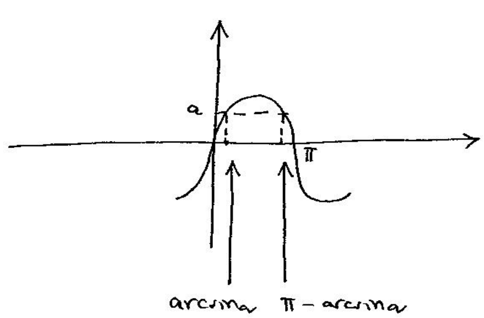

π
$\frac{\pi}{2}$
arccos
-1
1

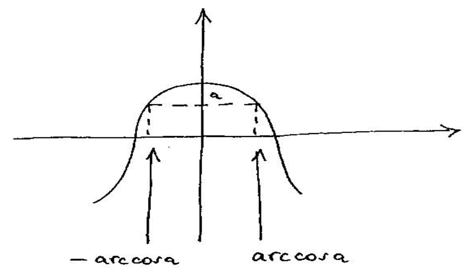




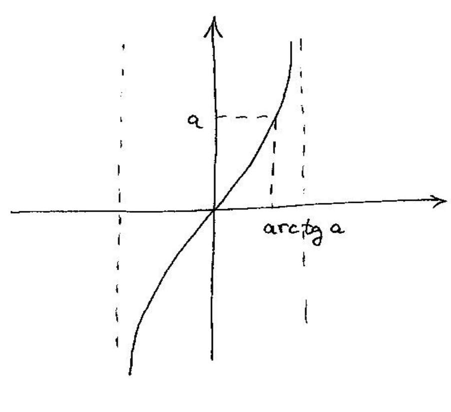
Trigonometrijske jednadžbe i nejednadžbe. Ideja je svesti trigonometrijsku jednadžbu na neki od oblika: $\sin x = a$, $\cos x = a$, $\operatorname{tg} x = a$, $\operatorname{ctg} x = a$. Odmah uočavamo da jednadžbe $\sin x = a$ i $\cos x = a$ nemaju rješenja ako je $a < -1$ ili $a > 1$ (tj. ako je $|\,a\,| > 1$). Jednadžbe $\operatorname{tg} x = a$ i $\operatorname{ctg} x = a$ imaju rješenje za svaki $a \in \mathbb{R}$.

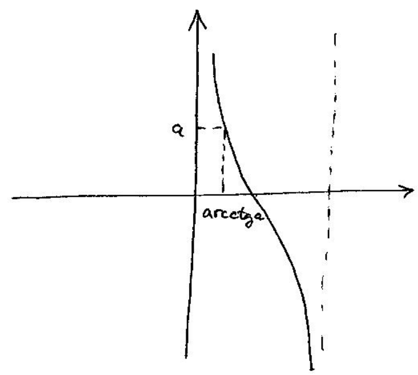
Ako je $-1 \leq a \leq 1$, rješenje jednadžbe $\sin x = a$ je $x = (-1)^k \arcsin a + k\pi, k \in \mathbb{Z}$, a rješenje jednadžbe $\cos x = a$ je $x = \pm \arccos a + 2k\pi, k \in \mathbb{Z}$.





Rješenje jednadžbe $\operatorname{tg} x = a$ je $x = \operatorname{arctg} a + k\pi, k \in \mathbb{Z}$, a jednadžbe $\operatorname{ctg} x = a$ je $x = \operatorname{arcctg} a + k\pi, k \in \mathbb{Z}$.





Primjer 6.10. *Riješimo jednadžbu*

$$\cos\frac{x}{2} = 1 + \cos x.$$

Uočimo da je desna strana jednadžbe jednaka $2\cos^2\frac{x}{2}$, *pa se jednadžba svodi na*

$$2\cos^2\frac{x}{2} - \cos\frac{x}{2} = 0$$

odnosno na

$$\cos\frac{x}{2}\big(2\cos\frac{x}{2} - 1\big) = 0.$$

Ako je $\cos\frac{x}{2} = 0$, *tada je* $\frac{x}{2} = \frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$, *tj.* $x = \pi + 2k\pi$, $k \in \mathbb{Z}$.

Ako je $2\cos\frac{x}{2} - 1 = 0$, *tada je* $\cos\frac{x}{2} = \frac{1}{2}$, *pa je* $\frac{x}{2} = \pm\arccos\frac{1}{2} + 2l\pi = \pm\frac{\pi}{3} + 2l\pi$ *i konačno* $x = \pm\frac{2\pi}{3} + 4l\pi$, $l \in \mathbb{Z}$.

Zadatak 6.11. *Riješite jednadžbe:*

(i) $2\sin^2 x = \cos 4x + 2$,
(ii) $(\operatorname{tg}^2 x + 1)(\sin 2x + 1) = 1$,
(iii) $\operatorname{tg} x + 2\operatorname{ctg} x = 3$,
(iv) $\sin x + \sin 2x + \sin 3x = 0$,
(v) $\cos x + 2 = 2\operatorname{tg}\frac{x}{2}$.

Kao i rješavanje trigonometrijskih jednadžbi, rješavanje trigonometrijskih nejednadžbi se svodi na rješavanje onih elementarnih. Elementarne trigonometrijske nejednadžbe su oblika

$$f(x) > a \quad \text{ili} \quad f(x) < a,$$

gdje je $a \in \mathbb{R}$, a f trigonometrijska funkcija. U rješavanju elementarnih trigonometrijskih nejednadžbi nam pomažu grafovi trigonometrijskih funkcija ili trigonometrijska kružnica.

Primjer 6.12. *Riješimo nejednadžbu*

$$\cos^2 x < \frac{1}{2}.$$

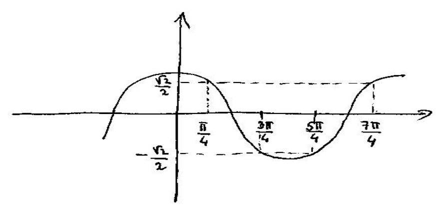
Dovoljno je ovu nejednadžbu riješiti za $x \in [0, 2\pi]$. *Nejednadžbu* $\cos^2 x < \frac{1}{2}$ *možemo zapisati u obliku*

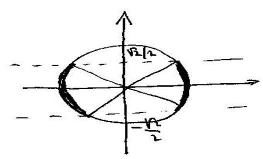
$$-\frac{\sqrt{2}}{2} < \cos x < \frac{\sqrt{2}}{2}.$$

Uočimo da se u ovom slučaju zapravo u zadanoj nejednadžbi krije jedan sustav koji se sastoji od dvije trigonometrijske nejednadžbe:

$$\cos x > -\frac{\sqrt{2}}{2}, \qquad \cos x < \frac{\sqrt{2}}{2}.$$

Sada promotrimo graf funkcije kosinus ili trigonometrijsku kružnicu.





Zaključujemo: $x \in \left\langle \frac{\pi}{4}, \frac{3\pi}{4} \right\rangle \cup \left\langle \frac{5\pi}{4}, \frac{7\pi}{4} \right\rangle$, *pa je konačno rješenje*

$$x \in \cup_{k\in\mathbb{Z}} \left(\left\langle \frac{\pi}{4} + 2k\pi, \frac{3\pi}{4} + 2k\pi \right\rangle \cup \left\langle \frac{5\pi}{4} + 2k\pi, \frac{7\pi}{4} + 2k\pi \right\rangle \right)$$

što se kraće može zapisati kao

$$x \in \cup_{k\in\mathbb{Z}} \left(\left\langle \frac{\pi}{4} + k\pi, \frac{3\pi}{4} + k\pi \right\rangle \right).$$

Zadatak 6.13. *Riješite nejednadžbe:*

(i) $2|\sin x| - 1 > 0$,
(ii) $\cos 2x > \sin x$,
(iii) $\operatorname{tg} x > \operatorname{tg} \frac{x}{3}$,
(iv) $\sin x + \cos^2 x \leq 1$,
(v) $\operatorname{ctg}\left(3x - \frac{\pi}{3}\right) \geq 1$.

8. **Hiperbolne i area funkcije.** Hiperbolne funkcije definiraju se redom na sljedeći način:

Sinus hiperbolni $\operatorname{sh} : \mathbb{R} \to \mathbb{R}$ definiran je sa

$$\operatorname{sh} x = \frac{e^x - e^{-x}}{2}, \quad \forall x \in \mathbb{R}.$$

Kosinus hiperbolni $\operatorname{ch} : \mathbb{R} \to \mathbb{R}$ definiran je sa

$$\operatorname{ch} x = \frac{e^x + e^{-x}}{2}, \quad \forall x \in \mathbb{R}.$$

Tangens hiperbolni $\operatorname{th} : \mathbb{R} \to \mathbb{R}$ definiran je sa

$$\operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x}, \quad \forall x \in \mathbb{R}.$$

Uočimo da kosinus hiperbolni nema nultočaka jer je

$$\operatorname{ch} x = \frac{e^x + e^{-x}}{2} > 0, \quad \forall x \in \mathbb{R}.$$

Zato je domena tangensa hiperbolnog cijeli $\mathbb{R}$. S druge strane, jedina nultočka sinusa hiperbolnog je $x = 0$. Zaista, imamo

$$\operatorname{sh}(x) = 0 \iff \frac{e^x - e^{-x}}{2} = 0 \iff e^{2x} = 1 \iff x = 0.$$

Zato je domena sljedeće funkcije $\mathbb{R} \setminus \{0\}$:

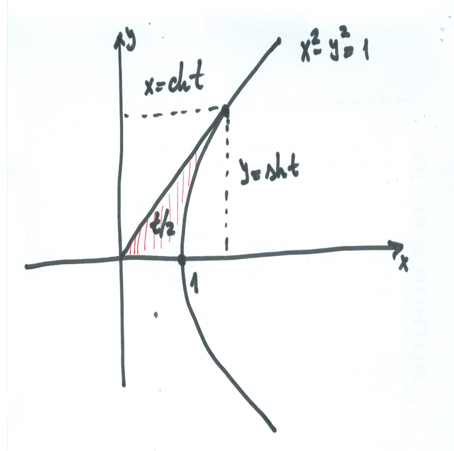
Kotangens hiperbolni $\operatorname{cth} : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ definiran je sa

$$\operatorname{cth} x = \frac{\operatorname{ch} x}{\operatorname{sh} x}, \quad \forall x \in \mathbb{R} \setminus \{0\}.$$

Zadatak 6.14. *Koristeći gornje definicije, dokažite ove identitete:*

$$\begin{aligned}
&\operatorname{sh}(-x) = -\operatorname{sh} x, && \operatorname{ch}(-x) = \operatorname{ch} x,\\
&\operatorname{th}(-x) = -\operatorname{th} x, && \operatorname{cth} x = -\operatorname{cth} x,\\
&\operatorname{sh}(x+y) = \operatorname{sh} x \operatorname{ch} y + \operatorname{ch} x \operatorname{sh} y, && \operatorname{ch}(x+y) = \operatorname{ch} x \operatorname{ch} y + \operatorname{sh} x \operatorname{sh} y,\\
&\operatorname{sh}(x-y) = \operatorname{sh} x \operatorname{ch} y - \operatorname{ch} x \operatorname{sh} y, && \operatorname{ch}(x-y) = \operatorname{ch} x \operatorname{ch} y - \operatorname{sh} x \operatorname{sh} y,\\
&\operatorname{th}(x+y) = \frac{\operatorname{th} x + \operatorname{th} y}{1 + \operatorname{th} x \operatorname{th} y}, && \operatorname{th}(x-y) = \frac{\operatorname{th} x - \operatorname{th} y}{1 - \operatorname{th} x \operatorname{th} y},\\
&\operatorname{sh} 2x = 2 \operatorname{sh} x \operatorname{ch} x, && \operatorname{ch} 2x = \operatorname{ch}^2 x + \operatorname{sh}^2 x,\\
&\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1.
\end{aligned}$$

Usporedite ove identitete s onima za sinus i kosinus. Uočite razlike u formulama. Naziv hiperbolne funkcije dolazi od toga što je $x = \operatorname{ch} t$ i $y = \operatorname{sh} t$, $t \in \mathbb{R}$, parametarski prikaz dijela istostrane hiperbole $x^2 - y^2 = 1$, koja se nalazi desno od osi y.



Prisjetimo se da je $x = \cos t$ i $y = \sin t$, $t \in [0, 2\pi\rangle$, parametarski prikaz jedinične kružnice $x^2 + y^2 = 1$.

Zadatak 6.15. *Koristeći zadatak 6.14, dokažite ove idenititete*

$$\begin{aligned} \operatorname{sh} x \operatorname{sh} y &= \frac{1}{2} \left[\operatorname{ch}(x+y) - \operatorname{ch}(x-y) \right], \\ \operatorname{ch} x \operatorname{ch} y &= \frac{1}{2} \left[\operatorname{ch}(x+y) + \operatorname{ch}(x-y) \right], \\ \operatorname{sh} x \operatorname{ch} y &= \frac{1}{2} \left[\operatorname{sh}(x+y) + \operatorname{sh}(x-y) \right]. \end{aligned}$$

Teorem 6.16. *Funkcije* sh, th *i* cth *su neparne, a* ch *je parna. Nadalje, imamo*

(i) sh *i* th *strogo rastu na* $\mathbb{R}$. *Za* $x > 0$ *vrijedi* $\operatorname{sh} x > 0$ *i* $\operatorname{th} x > 0$.
(ii) *Za svaki* $x \in \mathbb{R}$ *vrijedi* $\operatorname{ch}(x) \geq 1$. *Funkcija* ch *strogo pada na* $\langle -\infty, 0]$, *a strogo raste na* $[0, \infty\rangle$.
(iii) *Funkcija* cth *strogo pada na* $\langle -\infty, 0\rangle$ *i na* $\langle 0, +\infty\rangle$.

Dokaz. Zadatak 6.14 pokazuje da su funkcije sinus hiperbolni, tangens hiperbolni i kotangens hiperbolni neparne, a kosinus hiperbolni je parna funkcija. Dokažimo (i). Uočimo da možemo pisati

$$e^{-x} = \left(\frac{1}{e} \right)^x,$$

te da je $1/e < 1$. Prema teoremu 5.24, funkcija $x \mapsto e^{-x}$ strogo pada. Dakle, $x \mapsto -e^{-x}$ strogo raste. Kako i $x \mapsto e^x$ strogo raste, zbog

$$\operatorname{sh} x = \frac{e^x - e^{-x}}{2},$$

sh je suma dvije strogo rastuće funkcije te zato strogo raste. Posebno, za $x > 0$ imamo

$$\operatorname{sh} x > \operatorname{sh} 0 = 0.$$

Ovo dokazuje (i) za sinus hiperbolni. Dokažimo strogi rast za th. Za $x_1 < x_2$ imamo

$$\begin{aligned}\operatorname{th} x_2 - \operatorname{th} x_1 &= \frac{\operatorname{sh} x_1}{\operatorname{ch} x_1} - \frac{\operatorname{sh} x_2}{\operatorname{ch} x_2} = \frac{\operatorname{sh} x_1 \operatorname{ch} x_2 - \operatorname{ch} x_1 \operatorname{sh} x_2}{\operatorname{ch} x_1 \operatorname{ch} x_2} \\ &= \frac{\operatorname{sh}(x_2 - x_1)}{\operatorname{ch}(x_1)\operatorname{ch}(x_2)} > 0\end{aligned}$$

koristeći zadatak 6.14 i činjenicu da

$$x_1 < x_2 \implies x_2 - x_1 > 0 \implies \operatorname{sh}(x_2 - x_1) > \operatorname{sh} 0 = 0,$$

te da su vrijednosti kosinusa hiperbolnog uvijek pozitivne. Ovim je (i) dokazano.

Kako je $\operatorname{ch} x > 0$ za svaki x, prema zadatku 6.14 vrijedi

$$\operatorname{ch}(x) = \sqrt{1 + \operatorname{sh}^2(x)} \geq 1.$$

Kako prema (i) imamo $\operatorname{sh} x \geq \operatorname{sh} 0 = 0$ za svaki $x \geq 0$, to zaključujemo da $\operatorname{sh}^2 x$ strogo raste na $[0, \infty\rangle$. Dakle,

$$\operatorname{ch}(x) = \sqrt{1 + \operatorname{sh}^2(x)}$$

strogo raste na $[0, +\infty\rangle$. Kako je ch parna funkcija, odatle odmah slijedi da ch strogo pada na $\langle -\infty, 0]$. Ovim je (ii) dokazano.

Za dokaz tvrdnje (iii) uočimo da je

$$\operatorname{cth} x = \frac{1}{\operatorname{th} x}.$$

Tvrdnja sada slijedi iz (i), detalje ostavljamo čitatelju. □

Propozicija 6.17. *Slika funkcije* sh *je* $\mathbb{R}$. *Sinus hiperbolni je strogo rastuća bijekcija sa* $\mathbb{R}$ *na* $\mathbb{R}$. *Inverzna funkcija naziva se* ***area sinus hiperbolni*** *i dana je sa*

$$\operatorname{Arsh} x = \ln(x + \sqrt{x^2 + 1}).$$

Dokaz. Sinus hiperbolni je strogo rastuća bijekcija prema prethodnom teoremu. Posebno, zato je injekcija. Neka je $y \in \mathbb{R}$. Dokazat ćemo da jednadžba

$$y = \operatorname{sh} x = \frac{e^x - e^{-x}}{2}$$

ima jedinstveno rješenje po x. To će dokazivati surjektivnost i dati formulu za inverznu funkciju. Stavimo $t = e^x$. Onda gornja jednadžba postaje

$$\frac{t - t^{-1}}{2} = y \iff t^2 - 2yt - 1 = 0.$$

Odatle rješavanjem kvadratne jednadžbe dobivamo

$$t = y \pm \sqrt{y^2 + 1},$$

pa je

$$e^x = y \pm \sqrt{y^2 + 1}.$$

Međutim, $e^x > 0$, pa mora biti

$$e^x = y + \sqrt{y^2 + 1} \implies x = \ln(y + \sqrt{y^2 + 1}).$$

Zamjenom mjesta x i y nalazimo formulu za inverznu funkciju. □

Propozicija 6.18. *Slika funkcije* ch *je* $[1, \infty\rangle$. *Restrikcija kosinusa hiperbolnog, u oznaci* Ch, *na* $[0, \infty\rangle$ *je strogo rastuća bijekcija na* $[1, \infty\rangle$. *Inverz te restrikcije naziva se* ***area kosinus hiperbolni*** *i dan je sa*

$$\operatorname{Arch} x = \ln\left(x + \sqrt{x^2 - 1}\right).$$

Dokaz. Slično prethodnoj propoziciji. Samo računamo inverz (i dokazujemo da je Ch surjekcija sa $[0, \infty\rangle$ na $[1, \infty\rangle$).

Neka je $y \in [1, \infty\rangle$. Dokazat ćemo da jednadžba

$$y = \operatorname{ch} x = \frac{e^x + e^{-x}}{2},$$

ima jedinstveno rješenje po $x \geq 0$. Stavimo $t = e^x$. Onda gornja jednadžba postaje

$$\frac{t + t^{-1}}{2} = y \iff t^2 - 2yt + 1 = 0.$$

Odatle rješavanjem kvadratne jednadžbe zaključujemo

$$e^x = y \pm \sqrt{y^2 - 1}.$$

Međutim, $e^x \geq e^0 = 1$, pa mora biti

$$e^x = y + \sqrt{y^2 - 1} \implies x = \ln\left(y + \sqrt{y^2 - 1}\right).$$

Zamjenom mjesta x i y nalazimo formulu za inverznu funkciju. □

Zadatak 6.19. *Slika funkcije* th *je* $\langle -1, 1\rangle$. *Tangens hiperbolni je strogo rastuća bijekcija sa* $\mathbb{R}$ *na* $\langle -1, 1\rangle$. *Inverzna funkcija naziva se* ***area tangens hiperbolni*** *i dana je sa*

$$\operatorname{Arth} x = \frac{1}{2} \ln \frac{1 + x}{1 - x}.$$

Uputa. Koristeći formulu

$$\operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x} = \frac{e^x - e^{-x}}{e^x + e^{-x}},$$

izračunamo e^x kao u prehodnim zadacima. □

Zadatak 6.20. *Slika funkcije* cth *je* $\langle -\infty, -1\rangle \cup \langle 1, \infty\rangle$. *Restrikcija kotangensa hiperbolnog, u oznaci* Cth, *na* $\langle 0, \infty\rangle$ *je strogo padajuća bijekcija na* $\langle 1, \infty\rangle$. *Inverzna funkcija naziva se* ***area kotangens hiperbolni*** *i dana je sa*

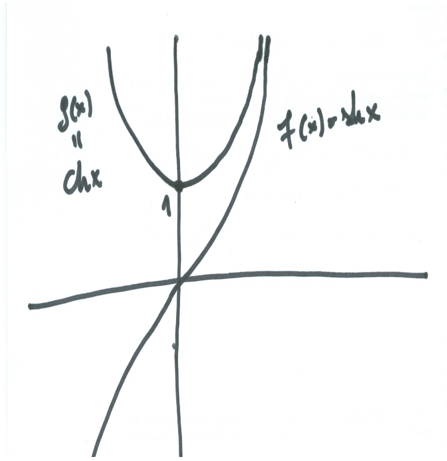
$$\operatorname{Arcth} x = \frac{1}{2} \ln \frac{x + 1}{x - 1}.$$

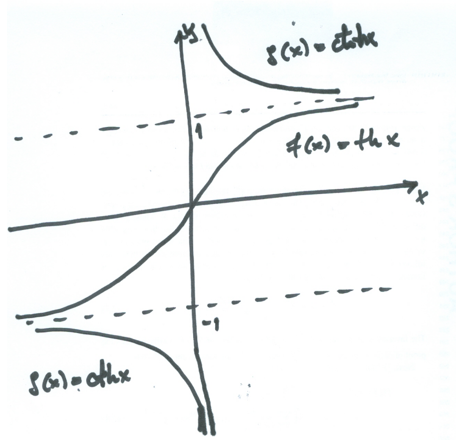
Uputa. Koristite prethodni zadatak i formulu

$$\operatorname{cth} x = \frac{1}{\operatorname{th} x}.$$

□

Naziv area funkcije dolazi od intepretacije parametra t kao polovice površine označene na prethodnoj slici. Grafovi hiperbolnih funkcija su sljedeći.


g(x) = ch x
f(x) = sh x
1


y
g(x) = cth x
1
f(x) = th x
x
-1
g(x) = cth x

7. Ekvipotentni skupovi

Definicija 7.1. *Neka je $f : D \to K$ preslikavanje. Za f kažemo da je* ***injekcija (injektivno preslikavanje)*** *ako*

$$(\forall x_1, x_2 \in D)(x_1 \neq x_2 \implies f(x_1) \neq f(x_2)).$$

Za f kažemo da je ***surjekcija (surjektivno preslikavanje)*** *ako*

$$(\forall y \in K)(\exists x \in D)(y = f(x)).$$

Za f kažemo da je ***bijekcija (bijektivno preslikavanje)*** *ako je i injekcija i surjekcija.*

Dakle, f je injekcija ako različite elemente domene preslikava u različite elemente kodomene. Obzirom na nepraktičnost ove definicije (jer najčešće nismo u stanju gledati sve različite mogućnosti), koristit ćemo ekvivalentnu definiciju injekcije dobivenu obratom po kontrapoziciji:

$$(\forall x_1, x_2 \in D)(f(x_1) = f(x_2) \implies x_1 = x_2).$$

Preslikavanja koja nisu injekcije imaju restrikcije koje su injekcije (uz izbor odgovarajućeg podskupa domene).

Ispitivanje surjektivnosti preslikavanja f se svodi na rješavanje jednadžbe $y = f(x)$. Uočimo da je preslikavanje f surjekcija ako i samo ako ima svojstvo da mu je slika jednaka kodomeni. Zato se često za surjektivno preslikavanje $f : D \to K$ kaže da je preslikavanje sa D **na** K. Svako preslikavanje postaje surjekcija ako za njegovu kodomenu uzmemo sliku tog preslikavanja. Međutim, sliku nekog preslikavanja obično nije lako odrediti.

Ako je $f : D \to K$ bijekcija, tada

$$(\forall y \in K)(\exists!\, x \in D)(y = f(x)).$$

Naime, kako je f surjekcija, takav x postoji, a kako je i injekcija, takav x je jedinstven.

Primjer 7.2. *Neka je $f : \mathbb{R} \to \mathbb{R}$ preslikavanje zadano formulom $f(x) = 2x + 1$. Najprije ispitajmo injektivnost preslikavanja f:*

$$f(x_1) = f(x_2) \implies 2x_1 + 1 = 2x_2 + 1 \implies 2x_1 = 2x_2 \implies x_1 = x_2.$$

Sada ispitajmo surjektivnost preslikavanja f. Uzmimo $y \in \mathbb{R}$ i pokušajmo riješiti jednadžbu $y = 2x + 1$. Imamo:

$$y = 2x + 1 \implies 2x = y - 1 \implies x = \frac{1}{2}(y - 1).$$

Vidimo da smo jednadžbu $y = 2x + 1$ mogli riješiti po x. Znači da za svaki $y \in \mathbb{R}$ postoji $x = \frac{1}{2}(y - 1) \in \mathbb{R}$ takav da je $f(x) = y$. Zaključujemo da je f surjekcija.

Prema tome, preslikavanje $f : \mathbb{R} \to \mathbb{R}$ definirano sa $f(x) = 2x+1$ je bijekcija.

Kako dokazati da neko preslikavanje nije injekcija odnosno nije surjekcija? Za opovrgavanje injektivnosti treba negirati sud

$$(\forall x_1, x_2 \in D)(x_1 \neq x_2 \implies f(x_1) \neq f(x_2)).$$

Negacijom se dobije sud

$$(\exists x_1, x_2 \in D)(x_1 \neq x_2 \ \& \ f(x_1) = f(x_2)).$$

Za opovrgavanje surjektivnosti negiramo sud

$$(\forall y \in K)(\exists x \in D)(y = f(x))$$

i dobivamo

$$(\exists y \in K)(\forall x \in D)(y \neq f(x)).$$

Primjer 7.3. *Neka je $f : \mathbb{R} \to \mathbb{R}$ preslikavanje zadano formulom $f(x) = x^2$. Kako je $f(1) = 1 = f(-1)$, preslikavanje f nije injekcija. Kako za $-1 \in \mathbb{R}$ jednadžba $-1 = x^2$ tj. $x^2 + 1 = 0$ nema rješenje u $\mathbb{R}$, to f nije niti surjekcija.*

Međutim, ako promatramo preslikavanje g zadano istom formulom, tj. sa $g(x) = x^2$, ali za domenu i kodomenu tog preslikavanja uzmemo $[0, +\infty\rangle$, dobili smo bijekciju (to će slijediti iz teorema 10.4).

Neka je $f : D \to K$ bijekcija. Definirajmo funkciju $g : K \to D$ sa $g(y) = x$ ako je $y = f(x)$. Uočimo da je definicija dobra jer za svaki $y \in K$ postoji jedinstven $x \in D$ takav da je $y = f(x)$, obzirom da je f bijekcija. Takvo preslikavanje g se naziva **inverzno preslikavanje** preslikavanja f i označava sa f^{-1}.

Uočimo: $f^{-1}(y) = x \Longleftrightarrow y = f(x)$.

U 4. poglavlju smo napomenuli da se oznaka f^{-1} koristi i za prasliku i za inverznu funkciju, pa je potreban oprez (praslika je skup, a inverzna funkcija je funkcija). Međutim, ako je f bijekcija, tada je praslika jednočlanog skupa također jednočlan skup i vrijedi

$$f^{-1}(\{y\}) = \{x\} \iff f(x) = y \iff f^{-1}(y) = x.$$

Propozicija 7.4. *Ako je $f : D \to K$ bijekcija, tada je i $f^{-1} : K \to D$ bijekcija.*

Dokaz. Neka su $y_1, y_2 \in K$ takvi da je $f^{-1}(y_1) = f^{-1}(y_2)$. Neka je $x_1 = f^{-1}(y_1)$ i $x_2 = f^{-1}(y_2)$. Znači da je $y_1 = f(x_1)$ i $y_2 = f(x_2)$. Obzirom da je $f^{-1}(y_1) = f^{-1}(y_2)$, imamo $x_1 = x_2$, pa je $f(x_1) = f(x_2)$ odnosno $y_1 = y_2$. Dakle, f je injekcija.

Neka je $x \in D$ zadan. Stavimo $y = f(x) \in K$. Tada je $f^{-1}(x) = y$. Dakle, postoji $y \in K$ takav da je $f^{-1}(x) = y$, pa je f surjekcija.

Dakle, f je bijekcija. □

Prisjetimo se da je identiteta na nepraznom skupu D preslikavanje $1_D : x \mapsto x$.

Sljedeća propozicija je očigledna:

Propozicija 7.5. *Neka je D neprazan skup. Preslikavanje $1_D : D \to D$ je bijekcija i samo sebi inverzno preslikavanje.*

Sada ćemo dokazati neka važna svojstva bijektivnih funkcija.

Teorem 7.6. *Neka su $f : D \to K$ i $g : K \to L$ bijekcije. Tada vrijede sljedeće tvrdnje:*

(i) $g \circ f : D \to L$ *je bijekcija,*
(ii) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$,
(iii) $f^{-1} \circ f = 1_D$,
(iv) $f \circ f^{-1} = 1_K$.

Dokaz. (i) Stavimo $h = g \circ f : D \to L$.

Neka su $x_1, x_2 \in D$ takvi da je $h(x_1) = h(x_2)$. To znači da je $g\big(f(x_1)\big) = g\big(f(x_2)\big)$. Kako je g injekcija, odatle slijedi $f(x_1) = f(x_2)$, a kako je i f injekcija, zaključujemo $x_1 = x_2$. Dakle, h je injekcija.

Neka je $z \in L$ zadan. Kako je g surjekcija, to postoji $y \in K$ takav da je $g(y) = z$. No i f je surjekcija, pa za $y \in K$ postoji $x \in D$ takav da je $f(x) = y$. Sada je $g\big(f(x)\big) = g(y) = z$ tj. $h(x) = z$. Dakle, h je surjekcija.

(ii) Stavimo $h = g \circ f : D \to L$.

Neka je $z \in L$ te neka je $y = g^{-1}(z) \in K$ i $x = f^{-1}(y) \in D$. Imamo:

$$(f^{-1} \circ g^{-1})(z) = f^{-1}\big(g^{-1}(z)\big) = f^{-1}(y) = x.$$

Međutim,

$$y = g^{-1}(z) \Longleftrightarrow g(y) = z \quad \text{i} \quad x = f^{-1}(y) \Longleftrightarrow f(x) = y.$$

Odatle je

$$h(x) = (g \circ f)(x) = g\big(f(x)\big) = g(y) = z,$$

pa je

$$x = h^{-1}(z).$$

Slijedi $(f^{-1} \circ g^{-1})(z) = h^{-1}(z)$ za svaki $z \in L$. Dakle, $f^{-1} \circ g^{-1} = h^{-1}$.

(iii) Neka je $x \in D$ te neka je $y = f(x)$. Znači da je $x = f^{-1}(y)$. Sada imamo

$$(f^{-1} \circ f)(x) = f^{-1}\big(f(x)\big) = f^{-1}(y) = x = 1_D(x).$$

Kako ova jednakost vrijedi za svaki $x \in D$, to je $f^{-1} \circ f = 1_D$.

(iv) Neka je $y \in K$ te neka je $x = f^{-1}(y)$. Znači da je $y = f(x)$, pa imamo

$$(f \circ f^{-1})(y) = f\big(f^{-1}(y)\big) = f(x) = y = 1_K(y).$$

Obzirom da to vrijedi za svaki $y \in K$, zaključujemo $f \circ f^{-1} = 1_K$. □

Naglasimo da je $f^{-1} \circ f : D \to D$, a $f \circ f^{-1} : K \to K$. Iako su oba preslikavanja identitete, općenito imaju različite domene / kodomene, pa se radi o različitim preslikavanjima (osim, naravno, ako je $D = K$).

Definicija 7.7. *Neka je S neprazan skup.* ***Permutacija skupa*** *S je svaka bijekcija $f : S \to S$.*

Iz propozicije 7.4, propozicije 7.5 i teorema 7.6 odmah slijedi:

Korolar 7.8. *Neka je S neprazan skup. Tada vrijede sljedeće tvrdnje:*

(i) *ako je f permutacija skupa S, tada je i f^{-1} permutacija skupa S,*
(ii) *1_S je permutacija skupa S,*
(iii) *ako su f i g permutacije skupa S, tada je i $g \circ f$ permutacija skupa S.*

Ponekad permutacije skupa označavamo i grčkim slovima σ, τ, σ_1, σ_2, $\dots$, τ_1, τ_2, $\dots$

Definicija 7.9. *Neka je $n \in \mathbb{N}$. Sa S_n označavamo skup svih permutacija skupa $\{1, 2, \dots, n\}$.*

Drugim riječima, S_n je skup svih bijekcija sa skupa prvih n prirodnih brojeva na njega samog.

Primjer 7.10. (a) *Za $n = 1$ promotrimo sve moguće permutacije skupa $\{1\}$, dakle sva moguća bijektivna preslikavanja $\sigma : \{1\} \to \{1\}$. Imamo samo jednu mogućnost: $\sigma(1) = 1$, pa pišemo:*

$$\sigma_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Općenito, u prvom retku popisujemo redom sve elemente skupa $\{1, 2, \dots, n\}$, a ispod svakog od njih bilježimo pripadnu vrijednost koju mu pridružuje bijekcija σ. Prema tome, gornji zapis zapravo znači $\sigma(1) = 1$.

(b) *U slučaju $n = 2$ promatramo sve permutacije skupa $\{1, 2\}$, tj. sva bijektivna preslikavanja $\sigma : \{1, 2\} \to \{1, 2\}$. Ovdje imamo više mogućnosti.*

Prvi slučaj: $\sigma(1) = 1$, $\sigma(2) = 2$. Tako dobivamo permutaciju

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}.$$

Drugi slučaj: $\sigma(1) = 2$, $\sigma(2) = 1$. Imamo permutaciju:

$$\sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

(c) *Za $n = 3$ gledamo sve permutacije skupa $\{1, 2, 3\}$:*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \dots$$

Uočimo:

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2,$$

$$\sigma_2 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_3,$$

$$\sigma_3 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2,$$

$$\sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_1,$$

$$\sigma_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_1.$$

Posebno, vrijedi: $\sigma_3 = {\sigma_2}^{-1}$, $\sigma_2 = {\sigma_3}^{-1}$.

Dobivene rezultate možemo zapisati u sljedeću tablicu:

$\circ$	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3
σ_2	σ_2	σ_3	σ_1
σ_3	σ_3	σ_1	σ_2

Evo i preostalih permutacija:

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Prema tome, skup svih permutacija skupa $\{1, 2, 3\}$ *je skup*

$$S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}.$$

Zadatak 7.11. *Popunite tablicu do kraja:*

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3			
σ_2	σ_2	σ_3	σ_1			
σ_3	σ_3	σ_1	σ_2			
σ_4						
σ_5						
σ_6						

Primjer 7.12. *Neka je* $\sigma \in S_7$ *zadana sa:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 6 & 1 & 2 & 3 \end{pmatrix}.$$

Kako odrediti σ^{-1}*? Prisjetimo se:*

$$y = \sigma(x) \Longleftrightarrow x = \sigma^{-1}(y).$$

Dovoljno je tablicu okrenuti naopako:

$$\sigma = \begin{pmatrix} 7 & 5 & 4 & 6 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

i složiti je redom:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 3 & 2 & 4 & 1 \end{pmatrix}.$$

Zadatak 7.13. (a) *Ako je* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, *odredite* σ^{-1}.

(b) *Ako je* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$, *odredite* τ^{-1}.

(c) *Ako su* σ *i* τ *kao gore, odredite:* $\sigma \circ \tau$, $\sigma \circ \tau^{-1}$, $\sigma^{-1} \circ \tau^{-1}$, $\sigma^{-1} \circ \tau$, $\tau \circ \sigma$, $\tau^{-1} \circ \sigma$, $\tau^{-1} \circ \sigma^{-1}$, $\tau \circ \sigma^{-1}$.

Teorem 7.14. *Neka je* $n \in \mathbb{N}$. *Tada je broj elemenata skupa* S_n, *u oznaci* $\#S_n$, *jednak* $n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$.

Dokaz. Trebamo popuniti donji redak:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \cdot & \cdot & \dots & \cdot \end{pmatrix}.$$

Prvi element, a to je $\sigma(1)$, možemo birati na n načina među elementima skupa $\{1, 2, \dots, n\}$, zatim $\sigma(2)$ možemo birati na $n-1$ način jer smo jedan element skupa $\{1, 2, \dots, n\}$ već uzeli, itd., na kraju $\sigma(n)$ možemo izabrati samo na jedan način (to je zadnji preostali element skupa $\{1, 2, \dots, n\}$). Ukupno imamo $1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$ mogućnosti i to je broj svih mogućih permutacija skupa $\{1, 2, \dots, n\}$. □

Tako smo u primjeru 7.10 za $n = 1$ dobili samo jednu premutaciju, za $n = 2$ smo dobili dvije, a za $n = 3$ šest permutacija.

Primjer 7.15. *Preslikavanje* $f : \mathbb{R} \to \mathbb{R}$ *zadano sa* $f(x) = x^3$ *je bijekcija (permutacija).*

Neka su $x_1, x_2 \in \mathbb{R}$ *takvi da je* $f(x_1) = f(x_2)$. *To znači da je* ${x_1}^3 = {x_2}^3$, *odnosno*

$${x_1}^3 - {x_2}^3 = 0.$$

Rastavljanjem na faktore dobivamo

$$(x_1 - x_2)({x_1}^2 + x_1 x_2 + {x_2}^2) = 0.$$

Pretpostavimo $x_1 \neq x_2$. *Tada je*

$${x_1}^2 + x_1 x_2 + {x_2}^2 = 0$$

što možemo napisati u obliku

$$\left(x_1 + \frac{1}{2} x_2\right)^2 + \frac{3}{4} {x_2}^2 = 0.$$

Slijedi

$$x_1 + \frac{1}{2} x_2 = x_2 = 0,$$

odnosno $x_1 = x_2 = 0$, *što je u suprotnosti s pretpostavkom* $x_1 \neq x_2$. *Zaključujemo da je* $x_1 = x_2$. *Dakle,* f *je injekcija, što nije bilo teško dokazati.*

Međutim, nije jednostavno dokazati činjenicu da je f surjekcija, tj. dokazati

$$(\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(x^3 = y).$$

Ova tvrdnja će slijediti iz korolara 10.6.

Definicija 7.16. *Za skupove S i T kažemo da su* **ekvipotentni** *i pišemo $S \sim T$ ako postoji bijekcija $f : S \to T$.*

Teorem 7.17. *Neka su S, T, R neprazni skupovi. Tada vrijede sljedeće tvrdnje:*

(i) $S \sim S$,
(ii) $S \sim T \implies T \sim S$,
(iii) $S \sim T \;\&\; T \sim R \implies S \sim R$.

Dokaz. (i) Prema propoziciji 7.5, preslikavanje $1_S : S \to S$ je bijekcija.

(ii) Kako je $S \sim T$, to postoji bijekcija $f : S \to T$. Propozicija 7.4 povlači da je tada i $f^{-1} : T \to S$ bijekcija. Dakle, $T \sim S$.

(iii) Kako je $S \sim T$ i $T \sim R$, to postoje bijekcije $f : S \to T$ i $g : T \to R$. Prema teoremu 7.6 je tada i $g \circ f : S \to R$ bijekcija. Prema tome, $S \sim R$. $\square$

Prema teoremu 7.17 je $\sim$ relacija ekvivalencije na kolekciji svih skupova (sjetimo se iz 2. poglavlja: kolekcija svih skupova nije skup!).

Klasa ekvivalencije kojoj pripada skup S se naziva **kardinalni broj skupa** S i označava sa $|S|$ ili $\operatorname{card} S$.

Kažemo da je skup S **konačan** ako postoji $n \in \mathbb{N}$ takav da je $S \sim \{1, \ldots, n\}$.

Kažemo da je skup S **prebrojiv** ako je $S \sim \mathbb{N}$.

Primjer 7.18. *Dokažimo da je $\mathbb{N} \sim \mathbb{Z}$. Sve prirodne brojeve trebamo bijektivno preslikati na sve cijele brojeve. To ćemo učiniti na sljedeći način:*

$$1 \mapsto 1, \quad 3 \mapsto 2, \quad 5 \mapsto 3, \quad 7 \mapsto 4, \quad \ldots$$

tj. $2k - 1 \mapsto k$ za $k \in \mathbb{N}$, i dalje

$$2 \mapsto 0, \quad 4 \mapsto -1, \quad 6 \mapsto -2, \quad 8 \mapsto -3, \quad \ldots$$

tj. $2k \mapsto 1 - k$ za $k \in \mathbb{N}$. Dakle, skup $\mathbb{Z}$ je prebrojiv.

Primjer 7.19. *Dokažimo da je $\mathbb{R} \sim \langle -1, 1\rangle$.*

Za svaki $x \in \mathbb{R}$ stavimo

$$f(x) = \frac{x}{1 + |x|}.$$

Iz $-|x| \le x \le |x|$ slijedi $-1 - |x| < x < 1 + |x|$, pa je $-1 < \frac{x}{1+|x|} < 1$ tj. $-1 < f(x) < 1$. Dakle, $f : \mathbb{R} \to \langle -1, 1\rangle$.

Preostaje dokazati da je f bijekcija.

Najprije dokažimo da je f injekcija. Neka su $x_1, x_2 \in \mathbb{R}$ takvi da je $f(x_1) = f(x_2)$. Imamo sljedeći niz ekvivalentnih jednakosti:

$$\begin{aligned} f(x_1) &= f(x_2), \\ \frac{x_1}{1+|x_1|} &= \frac{x_2}{1+|x_2|}, \\ x_1(1+|x_2|) &= x_2(1+|x_1|), \\ x_1 + x_1|x_2| &= x_2 + x_2|x_1|, \\ x_1 - x_2 &= x_2|x_1| - x_1|x_2|. \end{aligned}$$

Da bismo dokazali da je $x_1 = x_2$, dovoljno je dokazati da je $x_2|x_1| - x_1|x_2| = 0$. Uočimo da iz

$$\frac{x_1}{1+|x_1|} = \frac{x_2}{1+|x_2|}$$

slijedi

$$\frac{x_1}{x_2} = \frac{1+|x_1|}{1+|x_2|} > 0,$$

pa je ili $x_1, x_2 > 0$ ili $x_1, x_2 < 0$. U oba slučaja je $x_2|x_1| - x_1|x_2| = 0$. Dakle, $x_1 = x_2$, pa je f je injekcija.

Sada dokažimo da je f surjekcija. Neka je $-1 < y < 1$ zadan. Pitamo se postoji li $x \in \mathbb{R}$ takav da je $y = \frac{x}{1+|x|}$. Uočimo da, ako takav x postoji, tada ima isti predznak kao i y (jer je nazivnik $1+|x|$ uvijek pozitivan).

Ako je $y \geq 0$, tada se jednadžba $y = \frac{x}{1+|x|}$ svodi na $y = \frac{x}{1+x}$; imamo

$$y = \frac{x}{1+x} \Longleftrightarrow y + xy = x \Longleftrightarrow x - xy = y \Longleftrightarrow x = \frac{y}{1-y}.$$

Ako je $y < 0$, tada se jednadžba $y = \frac{x}{1+|x|}$ svodi na $y = \frac{x}{1-x}$; imamo

$$y = \frac{x}{1-x} \Longleftrightarrow y - xy = x \Longleftrightarrow x + xy = y \Longleftrightarrow x = \frac{y}{1+y}.$$

Naglasimo da je $-1 < y < 1$, pa posebno promatramo slučaj kada je $-1 < y < 0$ i slučaj kada je $0 \leq y < 1$.

Ako je $-1 < y < 0$, tada definiramo $x = \frac{y}{1+y} < 0$. Vrijedi

$$f(x) = \frac{x}{1+|x|} = \frac{x}{1-x} = \frac{\frac{y}{1+y}}{1 - \frac{y}{1+y}} = \frac{y}{(1+y)-y} = y.$$

Ako je $0 \leq y < 1$, definiramo $x = \frac{y}{1-y} > 0$. Vrijedi

$$f(x) = \frac{x}{1+|x|} = \frac{x}{1+x} = \frac{\frac{y}{1-y}}{1 + \frac{y}{1-y}} = \frac{y}{(1-y)+y} = y.$$

Dakle, za svaki $y \in \langle -1, 1\rangle$ postoji $x \in \mathbb{R}$ takav da je $y = \frac{x}{1+|x|}$. Zaključujemo da je f i surjekcija.

Spomenimo (bez dokaza) da skup $\mathbb{R}$ nije prebrojiv, tj. $\mathbb{N} \nsim \mathbb{R}$.

Sada možemo zaključiti i da $\langle -1, 1\rangle$ nije prebrojiv skup. Naime, ako pretpostavimo suprotno, tj. da je $\langle -1, 1\rangle$ prebrojiv, tada je $\langle -1, 1\rangle \sim \mathbb{N}$. No, $\sim$ je relacija ekvivalencije, pa iz $\mathbb{R} \sim \langle -1, 1\rangle$ i $\langle -1, 1\rangle \sim \mathbb{N}$ slijedi $\mathbb{R} \sim \mathbb{N}$, što je kontradikcija.

8. Prirodni i cijeli brojevi

Od ranije znamo da, zbog svoje važnosti u matematici, skup prirodnih i skup cijelih brojeva imaju svoje posebne, stalne oznake.

Pišemo

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

za skup prirodnih brojeva i

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

za skup cijelih brojeva. Pišemo i

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$$

za skup prirodnih brojeva zajedno s 0.

Na skupu prirodnih i cijelih brojeva imamo uobičajene operacije zbrajanja i množenja čija svojstva dobro znamo još iz osnovne škole. Strogu aksiomatsku izgradnju ovih struktura moguće je napraviti na osnovi tzv. **Peanovih aksioma** za skup prirodnih brojeva. Zainteresirani mogu čitati o tome u prvom poglavlju knjige S. Mardešić, Matematička analiza u n–dimenzionalnom realnom prostoru. Mi ovdje nećemo izložiti tu teoriju ovdje. Za nas će biti važan samo aksiom matematičke indukcije (koji je jedan od Peanovih aksioma).

Aksiom matematičke indukcije. Neka $S \subseteq \mathbb{N}$ ima sljedeća dva svojstva:

(a) $1 \in S$,
(b) $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$.

Tada je

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

Aksiom matematičke indukcije je intuitivno prihvatljiv. Najprije, zbog (a) imamo $1 \in S$. No, tada (2) povlači najprije $2 \in S$, zatim $3 \in S$ itd. Dobivamo redom

$$1, 2, 3, \ldots \in S.$$

Dakle

$$\mathbb{N} \subseteq S.$$

Kako je još i $S \subseteq \mathbb{N}$, to zaključujemo

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

Ovo je samo intuitivno obrazloženje aksioma matematičke indukcije i *nije dokaz*. Prisjetimo se, aksiomi se ne dokazuju, već ih smatramo istinitim tvrdnjama koje su nam manje-više intuitivno prihvatljive, pa je gornje obrazloženje i izloženo s namjerom lakšeg intuitivnog prihvaćanja istinitosti aksioma matematičke indukcije.

Obično se govori da je (a) **baza indukcije**, a (b) **korak indukcije**. Za valjanu upotrebu aksioma indukcije i (a) i (b) moraju vrijediti. Aksiom matematičke indukcije koristi se za dokazivanje brojnih tvrdnji, a temelji se na sljedećem principu.

Teorem 8.1 (Princip matematičke indukcije)**.** *Neka je $P(n)$ neka tvrdnja koja ovisi o prirodnom broju n. Prepostavimo da je*

(baza ind.) $P(1)$ *istina, te*
(korak ind.) *iz pretpostavke da je $P(n)$ istina za neki n slijedi da je i $P(n+1)$ istina.*

Tada je

$$P(n) \text{ istina za svaki prirodan broj } n.$$

Dokaz. Definirajmo skup

$$S = \{n \in \mathbb{N} \mid P(n) \text{ je istina}\}.$$

Tada imamo $S \subseteq \mathbb{N}$. Nadalje, S zadovoljava sljedeća dva svojstva:

(a) $1 \in S$ zbog **(baza ind.)**,
(b) $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$ zbog **(korak ind.)**.

Dakle, prema aksiomu matematičke indukcije vrijedi

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

To znači da je $P(n)$ istina za svaki prirodan broj n. □

Primjer 8.2. *Dokažimo da za svaki prirodan broj n vrijedi*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Označimo ovu jednakost sa $P(n)$. Za $n = 1$, $P(1)$ glasi

$$1 = \frac{1(1+1)}{2}$$

te je zato $P(1)$ istina. Ovim smo provjerili bazu indukcije. Pretpostavimo da je sada $P(n)$ istina za neki n tj. pretpostavimo da vrijedi

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{8.3}$$

Treba dokazati da je $P(n+1)$ istina tj. da je

$$1 + 2 + \cdots + n + (n+1) = \frac{(n+1)((n+1)+1)}{2}. \tag{8.4}$$

Zaista, iz (8.3) slijedi

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ = \frac{n(n+1) + 2(n+1)}{2} &= \frac{(n+2)(n+1)}{2} = \frac{(n+1)((n+1)+1)}{2}, \end{aligned}$$

što dokazuje (8.4) tj. istinitost jednakosti $P(n+1)$. Ovim smo provjerili i korak indukcije. Dakle, prema principu matematičke indukcije dane u teoremu 8.1, zaključujemo da je $P(n)$ istina za svaki prirodan broj n.

Naglasimo da je prilikom korištenja principa matematičke indukcije potrebno provjeriti i bazu i korak indukcije. Iako je bazu indukcije najčešće vrlo jednostavno provjeriti, taj dio se ne smije izostaviti, kao što pokazuje sljedeći primjer:

Primjer 8.5. *Svakom je jasno da je* $2 + 2^2 + \cdots + 2^n \neq 2^{n+1} - 1$ *jer je s lijeve strane paran broj dok je s desne strane neparan broj. Dakle, tvrdnja* $P(n)$ *dana sa* $2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ *nije istinita niti za jedan prirodan broj* n*!*

Međutim, ***korak indukcije formalno vrijedi*** *jer iz pretpostavke da je* $P(n)$ *istina za neki* n*, tj. iz*

$$2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

slijedi

$$\begin{aligned} &2 + 2^2 + \cdots + 2^n + 2^{n+1} = \big(2^{n+1} - 1\big) + 2^{n+1} = \big(2^{n+1} + 2^{n+1}\big) - 1 \\ &= 2 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1. \end{aligned}$$

Dakle, iz istinitosti jednakosti $P(n)$ *dobili smo istinost jednakosti* $P(n+1)$*.*

Baza indukcije ne vrijedi *jer je* $2 \neq 2^{1+1} - 1 = 3$*.*

Zadatak 8.6. *Matematičkom indukcijom dokažite*

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

za svaki prirodan broj n*. Nadalje, dokažite da za dani* $x \neq 1$ *vrijedi*

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}$$

za svaki prirodan broj n*. Uočite da za* $x = 2$ *dobivamo prvu tvrdnju.*

Ako jednakost iz zadatka 8.6 napišemo u obliku

$$x^{n+1} - 1 = (x-1)(x^n + x^{n-1} + \cdots + x + 1),$$

onda ona vrijedi i za $x = 1$. Stavljajući $x = \frac{a}{b}$, gdje je $b \neq 0$, dobivamo

$$\left(\frac{a}{b}\right)^{n+1} - 1 = \left(\frac{a}{b} - 1\right)\left(\left(\frac{a}{b}\right)^n + \left(\frac{a}{b}\right)^{n-1} \cdots + \left(\frac{a}{b}\right) + 1\right).$$

Množeći lijevu i desnu stranu sa $b^{n+1} = b \cdot b^n$, dobivamo

$$a^{n+1} - b^{n+1} = (a-b)(a^n + a^{n-1}b + \cdots + ab^{n-1} + b^n). \tag{8.7}$$

Naglasimo da je (8.7) dobiveno pod pretpostavkom $b \neq 0$. Međutim, za $b = 0$ se (8.7) svodi na $a^{n+1} = a \cdot a^n$ što je istina. Dakle, (8.7) vrijedi za sve a, b i n.

Istaknimo

$$n = 1 \implies a^2 - b^2 = (a-b)(a+b) \text{ (razlika kvadrata)}$$

$$n = 2 \implies a^3 - b^3 = (a-b)(a^2 + ab + b^2) \text{ (razlika kubova).}$$

Zadatak 8.8. *Matematičkom indukcijom dokažite (8.7).*

U praksi je nekada potrebno primijeniti princip poopćene indukcije koji se temelji na sljedećoj propoziciji:

Propozicija 8.9. *Neka je dan prirodan broj n_0. Pretpostavimo da skup $T \subseteq \mathbb{N}$ zadovoljava sljedeća dva svojstva:*

(a) $n_0 \in T$,
(b) $(\forall n \in \mathbb{N})(n \in T \implies n+1 \in T)$.

Tada je

$$\{n_0, n_0+1, n_0+2, \dots\} \subseteq T$$

tj. T sadrži sve prirodne broje n veće ili jednake n_0.

Dokaz. Zadajmo skup S sa

$$S = \{1, 2, \dots, n_0\} \cup T.$$

Tada je $S \subseteq \mathbb{N}$. Nadalje, S zadovoljava sljedeća dva svojstva:

(i) $1 \in S$,
(ii) $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$.

Odmah vidimo da (i) vrijedi iz same konstrukcije skupa S. Provjerimo (ii). Neka je $n \in S$. Tada je $n \in \{1, 2, \dots, n_0\}$ ili $n \in T$ jer je S unija ova dva istaknuta skupa. Ako je $n \in \{1, 2, \dots, n_0\}$, tada je ili $n \leq n_0 - 1$ ili $n = n_0$. Ako je $n \leq n_0 - 1$, onda je $n + 1 \leq n_0$ tj. $n + 1 \in \{1, 2, \dots, n_0\}$ tj. $n + 1 \in S$. Ako je $n = n_0$, onda je također $n_0 \in T$ jer vrijedi pretpostavka (a) naše propozicije. Sada iz pretpostavke (b) naše propozicije zaključujemo $n_0 + 1 \in T$ te je zato i $n_0 + 1 \in S$. Znači da i u slučaju $n = n_0$ imamo $n + 1 \in S$. Na kraju, ako je $n \in S$ i ako je $n > n_0$ onda je $n \in T$. Sada (b) povlači $n + 1 \in T$. Stoga je i $n + 1 \in S$. Ovim je (ii) potpuno provjereno.

Dakle, prema aksiomu matematičke indukcije vrijedi

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

Drugim riječima,

$$\{1, 2, \dots, n_0\} \cup T = \mathbb{N}.$$

Posebno, svaki prirodan broj n je sadržan u jednom od skupova $\{1, 2, \dots, n_0\}$ i T (jer je $\mathbb{N}$ unija ova dva skupa). Ako je n prirodan broj sa svojstvom $n > n_0$, on nije element skupa $\{1, 2, \dots, n_0\}$, pa mora biti element skupa T. Dakle,

$$\{n_0 + 1, n_0 + 2, \dots\} \subseteq T.$$

Kako je $n_0 \in T$ zbog pretpostavke (a) naše propozicije, to konačno zaključujemo

$$\{n_0, n_0 + 1, n_0 + 2, \dots\} \subseteq T.$$

□

Zadatak 8.10. *Koristeći propoziciju 8.9, formulirajte i dokažite odgovarajući princip matematičke indukcije po uzoru na onaj dan teoremom 8.1. Koristeći taj princip dokažite da za svaki prirodan broj $n \geq 3$ vrijedi nejednakost*

$$2^{n-1} \geq n + 1.$$

Uputa. Najprije formulirajmo princip.

Neka je dan prirodan broj n_0 i neka je $P(n)$ neka tvrdnja koja ovisi o prirodnom broju $n \geq n_0$. Prepostavimo da je

(baza ind.) $P(n_0)$ istina, te
(korak ind.) iz pretpostavke da je $P(n)$ istina za neki n slijedi da je i $P(n+1)$ istina.

Tada je

$$P(n) \text{ istina za svaki prirodan broj } n \geq n_0.$$

Sada dokažite istinitost tvrdnje

$$P(n) \ldots \quad 2^{n-1} \geq n+1$$

za svaki $n \geq 3$. Baza indukcije se sastoji u provjeri istinitosti tvrdnje $P(3)$. □

Postoje brojne druge varijacije principa matematičke indukcije. One su sadržaj sljedećih zadataka.

Zadatak 8.11. *Pretpostavimo da skup $T \subseteq \mathbb{N}_0$ zadovoljava sljedeća dva svojstva:*

(a) $0 \in T$,
(b) $(\forall n \in \mathbb{N}_0)(n \in T \implies n+1 \in T)$.

Tada je

$$T = \mathbb{N}_0.$$

Formulirajte i dokažite odgovarajući princip matematičke indukcije.

Uputa. Zbog (a) imamo $0 \in T$. Dakle, pretpostavka (b) povlači da je $1 = 0+1 \in T$. Definirajmo skup S sa

$$S = \{n \in T \mid n \in \mathbb{N}\}.$$

Koristeći aksiom matematičke indukcije dokažite da je $S = \mathbb{N}$. Odatle i iz (a) odmah slijedi da je $T = \mathbb{N}_0$. □

Zadatak 8.12. *Pretpostavimo da je $P(n)$ neka tvrdnja koja ovisi o prirodnom broju n. Prepostavimo:*

(baza ind.) *$P(1), P(2)$ su istinite, te*
(korak ind.) *za $n \geq 2$, iz pretpostavke da su tvrdnje $P(n-1)$i $P(n)$ istinite za neki n slijedi da je i $P(n+1)$ istina.*

Tada je

$$P(n) \textit{ istina za svaki prirodan broj } n.$$

Uputa. Definirajmo skup

$$S = \{n \in \mathbb{N} \mid \text{tvrdnje } P(1), \ldots, P(n) \text{ su istinite}\}.$$

Tada imamo $S \subseteq \mathbb{N}$. Nadalje, S zadovoljava sljedeća svojstva:

(i) $1 \in S$,
(ii) $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$.

Zaista, (i) vrijedi zbog toga što baza indukcije uključuje pretpostavku da je $P(1)$ istina. Ostaje dokazati (ii). Neka je $n \in S$. Treba dokazati da je $n+1 \in S$. Razlikujte dva slučaja: $n = 1$ i $n \geq 2$. Ako je $n = 1$, onda je $n+1 = 2$, pa je P(2) istina zbog toga što baza indukcije uključuje pretpostavku da je $P(2)$ istina. Dakle, imamo da su $P(1)$ i $P(2)$ istinite što znači da je $n+1 = 2 \in S$. Slučaj $n \geq 2$ ostavljamo za vježbu.

Sada (i) i (ii) prema aksiomu matematičke indukcije povlače $S = \mathbb{N}$. Posebno, imamo da je $P(n)$ istina za svaki prirodan broj n. □

Promotrimo jedan primjer u kojem koristimo princip indukcije iz zadatka 8.12.

Primjer 8.13. *Neka je S skup. Niz u skupu S je preslikavanje $a : \mathbb{N} \to S$. Umjesto $a(n)$ pišemo a_n za svaki $n \in \mathbb{N}$, a niz a označavamo sa (a_n). Ako je $S = \mathbb{N}$, govorimo o nizu prirodnih brojeva.*

Neka je (a_n) niz prirodnih brojeva zadan sa $a_1 = 2$, $a_2 = 6$ i $a_{n+1} = a_n + a_{n-1}$ za $n \geq 2$. Dakle, svaki član niza osim prva dva je suma prethodna dva: 2, 6, 8, 14, 22 itd. Dokažimo da je a_n paran za svaki $n \in \mathbb{N}$.

Zaista, označimo tu tvrdnju sa $P(n)$. Kako je $a_1 = 2$ i $a_2 = 6$, nalazimo da su $P(1)$ i $P(2)$ istinite. Ovo je baza indukcije. Pretpostavimo sada da je $n \geq 2$ i da su i $P(n-1)$ i $P(n)$ istinite tj. da su a_{n-1} i a_n parni. Tada je i $a_{n+1} = a_n + a_{n-1}$ paran jer je suma dva parna broja. Dakle, $P(n+1)$ je istina. Ovo je korak indukcije.

Završimo ovaj dio s još jednim primjerom principa matematičke indukcije.

Zadatak 8.14. *Pretpostavimo da neka je $P(n)$ neka tvrdnja koja ovisi o prirodnom broju n. Prepostavimo da je*

(baza ind.) *$P(1)$ istina, te*
(korak ind.) *iz pretpostavke da su tvrdnje $P(1), P(2), \dots, P(n)$ istinite za neki n slijedi da je i $P(n+1)$ istina.*

Tada je

$$P(n) \text{ istina za svaki prirodan broj } n.$$

Uputa. Postupajte slično kao u zadatku 8.12. □

Sada prelazimo na primjenu aksioma matematičke indukcije na dokazivanje važnih rezultata vezanih za skupove prirodnih i cijelih brojeva.

Prisjetimo se pojma minimuma iz definicije 3.13.

Ako je $(A, \leq)$ parcijalno uređen skup, minimum (ili minimalni element) skupa A je $a \in A$ sa svojstvom $a \leq b$ za svaki $b \in A$. Ukoliko takav a postoji, on je jedinstven (propozicija 3.14) i označavamo ga sa $\min A$. Primjerice,

$$\min \mathbb{N} = 1.$$

Općenito, egzistenciju takvog elementa dokazujemo u sljedećem teoremu:

Teorem 8.15. *Svaki neprazan podskup $A \subseteq \mathbb{N}$ ima minimalni element.*

Dokaz. Pretpostavimo da neprazan skup $A \subseteq \mathbb{N}$ nema minimalni element. Definiramo skup $S \subseteq \mathbb{N}$ sa

$$S = \{n \in \mathbb{N} \mid n < a, \forall a \in A\}.$$

Dokazat ćemo da S zadovoljava sljedeća svojstva:

(i) $1 \in S$,
(ii) $(\forall n \in \mathbb{N})(n \in S \implies n + 1 \in S)$.

Zaista, $1 \in S$ jer za svaki $a \in A$ (kao i za svaki prirodan broj) imamo $a \geq 1$. Međutim, $1 \notin A$ jer smo pretpostavili da A nema minimum pa ne moze sadržavati 1. Dakle, $1 \in S$, tj. vrijedi (i).

Pretpostavimo sada da je $n \in S$ tj. pretpostavimo da je

$$n < a, \quad \forall a \in A.$$

Kako je n prirodan broj, odatle zaključujemo

$$n + 1 \leq a, \quad \forall a \in A.$$

Ako bi za neki $a \in A$ vrijedila jednakost, onda bi $n+1$ morao biti minimum skupa, ali takav po našoj pretpostavci ne postoji, pa imamo strogu nejednakost za svaki $a \in A$, tj.

$$n + 1 < a, \quad \forall a \in A.$$

Ovo dokazuje da je $n+1 \in S$. Dakle vrijedi (ii). Sada prema aksiomu matematičke indukcije zaključujemo

$$S = \mathbb{N},$$

ali takvo što je nemoguće, jer bi onda bilo

$$A \subseteq S,$$

što nije jer se S sastoji od elemenata koji su strogo manji od svakog elementa iz A. □

Sada ćemo primijeniti teorem 8.15 na proučavanje aritmetike u skupu prirodnih i cijelih brojeva. O tvrdnji sljedećeg teorema je već bilo riječi u primjeru 3.18.

Teorem 8.16 (o dijeljenju s ostatkom)**.** *Neka je $m \in \mathbb{Z}$ i $n \in \mathbb{N}$. Tada postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, n-1\}$ takvi da vrijedi*

$$m = n \cdot q + r.$$

Iz primjera 3.18 se prisjetimo da se q naziva **kvocijent**, a r **ostatak** pri dijeljenju cijelog broja m prirodnim brojem n. Ukoliko je $r = 0$ onda je $m = n \cdot q$; kažemo da je m **djeljiv sa** n i pišemo $n \mid m$. U primjeru 3.18 smo vidjeli da za $m = 38$ i $n = 5$ imamo

$$38 = 5 \cdot 7 + 3, \text{ tj. } q = 7 \text{ i } r = 3,$$

a za $m = -38$ i $n = 5$ imamo

$$-38 = 5 \cdot (-8) + 2, \text{ tj. } q = -8 \text{ i } r = 2.$$

Kako smo došli do ovih prikaza?

$$5 \cdot 7 \leq 38 < 5 \cdot 8 \text{ daje } q = 7, \text{ a } r = m - n \cdot q = 38 - 5 \cdot 7 = 3,$$

odnosno

$$5 \cdot (-8) \leq -38 < 5 \cdot (-7) \text{ daje } q = -8, \text{ a } r = m - n \cdot q = -38 - 5 \cdot (-8) = 2.$$

Dokaz teorema 8.16. Egzistenciju brojeva $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, n-1\}$ takvih da vrijedi

$$m = n \cdot q + r$$

dokazujemo kao što smo objasnili u gornjem prikazu. Najprije, ako je $m = 0$, onda stavimo $q = 0$ i $r = 0$ jer je tada

$$0 = n \cdot 0 + 0.$$

Razmotrimo nadalje slučaj $m > 0$. Tada nađemo q takav da vrijedi

$$n \cdot q \leq m < n \cdot (q + 1).$$

Kako dokazati egzistenciju $q \in \mathbb{Z}$ s gornjim svojstvom? U primjeru 3.18 to nismo dokazivali jer nam je nedostajalo znanje o tvrdnji teorema 8.15. Definiramo skup

$$A = \{s \in \mathbb{N} \mid n \cdot s > m\}.$$

Skup A je neprazan jer je npr. $m + 1 \in A$. Zaista, $m \in \mathbb{Z}$ i $m > 0$ daje $m \in \mathbb{N}$ i

$$n \cdot (m + 1) \geq 1 \cdot (m + 1) = m + 1 > m.$$

Prema teoremu 8.15 neprazan skup A ima minimalan element, taj element označimo sa p. Vrijedi

$$n \cdot p > m \geq n \cdot (p - 1).$$

Nejednakost $n \cdot p > m$ vrijedi jer je $p \in A$. Dokažimo $m \geq n \cdot (p - 1)$. Ako je $p = 1$, ova nejednakost vrijedi zbog $m > 0$. Ako je $p > 1$, ova nejednakost vrijedi jer je $p - 1$ prirodan broj, ali nije u A (zbog $p = \min A$). Stavimo $q = p - 1 \in \mathbb{N}_0$.

Dakle, za $m > 0$ postoji $q \in \mathbb{N}_0$ takav da je

$$n \cdot q \leq m < n \cdot (q + 1).$$

Odatle slijedi da za $r = m - n \cdot q \in \mathbb{Z}$ vrijedi

$$0 \leq r < n,$$

pa je $r \in \{0, 1, \ldots, n - 1\}$. Prema tome, dokazali smo da za $m > 0$ postoje $q \in \mathbb{N}_0$ i $r \in \{0, 1, \ldots, n - 1\}$ takvi da je

$$m = n \cdot q + r.$$

Preostaje razmotriti slučaj $m < 0$. Tada je $-m \in \mathbb{N}$, pa prema dokazanom postoje $q_1 \in \mathbb{N}_0$ i $r_1 \in \{0, 1, \ldots, n - 1\}$ takvi da vrijedi

$$-m = n \cdot q_1 + r_1.$$

Odatle slijedi

$$m = -n \cdot q_1 - r_1 = n \cdot (-q_1) + (-r_1).$$

Kako je $r_1 \in \{0, 1, \dots, n-1\}$, to je $-r_1 \in \{0, -1, \dots, -(n-1)\}$. Takav r_1 nije ostatak, osim ako je $r_1 = 0$. Dakle, ako je $-r_1 \in \{-1, \dots, -(n-1)\}$, onda je

$$n - r_1 \in \{n-1, \dots, n-(n-1) = 1\} \subset \{0, 1, \dots, n-1\}.$$

Konačno,

$$m = n \cdot (-q_1) + (-r_1) = n \cdot (-q_1) + (n - r_1) - n = n \cdot (-q_1 - 1) + (n - r_1).$$

Dovoljno je staviti $q = -q_1 - 1 \in \mathbb{Z}$ i $r = n - r_1 \in \{0, 1, \dots, n-1\}$. Tada je

$$m = n \cdot q + r$$

traženi prikaz. Ovim se završava dokaz egzistencije.

Dokaz jedinstvenosti pogledajte u primjeru 3.18. □

Kao što smo već rekli, ako su $m \in \mathbb{Z}$ i $n \in \mathbb{N}$ takvi da je $m = n \cdot q$ za neki $q \in \mathbb{Z}$, kažemo da je m djeljiv sa n i pišemo $n \mid m$. Ova definicija ima smisla i ako su $m, n \in \mathbb{Z}$. Nadalje, ako su $m, n \in \mathbb{N}$ takvi da $n \mid m$, kaže se još i da je m višekratnik od n; tada je i $q \in \mathbb{N}$, pa je

$$m \in \{1 \cdot n, 2 \cdot n, 3 \cdot n, \dots\};$$

posebno je $n \leq m$.

Definicija 8.17. *Kažemo da je prirodan broj p* ***prost ili prim broj*** *ako vrijedi:*

(i) $p > 1$,
(ii) $(\forall n \in \mathbb{N})(n \mid p \implies n \in \{1, p\})$.

Prirodan broj koji nije prost, a strogo je veći od 1*, naziva se* ***složen****.*

Evo prvih nekoliko prostih brojeva:

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

Teorem 8.18. *Svaki složen broj je produkt barem dva prosta broja. Posebno, svaki prirodan broj $n > 1$ ima prostog djelitelja.*

Dokaz. Pretpostavimo da postoji složen broj koji nije produkt barem dva prosta broja. Onda je skup A definiran sa

$$A = \{n \mid n \text{ nije produkt barem dva prosta broja}\}$$

neprazan. Prema teoremu 8.15, skup A ima minimum, označimo ga sa m. Kako je $m \in A$, to je m složen broj. Znači da postoji $n \in \mathbb{N} \setminus \{1, m\}$ takav da $n \mid m$. Slijedi $m = n \cdot q$ za neki $q \in \mathbb{N}$, pa je $n < m$ i $q < m$. Tada $n \notin A$ i $q \notin A$, što znači da je n produkt barem dva prosta broja i q je produkt barem dva prosta broja. No, tada je i $m = n \cdot q$ produkt barem dva prosta broja, što je u kontradikciji sa $m \in A$.

Ako je n prirodan broj veći od 1, tada je ili prost ili složen. Ako je prost, tada očigledno ima prostog djelitelja (sebe samog). Ako je složen, tada je produkt barem dva prosta broja, pa ima prostog djelitelja. □

Konstrukcija niza prostih brojeva temelji se na principu da prost broj p nije višekratnik niti jednog prirodnog broja većeg od 1 (osim u trivijalnom slučaju $1 \cdot p$) te na činjenici da svaki prirodan broj $n > 1$ ima djelitelja koji je prost broj:

$$\boxed{1 \cdot p = p} \text{ je prost, ali } 2 \cdot p,\ 3 \cdot p, \dots \text{ nisu prosti.}$$

Prvi po redu prost broj je $p_1 = 2$. Dakle, niti jedan od brojeva

$$2 \cdot 2 = 4,\ 2 \cdot 3 = 6,\ 2 \cdot 4 = 8,\ \dots \text{ nije prost.}$$

Prekrižimo te brojeve u skupu prirodnih brojeva:

$$\boxed{p_1 = 2},\ 3,\ \cancel{4},\ 5,\ \cancel{6},\ 7, \cancel{8},\ 9, \cancel{1}0,\ 11,\ \cancel{1}2,\ 13, \cancel{1}4,\ 15, \dots$$

Najmanji preostali broj je $p_2 = 3$ i mora biti prost. Sada prekrižimo višekratnike od 3:

$$\boxed{p_1 = 2},\ \boxed{p_2 = 3},\ \cancel{4},\ 5,\ \cancel{6},\ 7, \cancel{8},\ \cancel{9}, \cancel{1}0,\ 11,\ \cancel{1}2,\ 13, \cancel{1}4,\ \cancel{1}5, \dots$$

Najmanji preostali broj je $p_3 = 5$ i mora biti prost itd.

Ovaj algoritam traženja prostih brojeva nazivamo **Eratostenovo sito.**

Zadatak 8.19. *Koristeći Eratostenovo sito nađite sve proste brojeve manje od* 50 *i sve proste brojeve manje od* 100.

Eratostenovo sito daje nam konstrukciju rastućeg niza prostih brojeva:

$$p_1 = 2 < p_2 = 3 < p_3 = 5 < p_4 = 7 < \dots .$$

Mozemo se zapitati je li taj niz konačan ili beskonačan? Odgovor daje poznati **Euklidov teorem.**

Teorem 8.20. *Postoji beskonačno prostih brojeva.*

Dokaz. Zaista, ako to nije istina, prostih brojeva ima konačno mnogo, recimo $p_1, p_2, \dots, p_r$. Stavimo

$$n = p_1 \cdot p_2 \cdots p_r + 1.$$

Kako je $n > 1$, to prema teoremu 8.18 broj n ima prostog djelitelja, dakle djelitelja među elementima skupa $\{p_1, p_2, \dots, p_r\}$; neka je to p_i. Tada je $n = p_i \cdot q$ za neki $q \in \mathbb{Z}$, pa je

$$1 = n - p_1 p_2 \cdots p_r = p_i(q - p_1 \cdots p_{i-1} p_{i+1} \cdots p_r)$$

odakle slijedi $p_i = 1$, pa p_i nije prost; kontradikcija. $\square$

Prosti brojevi su vrlo rijetki u skupu prirodnih brojeva. Može se pokazati da ako pišemo $\pi(n)$ za broj prostih brojeva $\leq n$ da je onda $\pi(n)$ približno $n/\ln(n)$ što je znatno manje od n kada n raste preko svih granica. Ovo je vrlo složen teorem za dokazati. Ipak, zamislimo da smo uzeli bilo koji prirodan broj $n > 1$. Podsjetimo da je $n! = 1 \cdot 2 \cdots n$. Očito vrijedi da $2 < n! + 2$ i 2 dijeli $n! + 2$ jer dijeli $n!$, $3 < n! + 3$ i 3 dijeli $n! + 3$ jer dijeli $n!$ itd. Dakle, svi uzastopni brojevi

$$n! + 2, n! + 3, \ldots, n! + n$$

su složeni brojevi. Ovo pokazuje da postoje po volji dugački nizovi uzastopnih prirodnih brojeva od kojih nije niti jedan prost!

Bez dokaza navodimo profinjenje teorema 8.18.

Teorem 8.21 (Osnovni teorem aritmetike)**.** *Za svaki prirodan broj $n > 1$ postoje jedinstveni prosti brojevi $q_1 < \cdots < q_l$ i prirodni brojevi $\alpha_1, \ldots, \alpha_l$ takvi da*

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_l^{\alpha_l}.$$

Definicija 8.22. ***Najveća zajednička mjera*** *cijelih brojeva $m, n \in \mathbb{Z} \setminus \{0\}$ je prirodan broj k, u oznaci $k = M(m, n)$, koji ima sljedeća svojstva:*

(i) *$k \mid m$ i $k \mid n$,*
(ii) *ako $l \in \mathbb{Z}$ zadovoljava $l \mid m$ i $l \mid n$, onda $l \mid k$.*

Najveća zajednička mjera cijelih brojeva $m, n \in \mathbb{Z} \setminus \{0\}$ je jedinstvena. Zaista, ako su k_1 i k_2 dvije takve onda zbog (ii) mora biti $k_1 \mid k_2$ i $k_2 \mid k_1$. Dakle, za neke prirodne brojeve a i b imamo $k_1 = a \cdot k_2$ i $k_2 = b \cdot k_1$. Zato je

$$k_1 = a \cdot k_2 = a \cdot (b \cdot k_1) = (a \cdot b) \cdot k_1 \implies a \cdot b = 1 \implies a = b = 1 \implies k_1 = k_2.$$

Definicija 8.22 pokazuje da je

$$M(-m, -n) = M(-m, n) = M(m, -n) = M(m, n),$$

što pokazuje da se prilikom određivanja najveće zajedničke mjere možemo ograničiti na prirodne brojeve. Najveća zajednička mjera se u tom slučaju određuje Euklidovim algoritmom (koji pokazuje da mjera postoji).

Euklidov algoritam. Neka su $m, n \in \mathbb{N}$. Uzastopno primjenjujemo teorem 8.16 o dijeljenju s ostatkom dok ne dostignemo nulu; zadnji nenul ostatak je najveća zajednička mjera $M(m, n)$:

$$\begin{aligned}
m &= n \cdot q_1 + r_1, \quad 0 \leq r_1 < n, \\
n &= r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2 \cdot q_3 + r_3, \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{i-1} &= r_i \cdot q_{i+1} + r_{i+1}, \quad 0 \leq r_{i+1} < r_i.
\end{aligned}$$

Kako je gornji niz ostataka strogo padajući, mora postojati indeks i takav da je $r_i > 0$, ali $r_{i+1} = 0$:

$$n > r_1 > r_2 > \cdots > r_i > r_{i+1} = 0.$$

Tada je

$$M(m,n) = r_i.$$

Valjanost Euklidovog algoritma je jednostavno dokazati. Naime, iz definicije najveće zajedničke mjere odmah slijedi da je

$$M(m,n) = M(n,r_1) \text{ ako je } r_1 \neq 0,$$

odnosno

$$M(m,n) = n \text{ ako je } r_1 = 0.$$

Sada ponavljamo ovu proceduru s ostalim ostacima:

$$M(m,n) = M(n,r_1) = M(r_1,r_2) = \cdots = M(r_{i-1},r_i) = r_i.$$

Primjer 8.23. *Odredite $M(12345,993)$. Imamo redom*

$$\begin{aligned}
&12345 = 993 \cdot 12 + 429, \quad r_1 = 429,\\
&993 = 429 \cdot 2 + 135, \quad r_2 = 135,\\
&429 = 135 \cdot 3 + 24, \quad r_3 = 24,\\
&135 = 24 \cdot 5 + 15, \quad r_4 = 15,\\
&24 = 15 \cdot 1 + 9, \quad r_5 = 9,\\
&15 = 9 \cdot 1 + 6, \quad r_6 = 6,\\
&9 = 6 \cdot 1 + 3, \quad r_7 = 3,\\
&6 = 3 \cdot 2 + 0, \quad \boxed{r_8 = 0}.
\end{aligned}$$

Dakle, $M(12345,993) = 3$.

Zadatak 8.24. *Odredite $M(12345,450)$ i $M(11111111,456)$.*

Kažemo da su $m,n \in \mathbb{Z}$ **relativno prosti** ako im je najveća zajednička mjera jednaka jedan. Primjerice, lako provjerimo da je $M(26,15) = 1$, pa su 26 i 15 relativno prosti brojevi.

Zadatak 8.25. *Neka su dani prirodni brojevi m i n.*

(a) *Dokažite da je $M(m,n) = 1$ ako je $m = 1$ ili $n = 1$.*

(b) *Neka je $m,n > 1$. Tada m i n možemo rastaviti na proste faktore kao u osnovnom teoremu aritmetike. Dokažite da su m i n relativno prosti ako i samo ako nemaju niti jedan prosti faktor koji se pojavljuje u oba rastava. Nadalje, dokažite da je najveća zajednička mjera $M(m,n)$ jednaka produktu brojeva p^α, gdje p prolazi po svim prostim brojevima p koji se pojavljuju u rastavu i od m i od n, dok je α određen kao manji od eksponenata od p*

koji se pojavljuju u rastavima od m *i* n*. Primjerice, ako su* $m = 2^3 \cdot 5^2 \cdot 7$ *i* $n = 5^9 \cdot 7^2$*, onda su mogući parovi* $(p, \alpha) = (5, 2), (7, 1)$*. Dakle*

$$M(m, n) = 5^2 \cdot 7.$$

Napomenimo da način određivanja najveće zajedničke mjere opisan u (b) nije jako efikasan jer njemu prethodni složeniji problem faktorizacije prirodnog broja u proste faktore. Euklidov algoritam ne zahtjeva faktorizaciju.

9. Racionalni brojevi

U 8. poglavlju smo proučavali skupove brojeva $\mathbb{N}$ i $\mathbb{Z}$. U ovom predavanju proučavat ćemo svojstva skupa racionalnih brojeva:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\},$$

koje znamo još iz osnovne škole. Zbrajanje, množenje i uređaj na skupu $\mathbb{Q}$ definirani su na sljedeći način:

$$\begin{aligned} &\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'}, \\ &\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'}, \\ &\frac{m}{n} \leq \frac{m'}{n'} \iff \frac{m'}{n'} - \frac{m}{n} = \frac{m'n - mn'}{nn'} \geq 0 \iff (m'n - mn')(nn') \geq 0. \end{aligned} \tag{9.1}$$

Vrijedi

$$\mathbb{Z} \subset \mathbb{Q}$$

uz identifikaciju

$$x = \frac{x}{1}.$$

Poznata svojstva zbrajanja, množenja i uređaja na $\mathbb{Q}$ sada nećemo ponavljati. Umjesto toga pokazat ćemo konstrukciju skupa racionalnih brojeva iz skupa cijelih brojeva te kako se zapravo strogo definiraju operacije dane sa (9.1). Na kraju predavanja iskazat ćemo teorem u kojem se dokazuju već poznata svojstva zbrajanja, množenja i uređaja na $\mathbb{Q}$.

Konstrukcija skupa $\mathbb{Q}$. Intuitivno, racionalni brojevi su kvocijenti

$$r = \frac{m}{n},\ m, n \in \mathbb{Z}, n \neq 0$$

te bi svakom racionalnom broju r trebao odgovarati uređen par cijelih brojeva

$$(m, n), \quad n \neq 0 \quad \text{tj.} \quad (m, n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}).$$

Taj par nije jedinstven; ako je također

$$r = \frac{m'}{n'},\ m', n' \in \mathbb{Z}, n' \neq 0,$$

tada je

$$\frac{m}{n} = \frac{m'}{n'} \iff mn' = m'n.$$

Ova intuitivna razmatranja nam pokazuju kako strogo zasnovati racionalne brojeve. Najprije, na skupu danom Kartezijevim produktom

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$$

definiramo relaciju

$$(m, n) \sim (m', n') \iff mn' = m'n.$$

Lema 9.2. *Relacija $\sim$ je relacija ekvivalencije na skupu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

Dokaz. Za definiciju relacije ekvivalencije vidite definiciju 3.16. Provjerimo redom svojstva koja se zahtijevaju:

Refleksivnost: $(m,n) \sim (m,n)$, $\forall (m,n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Ovo je jasno, jer po definiciji vrijedi

$$(m,n) \sim (m,n) \iff mn = mn.$$

Simetričnost: $(m,n) \sim (m',n') \implies (m',n') \sim (m,n)$, $\forall (m,n),(m',n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Imamo:

$$(m,n) \sim (m',n') \implies mn' = m'n \implies m'n = mn' \implies (m',n') \sim (m,n).$$

Tranzitivnost: $(m,n) \sim (m',n')$ i $(m',n') \sim (m'',n'') \implies (m,n) \sim (m'',n'')$, $\forall (m,n),(m',n'),(m'',n'') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Imamo:

$$(m,n) \sim (m',n') \implies mn' = m'n,$$
$$(m',n') \sim (m'',n'') \implies m'n'' = m''n'.$$

Ako je $m' = 0$, onda je iz prve jednakosti $mn' = 0$, a to povlači $m = 0$ jer je $n' \neq 0$, dok iz druge jednakosti slično zaključujemo $m'' = 0$. Dakle, ako je $m' = 0$, onda vrijedi $m = m'' = 0$. Zato imamo

$$mn'' = 0 = m''n \implies (m,n) \sim (m'',n'').$$

Ako je $m' \neq 0$, onda množenjem gornjih jednakosti dobivamo

$$(mn')(m'n'') = (m'n)(m''n') \implies (m'n')(mn'' - m''n) = 0$$
$$\implies mn'' - m''n = 0 \implies mn'' = m''n \implies (m,n) \sim (m'',n'').$$

Ovim je tranzitivnost provjerena.

Dakle, relacija $\sim$ je refleksivna, simetrična i tranzitivna te je stoga relacija ekvivalencije na skupu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. □

Sada definiramo racionalne brojeve kao klasu ekvivalencije za relaciju $\sim$ (vidite definiciju 3.20):

Definicija 9.3. *Neka je $(m,n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.* ***Racionalan broj*** *$\frac{m}{n}$ je klasa ekvivalencije određena sa (m,n), tj.*

$$\frac{m}{n} = [(m,n)] = \{(m',n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (m,n) \sim (m',n') \ \ \textit{tj.} \ \ mn' = m'n\}.$$

Skup racionalnih brojeva $\mathbb{Q}$ je skup svih takvih klasa ekvivalencije.

Primjer 9.4. $\frac{3}{1} = \{(m',n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (3,1) \sim (m',n') \ \ \textit{tj.} \ \ 3n' = m'\} = \{(3n',n') \mid n' \in \mathbb{Z} \setminus \{0\}\}$.

Primjer 9.5. $\frac{0}{5} = \{(m',n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (0,5) \sim (m',n') \ \ \textit{tj.} \ \ 0 = 5m'\} = \{(0,n') \mid n' \in \mathbb{Z} \setminus \{0\}\}$.

Primjer 9.6. $\frac{5}{0}$ *nije definirano jer* $(5,0) \notin \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Primjer 9.7. $\frac{1}{2} = \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (1,2) \sim (m', n') \ \ tj. \ \ n' = 2m'\} = \{(m', 2m') \mid m' \in \mathbb{Z} \setminus \{0\}\}$.

Primjer 9.8. $\frac{-3}{-4} = \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (-3,-4) \sim (m', n') \ \ tj. \ \ (-3)n' = (-4)m'\} = \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid 3n' = 4m'\} = \frac{3}{4}$.

Sljedeća lema dokazuje da je kraćenje koje smo naučili u osnovnoj školi korektno definirano:

$$\frac{6}{4} = \frac{\cancel{2} \cdot 3}{\cancel{2} \cdot 2} = \frac{3}{2}.$$

Lema 9.9. *Neka je $k \in \mathbb{Z} \setminus \{0\}$. Tada je*

$$\frac{k \cdot m}{k \cdot n} = \frac{m}{n}$$

za svaki $\frac{m}{n} \in \mathbb{Q}$.

Dokaz. Imamo redom

$$\begin{aligned} \frac{k \cdot m}{k \cdot n} &= \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid (k \cdot m, k \cdot n) \sim (m', n')\} \\ &= \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid kmn' = km'n\} \\ &= \{(m', n') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid mn' = m'n\} = \frac{m}{n}. \end{aligned}$$

Naglasimo da zbog $k \neq 0$ imamo

$$kmn' = km'n \iff k(mn' - m'n) = 0 \iff mn' - m'n = 0 \iff mn' = m'n.$$

$\square$

Iz leme 9.9 posebno slijedi

$$\frac{-m}{-n} = \frac{(-1) \cdot m}{(-1) \cdot n} = \frac{m}{n}.$$

Zato uvijek možemo zapisati racionalan broj u obliku

$$\frac{m}{n},$$

gdje je brojnik $m \in \mathbb{Z}$, a nazivnik $n \in \mathbb{N}$. Dakle,

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, \ n \in \mathbb{N} \right\}.$$

U sljedećem teoremu ćemo dokazati da svaki racionalan broj možemo zapisati u obliku $\frac{m}{n}$, gdje su $m \in \mathbb{Z}$ i $n \in \mathbb{N}$ relativno prosti brojevi (vidite definiciju ispred zadatka 8.25).

Teorem 9.10. *Za svaki racionalan broj $r \in \mathbb{Q}$, $r \neq \frac{0}{1}$, postoji jedinstveni cijeli broj m i jedinstveni prirodan broj n koji su relativno prosti takvi da je*

$$r = \frac{m}{n}.$$

Dokaz. Napišimo

$$r = \frac{m'}{n'},$$

gdje su $m' \in \mathbb{Z}$ i $n' \in \mathbb{N}$. Kako je $r \neq \frac{0}{1}$, to je $m' \neq 0$. Stoga je najveća zajednička mjera $M(m', n') \in \mathbb{N}$ brojeva m' i n' definirana (vidite definiciju 8.22). Tada $M(m', n')$ dijeli i m' i n', pa možemo pisati

$$m' = M(m', n') \cdot m, \quad m \in \mathbb{Z}; \qquad n' = M(m', n') \cdot n, \quad n \in \mathbb{N}.$$

Ove jednakosti pokazuju da je najveća zajednička mjera brojeva m i n jednaka 1 (tj. oni su relativno prosti) jer je $M(m', n')$ najveća zajednička mjera brojeva m' i n'. Sada je, prema lemi 9.9,

$$r = \frac{m'}{n'} = \frac{M(m', n') \cdot m}{M(m', n') \cdot n} = \frac{m}{n}.$$

Ovim je egzistencija barem jednog prikaza dokazana.

Ostaje dokazati jedinstvenost. Neka je

$$\frac{m}{n} = \frac{m_1}{n_1} \iff mn_1 = m_1 n,$$

gdje su m, m_1 cijeli brojevi različiti od nule (jer je $r \neq \frac{0}{1}$), $n, n_1 \in \mathbb{N}$, takvi da je

$$M(m, n) = M(m_1, n_1) = 1.$$

Moramo dokazati da vrijedi

$$m = m_1 \text{ i } n = n_1.$$

Kako je

$$mn_1 = m_1 n,$$

to su m i m_1 istog predznaka (sjetimo se da su različiti od nule te da su $n, n_1 > 0$ jer su to prirodni brojevi. Dakle, eventualnim množenjem te jednakosti s -1, možemo pretpostaviti da su m i m_1 prirodni brojevi. Brojeve m, n, m_1, n_1 rastavimo na proste faktore kao u osnovnom teoremu aritmetike (teorem 8.21). Kako je $mn_1 = m_1 n$, to je

$$\begin{aligned}&(\text{rastav na proste faktore od } m) \cdot (\text{rastav na proste faktore od } n_1) = \\ &= (\text{rastav na proste faktore od } m_1) \cdot (\text{rastav na proste faktore od } n).\end{aligned}$$

Kako je $M(m, n) = 1$, to prema zadatku 8.25 (b) brojevi m i n nemaju niti jedan prosti faktor koji se pojavljuje i u rastavu od m i u rastavu od n; analogno za m_1 i n_1. Znači da je $m = m_1$ i $m+ = n_1$. □

Sada prelazimo na definiciju zbrajanja, množenja i uređaja u $\mathbb{Q}$. One su dane sa (9.1). Jedino moramo provjeriti da tako definirane operacije ne ovise o izboru predstavnika klase. Započinjemo sa zbrajanjem i množenjem:

Lema 9.11. *Neka su* $(m,n),(m',n'),(m_1,n_1),(m_1',n_1') \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$. *Ako je* $(m,n)\sim(m_1,n_1)$ *i* $(m',n')\sim(m_1',n_1')$, *onda je*

$$\begin{aligned}&(mn'+m'n,nn')\sim(m_1n_1'+m_1'n_1,n_1n_1'),\\&(mm',nn')\sim(m_1m_1',n_1n_1').\end{aligned}$$

Prije samog dokaza leme 9.11, objasnimo njezino značenje. Stavimo

$$r=\frac{m}{n}=\frac{m_1}{n_1},\quad q=\frac{m'}{n'}=\frac{m_1'}{n_1'}.$$

Tada racionalan broj $r+q$ možemo definirati na dva načina:

$$r+q=\frac{m}{n}+\frac{m'}{n'}=\frac{mn'+m'n}{nn'}$$

i

$$r+q=\frac{m_1}{n_1}+\frac{m_1'}{n_1'}=\frac{m_1n_1'+m_1'n_1}{n_1n_1'}.$$

Rezultat mora biti isti tj.

$$\frac{mn'+m'n}{nn'}=\frac{m_1n_1'+m_1'n_1}{n_1n_1'}.$$

Gornja jednakost je ekvivalentna sa

$$(mn'+m'n,nn')\sim(m_1n_1'+m_1'n_1,n_1n_1').$$

Slično vrijedi i za produkt $r\cdot q$. Imamo dva prikaza:

$$r\cdot q=\frac{m}{n}\cdot\frac{m'}{n'}=\frac{mm'}{nn'}$$

i

$$r\cdot q=\frac{m_1}{n_1}\cdot\frac{m_1'}{n_1'}=\frac{m_1m_1'}{n_1n_1'}$$

koji moraju davati isti rezultat:

$$\frac{mm'}{nn'}=\frac{m_1m_1'}{n_1n_1'}.$$

Prethodna jednakost je ekvivalentna sa

$$(mm',nn')\sim(m_1m_1',n_1n_1').$$

Dokaz leme 9.11. Kako je $(m,n)\sim(m_1,n_1)$ i $(m',n')\sim(m_1',n_1')$, to imamo

$$mn_1=m_1n,\quad m'n_1'=m_1'n'.$$

Najprije dokažimo

$$(mm',nn')\sim(m_1m_1',n_1n_1'),$$

što je ekvivalentno sa

$$(n_1n_1')(mm')=(nn')(m_1m_1').$$

Ova jednakost slijedi množenjem jednakosti $mn_1=m_1n$ i $m'n_1'=m_1'n'$:

$$(mn_1)(m'n_1')=(m_1n)(m_1'n')\iff(n_1n_1')(mm')=(nn')(m_1m_1').$$

Sada dokažimo

$$(mn' + m'n, nn') \sim (m_1n_1' + m_1'n_1, n_1n_1').$$

To je ekvivalentno sa

$$(n_1n_1')(mn' + m'n) = (nn')(m_1n_1' + m_1'n_1),$$

pa računamo

$$\begin{aligned}
& (n_1n_1')(mn' + m'n) - (nn')(m_1n_1' + m_1'n_1) \\
= \ & mn'n_1n_1' + m'nn_1n_1' - m_1n_1'nn' - m_1'n_1nn' \\
= \ & (mn'n_1n_1' - m_1n_1'nn') + (m'nn_1n_1' - m_1'n_1nn') \\
= \ & (n'n_1')\,(mn_1 - m_1n) + (nn_1)\,(m'n_1' - m_1'n') \\
= \ & (n'n_1') \cdot 0 + (nn_1) \cdot 0 = 0.
\end{aligned}$$

Ovim je i $(mn' + m'n, nn') \sim (m_1n_1' + m_1'n_1, n_1n_1')$ dokazano. □

Sada provjeravamo da uređaj definiran trećom relacijom u (9.1) ne ovisi o izboru predstavnika. Kao i ranije, stavimo

$$r = \frac{m}{n} = \frac{m_1}{n_1}, \quad q = \frac{m'}{n'} = \frac{m_1'}{n_1'}.$$

Prema (9.1), uređaj može biti definiran na dva načina:

$$r < q \iff \frac{m}{n} \leq \frac{m'}{n'} \iff (m'n - mn')(nn') \geq 0$$

i

$$r < q \iff \frac{m_1}{n_1} \leq \frac{m_1'}{n_1'} \iff (m_1'n_1 - m_1n_1')(n_1n_1') \geq 0.$$

Moramo dokazati da su ti načini ekvivalentni. To je sadržaj sljedeće leme.

Lema 9.12. *Neka su $(m,n), (m',n'), (m_1,n_1), (m_1',n_1') \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Ako je $(m,n) \sim (m_1,n_1)$ i $(m',n') \sim (m_1',n_1')$, onda je*

$$(m'n - mn')(nn') \geq 0 \iff (m_1'n_1 - m_1n_1')(n_1n_1') \geq 0.$$

Dokaz. Kako je $(m,n) \sim (m_1,n_1)$ i $(m',n') \sim (m_1',n_1')$, to je

$$mn_1 = m_1n, \quad m'n_1' = m_1'n'.$$

Sada imamo

$$\begin{aligned}
& (m'n - mn')(nn')(n_1n_1')^2 \\
= \ & (nn'n_1n_1')(m'nn_1n_1' - mn'n_1n_1') \\
= \ & (nn'n_1n_1')\big((m'n_1')(nn_1) - (mn_1)(n'n_1')\big) \\
= \ & (nn'n_1n_1')\big((m_1'n')(nn_1) - (m_1n)(n'n_1')\big) \\
= \ & (nn')^2(n_1n_1')(m_1'n_1 - m_1n_1').
\end{aligned}$$

Kako su $n, n', n_1, n_1' \neq 0$, odatle slijedi

$$\begin{aligned}
& (m'n - mn')(nn') \geq 0 \iff (m'n - mn')(nn')(n_1n_1')^2 \geq 0 \\
& \iff (nn')^2(n_1n_1')(m_1'n_1 - m_1n_1') \geq 0 \iff (m_1'n_1 - m_1n_1')(n_1n_1') \geq 0.
\end{aligned}$$

Ovim je lema dokazana. □

Ostaje nam "smjestiti" $\mathbb{Z}$ u $\mathbb{Q}$. Mi ćemo identificirati skup $\mathbb{Z}$ s podskupom skupa $\mathbb{Q}$ preko preslikavanja:

$$f : \mathbb{Z} \to \mathbb{Q}, \quad f(x) = \frac{x}{1}.$$

Sljedeća lema pokazuje da su svojstva zbrajanja, množenja i uspoređivanja očuvana. Isto tako, možemo identificirati x i $f(x) = \frac{x}{1}$ jer je f injekcija pa različite elemente skupa $\mathbb{Z}$ preslikava u različite elemente skupa $\mathbb{Q}$.

Lema 9.13. *Preslikavanje $f : \mathbb{Z} \to \mathbb{Q}$ definirano sa $f(x) = \frac{x}{1}$ je injektivno te zadovoljava*

$$\begin{aligned}
&f(x+y) = f(x) + f(y) \quad \textit{tj.} \quad \frac{x+y}{1} = \frac{x}{1} + \frac{y}{1}, \quad \forall x, y \in \mathbb{Z},\\
&f(x \cdot y) = f(x) \cdot f(y) \quad \textit{tj.} \quad \frac{x \cdot y}{1} = \frac{x}{1} \cdot \frac{y}{1}, \quad \forall x, y \in \mathbb{Z},\\
&x \leq y \implies f(x) \leq f(y) \quad \textit{tj.} \quad \frac{x}{1} \leq \frac{y}{1}.
\end{aligned}$$

Dokaz. Dokazujemo samo injektivnost dok se ostala svojstva jednostavno provjere iz definicije zbrajanja, množenja i uređaja na $\mathbb{Q}$.

Za dokaz injektivnosti treba provjeriti

$$(\forall x, y \in \mathbb{Z})\ (f(x) = f(y) \implies x = y).$$

Imamo:

$$f(x) = f(y) \implies \frac{x}{1} = \frac{y}{1} \implies (x,1) \sim (y,1) \implies 1 \cdot x = 1 \cdot y \implies x = y.$$

$\square$

U sljedećem teoremu ćemo popisati svojstva koja zadovoljava $(\mathbb{Q}, +, \cdot, \leq)$. Napomenimo da navedena svojstva definiraju matematičku strukturu koju nazivamo uređeno polje.

Teorem 9.14. *Za $(\mathbb{Q}, +, \cdot, \leq)$ vrijede sljedeće tvrdnje:*

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

(2) *(postojanje neutralnog elementa za zbrajanje)* $x + 0 = 0 + x = x, \quad \forall x \in \mathbb{Q}$,
gdje je $0 \stackrel{def}{=} \dfrac{0}{1}$;

(3) *(postojanje suprotnog elementa)* $x + (-x) = (-x) + x = 0, \quad \forall x \in \mathbb{Q}$,
gdje je $-x \stackrel{def}{=} \dfrac{-m}{n}$ *ako je* $x = \dfrac{m}{n}$;

(4) *(komutativnost zbrajanja)* $x + y = y + x, \quad \forall x, y \in \mathbb{Q}$;

(5) *(asocijativnost množenja)* $(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in \mathbb{Q}$;

(6) *(postojanje jedinice za množenje)* $x \cdot 1 = 1 \cdot x = x, \quad \forall x \in \mathbb{Q}$,

gdje je $1 \overset{def}{=} \dfrac{1}{1}$;

(7) *(postojanje inverznog elementa)* $x \cdot x^{-1} = x^{-1} \cdot x = 1, \quad \forall x \in \mathbb{Q} \setminus \{0\}$,

gdje je $x^{-1} \overset{def}{=} \dfrac{n}{m}$ *ako je* $x = \dfrac{m}{n}$;

(8) *(komutativnost množenja)* $x \cdot y = y \cdot x, \quad \forall x, y \in \mathbb{Q}$;

(9) *(distributivnost množenja prema zbrajanju)* $(x + y) \cdot z = x \cdot z + y \cdot z$,
$\forall x, y, z \in \mathbb{Q}$;

(10) *(refleksivnost uređaja)* $x \leq x, \quad \forall x \in \mathbb{Q}$;

(11) *(antisimetričnost uređaja)* $x \leq y$ *i* $y \leq x \implies x = y, \quad \forall x, y \in \mathbb{Q}$;

(12) *(tranzitivnost uređaja)* $x \leq y$ *i* $y \leq z \implies y \leq z, \quad \forall x, y, z \in \mathbb{Q}$;

(13) *(usporedljivost)* $x \leq y$ *ili* $y \leq x, \quad \forall x, y \in \mathbb{Q}$;

(14) *(usklađenost uređaja i zbrajanja)* $x \leq y \implies x + z \leq y + z, \quad \forall x, y, z \in \mathbb{Q}$;

(15) *(usklađenost uređaja i množenja)* $x \leq y \implies x \cdot z \leq y \cdot z$,
$\forall x, y, z \in \mathbb{Q}, \quad z \geq 0$.

Uočimo da tvrdnje (10)-(13) pokazuju da je struktura $(\mathbb{Q}, \leq)$ totalno uređen skup (vidite definiciju 3.10).

Teorem 9.15 (Gustoća skupa racionalnih brojeva)**.** *Za sve* $x, y \in \mathbb{Q}$ *sa svojstvom* $x < y$ *postoji* $z \in \mathbb{Q}$ *takav da je* $x < z < y$.

Dokaz. Aritmetička sredina $z = \frac{x+y}{2} \in \mathbb{Q}$ i zadovoljava $x < z < y$. □

Razmještaj racionalnih brojeva na brojevni pravac. Neka je π ravnina i $p \subset \pi$ bilo koji pravac. Izaberimo na pravcu p točku O i neku drugu točku $E \neq O$.

Izborom točaka O i E konstruiramo razmještaj racionalnih pravaca na brojevni pravac. "Razmještaj" je preslikavanje $f : \mathbb{Z} \to p$ konstruirano na ovaj način:

Korak 1. Stavimo $f(0) = O$ i $f(1) = E$.

Korak 2. Konstrukcija točaka $f\left(\frac{1}{n}\right)$ kada n prolazi po prirodnim brojevima $n \geq 2$.

Ovdje smo isključili $n = 1$ jer je taj slučaj razmatran u prethodnom koraku.

Neka je stoga $n \geq 2$ dan. Ovaj korak se zasniva na podjeli dužine $\overline{OE}$ na n jednakih dijelova (detalji u kolegiju Elementarna geometrija). Ako su $E_1, E_2, \ldots, E_n = E$ točke koje dužinu $\overline{OE}$ dijele na n jednakih dijelova, tada je $f(\frac{1}{n}) = E_1$.

Korak 3. Konstrukcija točaka $r = \frac{m}{n}$, gdje je $m \in \mathbb{Z}$ i $n \in \mathbb{N}$.

Pretpostavimo da je $m \neq 0$ tako da je $r \neq 0$. Uzmimo da su m i n relativno prosti (te zato i jedinstveno određeni prema teoremu 9.10). Neka je $E_1 = f(\frac{1}{n})$.

Ako napišemo

$$r = \frac{m}{n} = m \cdot \frac{1}{n},$$

tada je točka $f(r)$ dobivena nanošenjem dužine $\overline{OE_1}$

- m puta od O u smjeru u kojem se nalazi E_1 ako je $m > 0$,
- $(-m)$ puta od O u smjeru suprotnom od onog u kojem se nalazi E_1 ako je $m < 0$.

10. Realni brojevi

Promotrimo kvadrat čija stranica ima duljinu 1. Ako duljinu dijagonale tog kvadrata označimo sa x, iz Pitagorinog teorema slijedi $x^2 = 1^2+1^2$ odnosno $x^2 = 2$. Možemo li ovu jednadžbu riješiti u skupu racionalnih brojeva? Sljedeći rezultat daje negativan odgovor na ovo pitanje.

Propozicija 10.1. *Jednadžba $x^2 = 2$ nema rješenja u skupu $\mathbb{Q}$.*

Dokaz. Pretpostavimo suprotno, tj. pretpostavimo da postoji $x \in \mathbb{Q}$ takav da je $x^2 = 2$. Očigledno je $x \neq 0$ i $(-x)^2 = x^2 = 2$, pa bez smanjenja općenitosti smijemo pretpostaviti $x > 0$.

Prema teoremu 7.10, za taj x postoje jedinstveni $m, n \in \mathbb{N}$ takvi da je $x = \frac{m}{n}$ i $M(m, n) = 1$.

Sada imamo:
$$2 = x^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2},$$
pa je $m^2 = 2n^2$. Odavde najprije slijedi $2 \mid m^2$, a zatim $2 \mid m$. Dakle, postoji $k \in \mathbb{N}$ takav da je $m = 2k$. Tada je
$$2n^2 = m^2 = (2k)^2 = 4k^2$$
odakle slijedi $n^2 = 2k^2$. Odavde zaključujemo $2 \mid n^2$ i konačno $2 \mid n$. Dakle, $2 \mid m$ i $2 \mid n$, pa je $M(m, n) \neq 1$. Kontradikcija.

Prema tome, jednadžba $x^2 = 2$ nema rješenja u skupu racionalnih brojeva. $\square$

Vidimo kako se javlja potreba da skup $\mathbb{Q}$ proširimo do skupa $\mathbb{R}$ čiji će elementi popuniti brojevni pravac. Elementi skupa $\mathbb{R}$ se zovu **realni brojevi**.

Sada dokažimo sljedeću tvrdnju:
$$(\forall r \in \mathbb{Q})(\exists n \in \mathbb{N})(r < n). \tag{10.2}$$
Ako je $r \leq 0$, tvrdnja je trivijalna jer se bilo koji prirodni broj može uzeti za takav n. Zato pretpostavimo da je $r > 0$ i stavimo $r = \frac{p}{q}$, gdje su $p, q \in \mathbb{N}$. Prema teoremu o dijeljenju s ostatkom (teorem 6.16), postoje jedinstveni $a \in \mathbb{Z}$ i $b \in \{0, 1, \ldots, q-1\}$ takvi da je
$$p = qa + b.$$
Slijedi
$$r = \frac{p}{q} = a + \frac{b}{q} < a + 1.$$
Bit će dovoljno dokazati da je $a + 1 \in \mathbb{N}$ jer tada možemo uzeti $n = a + 1$. Ako je $a \leq -1$, tada je $qa \leq -q$, pa je $qa + b \leq -q + b < 0$, odnosno $p < 0$; to je u kontradikciji sa $p \in \mathbb{N}$. Kako je $a \in \mathbb{Z}$, zaključujemo da je tada $a \in \mathbb{N} \cup \{0\}$ i stoga $a + 1 \in \mathbb{N}$, što je i trebalo dokazati.

Uočimo da smo zapravo dokazali da za svaki $p \in \mathbb{Z}$ i svaki $q \in \mathbb{N}$ postoji $n \in \mathbb{N}$ takav da je $n \cdot q > p$. Naime, dokazali smo da za $r = \frac{p}{q} \in \mathbb{Q}$ postoji $n \in \mathbb{N}$ takav da je $n > r$, pa je $n \cdot q > r \cdot q = p$.

Definirajmo sljedeće skupove:

$$A = \{r_1 \in \mathbb{Q} \,|\, r_1 > 0,\, {r_1}^2 < 2\},$$

$$B = \{r_2 \in \mathbb{Q} \,|\, r_2 > 0,\, {r_2}^2 > 2\}.$$

Neka su $r_1 \in A$ i $r_2 \in B$ izabrani po volji. Vrijedi ${r_1}^2 < 2 < {r_2}^2$. Slijedi

$$0 < {r_2}^2 - {r_1}^2 = (r_2 - r_1)(r_1 + r_2).$$

Kako su $r_1, r_2 > 0$, to je $r_1 + r_2 > 0$, pa iz gornje nejednakosti slijedi $r_2 - r_1 > 0$ odnosno $r_1 < r_2$. Drugim riječima, svaki element skupa A je manji od svakog elementa skupa B.

Sada ćemo dokazati da ne postoji $r \in \mathbb{Q}$ takav da je $r_1 \leq r \leq r_2$ za svaki $r_1 \in A$ i svaki $r_2 \in B$.

Pretpostavimo suprotno, tj. pretpostavimo da takav $r \in \mathbb{Q}$ postoji. Kako je $r_1 > 0$ za svaki $r_1 \in A$, to je i $r > 0$. Pretpostavimo $r \in A$. Znači da je $r^2 < 2$. Za svaki $n \in \mathbb{N}$ imamo

$$\left(r + \frac{1}{n}\right)^2 = r^2 + \frac{2}{n}r + \frac{1}{n^2} \leq r^2 + \frac{2r}{n} + \frac{1}{n} = r^2 + \frac{2r+1}{n}.$$

Uočimo da postoji $n_0 \in \mathbb{N}$ takav da je desna strana gornje nejednakosti manja od 2. Naime, $r^2 + \frac{2r+1}{n_0} < 2$ je ekvivalentno sa $\frac{2r+1}{2-r^2} < n_0$, a kako je $r \in \mathbb{Q}$, to je i $\frac{2r+1}{2-r^2} \in \mathbb{Q}$, pa (10.2) povlači egzistenciju takvog prirodnog broja. No, tada je i

$$\left(r + \frac{1}{n_0}\right)^2 < 2,$$

a obzirom da je $r + \frac{1}{n_0} > 0$, odatle slijedi $r + \frac{1}{n_0} \in A$. Međutim, $r_1 \leq r$ za svaki $r_1 \in A$. Posebno, $r + \frac{1}{n_0} \leq r$; kontradikcija. Prema tome, $r \notin A$.

Sada pretpostavimo $r \in B$. Slijedi $r^2 > 2$. Za svaki $n \in \mathbb{N}$ imamo

$$\left(r - \frac{1}{n}\right)^2 = r^2 - \frac{2}{n}r + \frac{1}{n^2} > r^2 - \frac{2r}{n}.$$

Uzmimo $n_0 \in \mathbb{N}$ takav da je desna strana gornje nejednakosti veća od 2. Dovoljno je uzeti $n_0 \in \mathbb{N}$ takav da je $\frac{2r}{r^2-2} < n_0$, obzirom da je ova nejednakost ekvivalentna sa $r^2 - \frac{2r}{n} > 2$. Slijedi

$$\left(r - \frac{1}{n_0}\right)^2 > 2.$$

Osim toga, iz $0 < \frac{2r}{r^2-2} < n_0$ slijedi $\frac{1}{n_0} < \frac{r^2-2}{2r}$, pa je

$$r - \frac{1}{n_0} > r - \frac{r^2-2}{2r} = \frac{r^2+2}{2r} > 0.$$

Dakle, $r - \frac{1}{n_0} \in B$. No, $r \leq r_2$ za svaki $r_2 \in B$; posebno je $r \leq r - \frac{1}{n_0}$; kontradikcija. Prema tome, $r \notin B$.

Došli smo do zaključka $r \notin A \cup B$. Uočimo:

$$r \in A \cup B \quad \Longleftrightarrow \quad r^2 < 2 \text{ ili } r^2 > 2 \quad \Longleftrightarrow \quad r^2 \neq 2.$$

Prema tome,

$$r \notin A \cup B \Longleftrightarrow r^2 = 2.$$

No, tada propozicija 8.1 povlači $r \notin \mathbb{Q}$, a to je u kontradikciji s pretpostavkom $r \in \mathbb{Q}$. Dakle, ne postoji $r \in \mathbb{Q}$ takav da je $r_1 \leq r \leq r_2$ za svaki $r_1 \in A$ i svaki $r_2 \in B$.

Upravo smo vidjeli ozbiljan nedostatak racionalnih brojeva. Realni brojevi imaju sva svojstva koja imaju i racionalni brojevi, a koja su navedena u teoremu 9.14, no realni brojevi se razlikuju od racionalnih po tome što za njih vrijedi sljedeći aksiom:

Aksiom potpunosti. Neka su A i B neprazni podskupovi od $\mathbb{R}$ sa svojstvom $a \leq b$ za svaki $a \in A$ i svaki $b \in B$. Tada postoji $c \in \mathbb{R}$ takav da je $a \leq c \leq b$ za svaki $a \in A$ i svaki $b \in B$.

Ponovo, neka je

$$A = \{r_1 \in \mathbb{Q} \,|\, r_1 > 0,\, {r_1}^2 < 2\},$$

$$B = \{r_2 \in \mathbb{Q} \,|\, r_2 > 0,\, {r_2}^2 > 2\}.$$

Dokazali smo da je $r_1 < r_2$ za svaki $r_1 \in A$ i svaki $r_2 \in B$ i dokazali smo da ne postoji $r \underline{\in \mathbb{Q}}$ takav da je $r_1 \leq r \leq r_2$ za svaki $r_1 \in A$ i svaki $r_2 \in B$. Međutim, prema aksiomu potpunosti, postoji takav $r \underline{\in \mathbb{R}}$.

Općenito, $c \in \mathbb{R}$ iz aksioma potpunosti ne mora biti jedinstven (aksiom potpunosti daje samo njegovu egzistenciju, ali ne i jedinstvenost).

Evo prve posljedice aksioma potpunosti.

Teorem 10.3 (Arhimedov aksiom)**.** *Neka su $x, y \in \mathbb{R}$, $x > 0$. Tada postoji $n \in \mathbb{N}$ takav da je $n \cdot x > y$.*

Dokaz. Pretpostavimo suprotno, tj. pretpostavimo

$$(\forall n \in \mathbb{N})(n \cdot x \leq y).$$

Definirajmo sljedeće skupove:

$$A = \{n \cdot x \,|\, n \in \mathbb{N}\},$$

$$B = \{b \in \mathbb{R} \,|\, (n \cdot x \leq b)(\forall n \in \mathbb{N})\}.$$

Skup A je očigledno neprazan, a zbog naše pretpostavke je $y \in B$, pa je i skup B neprazan.

Uočimo da je $a \leq b$ za svaki $a \in A$ i svaki $b \in B$. Prema aksiomu potpunosti, postoji $c \in \mathbb{R}$ takav da je $a \leq c \leq b$ za svaki $a \in A$ i svaki $b \in B$. Kako je $x > 0$, to je $c - x < c$, pa $c - x$ nije element skupa B. Znači da postoji $n \in \mathbb{N}$ takav da je $n \cdot x > c - x$, što je ekvivalentno sa $c < (n+1) \cdot x$. No, $(n+1) \cdot x$ je element skupa A, pa je $(n+1) \cdot x \leq c$. Tako smo došli do kontradikcije. Prema tome, postoji $n \in \mathbb{N}$ takav da je $n \cdot x > y$. $\square$

Primijetimo da smo u (10.2) direktno dokazali poseban slučaj Arhimedovog aksioma kada je $x \in \mathbb{N}$ i $y \in \mathbb{Z}$.

Sada promotrimo neke daljnje posljedice aksioma potpunosti.

Teorem 10.4. *Neka je $y \in \mathbb{R}$, $y > 0$. Tada postoji jedinstven $x \in \mathbb{R}$, $x > 0$, takav da je $x^2 = y$.*

Dokaz. Egzistencija. Definirajmo skupove

$$A = \{a \in \mathbb{R} \,|\, a > 0,\, a^2 < y\},$$

$$B = \{b \in \mathbb{R} \,|\, b > 0,\, b^2 > y\}.$$

Najprije dokažimo da su A i B neprazni skupovi. Ako je $y < 1$, tada je $y^2 < y$, pa je $y \in A$; također je $(\frac{1}{y})^2 > 1 > y$, pa je $\frac{1}{y} \in B$. Ako je $y > 1$, tada je $(\frac{1}{y})^2 < 1 < y$, pa je $\frac{1}{y} \in A$, a zbog $y^2 > y$ je $y \in B$. Ako je $y = 1$, tada je primjerice $\frac{1}{2} \in A$ i $2 \in B$.

Uočimo da je $a^2 \leq y < b^2$ za svaki $a \in A$ i svaki $b \in B$. Tada je $0 < b^2 - a^2 = (b-a)(b+a)$, pa je $b - a > 0$, tj. $a < b$ za svaki $a \in A$ i svaki $b \in B$. Aksiom potpunosti povlači egzistenciju realnog broja c sa svojstvom $a \leq c \leq b$ za svaki $a \in A$ i svaki $b \in B$. Kako su svi elementi skupa A pozitivni, to je $c > 0$.

Pretpostavimo $c^2 < y$. Tada za svaki $n \in \mathbb{N}$ vrijedi

$$\left(c + \frac{1}{n}\right)^2 = c^2 + \frac{2c}{n} + \frac{1}{n^2} \leq c^2 + \frac{2c}{n} + \frac{1}{n} = c^2 + \frac{2c+1}{n}.$$

Prema Arhimedovom aksiomu postoji $n_0 \in \mathbb{N}$ takav da je

$$n_0 \cdot 1 > \frac{2c+1}{y - c^2},$$

što je ekvivalentno sa

$$c^2 + \frac{2c+1}{n_0} < y.$$

Slijedi $(c + \frac{1}{n_0})^2 < y$. Kako je $c > 0$, to je i $c + \frac{1}{n_0} > 0$. Dakle, $c + \frac{1}{n_0} \in A$. No, tada mora biti $c + \frac{1}{n_0} \leq c$; kontradikcija.

Pretpostavimo $c^2 > y$. Tada za svaki $n \in \mathbb{N}$ imamo

$$\left(c - \frac{1}{n}\right)^2 = c^2 - \frac{2c}{n} + \frac{1}{n^2} > c^2 - \frac{2c}{n}.$$

Prema Arhimedovom aksiomu postoji $n_0 \in \mathbb{N}$ takav da je

$$n_0 > \frac{2c}{c^2 - y}.$$

To je ekvivalentno sa

$$c^2 - \frac{2c}{n_0} > y.$$

Slijedi $(c - \frac{1}{n_0})^2 > y$. Uočimo da iz $n_0 > \frac{2c}{c^2-y} > 0$ slijedi $\frac{1}{n_0} < \frac{c^2-y}{2c}$, pa je $c - \frac{1}{n_0} > c - \frac{c^2-y}{2c} = \frac{c^2+y}{2c} > 0$. Dakle, $c - \frac{1}{n_0} \in B$. No, tada je $c \leq c - \frac{1}{n_0}$; kontradikcija.

Zaključujemo $c^2 = y$. Prema tome, dovoljno je staviti $x = c$.

Jedinstvenost. Neka su $x_1, x_2 \in \mathbb{R}$, $x_1, x_2 > 0$, takvi da je ${x_1}^2 = y$ i ${x_2}^2 = y$. Slijedi $0 = {x_1}^2 - {x_2}^2 = (x_1 - x_2)(x_1 + x_2)$. Kako je $x_1, x_2 > 0$, to je $x_1 + x_2 > 0$ i stoga mora biti $x_1 - x_2 = 0$, tj. $x_1 = x_2$. □

Za dani pozitivni $y \in \mathbb{R}$, jedinstveni pozitivni $x \in \mathbb{R}$ sa svojstvom $x^2 = y$ naziva se **drugi korijen** iz y i označava sa $\sqrt{y}$.

Analogno teoremu 10.4 bi se dokazao i sljedeći teorem.

Teorem 10.5. *Neka je $n \in \mathbb{N}$ i $y \in \mathbb{R}$, $y > 0$. Tada postoji jedinstven $x \in \mathbb{R}$, $x > 0$, takav da je $x^n = y$.*

Neka je $n \in \mathbb{N}$. Za dani pozitivni $y \in \mathbb{R}$, jedinstveni pozitivni $x \in \mathbb{R}$ sa svojstvom $x^n = y$ naziva se **n-ti korijen** iz y i označava sa $\sqrt[n]{y}$.

Korolar 10.6. *Neka je $n \in \mathbb{N}$ neparan i $y \in \mathbb{R}$. Tada postoji jedinstven $x \in \mathbb{R}$ takav da je $x^n = y$.*

Zadatak 10.7. *Dokazati korolar 10.6 primjenom teorema 10.5.*

Teorem 10.5 i korolar 10.6 kompletiraju dokaz Propozicija 5.18 i 5.19.

Primijetimo da smo korolarom 10.6 uspjeli završiti primjer 7.15 (preciznije, dokazati surjektivnost preslikavanja $x \mapsto x^3$ sa $\mathbb{R}$ na $\mathbb{R}$) jer iz ovog korolara posebno slijedi $(\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(x^3 = y)$.

Rekli smo da realni brojevi zadovoljavaju sva svojstva navedena u teoremu 9.14 za racionalne brojeve. Posebno, relacija "$\leq$" na skupu $\mathbb{R}$ je relacija parcijalnog uređaja. Ranije smo za parcijalno uređen skup definirali njegovu gornju i donju među, supremum i infimum, maksimum i minimum (vidite definiciju 3.13 i zadatak 3.15). Znači da ovi pojmovi imaju smisla za sve neprazne podskupove skupa $\mathbb{R}$.

Istaknimo još jednom odgovarajuće definicije.

Definicija 10.8. *Neka je $S \subseteq \mathbb{R}$ neprazan skup.*

(a) *Kažemo da je skup S **odozgo omeđen** ako postoji $M \in \mathbb{R}$ takav da je $s \leq M$ za svaki $s \in S$. Takav $M \in \mathbb{R}$ se naziva **gornja međa** skupa S.*
(b) *Kažemo da je skup S **odozdo omeđen** ako postoji $m \in \mathbb{R}$ takav da je $m \leq s$ za svaki $s \in S$. Takav $m \in \mathbb{R}$ se naziva **donja međa** skupa S.*
(c) *Najmanja gornja međa skupa S se naziva **supremum** skupa S i označava sa $\sup S$.*
(d) *Najveća donja međa skupa S se naziva **infimum** skupa S i označava sa $\inf S$.*
(e) *Najveći element skupa S je $M \in S$ sa svojstvom $s \leq M$ za svaki $s \in S$. Takav $M \in S$ se naziva **maksimum** skupa S i označava sa $\max S$.*

(f) *Najmanji element skupa S je $m \in S$ sa svojstvom $m \leq s$ za svaki $s \in S$. Takav $m \in S$ se naziva **minimum** skupa S i označava sa* $\min S$.

Sljedeći važan rezultat je posljedica aksioma potpunosti (usporedite ga s propozicijom 3.14 i zadatkom 3.15). On opravdava oznake $\sup S$, $\inf S$, $\max S$ i $\min S$ za supremum, infimum, maksimum i minimum skupa S, redom.

Teorem 10.9. *Neka je $S \subseteq \mathbb{R}$ neprazan skup. Tada vrijede sljedeće tvrdnje:*

(i) *Ako je S odozgo omeđen skup, tada postoji supremum skupa S i on je jedinstven.*
(ii) *Ako je S odozdo omeđen skup, tada postoji infimum skupa S i on je jedinstven.*
(iii) *Ako postoji maksimum skupa S, tada je on jedinstven i jednak supremumu skupa S.*
(iv) *Ako postoji minimum skupa S, tada je on jedinstven i jednak infimumu skupa S.*

Dokaz. (i) Neka je

$$A = S, \quad B = \{b \in \mathbb{R} \mid b \text{ je gornja međa skupa } S\}.$$

Po pretpostavci su A i B neprazni skupovi. Očigledno je $a \leq b$ za svaki $a \in A$ i svaki $b \in B$. Prema aksiomu potpunosti postoji $c \in \mathbb{R}$ takav da je $a \leq c \leq b$ za svaki $a \in A$ i svaki $b \in B$. Jasno, c je gornja međa skupa $A = S$. Pretpostavimo da c nije najmanja gornja međa, tj. pretpostavimo da postoji gornja međa M skupa A takva da je $M < c$. Po definiciji skupa B vrijedi $M \in B$. No, tada je $c \leq M$; kontradikcija. Dakle, c je najmanja gornja međa skupa $A = S$ tj. supremum skupa S.

Ako su M_1 i M_2 supremumi skupa S, tada je $M_1 \leq M_2$ (jer je M_1 najmanja gornja međa, a M_2 je gornja međa) i $M_2 \leq M_1$ (jer je M_2 najmanja gornja međa, a M_1 je gornja međa). Slijedi $M_1 = M_2$. Prema tome, supremum skupa S je jedinstven.

(ii) Analogno kao (i), pri čemu se definira:

$$A = \{a \in \mathbb{R} \mid a \text{ je donja međa skupa } S\}, \quad B = S.$$

(iii) Neka je $M = \max S \in S$. Tada je $s \leq M$ za svaki $s \in S$. Ako postoji $M' \in S$ takav da je $s \leq M'$ za svaki $s \in S$, posebno je $M \leq M'$ (jer je M element skupa S, a M' maksimum skupa S) i $M' \leq M$ (jer je M' element skupa S, a M maksimum skupa S). Dakle, $M = M'$.

Jasno, M je gornja međa skupa S. Dokažimo da je najmanja. Ako nije, tada postoji gornja međa L skupa S takva da je $L < M$. Sada imamo: $s \leq L < M$ za svaki $s \in S$. Posebno je $M \leq L < M$; kontradikcija. Dakle, $M = \sup S$.

(iv) Analogno kao (iii). $\square$

Primjer 10.10. *Neka su $a, b \in \mathbb{R}$, $a \leq b$.*

- *Skup* $[a, b] = \{x \in \mathbb{R} \,|\, a \leq x \leq b\}$ *ima minimum* a *i maksimum* b.
- *Skup* $\langle a, b] = \{x \in \mathbb{R} \,|\, a < x \leq b\}$ *ima infimum* a *i maksimum* b; *nema minimum.*
- *Skup* $[a, b\rangle = \{x \in \mathbb{R} \,|\, a \leq x < b\}$ *ima minimum* a *i supremum* b; *nema maksimum.*
- *Skup* $\langle a, b\rangle = \{x \in \mathbb{R} \,|\, a < x < b\}$ *ima infimum* a *i supremum* b; *nema ni minumum ni maksimum.*
- *Skup* $\langle a, +\infty\rangle = \{x \in \mathbb{R} \,|\, x > a\}$ *ima infimum* a; *nema supremum; nema minimum.*
- *Skup* $\langle -\infty, a\rangle = \{x \in \mathbb{R} \,|\, x < a\}$ *ima supremum* a; *nema infimum; nema maksimum.*
- *Skup* $[a, +\infty\rangle = \{x \in \mathbb{R} \,|\, x \geq a\}$ *ima minimum* a; *nema supremum.*
- *Skup* $\langle -\infty, a] = \{x \in \mathbb{R} \,|\, x \leq a\}$ *ima maksimum* a; *nema infimum.*

Skup $[a, b]$ *zovemo* ***zatvoreni interval ili segment****, skup* $\langle a, b\rangle$ *se naziva* ***otvoreni interval****, a skupovi* $\langle a, b]$ *i* $[a, b\rangle$ ***poluotvoreni intervali****.*

Ako je $S \subseteq \mathbb{R}$ i odozdo i odozgo ograničen, tada on ima i infimum i supremum i vrijedi $\inf S \leq s \leq \sup S$ za svaki $s \in S$. Stoga je $S \subseteq [\inf S, \sup S]$.

Teorem 10.11. *Za svaki* $x \in \mathbb{R}$ *postoji jedinstven* $k \in \mathbb{Z}$ *takav da je*

$$k \leq x < k + 1.$$

Dokaz. Egzistencija. Neka je $x \geq 0$ te neka je $S = \{n \in \mathbb{N} \,|\, x < n\}$. Prema Arhimedovom aksiomu postoji $n \in \mathbb{N}$ takav da je $n \cdot 1 > x$, pa je skup S neprazan. Kako je S neprazan podskup od $\mathbb{N}$, to prema teoremu 6.15 ima minimalni element; taj element označimo sa m. Kako je $m \in S$, to je $x < m$. Pretpostavimo li $m - 1 \in S$, tada je $m \leq m - 1$ jer je $m = \min S$; kontradikcija. Dakle, $m - 1 \notin S$ i stoga vrijedi $x \geq m - 1$. Sada imamo: $m - 1 \leq x < m$. Prema tome, dovoljno je uzeti $k = m - 1 \in \mathbb{Z}$.

Neka je sada $x < 0$. Prema dokazanom, za $-x > 0$ postoji $m \in \mathbb{Z}$ takav da je $m \leq -x < m + 1$. Slijedi $-m \geq x > -m - 1$. Ako je $-m > x > -m - 1$, stavimo $k = -m - 1 \in \mathbb{Z}$ i imamo $k < x < k + 1$. Ako je $x = -m$, stavimo $k = -m \in \mathbb{Z}$.

Jedinstvenost. Pretpostavimo da su $k, l \in \mathbb{Z}$ takvi da je

$$k \leq x < k + 1 \quad \text{i} \quad l \leq x < l + 1.$$

Ako je $k < l$, tada je $k < l \leq x < k+1$, pa se cijeli broj l nalazi između dva susjedna cijela broja k i $k + 1$, što ne može biti. Ako je $l < k$, tada je $l < k \leq x < l + 1$, pa se cijeli broj k nalazi između dva susjedna cijela broja l i $l + 1$, što također ne može biti. Zaključujemo $k = l$. $\square$

Za $x \in \mathbb{R}$, takav $k \in \mathbb{Z}$ iz teorema 10.11 nazivamo **najveći cijeli broj manji ili jednak** x i označavamo sa $\lfloor x \rfloor$ ili $[x]$. O njemu smo već ranije govorili (vidite primjer 4.8), a teoremom 10.11 smo dokazali da je $x \mapsto \lfloor x \rfloor$ dobro definirano preslikavanje sa $\mathbb{R}$ na $\mathbb{Z}$. Restrikcija ovog preslikavanja na skup $\mathbb{Z}$ je identiteta na $\mathbb{Z}$.

U sljedećem teoremu promatramo niz segmenata (za definiciju niza vidite primjer 8.13).

Teorem 10.12 (Cantorov aksiom)**.** *Neka je* (Δ_n)*, gdje je* $\Delta_n = [a_n, b_n]$ *za svaki* $n \in \mathbb{N}$*, niz segmenata sa svojstvom* $\Delta_1 \supseteq \Delta_2 \supseteq \cdots$ *. Tada je*

$$\cap_{n\in\mathbb{N}}\Delta_n \neq \emptyset.$$

Dokaz. Neka je

$$A = \{a_n \,|\, n \in \mathbb{N}\}, \quad B = \{b_n \,|\, n \in \mathbb{N}\}.$$

Neka su $m, n \in \mathbb{N}$. Ako je $n \leq m$, tada zbog $\Delta_n \supseteq \Delta_m$ imamo $a_n \leq b_m$. Ako je $m < n$, tada zbog $\Delta_m \supseteq \Delta_n$ imamo $a_n \leq b_m$. Dakle, $a_n \leq b_m$ za sve $m, n \in \mathbb{N}$.

Drugim riječima, $a \leq b$ za svaki $a \in A$ i svaki $b \in B$. Prema aksiomu potpunosti, postoji $c \in \mathbb{R}$ takav da je $a \leq c \leq b$ za svaki $a \in A$ i svaki $b \in B$. Posebno, $a_n \leq c \leq b_n$ za svaki $n \in \mathbb{N}$, pa je $c \in \Delta_n$ za svaki $n \in \mathbb{N}$. Slijedi $c \in \cap_{n\in\mathbb{N}}\Delta_n$. □

Niz segmenata (Δ_n) sa svojstvom $\Delta_1 \supseteq \Delta_2 \supseteq \cdots$ često nazivamo silaznim nizom segmenata. Prema Cantorovom aksiomu, svaki silazni niz segmenata ima bar jednu zajedničku točku.

11. Decimalni zapis realnog broja

Dekadski brojevni sustav je brojevni sustav s bazom 10, što znači da ima ukupno 10 znamenaka (to su: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$), pri čemu vrijedi:

$$\begin{aligned} 1 &= 0+1, \\ 2 &= 1+1, \\ 3 &= 2+1, \\ &\vdots \\ 9 &= 8+1. \end{aligned}$$

U dekadskom brojevnom sustavu vrijednost znamenke ovisi o njenom položaju u zapisu broja. Sljedbenik broja 9 ima zapis 10, dakle

$$10 = 9 + 1.$$

Svaki prirodni broj ima jedinstven zapis u dekadskom brojevnom sustavu, što ćemo dokazati u sljedećem teoremu.

Teorem 11.1. *Neka je $n \in \mathbb{N}$. Tada postoje jedinstveni $m \in \mathbb{N} \cup \{0\}$ i $a_0, a_1, \ldots, a_m \in \{0, 1, \ldots, 9\}$, $a_m \neq 0$, takvi da je*

$$n = 10^m \cdot a_m + 10^{m-1} \cdot a_{m-1} + \cdots + 10 \cdot a_1 + a_0.$$

Dokaz. Ako je $n \in \{0, 1, \ldots, 9\}$, dovoljno je staviti $a_0 = n$; pri tome je $m = 0$.

Neka je sada $n \geq 10$. Prema teoremu o dijeljenju s ostatkom (teorem 6.16), postoje jedinstveni $n_1 \in \mathbb{Z}$ i $a_0 \in \{0, 1, \ldots, 9\}$ takvi da je

$$n = 10 \cdot n_1 + a_0.$$

Tada je

$$n_1 = \frac{n}{10} - \frac{a_0}{10} > \frac{n}{10} - 1 \geq 0$$

jer je $a_0 < 10$ i $n \geq 10$. Kako je $n_1 \in \mathbb{Z}$, to zaključujemo $n_1 \in \mathbb{N}$.

Ako je $n_1 \leq 9$, tada stavimo $a_1 = n_1$, pa smo gotovi; pri tome je $m = 1$. Ako je $n_1 \geq 10$, nastavljamo postupak: postoje jedinstveni $n_2 \in \mathbb{N}$ i $a_1 \in \{0, 1, \ldots, 9\}$ takvi da je

$$n_1 = 10 \cdot n_2 + a_1,$$

pa je

$$n = 10 \cdot n_1 + a_0 = 10 \cdot (10 \cdot n_2 + a_1) + a_0 = 10^2 \cdot n_2 + 10 \cdot a_1 + a_0.$$

Ako je $n_2 \leq 9$, tada stavimo $a_2 = n_2$ i gotovi smo, a ako je $n_2 \geq 10$, nastavljamo postupak sve dok ne dođemo do zapisa

$$n = 10^m \cdot n_m + 10^{m-1} \cdot a_{m-1} + \cdots + 10 \cdot a_1 + a_0,$$

pri čemu je $n_m \leq 9$. Preostaje staviti $a_m = n_m$, pa imamo

$$n = 10^m \cdot a_m + 10^{m-1} \cdot a_{m-1} + \cdots + 10 \cdot a_1 + a_0.$$

Dokažimo jedinstvenost takvog zapisa. Pretpostavimo da postoje $m \in \mathbb{N} \cup \{0\}$ i $a_0, \ldots, a_m \in \{0, 1, \ldots, 9\}$, $a_m \neq 0$, takvi da je

$$n = 10^m \cdot a_m + \cdots + a_0$$

te da postoje $k \in \mathbb{N} \cup \{0\}$ i $b_0, \ldots, b_k \in \{0, 1, \ldots, 9\}$, $b_k \neq 0$, takvi da je

$$n = 10^k \cdot b_k + \cdots + b_0.$$

Bez smanjenja općenitosti smijemo pretpostaviti $m \leq k$. Imamo

$$n = 10^k \cdot b_k + \cdots + 10^m \cdot b_m + \cdots + b_0.$$

Slijedi

$$10^m \cdot a_m + \cdots + a_0 = 10^k \cdot b_k + \cdots + 10^m \cdot b_m + \cdots + b_0,$$

odnosno

$$10^k \cdot b_k + \cdots + 10^{m+1} \cdot b_{m+1} + 10^m \cdot (b_m - a_m) + \cdots + 10 \cdot (b_1 - a_1) + b_0 - a_0 = 0.$$

Odatle slijedi

$$10 \cdot \big(10^{k-1} \cdot b_k + \cdots + (b_1 - a_1)\big) = a_0 - b_0,$$

odnosno $10 \cdot p = a_0 - b_0$, gdje je

$$p = 10^{k-1} \cdot b_k + \cdots + (b_1 - a_1) \in \mathbb{Z}.$$

Znači da $10 \mid a_0 - b_0$. Zbog $a_0, b_0 \in \{0, 1, \ldots, 9\}$ imamo $b_0 - a_0 \in \{-9, \ldots, 0, \ldots, 9\}$. Stoga $10 \mid a_0 - b_0$ ako i samo ako je $a_0 - b_0 = 0$, odnosno $b_0 = a_0$. Odatle slijedi $p = 0$, odnosno

$$10 \cdot \big(10^{k-2} \cdot b_k + \cdots + (b_2 - a_2)\big) = a_1 - b_1.$$

Dakle, $10 \cdot q = a_1 - b_1$, gdje je

$$q = 10^{k-2} \cdot b_k + \cdots + (b_2 - a_2) \in \mathbb{Z}.$$

Slijedi $10 \mid a_1 - b_1$, pa je $b_1 = a_1$. Nastavimo postupak sve dok ne zaključimo $b_i = a_i$ za svaki $i \in \{0, 1, \ldots, m\}$. Ako je $k \neq m$, tada nam ostaje

$$10^{k-m-1} \cdot b_k + \cdots + 10 \cdot b_{m+2} + b_{m+1} = 0$$

pa $10 \mid b_{m+1} \in \{0, 1, \ldots, 9\}$, odakle slijedi $b_{m+1} = 0$; analogno nastavimo postupak sve dok ne zaključimo $b_k = 0$; kontradikcija. Dakle, $k = m$, a već smo dokazali da je $b_i = a_i$ za svaki $i \in \{0, 1, \ldots, m\}$. Tako smo dokazali jedinstvenost danog zapisa. □

Prema teoremu 11.1, prirodan broj n možemo zapisati u obliku

$$n = \overline{a_m a_{m-1} \ldots a_0}$$

što je praktičniji oblik zapisa

$$n = 10^m \cdot a_m + 10^{m-1} \cdot a_{m-1} + \cdots + 10 \cdot a_1 + a_0,$$

gdje je $m \in \mathbb{N} \cup \{0\}$ i $a_0, a_1, \ldots, a_m \in \{0, 1, \ldots, 9\}$, $a_m \neq 0$. U tom slučaju kažemo da prirodni broj n ima $m+1$ znamenaka odnosno kažemo da je $(m+1)$-znamenkast.

Primjer 11.2. $n = 41352 = 10^4 \cdot 4 + 10^3 \cdot 1 + 10^2 \cdot 3 + 10^1 \cdot 5 + 2$; *n je peteroznamenkast broj.*

Ako je n negativan cijeli broj, tada je $-n \in \mathbb{N}$, pa je moguć zapis oblika

$$-n = \overline{a_m a_{m-1} \dots a_0}$$

odakle slijedi

$$n = -\overline{a_m a_{m-1} \dots a_0}.$$

Brojeve oblika

$$r = \frac{n}{10^p} \qquad (\text{gdje je } n \in \mathbb{Z},\ p \in \mathbb{N})$$

nazivamo **decimalni brojevi**.

Pretpostavimo $r > 0$. Tada je $n \in \mathbb{N}$. Prema teoremu 11.1, postoje jedinstveni $m \in \mathbb{N} \cup \{0\}$ i $a_0, a_1, \dots, a_m \in \{0, 1, \dots, 9\}$, $a_m \neq 0$, takvi da je

$$n = 10^m \cdot a_m + 10^{m-1} \cdot a_{m-1} + \cdots + 10 \cdot a_1 + a_0.$$

Tada je

$$r = \frac{n}{10^p} = 10^{m-p} \cdot a_m + 10^{m-1-p} \cdot a_{m-1} + \cdots + 10^{1-p} \cdot a_1 + 10^{-p} \cdot a_0.$$

Uočimo da su svi eksponenti broja 10 oblika $i - p$ za $i = m, m-1, \dots, 0$. Kako je zadnji među ovim eksponentima jednak $-p$, dakle negativan je, to znači da postoji $k \in \{m, m-1, \dots, 0\}$ takav da su svi eksponenti od $k - p$ do $-p$ negativni. Ako je $k < m$, tada je

$$r = \overline{a_m a_{m-1} \dots a_{k+1} \,.\, a_k \dots a_0},$$

a ako je $k = m$, tada je

$$r = \overline{0 \,.\, a_m \dots a_0}.$$

Pri tome se eventualne nule na kraju zapisa (iza decimalne točke) obično izostavljaju. Dakle, decimalni brojevi imaju konačan decimalan zapis (tj. zapis pomoću znamenaka $0, 1, \dots, 9$ i decimalne točke, pri čemu se iza decimalne točke nalazi konačno mnogo znamenaka).

Ako je $r < 0$, tada je $-r > 0$, pa prema dokazanom $-r$ ima konačan decimalan zapis oblika

$$-r = \overline{a_m a_{m-1} \dots a_{k+1} \,.\, a_k \dots a_0},$$

odakle slijedi

$$r = -\overline{a_m a_{m-1} \dots a_{k+1} \,.\, a_k \dots a_0}.$$

Očigledno vrijedi i obrat, tj. brojevi oblika

$$r = (\pm)\overline{a_m a_{m-1} \dots a_{k+1} \,.\, a_k \dots a_0}$$

su decimalni brojevi.

Primjer 11.3.

$$\begin{aligned} 245.3291 &= 10^2 \cdot 2 + 10^1 \cdot 4 + 5 + 10^{-1} \cdot 3 + 10^{-2} \cdot 2 + 10^{-3} \cdot 9 + 10^{-4} \cdot 1 \\ &= 10^2 \cdot 2 + 10^1 \cdot 4 + 5 + \frac{3}{10} + \frac{2}{10^2} + \frac{9}{10^3} + \frac{1}{10^4}. \end{aligned}$$

Svaki decimalan broj je po definiciji racionalan.

Sada se bavimo određivanjem decimalnog zapisa realnog broja x. Ograničimo se samo na slučaj $x \geq 0$. Ako je $x < 0$, tada gledamo $-x$.

Neka je $n = [x] \in \mathbb{N}_0$ (za objašnjenje oznake $[x]$ vidite tekst iza teorema 10.11 i primjer 4.8). To znači da je

$$n \leq x < n + 1$$

odnosno

$$0 \leq x - n < 1.$$

Stavimo li $y = x - n$, imamo

$$0 \leq y < 1.$$

Ne znamo je li y decimalan broj tj. ne znamo ima li konačan decimalan zapis. Sljedeći algoritam pokazuje kako to ispitati.

<u>1. korak:</u> Neka je $b_1 = [10y]$. Kako je

$$b_1 \leq 10y < b_1 + 1,$$

vrijedi

$$\frac{b_1}{10} \leq y < \frac{b_1 + 1}{10}$$

odnosno

$$0 \leq y - \frac{b_1}{10} < \frac{1}{10}.$$

<u>2. korak:</u> Neka je $b_2 = \left[100\left(y - \frac{b_1}{10}\right)\right]$. Tada je

$$b_2 \leq 100\left(y - \frac{b_1}{10}\right) < b_2 + 1,$$

pa je

$$\frac{b_2}{100} \leq y - \frac{b_1}{10} < \frac{b_2 + 1}{100}$$

odnosno

$$0 \leq y - \frac{b_1}{10} - \frac{b_2}{10^2} < \frac{1}{10^2}.$$

Itd.

Općenito u <u>m-tom koraku</u> definiramo

$$b_m = \left[10^m\left(y - \frac{b_1}{10} - \cdots - \frac{b_{m-1}}{10^{m-1}}\right)\right].$$

Imamo

$$b_m \leq 10^m\left(y - \frac{b_1}{10} - \cdots - \frac{b_{m-1}}{10^{m-1}}\right) < b_m + 1,$$

pa je
$$\frac{b_m}{10^m} \leq y - \frac{b_1}{10} - \cdots - \frac{b_{m-1}}{10^{m-1}} < \frac{b_m+1}{10^m}.$$
Slijedi
$$0 \leq y - \frac{b_1}{10} - \cdots \frac{b_{m-1}}{10^{m-1}} - \frac{b_m}{10^m} < \frac{1}{10^m}.$$

Moguća su dva slučaja:

1. slučaj. Za neki $m \in \mathbb{N}$ se u m-tom koraku dobije
$$y - \frac{b_1}{10} - \cdots \frac{b_{m-1}}{10^{m-1}} - \frac{b_m}{10^m} = 0.$$
Tada je
$$x = n + y = n + \frac{b_1}{10} + \cdots + \frac{b_{m-1}}{10^{m-1}} + \frac{b_m}{10^m} = \overline{n\,.\,b_1\ldots b_{m-1}b_m}$$
tj. x je decimalan broj.

2. slučaj. Za svaki $m \in \mathbb{N}$ je
$$y - \frac{b_1}{10} - \cdots \frac{b_{m-1}}{10^{m-1}} - \frac{b_m}{10^m} \neq 0,$$
preciznije
$$0 < y - \frac{b_1}{10} - \cdots \frac{b_{m-1}}{10^{m-1}} - \frac{b_m}{10^m} < \frac{1}{10^m}.$$
Slijedi da za svaki $m \in \mathbb{N}$ imamo
$$\frac{b_1}{10} + \frac{b_2}{10^2} + \cdots + \frac{b_{m-1}}{10^{m-1}} + \frac{b_m}{10^m} < y < \frac{b_1}{10} + \frac{b_2}{10^2} + \cdots + \frac{b_{m-1}}{10^{m-1}} + \frac{b_m+1}{10^m},$$
pa y nije decimalan broj.

Uočimo da u 2. slučaju nije moguće da broj y završava repom devetki tj. ne postoji $k \in \mathbb{N}$ takav da je $b_m = 9$ za svaki $m \geq k$.

Zašto? Pretpostavimo da je $y = 0.9999\cdots = 0.\dot{9}$. Tada je
$$y = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \cdots$$
Za svaki $n \in \mathbb{N}$ stavimo
$$\begin{aligned} y_n &= \frac{9}{10} + \frac{9}{10^2} + \cdots + \frac{9}{10^n} \\ &= \frac{9}{10} \cdot \left(1 + \frac{1}{10} + \cdots + \frac{1}{10^{n-1}}\right) \\ &= \frac{9}{10} \cdot \frac{1 - \frac{1}{10^n}}{1 - \frac{1}{10}} \\ &= 1 - \frac{1}{10^n}. \end{aligned}$$
Uzimajući sve veći i veći n, broj y_n je s jedne strane sve bliži broju y, a s druge strane je sve bliži broju 1 (jer je $\frac{1}{10^n}$ sve bliži nuli). Slijedi $y = 1$, pa je y decimalan broj.

Ako pretpostavimo da je $y = \overline{0.b_1 \dots b_{k-1}b_k999\dots}$, pri čemu je $b_k < 9$, tada je

$$\begin{aligned} y &= \overline{0.b_1 \dots b_{k-1}b_k999\dots} \\ &= \overline{0.b_1 \dots b_{k-1}b_k} + 0.\underbrace{0\dots0}_{k}\dot{9} \\ &= \overline{0.b_1 \dots b_{k-1}b_k} + \frac{1}{10^k} \cdot 0.\dot{9} \\ &= \overline{0.b_1 \dots b_{k-1}b_k} + \frac{1}{10^k} \\ &= \overline{0.b_1 \dots b_{k-1}(b_k+1)}. \end{aligned}$$

Kako je $b_k < 9$, to je $b_k + 1 \leq 9$, pa je y decimalan broj.

Napomenimo da gornji račun zapravo pokazuje da se svaki broj oblika

$$y = \overline{0.b_1 \dots b_{k-1}b_k999\dots},$$

pri čemu je $b_k < 9$, može zapisati u obliku

$$\overline{0.b_1 \dots b_{k-1}(b_k+1)},$$

dakle decimalan je.

Primjerice,

$$0.57399999\cdots = 0.573\dot{9} = 0.574.$$

Prethodnim razmatranjima smo dokazali sljedeći teorem.

Teorem 11.4. *Svaki $x \in \mathbb{R}$ ima ili konačan decimalan zapis, tj. zapis oblika*

$$x = \overline{n\,.\,b_1 \dots b_{m-1}b_m},$$

ili ima beskonačan decimalan zapis, tj. zapis oblika

$$x = \overline{n\,.\,b_1b_2\dots},$$

pri čemu ne postoji $k \in \mathbb{N}$ takav da je $b_m = 9$ za svaki $m \geq k$.

Naglasimo: ako realan broj x ima konačan decimalan zapis, tada je x decimalan broj, a ako ima beskonačan decimalan zapis koji ne završava repom devetki, tada x nije decimalan broj (međutim, takvi se brojevi često nazivaju opći decimalni brojevi).

Primjer 11.5. *Ako je $x = \frac{1}{3}$, tada je*

$$n = [x] = \left[\frac{1}{3}\right] = 0, \quad y = x - n = \frac{1}{3} - 0 = \frac{1}{3}.$$

Neka je $b_1 = \left[10 \cdot \frac{1}{3}\right] = \left[\frac{10}{3}\right] = 3$. Imamo

$$\frac{3}{10} < \frac{1}{3} < \frac{4}{10}.$$

Vrijedi

$$y - \frac{b_1}{10} = \frac{1}{3} - \frac{3}{10} = \frac{10-9}{30} = \frac{1}{30} = \frac{1}{3\cdot 10}.$$

Neka je $b_2 = \left[100 \cdot \frac{1}{3\cdot 10}\right] = \left[\frac{10}{3}\right] = 3$. *Imamo*

$$\frac{3}{10^2} < \frac{1}{3\cdot 10} < \frac{4}{10^2}$$

i vrijedi

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} = \frac{1}{3} - \frac{3}{10} - \frac{3}{10^2} = \frac{1}{3\cdot 10} - \frac{3}{10^2} = \frac{10-9}{3\cdot 10^2} = \frac{1}{3\cdot 10^2}.$$

Dalje neka je $b_3 = \left[1000 \cdot \frac{1}{3\cdot 10^2}\right] = \left[\frac{10}{3}\right] = 3$. *Vrijedi*

$$\frac{3}{10^3} < \frac{1}{3\cdot 10^2} < \frac{4}{10^3},$$

kao i

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} - \frac{b_3}{10^3} = \frac{1}{3} - \frac{3}{10} - \frac{3}{10^2} - \frac{3}{10^3} = \frac{1}{3\cdot 10^2} - \frac{3}{10^3} = \frac{10-9}{3\cdot 10^3} = \frac{1}{3\cdot 10^3}.$$

Itd.

Pretpostavimo da za neki $m \in \mathbb{N}$ *vrijedi*

$$b_1 = \cdots = b_m = 3, \qquad y - \frac{b_1}{10} - \frac{b_2}{10^2} - \cdots - \frac{b_m}{10^m} = \frac{1}{3\cdot 10^m}.$$

Imamo

$$b_{m+1} = \left[10^{m+1}\left(y - \frac{b_1}{10} - \cdots \frac{b_m}{10^m}\right)\right] = \left[10^{m+1} \cdot \frac{1}{3\cdot 10^m}\right] = \left[\frac{10}{3}\right] = 3.$$

Dalje je

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} - \cdots - \frac{b_m}{10^m} - \frac{b_{m+1}}{10^{m+1}} = \frac{1}{3\cdot 10^m} - \frac{3}{10^{m+1}} = \frac{10-9}{3\cdot 10^{m+1}} = \frac{1}{3\cdot 10^{m+1}}.$$

Tako smo matematičkom indukcijom dokazali da za svaki $m \in \mathbb{N}$ *vrijedi* $b_m = 3$ *i*

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} - \cdots - \frac{b_m}{10^m} = \frac{1}{3\cdot 10^m}.$$

Za svaki $m \in \mathbb{N}$ *očigledno vrijedi*

$$\frac{3}{10^{m+1}} < \frac{1}{3\cdot 10^m} < \frac{4}{10^{m+1}},$$

pa je

$$\frac{3}{10^{m+1}} < y - \frac{b_1}{10} - \frac{b_2}{10^2} - \cdots - \frac{b_m}{10^m} < \frac{4}{10^{m+1}},$$

odnosno, uzevši u obzir da je $y = \frac{1}{3}$ *i* $b_m = 3$ *za svaki* $m \in \mathbb{N}$,

$$\frac{3}{10^{m+1}} < \frac{1}{3} - \frac{3}{10} - \frac{3}{10^2} - \cdots - \frac{3}{10^m} < \frac{4}{10^{m+1}}.$$

Prema tome, za svaki $m \in \mathbb{N}$ imamo

$$\frac{3}{10}+\frac{3}{10^2}+\cdots+\frac{3}{10^m}+\frac{3}{10^{m+1}}<\frac{1}{3}<\frac{3}{10}+\frac{3}{10^2}+\cdots+\frac{3}{10^m}+\frac{4}{10^{m+1}},$$

što znači da je nastupio 2. slučaj iz teorema 11.4.

Dakle, broj $\frac{1}{3}$ nije decimalan, ali ga možemo prikazati pomoću repa trojki:

$$\frac{1}{3}=0.33333\cdots=0.\dot{3}.$$

Općenito: kažemo da realan broj x ima **periodičan decimalan zapis** ako je oblika

$$x=\overline{n.a_1\ldots a_n b_1\ldots b_p b_1\ldots b_p b_1\ldots b_p\ldots},$$

gdje je $n \in \mathbb{Z}$ i $a_1,\ldots,a_n,b_1,\ldots,b_p \in \{0,1,\ldots,9\}$.

Primjerice,

$$\frac{7}{12}=\frac{1}{4}+\frac{1}{3}=0.25+0.33333\cdots=0.58333\cdots=0.58\dot{3}.$$

Vrijedi sljedeći teorem:

Teorem 11.6. *Realan broj x je racionalan ako i samo ako ima periodičan decimalan zapis.*

Primjer 11.7. *Broj $\sqrt{2}$ nije racionalan (vidite propoziciju 10.1), pa nema periodičan decimalan zapis.*

Primjer 11.8. *Kako je broj $\frac{5}{7}$ racionalan, to ima periodičan decimalan zapis. Odredimo ga. Stavimo $y=\frac{5}{7}$.*

Neka je $b_1=\left[10\cdot\frac{5}{7}\right]=7$. Tada je

$$y-\frac{b_1}{10}=\frac{5}{7}-\frac{7}{10}=\frac{1}{70}.$$

Neka je $b_2=\left[100\cdot\frac{1}{70}\right]=\left[\frac{10}{7}\right]=1$. Tada je

$$y-\frac{b_1}{10}-\frac{b_2}{100}=\frac{1}{70}-\frac{1}{100}=\frac{3}{700}.$$

Neka je $b_3=\left[10^3\cdot\frac{3}{700}\right]=\left[\frac{30}{7}\right]=4$. Tada je

$$y-\frac{b_1}{10}-\frac{b_2}{10^2}-\frac{b_3}{10^3}=\frac{3}{700}-\frac{4}{10^3}=\frac{2}{7\cdot 10^3}.$$

Neka je $b_4=\left[10^4\cdot\frac{2}{7\cdot 10^3}\right]=\left[\frac{20}{7}\right]=2$. Tada je

$$y-\frac{b_1}{10}-\frac{b_2}{10^2}-\frac{b_3}{10^3}-\frac{b_4}{10^4}=\frac{2}{7\cdot 10^3}-\frac{2}{10^4}=\frac{6}{7\cdot 10^4}.$$

Neka je $b_5 = \left[10^5 \cdot \frac{6}{7\cdot 10^4}\right] = \left[\frac{60}{7}\right] = 8$. *Tada je*

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} - \frac{b_3}{10^3} - \frac{b_4}{10^4} - \frac{b_5}{10^5} = \frac{6}{7\cdot 10^4} - \frac{8}{10^5} = \frac{4}{7\cdot 10^5}.$$

Neka je $b_6 = \left[10^6 \cdot \frac{4}{7\cdot 10^5}\right] = \left[\frac{40}{7}\right] = 5$. *Tada je*

$$y - \frac{b_1}{10} - \frac{b_2}{10^2} - \frac{b_3}{10^3} - \frac{b_4}{10^4} - \frac{b_5}{10^5} - \frac{b_6}{10^6} = \frac{4}{7\cdot 10^5} - \frac{5}{10^6} = \frac{5}{7\cdot 10^6}.$$

Neka je $b_7 = \left[10^7 \cdot \frac{5}{7\cdot 10^6}\right] = \left[\frac{50}{7}\right] = 7$, *a vidimo da je to isto što i* b_1.

Sada je dovoljno uočiti da je

$$10^6 \cdot \left(y - \frac{b_1}{10} - \frac{b_2}{10^2} - \frac{b_3}{10^3} - \frac{b_5}{10^5} - \frac{b_6}{10^6}\right) = \frac{5}{7},$$

pa se cijeli postupak ponavlja.

Kraće:

$$\begin{array}{l} 5 \;:\; 7 = 0.714285\ldots \\ 50 \\ \;\;10 \\ \;\;\;\;30 \\ \;\;\;\;\;\;20 \\ \;\;\;\;\;\;\;\;60 \\ \;\;\;\;\;\;\;\;\;\;40 \\ \;\;\;\;\;\;\;\;\;\;\;\;50 \\ \;\;\;\;\;\;\;\;\;\;\;\;\;\vdots \end{array}$$

Dakle,

$$\frac{5}{7} = 0.714285714285... = 0.\dot{7}1428\dot{5}.$$

Sljedećim teoremom je dan obrat prethodnih razmatranja.

Teorem 11.9. *Neka je* $a_0 \in \mathbb{N}$ *znamenka i* (a_n) *niz znamenaka (tj.* $a_n \in \{0, 1, \ldots, 9\}$ *za svaki* $n \in \mathbb{N}_0$*), pri čemu ne postoji* $k \in \mathbb{N}$ *takav da je* $b_m = 9$ *za neki* $m \geq k$. *Tada postoji jedinstven realan broj* $x \geq 0$ *takav da je*

$$\begin{gathered} a_0 \leq x < a_0 + 1, \\ a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10}, \\ a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} \leq x < a_0 + \frac{a_1}{10} + \frac{a_2 + 1}{10^2}, \\ \vdots \\ a_0 + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \cdots + \frac{a_n + 1}{10^n}, \\ \vdots \end{gathered}$$

Decimalan zapis broja x *je dan sa* $\overline{a_0.a_1a_2\ldots}$

Dokaz. Stavimo

$$\Delta_1 = [a_0,\, a_0 + 1],$$

$$\Delta_2 = \left[a_0 + \frac{a_1}{10},\, a_0 + \frac{a_1 + 1}{10}\right],$$

općenito za svaki $n \in \mathbb{N}$:

$$\Delta_n = \left[a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1}}{10^{n-1}},\, a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1} + 1}{10^{n-1}}\right].$$

Vrijedi:

$$\Delta_1 \supseteq \Delta_2 \supseteq \ldots$$

Prema Cantorovom aksiomu (teorem 10.12) postoji $x \in \cap_{n\in\mathbb{N}}\Delta_n$. Dakle, dokazali smo egzistenciju takvog $x \in \mathbb{R}$.

Sada dokažimo jedinstvenost. Neka je $y \in \cap_{n\in\mathbb{N}}\Delta_n$, pri čemu je $y \neq x$. Tada imamo: $x, y \in \Delta_n$ za svaki $n \in \mathbb{N}$ odnosno

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1}}{10^{n-1}} \leq x, y \leq a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1} + 1}{10^{n-1}}.$$

Dakle, vrijede sljedeće nejednakosti:

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1}}{10^{n-1}} \leq x \leq a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1} + 1}{10^{n-1}},$$

$$-(a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1} + 1}{10^{n-1}}) \leq -y \leq -(a_0 + \frac{a_1}{10} + \cdots + \frac{a_{n-1}}{10^{n-1}}),$$

Zbrajanjem gornjih nejednakosti slijedi da za svaki $n \in \mathbb{N}$ vrijedi

$$-\frac{1}{10^{n-1}} \leq x - y \leq \frac{1}{10^{n-1}},$$

što je ekvivalentno sa

$$0 \leq |x - y| \leq \frac{1}{10^{n-1}}.$$

Uzimajući sve veći i veći n, pozitivan broj $\frac{1}{10^{n-1}}$ postaje sve bliži nuli. Slijedi $|x - y| = 0$ i konačno $y = x$. Prema tome, takav $x \in \cap_{n\in\mathbb{N}}\Delta_n$ je jedinstven. $\square$

12. Kompleksni brojevi

Skup $\mathbb{C}$ je Kartezijev produkt skupa $\mathbb{R}$ sa samim sobom:

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

(za definiciju Kartezijevog produkta vidite definiciju 2.14). Prema teoremu 2.15,

$$(x, y) = (x', y') \iff x = x' \text{ i } y = y'.$$

Za bilo koja dva uređena para $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$ definiramo operacije zbrajanja i množenja na sljedeći način:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2),$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2 - y_1 \cdot y_2,\ x_1 \cdot y_2 + x_2 \cdot y_1).$$

Može se provjeriti da ove operacije imaju svojstva (1)-(9) iz teorema 9.14.

Preslikavanje $f : \mathbb{R} \to \mathbb{R} \times \{0\}$ definirano sa $f(x) = (x, 0)$ je bijekcija, pa možemo identificirati skupove $\mathbb{R}$ i $\mathbb{R} \times \{0\}$. Posebno, skup $\mathbb{R}$ možemo smatrati podskupom skupa $\mathbb{C}$. Umjesto $(x, 0)$ pišemo jednostavno x i to je realan broj.

Kompleksan broj $(0, 1)$ zovemo **imaginarna jedinica** i označavamo sa i.

Neka je $z = (x, y) \in \mathbb{C}$. Kako je

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0),$$

to je

$$z = x + iy.$$

Zapis $x + iy$ kompleksnog broja z se naziva **standardni zapis kompleksnog broja**. Broj x se naziva realni dio od z i označava sa $\mathrm{Re}z$, a y se naziva imaginarni dio od z i označava sa $\mathrm{Im}z$. Dva kompleksna broja su jednaka ako i samo ako imaju jednake realne i jednake imaginarne dijelove.

Sada odredimo **trigonometrijski zapis kompleksnog broja** $z = x+iy \neq 0$.

Preslikavanje $z \mapsto (x, y)$ svakom kompleksnom broju pridružuje točku u Kartezijevoj koordinatnoj ravnini. Udaljenost te točke od ishodišta označavamo sa r, a kut koji zatvaraju os x i pravac određen ishodištem i točkom (x, y) označavamo sa φ. Jasno je da je $r > 0$ i $\varphi \in [0, 2\pi\rangle$. Broj r se naziva **modul kompleksnog broja** z i često označava sa $|z|$, a φ se naziva **argument kompleksnog broja** z.

Primjenom trigonometrije pravokutnog trokuta zaključujemo da je $x = r\cos\varphi$ i $y = r\sin\varphi$. Slijedi

$$z = r(\cos\varphi + i\sin\varphi).$$

Ovakav zapis kompleksnog broja se naziva **trigonometrijski zapis kompleksnog broja**.

Uočimo da vrijedi

$$x = r\cos\varphi,\ y = r\sin\varphi \implies x^2 + y^2 = r^2 \implies r = \sqrt{x^2 + y^2},$$

$$\cos\varphi = \frac{x}{\sqrt{x^2 + y^2}},\ \sin\varphi = \frac{y}{\sqrt{x^2 + y^2}}.$$

Dakle, r i φ su jedinstveno određeni sa x i y.

Primjer 12.1. *Odredimo trigonometrijske zapise nekih kompleksnih brojeva:*

$$z_1 = 1 + i = \sqrt{2}\left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right) = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right),$$

$$z_2 = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3},$$

$$z_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3},$$

$$z_4 = 1 - i\sqrt{3} = 2\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right).$$

Neka je $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ i $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Odredimo trigonometrijski zapis produkta i kvocijenta kompleksnih brojeva z_1 i z_2:

Za produkt imamo

$$\begin{aligned} z_1 \cdot z_2 &= r_1 r_2(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) \\ &= r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i\sin\varphi_1\cos\varphi_2 + i\cos\varphi_1\sin\varphi_2) \\ &= r_1 r_2\big(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\big). \end{aligned}$$

Za kvocijent imamo

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{r_1}{r_2} \cdot \frac{\cos\varphi_1 + i\sin\varphi_1}{\cos\varphi_2 + i\sin\varphi_2} \cdot \frac{\cos\varphi_2 - i\sin\varphi_2}{\cos\varphi_2 - i\sin\varphi_2} \\ &= \frac{r_1}{r_2} \cdot \frac{\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2 + i\sin\varphi_1\cos\varphi_2 - i\cos\varphi_1\sin\varphi_2}{\cos^2\varphi_2 - i^2\sin^2\varphi_2} \\ &= \frac{r_1}{r_2}\big(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)\big). \end{aligned}$$

Napomenimo da $\varphi_1+\varphi_2$ odnosno $\varphi_1-\varphi_2$ ne moraju biti argumenti kompleksnih brojeva $z_1 \cdot z_2$ odnosno $\frac{z_1}{z_2}$. Naime, moguće je da $\varphi_1+\varphi_2 \notin [0, 2\pi\rangle$ ili $\varphi_1-\varphi_2 \notin [0, 2\pi\rangle$. U tom slučaju im treba dodati / oduzeti odgovarajući višekratnik od 2π tako da se dobije kut u intervalu $[0, 2\pi\rangle$.

Za $z = |z|(\cos\varphi + i\sin\varphi)$ primjenom upravo izvedene formule za produkt dobivamo

$$z^2 = |z|^2(\cos 2\varphi + i\sin 2\varphi).$$

Matematičkom indukcijom dokažimo da je

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$$

za svaki $n \in \mathbb{N}$. Baza indukcije je upravo trigonometrijski zapis broja z.

Ako gornja jednakost vrijedi za neki $n \in \mathbb{N}$, tada primjena formule za produkt kompleksnih brojeva daje

$$\begin{aligned} z^{n+1} &= z^n \cdot z = |z|^n \cdot |z| \cdot (\cos n\varphi + i\sin n\varphi)(\cos\varphi + i\sin\varphi) \\ &= |z|^{n+1}\big(\cos(n+1)\varphi + i\sin(n+1)\varphi\big). \end{aligned}$$

Tvrdnja sada slijedi iz principa matematičke indukcije.

Ako je $-n \in \mathbb{N}$, tada imamo redom

$$\begin{aligned} z^{-n} &= |z|^{-n}\big(\cos(-n\varphi) + i\sin(-n\varphi)\big), \\ z^{-n} &= |z|^{-n}(\cos n\varphi - i\sin n\varphi), \\ z^{n} &= |z|^{n} \cdot \frac{1}{\cos n\varphi - i\sin n\varphi}, \\ z^{n} &= |z|^{n} \cdot \frac{1}{\cos n\varphi - i\sin n\varphi} \cdot \frac{\cos n\varphi + i\sin n\varphi}{\cos n\varphi + i\sin n\varphi}, \\ z^{n} &= |z|^{n}(\cos n\varphi + i\sin n\varphi). \end{aligned}$$

Također, $z^0 = 1 = |z|^0(\cos 0 + i\sin 0)$.

Prema tome, dokazali smo da za svaki $n \in \mathbb{Z}$ vrijedi

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi).$$

Ova formula se zove **Moivreova formula za potenciranje**.

Definicija 12.2. *Neka je $w \in \mathbb{C}$ i $n \in \mathbb{N}$. Skup svih rješenja jednadžbe $z^n - w = 0$ se naziva **skup n-tih korijena iz** w.*

Ako je $w = 0$, tada imamo:

$$z^n = 0 \iff |z|^n(\cos n\varphi + i\sin n\varphi) = 0 \iff |z| = 0 \iff z = 0.$$

Sada pretpostavimo da je $w \neq 0$ i zapišimo kompleksne brojeve w i z u trigonometrijskom obliku:

$$w = |w|(\cos\alpha + i\sin\alpha), \quad \alpha \in [0, 2\pi\rangle,$$

$$z = |z|(\cos\varphi + i\sin\varphi), \quad \varphi \in [0, 2\pi\rangle.$$

Tada iz $z^n = w$ slijedi

$$|z|^n(\cos n\varphi + i\sin n\varphi) = |w|(\cos\alpha + i\sin\alpha),$$

pa usporedba realnih i imaginarnih dijelova daje

$$|z|^n\cos n\varphi = |w|\cos\alpha, \quad |z|^n\sin n\varphi = |w|\sin\alpha.$$

Slijedi

$$|z|^{2n} = (|z|^n \cos n\varphi)^2 + (|z|^n \sin n\varphi)^2 = (|w| \cos\alpha)^2 + (|w| \sin\alpha)^2 = |w|^2,$$

pa je $|z| = \sqrt[n]{|w|}$ i stoga mora biti $\cos n\varphi = \cos\alpha$ i $\sin n\varphi = \sin\alpha$. To povlači $n\varphi = \alpha + 2k\pi, k \in \mathbb{Z}$, odnosno $\varphi = \frac{\alpha+2k\pi}{n}, k \in \mathbb{Z}$. Konačno imamo

$$z = \sqrt[n]{|w|}\left(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n}\right), \quad k \in \mathbb{Z}.$$

Primjenom Moivreove formule za potenciranje odmah slijedi da vrijedi i obrat, tj. gornja jednakost povlači $z^n = w$.

Uočimo: kako se $k \in \mathbb{Z}$ prema teoremu o dijeljenju s ostatkom (teorem 8.16) može jedinstveno prikazati u obliku $k = nq + r$, gdje je $r \in \{0, 1, \ldots, n-1\}$, to je

$$\frac{\alpha+2k\pi}{n} = \frac{\alpha+2nq\pi+2r\pi}{n} = \frac{\alpha+2r\pi}{n} + 2q\pi$$

i vrijedi

$$0 \le \frac{\alpha+2r\pi}{n} < \frac{2\pi+2(n-1)\pi}{n} = 2\pi,$$

pa je argument kompleksnog broja z jednak $\frac{\alpha+2r\pi}{n}$, gdje je $r \in \{0, 1, \ldots, n-1\}$.

Prema tome, različite vrijednosti n-tog korijena iz nenul kompleksnog broja w dobiju se za $r = 0, 1, \ldots, n-1$.

Dakle,

$$z_r = \sqrt[n]{|w|}\left(\cos\frac{\alpha+2r\pi}{n} + i\sin\frac{\alpha+2r\pi}{n}\right), \quad r = 0, 1, \ldots, n-1$$

su svi n-ti korijeni iz w; ova formula se naziva **Moivreova formula za korjenovanje**.

Kako je $|z_r| = \sqrt[n]{|w|}$ za svaki $r \in \{0, 1, \ldots, n-1\}$, to se svi n-ti korijeni iz $w \neq 0$ nalaze na kružnici polumjera $\sqrt[n]{|w|}$.

Vrijedi

$$\frac{\alpha+2(r+1)\pi}{n} - \frac{\alpha+2r\pi}{n} = \frac{2\pi}{n},$$

što znači da se argumenti dva "susjedna" korijena z_r i z_{r+1} razlikuju za $\frac{2\pi}{n}$. Dakle, $z_0, z_1, \ldots, z_{n-1}$ su vrhovi pravilnog n-terokuta.

Primjer 12.3. *(a) Riješimo jednadžbu $z^4 + 1 = 0$. Tada je $n = 4$ i $w = -1$. Argument α kompleksnog broja w je jednak π. Moivreova formula za korjenovanje daje*

$$z_r = \cos\frac{\pi+2r\pi}{4} + i\sin\frac{\pi+2r\pi}{4}, \quad r = 0, 1, 2, 3,$$

pa je

$$z_0 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \qquad z_1 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$$
$$z_2 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \qquad z_3 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.$$

Pritom su z_0, z_1, z_2, z_3 *vrhovi kvadrata.*

(b) Sada riješimo jednadžbu $z^3 - 1 = 0$. *Imamo* $n = 3$ *i* $w = 1$. *Dakle,* $\alpha = 0$. *Moivreova formula za korjenovanje daje*

$$z_r = \cos\frac{2r\pi}{3} + i\sin\frac{2r\pi}{3}, \quad r = 0, 1, 2,$$

pa je

$$z_0 = 1, \qquad z_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad z_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Pritom su z_0, z_1, z_2 *vrhovi jednakostraničnog trokuta.*

(c) Na kraju riješimo jednadžbu $z^4 - 1 = 0$. *Imamo* $n = 4$ *i* $w = 1$. *Ponovo je* $\alpha = 0$. *Moivreova formula za korjenovanje daje*

$$z_r = \cos\frac{2r\pi}{4} + i\sin\frac{2r\pi}{4}, \quad r = 0, 1, 2, 3.$$

Slijedi

$$z_0 = 1, \qquad z_1 = i, \qquad z_2 = -1, \qquad z_3 = -i.$$

Kompleksni brojevi z_0, z_1, z_2, z_3 *su vrhovi kvadrata.*

13. Prsten polinoma u jednoj varijabli

Neka je $\mathbb{K}$ jedan od skupova brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$. Funkcija

$$f : \mathbb{K} \longrightarrow \mathbb{K}$$

zadana formulom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{K}$ i $n \in \mathbb{N}_0$, naziva se **polinom**.

Konstante $a_0, a_1, \ldots, a_n \in \mathbb{K}$, koje određuju polinom, nazivaju se **koeficijenti polinoma**. Kako su koeficijenti iz $\mathbb{K}$, to vidimo da vrijedi:

$$x \in \mathbb{K} \implies f(x) \in \mathbb{K},$$

jer se vrijednost $f(x)$ dobije iz x množenjem i zbrajanjem (oduzimanjem) elemenata iz $\mathbb{K}$ konačan broj puta. Ovo pokazuje da je gornja funkcija dobro definirana. Skup svih takvih funkcija označavamo sa

$$\mathbb{K}[x]$$

i nazivamo **prsten polinoma u jednoj varijabli**. Pojam prstena polinoma ćemo objasniti malo kasnije. Ovdje je važno naglasiti da su polinomi najjednostavnije, ali netrivijalne funkcije i zbog toga su vrlo važne u matematici.

Najjednostavniji polinomi su potencije od x:

$$x^0 = 1,\ x^1 = x,\ x^2 = x \cdot x,\ x^3 = x^2 \cdot x,\ \ldots, x^n = x^{n-1} \cdot x,\ \ldots.$$

Napomenimo da u računima s polinomima uvijek stavljamo da je $0^0 = 1$.

Monom je polinom oblika

$$f(x) = cx^k,$$

za neki $c \in \mathbb{K}$ i $k \in \mathbb{N}_0$. Ako je $c = 0$, onda govorimo da je f **nul monom**. Svaki polinom je suma monoma. Polinom $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ je suma monoma

$$a_0 = a_0 x^0,\ a_1 x^1 = a_1 x,\ a_2 x^2,\ a_3 x^3,\ \ldots, a_n x^n.$$

Broj a_0 se naziva **slobodan član** polinoma f.

Polinom f je **nul polinom** ako vrijedi

$$a_0 = a_1 = \cdots = a_n = 0.$$

Ako f nije nul polinom, tada postoje monomi $a_i x^i$ u njegovom izrazu takvi da $a_i \neq 0$. Jasno, oni monomi $a_j x^j$ za koje je $a_j = 0$ nisu od interesa i najčešće se ispuštaju. Dakle, ako f nije nul polinom, onda u izrazu koji ga definira možemo pretpostaviti da je

$$a_n \neq 0.$$

Radi se o tome da smo izabrali najveći $n \in \mathbb{N}_0$ takav da je $a_n \neq 0$. Tada se $a_n x^n$ naziva **vodeći monom**, a koeficijent a_n se naziva **vodeći koeficijent**. Ako je vodeći koeficijent jednak jedan ($a_n = 1$), onda kažemo da je polinom f **normiran**. **Stupanj ne nul polinoma** je indeks n vodećeg monoma, pišemo

$$\deg(f) = n.$$

Korolar 13.3 iskazan niže osigurava da je stupanj dobro definiran.

Uočimo da za stupanj nenul polinoma f vrijedi $\deg(f) \in \mathbb{N}_0$. Posebno:

(1) **Polinom stupnja nula** je oblika $f(x) = a_0$, gdje je $a_0 \neq 0$, uz napomenu da je **konstantan polinom** oblika $f(x) = a_0$, pri čemu dozvoljavamo da je i $a_0 = 0$. Ako je $a_0 = 0$, onda imamo nul polinom i njegov stupanj ne definiramo. Napomenimo da neki autori definiraju stupanj nul polinoma kao $-\infty$ ili kao -1.
(2) **Linearan polinom** je polinom stupnja jedan: $f(x) = a_1x + a_0$, gdje je $a_1 \neq 0$.
(3) **Kvadratni polinom** je polinom stupnja dva: $f(x) = a_2x^2 + a_1x + a_0$, gdje je $a_2 \neq 0$.
(4) **Kubni polinom** je polinom stupnja tri: $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, gdje je $a_3 \neq 0$.
(5) Polinom stupnja četiri: $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, gdje je $a_4 \neq 0$, itd.

Primjer 13.1. *Neka je $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ zadan sa*

$$f(x) = 0 \cdot x^7 + x^5 + 2x^2 - x + 23.$$

Monom $0 \cdot x^7$ nema nikakav utjecaj na polinom te zato možemo pisati

$$f(x) = x^5 + 2x^2 - x + 23.$$

U ovom polinomu je

$$a_0 = 23,\ a_1 = -1,\ a_2 = 2,\ a_3 = a_4 = 0,\ a_5 = 1.$$

Dakle, slobodan koeficijent je $a_0 = 23$, a vodeći koeficijent je $a_5 = 1$. Zato je stupanj polinoma jednak 5:

$$\deg\left(0 \cdot x^7 + x^5 + 2x^2 - x + 23\right) = \deg\left(x^5 + 2x^2 - x + 23\right) = 5.$$

Kako je

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

to možemo smatrati

$$\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x].$$

Primjerice, kada pišemo $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ onda identificiramo $\mathbb{Z}[x]$ sa skupom svih polinoma iz $\mathbb{Q}[x]$ koje imaju cjelobrojne koeficijente (takvi polinomi nazivaju se **cjelobrojni polinomi**). Primjerice, polinom

$$f : \mathbb{Z} \to \mathbb{Z}, \quad f(x) = x - 1,$$

identificiramo s polinomom koji je dobiven proširenjem na $\mathbb{Q}$:

$$f : \mathbb{Q} \to \mathbb{Q}, \quad f(x) = x - 1.$$

Dakle, svi polinomi u ovom smislu pripadaju skupu $\mathbb{C}[x]$. Ako je $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$, te $f \in \mathbb{C}[x]$ ima koeficijente iz $\mathbb{K}$, onda f identificiran sa svojom restrikcijom pripada skupu $\mathbb{K}[x]$.

Očigledno je polinom nul funkcija (tj. $f(x) = 0$ za sve $x \in \mathbb{K}$) ako je nul polinom tj. ako su mu svi koeficijenti jednaki nuli. Sljedeća propozicija pokazuje da vrijedi i obrat.

Propozicija 13.2. *Neka je* $f : \mathbb{K} \longrightarrow \mathbb{K}$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$. *Ako je*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n = 0, \quad \forall x \in \mathbb{K},$$

onda je $a_0 = a_1 = \cdots = a_n = 0$.

Dokaz. Objasnimo ideju dokaza pod pretpostavkom da je $\mathbb{K} = \mathbb{R}$.

Pretpostavimo suprotno tj. $f(x) = a_0 + a_1x + \cdots + a_nx^n$ nije nul polinom, ali vrijedi

$$a_0 + a_1x + \cdots + a_nx^n = 0, \quad \forall x \in \mathbb{R}.$$

Kako f nije nul polinom, možemo pretpostaviti da je $a_n \neq 0$ tj. da je a_n upravo vodeći koeficijent. Neka je $x \neq 0$. Podijelimo gornji izraz sa x^n. Imamo

$$a_0\frac{1}{x^n} + a_1\frac{1}{x^{n-1}} + \cdots + a_{n-1}\frac{1}{x} + a_n = 0 \implies$$
$$a_0\frac{1}{x^n} + a_1\frac{1}{x^{n-1}} + \cdots + a_{n-1}\frac{1}{x} = -a_n.$$

Ako se ograničimo na $x > 0$ i zamislimo da x raste preko svih granica, primjerice $x = 10, 10^2, 10^3, \ldots, 10^{100}, \ldots, 10^{1000}$, i tako do u beskonačnost, tada svaki od $\frac{1}{x}, \cdots, \frac{1}{x^n}$ postaje po volji malen pozitivan i blizak nuli. Dakle, za jako velike x,

$$a_0\frac{1}{x^n} + a_1\frac{1}{x^{n-1}} + \cdots + a_{n-1}\frac{1}{x}$$

je po volji blizu nuli. S druge strane je to uvijek jednako

$$-a_n \neq 0.$$

Jasno, ovo je nemoguće. Koristeći Arhimedov aksiom (teorem 10.3), ovaj argument bi se mogao strogo napisati.

U slučaju $\mathbb{K} = \mathbb{Q}$ ili $\mathbb{K} = \mathbb{Z}$ dokaz ne zahtijeva nikakav "granični proces" (x ide u ∞) i može se provesti ovako. Najprije uočimo: ako je

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

nenul polinom s racionalnim koeficijentima te ako je cijeli broj q produkt nazivnika svih a_n napisanih u obliku $a_n = \frac{p_n}{q_n}$, $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}$, tj. $q = q_1 \cdots q_n$, onda je

$$q \cdot f(x) = (qa_0) + (qa_1)x + \cdots + (qa_n)x^n$$

polinom s cjelobrojnim koeficijentima, jer su

$$qa_0,\ qa_1,\ \ldots,\ qa_n\ \in \mathbb{Z}.$$

Konkretno, za

$$f(x) = 1 + \frac{1}{2}x - \frac{5}{7}x^3 = \frac{1}{1} + \frac{1}{2}x + \frac{0}{1}x^2 + \frac{-5}{7}x^3$$

imamo
$$q = 1 \cdot 2 \cdot 1 \cdot 7 = 14.$$
Dakle
$$q \cdot f(x) = 14 \cdot \left(1 + \frac{1}{2}x - \frac{5}{7}x^3\right) = 14 + 7x - 10x^3 \in \mathbb{Z}[x].$$
Na taj način se dokaz za $\mathbb{K} = \mathbb{Q}$ svodi na dokaz za $\mathbb{K} = \mathbb{Z}$. Konačno tvrdnju dokazujemo za $\mathbb{K} = \mathbb{Z}$.

Neka su $a_0,\ a_1,\ \ldots,\ a_n \in \mathbb{Z}$ takvi da vrijedi
$$f(x) = a_0 + a_1x + \cdots + a_nx^n = 0, \quad \forall x \in \mathbb{Z}.$$
Moramo dokazati da je f nul polinom. Ako nije, onda možemo pretpostaviti da je $a_n \neq 0$ tj. da je a_n upravo vodeći koeficijent. Sada gledamo redom $a_0,\ a_1,\ \ldots$ dok ne naiđemo na prvi $a_m \neq 0$. Gornja jednakost onda postaje
$$\begin{aligned} & a_mx^m + \cdots + a_nx^n = 0, \quad \forall x \in \mathbb{Z}, \\ & \implies x^m \cdot \left(a_m + a_{m+1}x + \cdots + a_nx^{n-m}\right) = 0, \quad \forall x \in \mathbb{Z}, \\ & \implies a_m + a_{m+1}x + \cdots + a_nx^{n-m} = 0, \quad \forall x \in \mathbb{Z},\ x \neq 0. \end{aligned}$$
Dakle, imamo $a_m \neq 0$ i $a_m + a_{m+1}x + \cdots + a_nx^{n-m} = 0$ za sve $x \in \mathbb{Z},\ x \neq 0$. Ako je $m = n$, ta jednakost se svodi na $a_n = a_m = 0$ što je kontradikcija. Ako je $n > m$, onda imamo
$$-a_m = x \cdot \left(a_{m+1} + \cdots + a_nx^{n-m-1}\right).$$
Odatle vidimo da je cijeli broj $a_m \neq 0$ djeljiv sa svakim prirodnim brojem $x = 1, 2, 3, \ldots, 1000, \ldots, 1000000, \ldots$. Očigledno smo došli do kontradikcije. $\square$

Korolar 13.3 (o jednakosti polinoma)**.** *Nenul polinomi*
$$\begin{aligned} f(x) &= a_0 + a_1x + \cdots + a_nx^n, \quad \text{gdje je } a_n \neq 0, \\ g(x) &= b_0 + b_1x + \cdots + b_mx^m, \quad \text{gdje je } b_m \neq 0, \end{aligned}$$
su jednaki, tj.
$$f(x) = g(x), \quad \forall x \in \mathbb{K},$$
ako i samo ako su im stupnjevi jednaki, tj.
$$n = m$$
te odgovarajući koeficijenti jednaki, tj.
$$a_0 = b_0,\ a_1 = b_1,\ \ldots, a_m = b_m.$$

Dokaz. Bez umanjenja općenitosti pretpostavimo $n \geq m$. Razliku polinoma
$$f(x) - g(x)$$
napišimo ovako:

- ako je $n > m$:
$$(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_m - b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n,$$
- ako je $n = m$:
$$(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_n - b_n)x^n.$$

Iz pretpostavke korolara nalazimo da je razlika jednaka nuli za svaki $x \in \mathbb{K}$. Prema propoziciji 13.2, zbog $a_n \neq 0$, prvi slučaj nije moguć. Primjena propozicije 13.2 na drugi slučaj daje tvrdnju korolara. $\square$

Sada ćemo objasniti što znači prsten polinoma $\mathbb{K}[x]$. Pojam prstena polinoma vezan je za svojstva zbrajanja i množenja polinoma.

Zbrajanje i množenje polinoma definiramo na uobičajen način. Neka su $f, g \in \mathbb{K}[x]$. Definiramo funkciju

$$h : \mathbb{K} \longrightarrow \mathbb{K}$$

formulom

$$h(x) = f(x) + g(x), \quad x \in \mathbb{K}.$$

Takvu funkciju nazivamo zbroj funkcija f i g i označavamo sa $h = f + g$. Za sada, pojam zbroja funkcije je vrlo općenit i a priori nema nikakve veze s polinomima, ali u našem slučaju je h polinom iz $\mathbb{K}[x]$. To lako vidimo ako napišemo f i g u obliku

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_M x^M, \\ g(x) &= b_0 + b_1 x + \cdots + b_M x^M, \end{aligned}$$

gdje smo na "početak" ili na eventualna "prazna mjesta" od f i g dodali dovoljan broj monoma $0 \cdot x^k$ kako bismo postigli da se pojavljuju iste potencije od x. Primjerice,

$$\begin{aligned} f(x) &= 1 + 3x^2 = 1 + 0x + 3x^2 + 0x^3 + 0x^4 + 0x^5, \\ g(x) &= 3 - x + x^3 + x^5 = 3 - x + 0x^2 + x^3 + 0x^4 + x^5. \end{aligned}$$

Vrijedi

$$h(x) = f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_M + b_M)x^M.$$

Dakle, vidimo da je $h \in \mathbb{K}[x]$. U našem primjeru, u kojem je

$$\begin{aligned} f(x) &= 1 + 3x^2 = 1 + 0x + 3x^2 + 0x^3 + 0x^4 + 0x^5, \\ g(x) &= 3 - x + x^3 + x^5 = 3 - x + 0x^2 + x^3 + 0x^4 + x^5, \end{aligned}$$

imamo

$$\begin{aligned} & f(x) + g(x) \\ = \ & (1+3) + (0-1)x + (3+0)x^2 + (0+1)x^3 + (0+0)x^4 + (0+1)x^5 \\ = \ & 4 - x + 3x^2 + x^3 + x^5. \end{aligned}$$

Neka su $f, g \in \mathbb{K}[x]$. Definiramo funkciju

$$h : \mathbb{K} \longrightarrow \mathbb{K}$$

formulom

$$h(x) = f(x) \cdot g(x), \quad x \in \mathbb{K}.$$

Takvu funkciju nazivamo produkt funkcija f i g i označavamo sa $h = f \cdot g$. Za sada, kao i kod zbroja, pojam produkta funkcija je vrlo općenit i a priori nema nikakve veze s polinomima, ali u našem slučaju je h polinom iz $\mathbb{K}[x]$. To lako vidimo na sljedeći način. Ako je f ili g nul polinom, onda je

$$h(x) = f(x) \cdot g(x) = 0, \quad \forall x \in \mathbb{K}.$$

Dakle, h je nul–polinom. Neka su sada f i g nenul polinomi. Tada možemo pisati

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0, \\ g(x) &= b_0 + b_1 x + \cdots + b_m x^m, \quad b_m \neq 0. \end{aligned}$$

Zato imamo direktnim množenjem

$$\begin{aligned} & h(x) = f(x) \cdot g(x) \\ & = (a_0 + a_1 x + \cdots + a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_m x^m) \\ & = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \cdots + (a_n b_m)x^{n+m}. \end{aligned}$$

Ovo pokazuje je produkt polinoma opet polinom. Nadalje,

$$a_n \neq 0, \; b_m \neq 0 \implies a_n b_m \neq 0$$

pokazuje da koeficijent uz x^{n+m} nije nula. Dakle, primjenjući propoziciju 13.2, vidimo da produkt dva nenul polinoma nije nul polinom te da je njegov stupanj jednak $n+m$ tj. vrijedi

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Ovim smo dokazali ovaj važan rezultat:

Lema 13.4. *Produkt dva nenul polinoma f i g iz $\mathbb{K}[x]$ je opet nenul polinom iz $\mathbb{K}[x]$, a njegov stupanj jednak je zbroju stupnjeva polinoma f i g.*

Gornja definicija množenja korisna je za teorijska razmatranja, ali u praksi mi postupamo na sljedeći način (ili neki sličan).

Primjer 13.5. *Neka je*

$$\begin{aligned} f(x) &= x^7 - x^5 + 2x^3 + 3x^2 + x + 1, \\ g(x) &= x^4 + x^2 + 2. \end{aligned}$$

Tada imamo množenjem član po član

$$\begin{aligned} f(x) \cdot g(x) &= \big(x^7 - x^5 + 2x^3 + 3x^2 + x + 1\big) \cdot \big(x^4 + x^2 + 2\big) \\ &= \big(x^7 - x^5 + 2x^3 + 3x^2 + x + 1\big) \cdot x^4 \\ &\quad + \big(x^7 - x^5 + 2x^3 + 3x^2 + x + 1\big) \cdot x^2 \\ &\quad + \big(x^7 - x^5 + 2x^3 + 3x^2 + x + 1\big) \cdot 2 \\ &= \big(x^{11} - x^9 + 2x^7 + 3x^6 + x^5 + x^4\big) \\ &\quad + \big(x^9 - x^7 + 2x^5 + 3x^4 + x^3 + x^2\big) \\ &\quad + \big(2x^7 - 2x^5 + 4x^3 + 6x^2 + 2x + 2\big) \\ &= x^{11} + 3x^7 + 3x^6 + x^5 + 4x^4 + 5x^3 + 7x^2 + 2x + 2. \end{aligned}$$

Sljedeći teorem daje neka svojstva uvedenih operacija na $\mathbb{K}[x]$. Napomenimo da 0 označava nulpolinom, a 1 konstantni polinom dan sa $1(x) = 1$ za svaki $x \in \mathbb{K}$.

Teorem 13.6. *Neka je $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Onda za sve $f, g, h \in \mathbb{K}[x]$ vrijedi:*

(1) *(asocijativnost zbrajanja)* $(f + g) + h = f + (g + h)$,

(2) *(postojanje neutralnog elementa za zbrajanje)* $f + 0 = 0 + f = f$,

(3) *(postojanje suprotnog elementa)* $f + (-f) = (-f) + f = 0$,

(4) *(komutativnost zbrajanja)* $f + g = g + f$,

(5) *(asocijativnost množenja)* $(f \cdot g) \cdot h = f \cdot (g \cdot h)$,

(6) *(postojanje jedinice za množenje)* $f \cdot 1 = 1 \cdot f = f$,

(7) *(komutativnost množenja)* $f \cdot g = g \cdot f$,

(8) *(distributivnost množenja prema zbrajanju)* $(f + g) \cdot h = f \cdot h + g \cdot f$,

(9) *(nema djelitelja nule)* $f \cdot g = 0 \implies f = 0$ *ili* $g = 0$.

Dokaz. Svojstva (1)–(8) provjere se direktno i vrijede za sve funkcije sa $\mathbb{K}$ u $\mathbb{K}$ uz ranije definirana množenja i zbrajanja funkcija:

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in \mathbb{K}, \qquad (f \cdot g)(x) = f(x) \cdot g(x), \quad \forall x \in \mathbb{K},$$

a dolaze iz svojstava koja zadovoljavaju skupovi brojeva (vidite primjerice teorem 9.14). Svojstvo (9) je suptilnije svojstvo i slijedi iz leme 13.4 obratom po kontrapoziciji. $\square$

Svojstva (1)–(8) definiraju **komutativan prsten s jedinicom** 1. Otuda naziv prsten polinoma za $\mathbb{K}[x]$. Ako vrijede svojstva (1)–(9), onda se govori o **integralnoj domeni**. Uočimo da su također $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$ integralne domene. Zapravo, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$ su polja jer zadovoljavaju analogone svojstava (1)–(9) iz teorema 9.14. Za razliku od njih, $(\mathbb{Z}, +, \cdot)$ zadovoljava svojstva (1)–(6) i (8)–(9), ali ne i (7) jer inverzni elementi x^{-1} elemenata $x \in \mathbb{Z} \setminus \{0\}$ općenito nisu iz $\mathbb{Z}$. Struktura $(\mathbb{K}[x], +, \cdot)$ je ipak sličnija $(\mathbb{Z}, +, \cdot)$ nego ostalim navedenim jer teorem 13.6 pokazuje da analogoni tvrdnji (1)–(6) i (8)–(9) teorema 9.14 vrijede, ali ne i (7). Konačno, $(\mathbb{K}[x], +, \cdot)$ i $(\mathbb{Z}, +, \cdot)$ su oba integralne domene.

Kažemo da je $f \in \mathbb{K}[x]$ **djeljiv** sa $g \in \mathbb{K}[x]$ (ili kažemo da g dijeli f) i pišemo $g \mid f$ ako postoji $h \in \mathbb{K}[x]$ takav da je

$$f = g \cdot h.$$

Lema 13.7. *Neka su $f, g \in \mathbb{K}[x]$ nenul polinomi za koje vrijedi $g \mid f$ i $f \mid g$. Onda postoji $c \in \mathbb{K}$, $c \neq 0$, takav da je $f = c \cdot g$. Nadalje, ako je $\mathbb{K} = \mathbb{Z}$, onda je $c = \pm 1$.*

Dokaz. Iz $g \mid f$ slijedi da postoji $h \in \mathbb{K}[x]$ takav da je

$$f = g \cdot h.$$

Isto tako iz $f \mid g$ slijedi da postoji $h_1 \in \mathbb{K}[x]$ takav da je

$$g = f \cdot h_1.$$

Množenjem gornjih jednakosti dobivamo

$$f \cdot g = (g \cdot h) \cdot (f \cdot h_1) \implies (f \cdot g) \cdot (1 - h \cdot h_1) = 0.$$

Kako je $f, g \neq 0$, imamo $f \cdot g \neq 0$ prema lemi 13.4. Zato iz

$$(f \cdot g) \cdot (1 - h \cdot h_1) = 0,$$

opet prema lemi 13.4, slijedi

$$1 - h \cdot h_1 = 0$$

odnosno

$$h \cdot h_1 = 1.$$

Opet lema 13.4 daje

$$\deg(h) + \deg(h_1) = \deg(h \cdot h_1) = \deg(1) = 0.$$

Kako je $\deg(h) \geq 0$ i $\deg(h_1) \geq 0$, to zaključujemo $\deg(h) = \deg(h_1) = 0$. Dakle, h i h_1 su konstantni nenul polinomi, tj. postoje $c, c_1 \in \mathbb{K} \setminus \{0\}$ takvi da je $h(x) = c$ i $h_1(x) = c_1$ za sve $x \in \mathbb{K}$. Zbog $h \cdot h_1 = 1$ imamo $cc_1 = 1$. Ako je $\mathbb{K} = \mathbb{Z}$, onda imamo $c = \pm 1$. Na kraju,

$$f = g \cdot h = g \cdot c = c \cdot g.$$

$\square$

Sada ćemo pokazati da postoje još neke analogije izmedju $\mathbb{Z}$ i $\mathbb{K}[x]$, ali samo za $K \neq \mathbb{Z}$. Usporedite sljedeći teorem s teoremom 8.16.

Teorem 13.8 (o dijeljenju s ostatkom)**.** *Neka je* $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. *Tada za sve* $f, g \in \mathbb{K}[x]$, $g \neq 0$, *postoje jedinstveni* $q, r \in \mathbb{K}[x]$ *takvi da vrijedi*

$$\begin{aligned} &f = g \cdot q + r, \\ &r = 0 \text{ ili } \deg(r) < \deg(g). \end{aligned}$$

Dokaz. Egzistencija. Ako je $f = 0$, onda stavimo $q = r = 0$. Za $f \neq 0$ tvrdnju dokazujemo indukcijom po stupnju $\deg(f)$. Ako je f polinom sa svojstvom

$$0 \leq \deg(f) < \deg(g),$$

onda stavimo $q = 0$ i $r = f$.

Neka je sada $\deg(f) \geq \deg(g)$. Napišimo

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0 \\ g(x) &= b_0 + b_1 x + \cdots + b_m x^m, \quad b_m \neq 0. \end{aligned}$$

Tada je $n \geq m$. Zato je

$$\frac{a_n}{b_m} x^{n-m}$$

monom. Stoga možemo definirati polinom

$$\begin{aligned} F &= f - \frac{a_n}{b_m} x^{n-m} g \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1} \right) x^{n-1} + \cdots \end{aligned}$$

Kako je stupanj svih preostalih monoma manji od $n-1$, to je $\deg(F) \leq n-1$. Na polinom F primijenimo induktivnu pretpostavku. Dobivamo

$$g \cdot Q + R = F = f - \frac{a_n}{b_m} x^{n-m} g.$$

Odatle je

$$f = g \cdot \left(Q + \frac{a_n}{b_m} x^{n-m} \right) + R.$$

Lako vidimo da možemo uzeti

$$q = Q + \frac{a_n}{b_m} x^{n-m}, \quad r = R.$$

Ovim se dokaz egzistencije završava.

<u>Jedinstvenost.</u> Neka je uz

$$\begin{aligned} &f = g \cdot q + r, \\ &r = 0 \text{ ili } \deg(r) < \deg(g), \end{aligned}$$

još i

$$\begin{aligned} &f = g \cdot q' + r', \\ &r' = 0 \text{ ili } \deg(r') < \deg(g). \end{aligned}$$

Tada imamo

$$g \cdot q + r = f = g \cdot q' + r' \implies g \cdot (q - q') = r - r'.$$

Ako je $r - r' = 0$ onda teorem 13.6 (9) povlači $q - q' = 0$, te jedinstvenost slijedi. Ako je $r - r' \neq 0$, onda uspoređujući stupnjeve zaključujemo

$$\deg(g) + \deg(q - q') = \deg(r - r') \leq \max(\deg(r),\ \deg(r'))$$

jer je razlika dva polinoma ili nulpolinom ili polinom stupnja ne većeg od stupnja svakog od tih polinoma. Kako je, nadalje, $\deg(r) < \deg(g)$ i $\deg(r') < \deg(g)$, to imamo

$$\begin{aligned} \deg(g) &\leq \deg(g) + \deg(q - q') = \deg(r - r') \\ &\leq \min(\deg(r),\ \deg(r')) < \deg(g). \end{aligned}$$

To je kontradikcija. □

Još jednom naglasimo da u teoremu 13.8 pretpostavljamo $\mathbb{K} \neq \mathbb{Z}$!

Dokaz sljedećeg teorema ostavljamo čitateljima (vidite dokaz teorema 13.8).

Teorem 13.9 (o dijeljenju s ostatkom za $\mathbb{Z}$). *Neka je $\mathbb{K} = \mathbb{Z}$. Tada za sve $f, g \in \mathbb{Z}[x]$, gdje je $g \neq 0$ i* ***vodeći koeficijent od*** g ***jednak je*** ± 1*, postoje jedinstveni $q, r \in \mathbb{Z}[x]$ takvi da vrijedi*

$$\begin{aligned} &f = g \cdot q + r, \\ &r = 0 \textit{ ili } \deg(r) < \deg(g). \end{aligned}$$

Dokaz egistencije u teoremima 13.8 i 13.9 je zapravo nama dobro poznat algoritam dijeljenja polinoma. Prisjetimo se tog algoritma u sljedećem primjeru.

Primjer 13.10. *Neka je*

$$f(x) = 3x^4 - 10x^3 + 22x^2 - 24x + 10,$$
$$g(x) = x^2 - 2x + 3.$$

Odredimo kvocijent q i ostatak r pri dijeljenju f sa g.

1. korak: Kako je $\deg(f) = 4 > \deg(g) = 2$*, to gledamo monom dobiven dijeljenjem vodećih monoma*

$$\frac{3x^4}{x^2} = 3x^2.$$

Stavimo

$$\begin{aligned} f_1 = f - 3x^2 g &= (3x^4 - 10x^3 + 22x^2 - 24x + 10) - 3x^2(x^2 - 2x + 3) \\ &= -4x^3 + 13x^2 - 24x + 10. \end{aligned}$$

2. korak: Kako je $\deg(f_1) = 3 > \deg(g) = 2$*, to gledamo monom dobiven dijeljenjem vodećih monoma*

$$\frac{-4x^3}{x^2} = -4x.$$

Stavimo

$$\begin{aligned} f_2 = f_1 - (-4x)g &= (-4x^3 + 13x^2 - 24x + 10) - (-4x)(x^2 - 2x + 3) \\ &= 5x^2 - 12x + 10. \end{aligned}$$

3. korak: Kako je $\deg(f_2) = 2 \geq \deg(g) = 2$*, to gledamo monom dobiven dijeljenjem vodećih monoma*

$$\frac{5x^2}{x^2} = 5.$$

Stavimo

$$\begin{aligned} f_3 = f_2 - 5g &= (5x^2 - 12x + 10) - 5(x^2 - 2x + 3) \\ &= -2x - 5. \end{aligned}$$

4. korak: Kako je $\deg(f_3) = 1 < \deg(g) = 2$*, to je*

$$r = f_3 = -2x - 5$$

i vrijedi

$$\begin{aligned} f_1 = f - 3x^2 g &\implies f = f_1 + 3x^2 g, \\ f_2 = f_1 - (-4x)g &\implies f_1 = f_2 + (-4x)g, \\ f_3 = f_2 - 5g &\implies f_2 = f_3 + 5g. \end{aligned}$$

Zbrajanjem tih jednakosti dobivamo

$$\begin{aligned} f &= (3x^2 - 4x + 5)g + f_3 \\ &= (3x^2 - 4x + 5)g + r \\ &= (3x^2 - 4x + 5)g + (-2x - 5). \end{aligned}$$

Dakle,

$$q = 3x^2 - 4x + 5.$$

Kratko, ovaj algoritam provodimo ovako:

$$
\begin{aligned}
&(3x^4 - 10x^3 + 22x^2 - 24x + 10) : (x^2 - 2x + 3) = 3x^2 - 4x + 5 \\
&-\underline{(3x^4 - 6x^3 + 9x^2)} \\
&\qquad - 4x^3 + 13x^2 - 24x \\
&\quad - \underline{(-4x^3 + 8x^2 - 12x)} \\
&\qquad\qquad 5x^2 - 12x + 10 \\
&\qquad\quad - \underline{(5x^2 - 10x + 15)} \\
&\qquad\qquad\quad \boxed{-2x - 5} \quad \mathit{STOP}
\end{aligned}
$$

jer smo dobili polinom manjeg stupnja od stupnja polinoma $x^2 - 2x + 3$.

Ponekad se može odrediti ostatak bez provođenja cijelog postupka dijeljenja. O tome govori sljedeći primjer.

Primjer 13.11. *Neka je*

$$
\begin{aligned}
f(x) &= x^{100} + 3x^{99} + x^2 - 3x + 9, \\
g(x) &= x^2 + 2x - 3.
\end{aligned}
$$

Odredite ostatak r *pri dijeljenju polinoma* f *sa* g*. Koristeći teorem 13.8 ili teorem 13.9, zaključujemo da je ostatak ili nul polinom* $r(x) = 0$ *ili polinom najviše prvog stupnja (jer mora biti stupnja manjeg od* $\deg(g) = 2$*). Takav polinom je oblika* $r(x) = Ax+B$ *gdje su* A *i* B *(cjelobrojne) konstante. Prema teoremima o dijeljenju s ostatkom mora postojati* $q \in \mathbb{Z}[x]$ *tako da vrijedi*

$$
\begin{aligned}
f(x) = g(x)q(x) + r(x) &= (x^2 + 2x - 3)q(x) + Ax + B \\
&= (x - 1)(x + 3)q(x) + Ax + B.
\end{aligned}
$$

Odatle uvrštavanjem $x = 1$ *i* $x = -3$ *dobivamo*

$$
\begin{aligned}
A + B &= f(1) = 11 \\
-3A + B &= f(-3) = 27.
\end{aligned}
$$

Dakle, $A = -4$ *i* $B = 15$.

Neka je $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Neka su $f, g \in \mathbb{K}[x]$ različiti od nule.

Najveća zajednička mjera polinoma f i g je **svaki** polinom $h \in \mathbb{K}[x]$ koji zadovoljava sljedeća dva uvjeta:

(i) $h \mid f$, i $h \mid g$,
(ii) ako $k \mid f$ i $k \mid g$ za neki $k \in \mathbb{K}[x]$, onda $k \mid h$

(usporedite s definicijom 8.22).

Uočimo da najveća zajednička mjera nije jedinstvena. Naime, ako polinom h zadovoljava gornja svojstva, onda ih zadovoljava i polinom $c \cdot h$ gdje je $c \in \mathbb{K} \setminus \{0\}$ ako je $\mathbb{K} \neq \mathbb{Z}$ i $c = \pm 1$ ako je $\mathbb{K} = \mathbb{Z}$. Sljedeća lema dokazuje obrat.

Lema 13.12. *Neka su $f, g \in \mathbb{K}[x]$ nenul polinomi. Ako najveća zajednička mjera polinoma f i g postoji, onda je ona jedinstvena do na umnožak sa $c \in \mathbb{K} \setminus \{0\}$ koji nužno zadovoljava $c = \pm 1$ ako je $\mathbb{K} = \mathbb{Z}$.*

Dokaz. Neka su h i h' dvije najveće zajedničke mjere polinoma f i g. Tada:

- $h \mid f, \quad h \mid g$,
- ako $k \mid f$ i $k \mid g$ za neki $k \in \mathbb{K}[x]$, onda $k \mid h$,
- $h' \mid f, \quad h' \mid g$,
- ako $k' \mid f$ i $k' \mid g$ za neki $k' \in \mathbb{K}[x]$, onda $k' \mid h'$.

Uzimajući gore $k = h'$ i $k' = h$, zaključujemo

$$h' \mid h \ \text{ i } \ h \mid h'.$$

Sada lema 13.7 povlači tvrdnju. □

Određivanje zajedničke mjere u $\mathbb{Z}[x]$ je relativno komplicirano i u ovom kolegiju se nećemo njime baviti. Neka je do kraja ovog predavanja $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Dakle, $\mathbb{K} \neq \mathbb{Z}$. Tada se najveća zajednička mjera polinoma $f, g \in \mathbb{K}[x]$, $f, g \neq 0$, određuje Euklidovim algoritmom dijeljenja sličnim onom kojim smo određivali najveću zajedničku mjeru cijelih brojeva (vidite kraj 8. poglavlja).

Euklidov algoritam.

$$\begin{aligned}
f &= g \cdot q_1 + r_1, \quad r_1 = 0 \text{ ili } 0 \leq \deg(r_1) < \deg(g), \\
g &= r_1 \cdot q_2 + r_2, \quad r_2 = 0 \text{ ili } 0 \leq \deg(r_2) < \deg(r_1), \\
r_1 &= r_2 \cdot q_3 + r_3, \quad r_3 = 0 \text{ ili } 0 \leq \deg(r_3) < \deg(r_2), \\
&\vdots \\
r_{i-1} &= r_i \cdot q_{i+1} + r_{i+1}, \quad r_{i+1} = 0 \text{ ili } 0 \leq \deg(r_{i+1}) < \deg(r_i).
\end{aligned}$$

Kako gornji niz ostataka različitih od nul polinoma ima strogo padajuće stupnjeve, mora postojati i takav da je $r_i \neq 0$, ali $r_{i+1} = 0$. Dakle, imamo

$$\begin{aligned}
f &= g \cdot q_1 + r_1, \\
g &= r_1 \cdot q_2 + r_2, \\
r_1 &= r_2 \cdot q_3 + r_3, \\
&\vdots \\
r_{i-2} &= r_{i-1} \cdot q_i + r_i, \\
r_{i-1} &= r_i \cdot q_{i+1}.
\end{aligned} \tag{13.13}$$

Lema 13.14. *Neka su $f, g \in \mathbb{K}[x]$ nenul polinomi. Najveća zajednička mjera polinoma f i g je polinom r_i (zadnji nenul ostatak) u Euklidovom algoritmu.*

Dokaz. Iz zadnje jednakosti u (13.13) zaključujemo $r_i \mid r_{i-1}$, a onda iz predzadnje zaključujemo $r_i \mid r_{i-2}$. Naime,

$$r_{i-2} = r_{i-1} \cdot q_i + r_i = (r_i \cdot q_{i+1}) \cdot q_i + r_i = r_i \cdot (q_{i+1} \cdot q_i + 1) \implies r_i \mid r_{i-2}.$$

Ponavljajući ovaj postupak zaključujemo redom:

$$r_i \mid r_{i-1},\ r_i \mid r_{i-2},\ \ldots,\ r_i \mid r_2,\ r_i \mid r_1,\ \boxed{r_i \mid g,\quad r_i \mid f}.$$

Obratno, ako $k \in \mathbb{K}[x]$ dijeli f i g iz prve jednakosti u (13.13) vidimo da $k|r_1$, a onda iz druge vidimo da $k|r_2$ itd. Dakle,

$$k \mid f,\ k \mid g,\ k \mid r_1,\ k \mid r_2,\ \ldots,\ k \mid r_{i-1},\ \boxed{k \mid r_i}.$$

Rezimirajmo

(i) $r_i \mid f,\ r_i \mid g$,

(ii) ako $k \mid f$ i $k \mid g$ za neki $k \in \mathbb{K}[x]$, onda $k \mid r_i$.

Ovim je lema dokazana. □

Svaki od polinoma $c \cdot r_i$, $c \in \mathbb{K} \setminus \{0\}$ također je najveća zajednička mjera polinoma f i g i na taj način su opisane sve najveće zajedničke mjere (vidite lemu 13.14).

Zadatak 13.15. *Odredite najveću zajedničku mjeru polinoma*

$$x^4 + x^3 + 2x^2 + x + 1 \quad \text{i} \quad x^3 - 2x^2 + x - 2.$$

14. Nultočke polinoma, Hornerov algoritam i primjene

U prethodnom poglavlju u teoremima 13.8 i 13.9 smo studirali dijeljenje polinoma s ostatkom. Posebno važan slučaj je dijeljenje polinomom prvog stupnja.

Teorem 14.1. *Neka je $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Tada za svaki $f \in \mathbb{K}[x]$ i svaki $\alpha \in \mathbb{K}$ postoji jedinstven $q \in \mathbb{K}[x]$ tako da vrijedi*

$$f(x) = (x - \alpha) \cdot q(x) + f(\alpha).$$

Dokaz. Dijelimo polinom f polinomom $g(x) = x - \alpha$ čiji je vodeći koeficijent jednak 1. Dakle, prema teoremima 13.8 i 13.9 zaključujemo da postoje jedinstveni $q, r \in \mathbb{K}[x]$ takvi da vrijedi

$$\begin{aligned} &f(x) = (x - \alpha) \cdot q + r(x), \\ &r = 0 \text{ ili } \deg(r) < \deg(g) = 1. \end{aligned}$$

Vidimo, dakle, da je r konstantan polinom, čiju vrijednost možemo izračunati iz prve jednakosti, tj. iz

$$f(x) = (x - \alpha) \cdot q(x) + r, \quad \forall x \in \mathbb{K},$$

uzimajući $x = \alpha$:

$$f(\alpha) = (\alpha - \alpha) q(\alpha) + r \implies r = f(\alpha).$$

□

Hornerov algoritam. Hornerov algoritam daje vrlo efikasan način određivanja polinoma q i vrijednosti $f(\alpha)$ o kojima se govori u teoremu 14.1. Cijeli postupak se temelji na **metodi neodređenih koeficijenata** koju ćemo sada opisati. Zadan je polinom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{K}$, $a_n \neq 0$ (tako da je f stupnja n), i zadan je

$$\alpha \in \mathbb{K}.$$

Određujemo

$$q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

gdje su $b_0, b_1, \ldots, b_m \in \mathbb{K}$ nepoznati koeficijenti, te računamo $f(\alpha)$. Otuda i naziv **metoda neodređenih koeficijenata.**

Krećemo od jednakosti koju daje teorem 14.1:

$$f(x) = (x - \alpha) \cdot q(x) + f(\alpha).$$

Uvrstimo gornje podatke i dobivamo:

$$\begin{aligned} & a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ = \; & (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0)(x - \alpha) + f(\alpha) \\ = \; & b_{m+1} x^{m+1} + (b_{m-1} - \alpha b_m) x^m + \cdots + (b_0 - \alpha b_1) x + (f(\alpha) - b_0). \end{aligned}$$

Prema korolaru 13.3 (koji govori o jednakosti polinoma!), gornja jednakost vrijedi za svaki $x \in \mathbb{K}$ ako i samo ako vrijedi:

$$\begin{array}{lcl}
n = m + 1 & \Longrightarrow & m = n - 1 \\
a_n = b_{n-1} & \Longrightarrow & b_{n-1} = a_n \\
a_{n-1} = b_{n-2} - \alpha b_{n-1} & \Longrightarrow & b_{n-2} = \alpha b_{n-1} + a_{n-1} \\
\vdots & & \vdots \\
a_1 = b_0 - \alpha b_1 & \Longrightarrow & b_0 = \alpha b_1 + a_1 \\
a_0 = f(\alpha) - \alpha b_0 & \Longrightarrow & f(\alpha) = \alpha b_0 + a_0.
\end{array}$$

Iz ove sheme koeficijente polinoma q i $f(\alpha)$ računamo redom odozgo prema dolje koristeći desni stupac. **Hornerov algoritam** zahtijeva samo da se ova tablica zarotira za 90°:

Hornerov algoritam:

	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
α	$\underbrace{b_{n-1}}_{a_n}$	$\underbrace{b_{n-2}}_{\alpha b_{n-1}+a_{n-1}}$	$\cdots$	$\underbrace{b_1}_{\alpha b_2+a_2}$	$\underbrace{b_0}_{\alpha b_1+a_1}$	$\underbrace{f(\alpha)}_{\alpha b_0+a_0}$

Primjer 14.2. *Koristeći Hornerov algoritam odredimo $f(2)$ i kvocijent pri dijeljenju polinoma f sa g ako je:*

$$f(x) = 3x^5 - x^4 + 7x^2 + 2x - 6,$$
$$g(x) = x - 2.$$

Najprije, a to treba napraviti pažljivo jer je to načešća greška:

$$x - \alpha = x - 2 \Longrightarrow \boxed{\alpha = 2.}$$

Nadalje, računamo

	3	-1	0	7	2	-6
$\alpha = 2$	3	$2\cdot 3+(-1)$ $=5$	$2\cdot 5+0$ $=10$	$2\cdot 10+7$ $=27$	$2\cdot 27+2$ $=56$	$2\cdot 56-6$ $=106$

Rezultat:

$$g(x) = 3x^4 + 5x^3 + 10x^2 + 27x + 56,$$
$$f(2) = 106.$$

Primjer 14.3. *Koristeći Hornerov algoritam odredimo kvocijent i ostatak pri dijeljenju f sa g ako je:*

$$f(x) = 3x^5 - x^4 + 7x^2 + 2x - 6,$$
$$g(x) = x + 1.$$

Najprije odredimo α:

$$x - \alpha = x + 1 \Longrightarrow \boxed{\alpha = -1.}$$

Nadalje, računamo

	3	-1	0	7	2	-6
$\alpha=-1$	3	$(-1)\cdot 3+(-1)$ $=-4$	$(-1)\cdot(-4)+0$ $=4$	$(-1)\cdot(4)+7$ $=3$	$(-1)\cdot(3)+2$ $=-1$	$(-1)\cdot(-1)-6$ $=-5$

Rezultat:

$$\begin{aligned}
&g(x)=3x^4-4x^3+4x^2+3x-1,\\
&f(-1)=-5.
\end{aligned}$$

Taylorov razvoj polinoma. U nastavku je također $\mathbb{K}\in\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$. Svaki polinom zapisan na standardan način

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

gdje su $a_0,a_1,\ldots,a_n\in\mathbb{K}$ i $n\in\mathbb{N}_0$, je **razvoj po potencijama od** x**:** $x^0,\ x^1=x,\ x^2,\ldots$ Međutim, potencije od x nisu ni po čemu posebne jer vrijedi:

Teorem 14.4 (Taylorov razvoj oko $\alpha\in\mathbb{K}$)**.** *Neka je $\alpha\in\mathbb{K}$. Tada za svaki $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{K}[x]$, $a_n\neq 0$, postoje jedinstveni*

$$A_0,\ A_1,\ldots,\ A_n\in\mathbb{K}$$

takvi da vrijedi

$$f(x)=A_n(x-\alpha)^n+A_{n-1}(x-\alpha)^{n-1}+\cdots+A_1(x-\alpha)+A_0.$$

Nadalje, $A_n=a_n$ i $A_0=f(\alpha)$.

Dokaz. Ako je $n=0$, onda je $f(x)=a_0$ i dovoljno je samo staviti $A_0=a_0$ da se dobije traženi razvoj. Neka je zato $n\geq 1$. Koristimo uzastopno teorem 14.1, opažajući da kvocijent uvijek ima isti vodeći koeficijent kao polazni polinom f (a to slijedi iz ranije diskusije oko Hornerovog algoritma). Dakle, dijelimo n puta sa $(x-\alpha)$:

$$\begin{aligned}
&f(x)=(x-\alpha)q_0(x)+A_0,\quad A_0=f(\alpha),\quad \deg(q_0)=n-1,\\
&q_0(x)=(x-\alpha)q_1(x)+A_1,\quad A_1=q_0(\alpha),\quad \deg(q_1)=n-2,\\
&q_1(x)=(x-\alpha)q_2(x)+A_2,\quad A_2=q_1(\alpha),\quad \deg(q_2)=n-3,\\
&\vdots\\
&q_{n-3}(x)=(x-\alpha)q_{n-2}(x)+A_{n-2},\quad A_{n-2}=q_{n-3}(\alpha),\quad \deg(q_{n-2})=1,\\
&q_{n-2}(x)=(x-\alpha)q_{n-1}(x)+A_{n-1},\quad A_{n-1}=q_{n-2}(\alpha),\quad \deg(q_{n-1})=0.
\end{aligned}$$

Kako smo već istaknuli, svi kvocijenti $q_0,q_1,\ldots,q_{n-1}$ imaju isti vodeći koeficijent jednak onom od f tj. jednak a_n. Kako je polinom q_{n-1} stupnja nula (vidite gornju shemu dijeljenja), to mora biti jednak svom vodećem članu, tj. $q_{n-1}(x)=a_n$.

Stavimo $A_n = a_n$. Uzimajući to u obzir, gornja shema dijeljenja izgleda ovako:

$$\begin{aligned}
f(x) &= (x-\alpha)q_0(x) + A_0,\\
q_0(x) &= (x-\alpha)q_1(x) + A_1,\\
q_1(x) &= (x-\alpha)q_2(x) + A_2,\\
&\vdots\\
q_{n-3}(x) &= (x-\alpha)q_{n-2}(x) + A_{n-2},\\
&\boxed{q_{n-2}(x) = A_n \cdot (x-\alpha) + A_{n-1}}
\end{aligned}$$

Na kraju uvrštavamo odozdo prema gore:

$$\begin{aligned}
q_{n-3}(x) &= (x-\alpha)q_{n-2}(x) + A_{n-2}\\
&= (x-\alpha)\left(A_n \cdot (x-\alpha) + A_{n-1}\right) + A_{n-2}\\
&= A_n(x-\alpha)^2 + A_{n-1}(x-\alpha) + A_{n-2},\\
&\vdots\\
q_1(x) &= A_n(x-\alpha)^{n-2} + A_{n-1}(x-\alpha)^{n-3} + \cdots + A_3(x-\alpha) + A_2,\\
q_0(x) &= (x-\alpha)q_1(x) + A_1\\
&= A_n(x-\alpha)^{n-1} + A_{n-1}(x-\alpha)^{n-2} + \cdots + A_2(x-\alpha) + A_1,\\
f(x) &= (x-\alpha)q_0(x) + A_0\\
&= A_n(x-\alpha)^n + A_{n-1}(x-\alpha)^{n-1} + \cdots + A_1(x-\alpha) + A_0.
\end{aligned}$$

Ovim je egzistencija razvoja dokazana. Jedinstvenost slijedi iz jedinstvenosti u teoremu o dijeljenju s ostatkom. □

U teoremu 14.4 smo izrazili A_n i A_0. Ostali koeficijenti A_i se mogu izraziti preko derivacija od f izračunatih u α, ali naš dokaz daje efikasan opći način računanja koeficijenata A_i temeljen na Hornerovom algoritmu.

Kada se metoda iz dokaza prethodnog teorema kombinira s Hornerovim algoritmom, dobije se vrlo efikasan algoritam za određivanje koeficijenata.

Primjer 14.5. *Razvijte polinom* $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$ *oko* $\alpha = -1$. *Drugim riječima, treba polinom razviti po potencijama od*

$$x - \alpha = x - (-1) = x + 1.$$

Koristimo $n = 4$ *puta Hornerovu shemu:*

	1	2	-3	-4	1
$\alpha = -1$	1	1	-4	0	$\boxed{A_0 = 1}$
$\alpha = -1$	1	0	-4	$\boxed{A_1 = 4}$	
$\alpha = -1$	1	-1	$\boxed{A_2 = -3}$		
$\alpha = -1$	1	$\boxed{A_3 = -2}$			
$\alpha = -1$	$\boxed{A_4 = 1}$				

Rezultat:

$$f(x) = (x+1)^4 - 2(x+1)^3 - 3(x+1)^2 + 4(x+1) + 1.$$

Zadatak 14.6. *Razvijte polinom $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$ oko $\alpha = 1$. Drugim riječima, treba polinom razviti po potencijama od $x - \alpha = x - 1$.*

Nultočke polinoma. Kažemo da je $\alpha \in \mathbb{K}$ **nultočka ili korijen polinoma** $f \in \mathbb{K}[x]$ ako vrijedi $f(\alpha) = 0$.

Propozicija 14.7. *$\alpha \in \mathbb{K}$ je nultočka polinoma $f \in \mathbb{K}[x]$ ako i samo ako $x - \alpha \mid f(x)$ u $\mathbb{K}[x]$.*

Dokaz. Prema teoremu 14.1, postoji $q \in \mathbb{K}[x]$ tako da vrijedi

$$f(x) = (x - \alpha) \cdot q + f(\alpha).$$

Propozicija odmah slijedi iz ove jednakosti jer je $f(\alpha)$ ostatak pri dijeljenju polinoma f sa $x - \alpha$. □

Kratnost nultočke. Neka je $f \in \mathbb{K}[x]$, $f \neq 0$. Definiramo **kratnost ili red** od $\alpha \in \mathbb{K}$, u oznaci $\nu_\alpha(f)$, kao cijeli broj

$$m = \nu_\alpha(f),$$

određen sa

$$(x-\alpha)^m \mid f(x), \quad (x-\alpha)^{m+1} \nmid f(x).$$

Očigledno je broj m potpuno određen ovom karakterizacijom. Zaista, imamo

$$(x-\alpha)^0 = 1 \mid f(x) \ \text{ i } \ (x-\alpha)^{n+1} \nmid f(x), \ \text{ gdje je } n = \deg(f),$$

jer polinom stupnja $n+1$ ne dijeli polinom stupnja n. Dakle, svakako postoji m s traženim svojstvom:

$$(x-\alpha)^0 = 1 \mid f(x), \ \ldots, \ (x-\alpha)^m \mid f(x), \ (x-\alpha)^{m+1} \nmid f(x), \ \ldots, \ (x-\alpha)^{n+1} \nmid f(x).$$

(Naime, niz počinje djeljivošću, pa je m definiran kao "posljednje mjesto" gdje imamo djeljivost.)

Osnovna svojstva ovog pojma sadržana su u sljedećoj lemi:

Lema 14.8. *Neka su $f \in \mathbb{K}[x]$, $f, g \neq 0$. Neka je $\alpha \in \mathbb{K}$. Tada vrijedi:*

(i) *Postoji $q \in \mathbb{K}[x]$ takav da je*

$$f(x) = (x-\alpha)^{\nu_\alpha(f)} q(x), \quad q(\alpha) \neq 0.$$

(ii) *Obratno, ako postoje $m \geq 0$ i $q \in \mathbb{K}[x]$ takvi da je*

$$f(x) = (x-\alpha)^m q(x), \quad q(\alpha) \neq 0,$$

onda je

$$\nu_\alpha(f) = m.$$

(iii) *Ako je* $\alpha \in \mathbb{K}$ *nultočka polinoma* f, *onda vrijedi*

$$\nu_f(\alpha) \geq 1.$$

(iv) $\nu_\alpha(f \cdot g) = \nu_\alpha(f) + \nu_\alpha(g)$.

Dokaz. (i) Po definiciji vrijede sljedeće tvrdnje:

$$(x-\alpha)^{\nu_\alpha(f)} \mid f(x), \quad (x-\alpha)^{\nu_\alpha(f)+1} \nmid f(x).$$

Iz prve tvrdnje zaključujemo da postoji $q \in \mathbb{K}[x]$ takav da je

$$f(x) = (x-\alpha)^{\nu_\alpha(f)} q(x),$$

a iz druge zaključujemo $q(\alpha) \neq 0$, jer bismo inače prema propoziciji 14.7 imali $x - \alpha \mid q(x)$, a zato i

$$(x-\alpha)^{\nu_\alpha(f)+1} \mid f(x),$$

što nije moguće.

(ii) Kako je $f(x) = (x-\alpha)^m q(x)$, to vrijedi $(x-\alpha)^m \mid f(x)$. Ako $(x-\alpha)^{m+1} \mid f(x)$, onda za neki $q_1 \in \mathbb{K}[x]$ vrijedi

$$f(x) = (x-\alpha)^{m+1} q_1(x).$$

Dakle,

$$\begin{aligned}
&(x-\alpha)^m q(x) = (x-\alpha)^{m+1} q_1(x) \\
&\implies (x-\alpha)^m \big(q(x) - (x-\alpha) q_1(x)\big) = 0 \\
&\underbrace{\implies}_{\text{lema } 13.4} q(x) = (x-\alpha) q_1(x).
\end{aligned}$$

Odatle slijedi $q(\alpha) = 0$. Ovo je kontradikcija s pretpostavkom $q(\alpha) \neq 0$. Dakle, $(x-\alpha)^{m+1} \nmid f(x)$. Konačno zaključujemo $\nu_\alpha(f) = m$.

(iii) Prema propoziciji 14.7 vrijedi $x - \alpha \mid f(x)$. Dakle, $\nu_\alpha(f) \geq 1$.

(iv) Prema (i), postoje $q_1, q_2 \in \mathbb{K}[x]$ tako da je

$$\begin{aligned}
f(x) &= (x-\alpha)^{\nu_\alpha(f)} q_1(x), \quad q_1(\alpha) \neq 0, \\
g(x) &= (x-\alpha)^{\nu_\alpha(g)} q_2(x), \quad q_2(\alpha) \neq 0.
\end{aligned}$$

Dakle,

$$f(x) \cdot g(x) = (x-\alpha)^{\nu_\alpha(f)+\nu_\alpha(g)} q_1(x) q_2(x), \quad q_1(\alpha) \cdot q_2(\alpha) \neq 0.$$

Tvrdnja sada slijedi iz (ii). □

Korolar 14.9. *Neka je* $f \in \mathbb{K}[x]$ *polinom stupnja* $n \geq 1$. *Neka su* $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{K}$ ***različite nultočke*** *od* f *u* $\mathbb{K}$, *redom s kratnostima* $k_1, \ldots, k_m$. *Tada postoji polinom* $q \in \mathbb{K}[x]$ *takav da je*

$$f(x) = (x-\alpha_1)^{k_1} \cdots (x-\alpha_m)^{k_m} q(x),$$

$q(\alpha_i) \neq 0$ *za svaki* $i = 1, \ldots, m$.

Dokaz. Lema 14.8 (i) povlači da postoji $q_1 \in \mathbb{K}[x]$ takav da je

$$f(x) = (x - \alpha_1)^{k_1} q_1(x), \quad q_1(\alpha_1) \neq 0.$$

Nadalje, zbog leme 14.8 (iv), vrijedi

$$k_2 = \nu_{\alpha_2}(f) = \nu_{\alpha_2}((x - \alpha_1)^{k_1}) + \nu_{\alpha_2}(q_1) = 0 + \nu_{\alpha_2}(q_1) = \nu_{\alpha_2}(q_1).$$

Lema 14.8 (i) povlači

$$q_1(x) = (x - \alpha_2)^{k_2} q_2(x), \quad q_2(\alpha_2) \neq 0.$$

Uz to, vrijedi i

$$f(x) = (x - \alpha_1)^{k_1} q_1(x) = (x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} q_2(x), \quad q_2(\alpha_1) \neq 0, \; q_2(\alpha_2) \neq 0.$$

Sada ovaj postupak ponavljamo dok ne iscrpimo sve α_i. □

Teorem 14.10. *Neka je $f \in \mathbb{K}[x]$ polinom stupnja $n \geq 1$. Neka su $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{K}$* ***različite nultočke*** *od f u $\mathbb{K}$, redom s kratnostima $k_1, \ldots, k_m$. Tada je*

$$k_1 + \cdots + k_m \leq n.$$

Posebno, polinom $f \in \mathbb{K}[x]$ stupnja $n \geq 1$ ima najviše n različitih nultočaka u $\mathbb{K}$.

Dokaz. Prema korolaru 14.9, postoji polinom $q \in \mathbb{K}[x]$ takav da je

$$f(x) = (x - \alpha_1)^{k_1} \cdots (x - \alpha_m)^{k_m} q(x).$$

Uspoređući stupnjeve, zaključujemo

$$\begin{aligned} n = \deg(f) &= \deg((x - \alpha_1)^{k_1}) + \cdots + \deg((x - \alpha_m)^{k_m}) + \deg(q(x)) \\ &= k_1 + \cdots + k_m + \deg(q(x)) \\ &\geq k_1 + \cdots + k_m. \end{aligned}$$

□

Teorem 14.10 se često formulira na sljedeći način:

Polinom stupnja n ima najviše n nultočaka računatih s kratnostima.

Hornerov algoritam daje nam efikasan algoritam za određivanje kratnosti nultočaka. Taj algoritam se temelji na sljedećoj propoziciji čiji dokaz ostavljamo čitatelju.

Propozicija 14.11. *Neka je $f \in \mathbb{K}[x]$, $f \neq 0$, $\deg(f) = n$ te $\alpha \in \mathbb{K}$. Neka je $f(x) = A_n(x - \alpha)^n + A_{n-1}(x - \alpha)^{n-1} + \cdots + A_1(x - \alpha) + A_0$ Taylorov razvoj polinoma f oko točke α. Tada je $\nu_f(\alpha)$ najmanji indeks m sa svojstvom $A_m \neq 0$.*

Primjer 14.12. *Dokažimo da je $\alpha = 1$ nultočka polinoma*

$$f(x) = x^5 - 2x^4 + x^3 + x^2 - 2x + 1$$

i odredimo njezinu kratnost.

	1	-2	1	1	-2	1
$\alpha = 1$	1	-1	0	1	-1	$\boxed{A_0 = 0}$
$\alpha = 1$	1	0	0	1	$\boxed{A_1 = 0}$	
$\alpha = 1$	1	1	1	$\boxed{A_2 = 2}$		

Rezultat:

$$m = 2.$$

Određivanje cjelobrojnih nultočaka polinoma s cjelobrojnim koeficijentima. Neka je $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$, $a_n \neq 0$. Neka je $m \geq 0$ najmanji indeks takav da je $a_m \neq 0$. Tada možemo pisati

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x = x^m (a_n x^{n-m} + a_{n-1}x^{n-m-1} + \cdots + a_m).$$

Vidimo da je $\alpha = 0$ kratnosti m ako je $m \geq 1$. Na taj način problem određivanja racionalnih nultočaka svodimo na određivanje racionalnih nultočaka polinoma

$$a_n x^{n-m} + a_{n-1}x^{n-m-1} + \cdots + a_m$$

u kojem je $a_n, a_m \neq 0$. Taj polinom nema $\alpha = 0$ kao nultočku. Zbog toga u sljedećem teoremu pretpostavljamo da je slobodan član različit od nule.

Teorem 14.13. *Ako je $\alpha \in \mathbb{Z}$ nultočka polinoma f onda $\alpha \mid a_0$, tj. cjelobrojne nultočke polinoma s cjelobrojnim koeficijentima nalaze se (ako postoje!) među djeliteljima slobodnog člana.*

Dokaz. Po pretpostavci,

$$\begin{aligned} 0 = & f(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0 \\ & \implies a_0 = -\alpha \cdot \left(a_n \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1\right). \end{aligned}$$

Odatle slijedi $\alpha \mid a_0$ u $\mathbb{Z}$. $\square$

Primjer 14.14. *Odredimo cjelobrojne nultočke polinoma*

$$f(x) = x^5 - 2x^4 + x^3 + x^2 - 2x + 1.$$

Ovdje je ***slobodni član*** $a_0 = 1$. *Njegovi djelitelji su elementi skupa*

$$\{-1, 1\}.$$

Računamo Hornerovom shemom (ali ne uzastopno već uvijek radimo s koeficijentima polinoma f):

	1	-2	1	1	-2	1
$\alpha = 1$	1	-1	0	1	-1	$\boxed{0}$
$\alpha = -1$	1	-3	4	-3	1	$\boxed{0}$

Rezultat: sve cjelobrojne nultočke polinoma f su $-1, 1$.

Primjer 14.15. *Odredimo cjelobrojne nultočke polinoma*

$$f(x) = 2x^3 - 3x^2 - x - 2.$$

Ovdje je ***slobodni član*** $a_0 = -2$*. Njegovi djelitelji su elementi skupa*

$$\{-1, 1, -2, 2\}.$$

Računamo Hornerovom shemom (ali ne uzastopno već uvijek radimo s koeficijentima polinoma f*):*

	2	-3	-1	-2
$\alpha = -1$	2	-5	4	-6
$\alpha = 1$	2	-1	-2	-4
$\alpha = -2$	2	-7	13	-28
$\alpha = 2$	2	1	1	$\boxed{0}$

Rezultat: jedina cjelobrojna nultočka polinoma f *je* 2.

Određivanje racionalnih nultočaka polinoma s cjelobrojnim koeficijentima. Kao u prethodnoj točki, kod određivanja racionalnih nultočaka promatramo samo polinome kojima je slobodan član različit od nule.

Prema teoremu 9.10, svaki racionalan broj α je ili jednak nuli tj. $\alpha = \frac{0}{1}$ ili je $\alpha = \frac{p}{q}$, gdje su $p \in \mathbb{Z}$, $q \in \mathbb{N}$ **relativno prosti**.

Teorem 14.16. *Neka je* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$, $a_n \neq 0$ *i* $a_0 \neq 0$*. Ako je* $\alpha = \frac{p}{q}$*, gdje su* $p \in \mathbb{Z} \setminus \{0\}$*,* $q \in \mathbb{N}$ ***relativno prosti****, nultočka polinoma* f*, onda* $p \mid a_0$ *i* $q \mid a_n$*.*

Dokaz. Po pretpostavci,

$$0 = f(\alpha) = a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0.$$

Množenjem sa q^n dobivamo

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Odatle imamo

$$\begin{aligned} -a_n p^n &= q(a_{n-1}p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}, \\ -a_0 q^n &= p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}). \end{aligned}$$

Prva jednakost daje $q \mid a_n p^n$, a kako su p i q relativno prosti, zaključujemo $q \mid a_n$. Druga jednakost daje $p \mid a_0 q^n$, pa na isti način dolazimo do $\alpha \mid a_0$. □

Napomena 14.17. *Ostanimo još malo u oznakama i pretpostavkama dokaza teorema. Kako je* $\frac{p}{q}$ *nultočka polinoma* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *s cjelobrojnim koeficijentima, to vrijedi*

$$0 = f(\alpha) = a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0.$$

Množenjem sa q^n dobivamo ekvivalentnu tvrdnju

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0.$$

To nam pokazuje da je cijeli broj p nultočka cjelobrojnog polinoma $g(x) = a_n x^n + a_{n-1}qx^{n-1} + \cdots + a_1 q^{n-1}x + a_0 q^n$. Lako vidimo da je $\frac{p}{q}$ nultočka polinoma f ako i samo ako je p cjelobrojna nultočka polinoma g. Ovo je ponekad korisno za praktičnu provjeru je li $\frac{p}{q}$ racionalna nultočka jer izbjegavamo račun s razlomcima u Hornerovom algoritmu. Primjere ćemo dati niže.

Dokaz sljedećeg korolara prepuštamo čitatelju.

Korolar 14.18. *Neka je $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, gdje je $n \geq 1$, takav da $a_n = \pm 1$. Tada su sve racionalne nultočke cjelobrojne (jasno, ako postoje!).*

Hornerov algoritam. Uz oznake iz teorema 14.16, kod određivanja racionalnih nultočaka postupamo ovako:

(1) Napišemo sve djelitelje od a_0 u $\mathbb{Z}$. To su kandidati za p.
(2) Napišemo sve djelitelje od a_n u $\mathbb{N}$. To su kandidati za q.
(3) Formiramo sve moguće $\frac{p}{q}$ koristeći (1) i (2), a između njih uzmemo one koji su potpuno skraćeni (jer p i q moraju biti relativno prosti). Za svaki takav $\alpha = \frac{p}{q}$ idemo na sljedeć i korak
(4) Hornerovim algoritmom provjerimo vrijedi li $f(\alpha) = 0$ **(možemo postupati kao u napomeni 14.17)**.

Primjer 14.19. *Odredimo racionalne nultočke polinoma $2x^3+x^2+x-1$. Polinom ima cjelobrojne koeficijente te su kandidati za racionalne nultočke $\frac{p}{q}$, pri čemu $p|-1$ i $q|2$ tj. $\pm 1, \pm\frac{1}{2}$. Direktnom provjerom Hornerovim algoritmom vidimo da ± 1 nisu nultočke. Za $\frac{1}{2}$ ne provjeravamo direktno već koristimo napomenu 14.17. Stavimo $p = 1$ i $q = 2$ i formiramo novi polinom s cjelobrojnim koeficijentima $g(x) = 2x^3 + qx^2 + q^2x - q^3 \cdot 1 = 2x^3 + 2x^2 + 4x - 8$. Hornerovim algoritmom provjerimo da je $p = 1$ cjelobrojna nultočka polinoma g. To pokazuje da je $\frac{1}{2}$ racionalna nultočka polinoma $2x^3 + x^2 + x - 1$. Slično provjerimo da $-\frac{1}{2}$ nije nultočka polinoma $2x^3+x^2+x-1$. Dakle, $\frac{1}{2}$ jedina je racionalna nultočka polinoma $2x^3 + x^2 + x - 1$.*

Zadatak 14.20. *Odredite racionalne nultočke polinoma $2x^3 - x^2 + 10x - 5$.*

Zadatak 14.21. *Odredite racionalne nultočke polinoma $x^3 + x^2 + x + 3$.*

Racionalne nultočke polinoma s racionalnim koeficijentima. Određivanje racionalnih nultočaka polinoma s racionalnim koeficijentima svodi se na prethodni slučaj ako polinom pomnožimo primjerice s produktom nazivnika svih koeficijenata (ili s nekim drugim pogodnim cijelim brojem, pa u dobivenom polinomu izlučimo najveću zajedničku mjeru svih koeficijenata različitih od nule); na taj način imamo cjelobrojni polinom koji ima isti skup nultočaka kao i polazni polinom. Primjerice,

$$\frac{1}{2}x^3 + \frac{1}{5}x^2 + 3 \in \mathbb{Q}[x] \implies 2 \cdot 5 \cdot \left(\frac{1}{2}x^3 + \frac{1}{5}x^2 + 3\right) = 5x^3 + 2x^2 + 30 \in \mathbb{Z}[x].$$

Pogledajmo sada neke primjene.

Primjer 14.22. *Dokažimo da je $\sqrt{2}$ iracionalan. Zaista, $\sqrt{2}$ je korijen polinoma s cjelobrojnim koeficijentima danog sa $x^2 - 2$. Prema korolaru 14.18, jedine racionalne nultočke tog polinoma su cjelobrojne i to su djelitelji od -2. Kandidati su, dakle, $\pm 1, \pm 2$. Direktnom provjerom vidimo da niti jedan od njih nije korijen polinoma $x^2 - 2$. Prema tome $\sqrt{2}$ nije racionalan.*

Primjer 14.23. *Dokažimo da je $\sqrt[3]{22}$ iracionalan. Zaista, $\sqrt[3]{22}$ je korijen polinoma s cjelobrojnim koeficijentima danog sa $x^3 - 22$. Prema korolaru 14.18 jedine racionalne nultočke su cjelobrojne i to su djelitelji od -22. Kandidati su, dakle, $\pm 1, \pm 2, \pm 11, \pm 22$. Direktnom provjerom vidimo da niti jedan od njih nije korijen polinoma $x^3 - 22$. Prema tome $\sqrt{2}$ nije racionalan.*

Zadatak 14.24. *Dokažite da je $\sqrt[5]{2}$ iracionalan.*

Zadatak 14.25. *Dokažite da je $\sqrt[7]{7}$ iracionalan.*

Teorem 14.26. *Neka je $a, n \in \mathbb{N}$. Tada je ili a jednak n–toj potenciji nekog prirodnog broja ili je $\sqrt[n]{a}$ iracionalan.*

Dokaz. Prisjetimo se, $\sqrt[n]{a}$ je po definiciji jedinstveno pozitivno rješenje jednadžbe $x^n - a = 0$ (vidite teorem 10.5).

Pretpostavimo da je $\sqrt[n]{a}$ racionalan. Svi racionalni korijeni su cjelobrojni prema korolaru 14.18 i to su djelitelji od a. Neka je, dakle, $p \in \mathbb{Z}$ djelitelj od a. Ako je $p^n - a = 0$, onda je

$$p^n = a.$$

Ako je n paran, onda zbog

$$(-p)^n = (-1)^n p^n = p^n = a$$

možemo uzeti da je $p \in \mathbb{N}$. Ako je n neparan, onda je nužno $p \in \mathbb{N}$. Dakle, a je n–ta potencija prirodnog broja p. $\square$

15. Osnovni teorem algebre

Neka su $a_0, a_1, \dots, a_n \in \mathbb{K}$, $a_n \neq 0$. Neka je polinom $f : \mathbb{K} \to \mathbb{K}$ zadan sa

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Ima li polinom f nultočku $\alpha \in \mathbb{K}$? U prethodnom poglavlju smo odgovorili na ovo pitanje u slučajevima $\mathbb{K} = \mathbb{Z}$ i $\mathbb{K} = \mathbb{Q}$. Slučaj $\mathbb{K} = \mathbb{R}$ je znatno kompliciraniji.

Promotrimo polinome stupnja 1 i 2:

$\underline{n = 1}$: $\qquad f(x) = a_1 x + a_0$

Rješavamo jednadžbu $f(x) = 0$:

$$\begin{aligned} a_1 x + a_0 &= 0, \\ a_1 x &= -a_0, \\ x &= -\frac{a_0}{a_1}. \end{aligned}$$

Dakle, $\alpha = -\frac{a_0}{a_1}$ je nultočka polinoma f.

$\underline{n = 2}$: $\qquad f(x) = a_2 x^2 + a_1 x + a_0$

Rješavamo jednadžbu $f(x) = 0$:

$$\begin{aligned} a_2 x^2 + a_1 x + a_0 &= 0, \\ x^2 + \frac{a_1}{a_2} x + \frac{a_0}{a_2} &= 0, \\ x^2 + 2 \cdot \frac{a_1}{2a_2} x + \left(\frac{a_1}{2a_2}\right)^2 - \left(\frac{a_1}{2a_2}\right)^2 + \frac{a_0}{a_2} &= 0, \\ \left(x + \frac{a_1}{2a_2}\right)^2 + \frac{-{a_1}^2 + 4a_0 a_2}{4{a_2}^2} &= 0, \\ \left(x + \frac{a_1}{2a_2}\right)^2 &= \frac{{a_1}^2 - 4a_0 a_2}{4{a_2}^2}. \end{aligned}$$

Realne nultočke se dobiju ako i samo ako je ${a_1}^2 - 4a_0 a_2 \geq 0$. Tada je

$$x + \frac{a_1}{2a_2} = \pm \frac{\sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}$$

odnosno

$$x = \frac{-a_1 \pm \sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}.$$

Dakle, polinom f ima realnu nultočku ako i samo ako je ${a_1}^2 - 4a_0 a_2 \geq 0$. Ako je ${a_1}^2 - 4a_0 a_2 = 0$, tada f ima jedinstvenu nultočku $\alpha = -\frac{a_1}{2a_2}$, a ako je ${a_1}^2 - 4a_0 a_2 > 0$, tada f ima dvije različite nultočke:

$$\alpha_1 = \frac{-a_1 + \sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}, \quad \alpha_2 = \frac{-a_1 - \sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}.$$

Vidimo da se slučajevi $n = 1$ i $n = 2$ razlikuju - polinomi prvog stupnja uvijek imaju realnu nultočku, dok među polinomima drugog stupnja ima i onih koji nemaju realnih nultočaka.

Može se dokazati da vrijedi sljedeći teorem:

Teorem 15.1. *Svaki polinom neparnog stupnja s realnim koeficijentima ima bar jednu realnu nultočku.*

Što je sa slučajem $\mathbb{K} = \mathbb{C}$? Prema ranijem računu, i polinom prvog stupnja i polinom drugog stupnja imaju kompleksnu nultočku. Zapravo, polinom bilo kojeg stupnja $n \geq 1$ ima kompleksnu nultočku. O tome govori osnovni teorem algebre kojeg navodimo bez dokaza:

Teorem 15.2 (Osnovni teorem algebre)**.** *Neka je*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, *polinom stupnja* $n \geq 1$. *Tada postoji* $z_0 \in \mathbb{C}$ *takav da je* $f(z_0) = 0$.

Polinom $f(x) = a_1 x + a_0$ prvog stupnja ima nultočku $\alpha_1 = -\frac{a_0}{a_1}$. Uočimo da je

$$f(x) = a_1\left(x + \frac{a_0}{a_1}\right) = a_1(x - \alpha_1).$$

Polinom $f(x) = a_2 x^2 + a_1 x + a_0$ drugog stupnja ima nultočke

$$\alpha_1 = \frac{-a_1 + \sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}, \quad \alpha_2 = \frac{-a_1 - \sqrt{{a_1}^2 - 4a_0 a_2}}{2a_2}.$$

Uočimo da je

$$\alpha_1 + \alpha_2 = -\frac{a_1}{a_2} \quad \text{i} \quad \alpha_1 \cdot \alpha_2 = \frac{a_0}{a_2},$$

pa je

$$f(x) = a_2\left(x^2 + \frac{a_1}{a_2}x + \frac{a_0}{a_2}\right) = a_2\big(x^2 - (\alpha_1 + \alpha_2)x + \alpha_1 \cdot \alpha_2\big) = a_2(x - \alpha_1)(x - \alpha_2).$$

Posebno, ako je $\alpha_1 = \alpha_2$, možemo pisati $f(x) = a_2(x - \alpha_1)^2$.

Teorem 15.3. *Neka je*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, *polinom stupnja* $n \geq 1$. *Tada postoje jedinstveni različiti* $z_1, \ldots, z_k \in \mathbb{C}$ *i* $n_1, \ldots, n_k \in \mathbb{N}$ *takvi da je*

$$f(x) = a_n(x - z_1)^{n_1} \cdots (x - z_k)^{n_k}$$

i $n_1 + \cdots + n_k = n$.

Dokaz. Prema osnovnom teoremu algebre, polinom f ima nultočku $z_1 \in \mathbb{C}$. Propozicija 14.7 povlači $x - z_1 \mid f(x)$ odnosno postoji $f_1 \in \mathbb{C}[x]$ takav da je

$$f(x) = (x - z_1)f_1(x).$$

Pri tome je f_1 polinom stupnja $n-1$. Ako je $n-1 \geq 1$, polinom f_1 ima nultočku $z_2 \in \mathbb{C}$, pa $x - z_2 \mid f_1(x)$ i stoga postoji $f_2 \in \mathbb{C}[x]$ takav da je

$$f_1(x) = (x - z_2)f_2(x).$$

Polinom f_2 je stupnja $n-2$. Slijedi

$$f(x) = (x - z_1)(x - z_2)f_2(x).$$

Postupak nastavimo sve dok ne dođemo do polinoma f_n koji je nultog stupnja. Znači da postoji $c \in \mathbb{C}$ takav da je $f_n(x) = c$ za svaki $x \in \mathbb{C}$. Tada je

$$f(x) = c(x - z_1)(x - z_2)\cdots(x - z_n).$$

Polinom f ima vodeći koeficijent a_n, a polinom s desne strane jednakosti ima vodeći koeficijent c. Iz korolara 13.3 slijedi $c = a_n$. Preostaje grupirati iste faktore. $\square$

Umjesto zapisa

$$f(x) = a_n(x - z_1)^{n_1}\cdots(x - z_k)^{n_k}$$

iz teorema 15.3, možemo pisati i

$$f(x) = a_n\prod_{i=1}^{k}(x - z_i)^{n_i}.$$

Kako su u tom zapisu $z_1, \ldots, z_k \in \mathbb{C}$ međusobno različiti, to je n_i kratnost nultočke z_i $(i = 1, \ldots, k)$. Dokažimo tu tvrdnju.

Prisjetimo se, u prethodnom poglavlju smo definirali kratnost nultočke α kao cijeli broj m sa svojstvom

$$(x - \alpha)^m \mid f(x), \qquad (x - \alpha)^{m+1} \nmid f(x).$$

Za nultočku z_i $(i = 1, \ldots, k)$ polinoma f očigledno vrijedi $(x - z_i)^{n_i} \mid f(x)$. Ako $(x - \alpha)^{n_i+1} \mid f(x)$, tada postoji polinom g sa svojstvom

$$f(x) = g(x)(x - z_i)^{n_i+1},$$

pa je

$$a_n(x - z_1)^{n_1}\cdots(x - z_{i-1})^{n_{i-1}}(x - z_{i+1})^{n_{i+1}}\cdots(x - z_k)^{n_k} = g(x)(x - z_i).$$

Posebno za $x = z_i$ dobivamo

$$a_n(z_i - z_1)^{n_1}\cdots(z_i - z_{i-1})^{n_{i-1}}(z_i - z_{i+1})^{n_{i+1}}\cdots(z_i - z_k)^{n_k} = 0,$$

pa je $z_i = z_j$ za neki $j \neq i$. To je u kontradikciji s pretpostavkom da su svi $z_1, \ldots, z_k$ različiti. Dakle, $(x - \alpha)^{n_i+1} \nmid f(x)$, pa je n_i kratnost nultočke z_i za $i = 1, \ldots, k$.

Sada nas zanimaju kompleksne nultočke polinoma s realnim koeficijentima.

Lema 15.4. *Ako je $z_0 = a + ib$, gdje su $a, b \in \mathbb{R}$, $b \neq 0$, nultočka polinoma*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$, tada je i $\overline{z_0} = a - ib$ također nultočka polinoma f.

Dokaz. Kako je $f(a + ib) = 0$, to je

$$a_n(a + ib)^n + \cdots + a_1(a + ib) + a_0 = 0.$$

Kompleksnim konjugiranjem se odavde dobije

$$a_n(a - ib)^n + \cdots + a_1(a - ib) + a_0 = 0$$

tj. $f(a - ib) = 0$. □

Lema 15.5. *Ako je $a + ib$, gdje su $a, b \in \mathbb{R}$, $b \neq 0$, nultočka polinoma $f \in \mathbb{R}[x]$, tada $x^2 - 2ax + a^2 + b^2 \mid f(x)$ u $\mathbb{R}[x]$.*

Dokaz. Kako je $f(a+ib) = 0$, propozicija 14.7 povlači $x-(a+ib) \mid f(x)$. Međutim, iz leme 15.4 slijedi i da je $f(a - ib) = 0$, pa vrijedi i $x - (a - ib) \mid f(x)$. Dakle, $f(x)$ je djeljiv sa

$$\begin{aligned} \big(x - (a + ib)\big)\big(x - (a - ib)\big) &= (x - a - ib)(x - a + ib) = (x - a)^2 - i^2 b^2 \\ &= (x - a)^2 + b^2 = x^2 - 2ax + a^2 + b^2, \end{aligned}$$

a to je polinom s realnim koeficijentima. □

Teorem 15.6. *Neka je*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$, polinom stupnja $n \geq 1$. Tada postoje jedinstveni $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$, $n_1, \ldots, n_k \in \mathbb{N}$, $p_1, \ldots, p_l \in \mathbb{R}$, $q_1, \ldots, q_l \in \mathbb{R}$, $m_1, \ldots, m_l \in \mathbb{N}$ takvi da je

$$f(x) = a_n(x - \alpha_1)^{n_1} \ldots (x - \alpha_k)^{n_k} (x^2 + p_1 x + q_1)^{m_1} \ldots (x^2 + p_l x + q_l)^{m_l};$$

$p_i^2 - 4q_i < 0$, $i = 1, \ldots, l$; $\quad n = n_1 + \cdots + n_k + 2m_1 + \cdots + 2m_l$.

Teorem 15.6 slijedi iz teorema 15.3 i leme 15.5 (kvadratni faktori, tj. faktori oblika $x^2 + p_i x + q_i$, su dobiveni iz parova kompleksno konjugiranih nultočaka polinoma f).

Prisjetimo se, ako je

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, polinom stupnja $n \geq 1$, tada postoje $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (ne nužno različiti!) takvi da je

$$f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n).$$

Pogledajmo što možemo zaključiti iz ovog zapisa u slučajevima $n = 2$ i $n = 3$.

$\underline{n=2}$:

$$\begin{aligned}
a_2x^2+a_1x+a_0 &= a_2(x-\alpha_1)(x-\alpha_2),\\
a_2\left(x^2+\frac{a_1}{a_2}x+\frac{a_0}{a_2}\right) &= a_2\big(x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2\big),\\
x^2+\frac{a_1}{a_2}x+\frac{a_0}{a_2} &= x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2.
\end{aligned}$$

Prema korolaru 13.3 (o jednakosti polinoma) imamo:

$$\begin{aligned}
\alpha_1+\alpha_2 &= -\frac{a_1}{a_2},\\
\alpha_1\alpha_2 &= \frac{a_0}{a_2}.
\end{aligned}$$

$\underline{n=3}$:

$$\begin{aligned}
a_3x^3+a_2x^2+a_1x+a_0 &= a_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3,)\\
a_3\left(x^3+\frac{a_2}{a_3}x^2+\frac{a_1}{a_3}x+\frac{a_0}{a_3}\right) &= a_3\big(x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2\big)(x-\alpha_3),\\
x^3+\frac{a_2}{a_3}x^2+\frac{a_1}{a_3}x+\frac{a_0}{a_3} &= x^3-(\alpha_1+\alpha_2+\alpha_3)x^2\\
&\quad +(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)x-\alpha_1\alpha_2\alpha_3.
\end{aligned}$$

Slijedi

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= -\frac{a_2}{a_3},\\
\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 &= \frac{a_1}{a_3},\\
\alpha_1\alpha_2\alpha_3 &= -\frac{a_0}{a_3}.
\end{aligned}$$

Općenito vrijede sljedeće tzv. Vièteove formule:

$$\begin{aligned}
\alpha_1+\alpha_2+\cdots+\alpha_n &= -\frac{a_{n-1}}{a_n},\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_1\alpha_n+\alpha_2\alpha_3+\alpha_2\alpha_4+\cdots+\alpha_{n-1}\alpha_n &= \frac{a_{n-2}}{a_n},\\
\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\cdot+\alpha_{n-2}\alpha_{n-1}\alpha_n &= -\frac{a_{n-3}}{a_n},\\
&\vdots\\
\alpha_1\alpha_2\cdots\alpha_n &= (-1)^n\frac{a_0}{a_n}.
\end{aligned}$$

Vièteove formule nam, među ostalim, omogućuju odrediti neke veze među nultočkama danog polinoma ne računajući efektivno te nultočke.

Primjer 15.7. *Neka je $f(x)=2x^3-x^2+2x-5$. Izračunajmo $\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\frac{1}{\alpha_3}$, gdje su $\alpha_1,\alpha_2,\alpha_3$ nultočke polinoma f.*

Prema Vièteovim formulama je

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3&=-\frac{-1}{2}=\frac{1}{2},\\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_3\alpha_1&=\frac{2}{2}=1,\\ \alpha_1\alpha_2\alpha_3&=-\frac{-5}{2}=\frac{5}{2}.\end{aligned}$$

Slijedi

$$\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\frac{1}{\alpha_3}=\frac{\alpha_2\alpha_3+\alpha_1\alpha_3+\alpha_1\alpha_2}{\alpha_1\alpha_2\alpha_3}=\frac{1}{\frac{5}{2}}=\frac{2}{5}.$$

16. Rastav racionalne funkcije na parcijalne razlomke

Neka su $f, g \in \mathbb{R}[x]$ polinomi i neka g nije nulpolinom. Funkcija

$$x \mapsto \frac{f(x)}{g(x)}$$

se naziva **racionalna funkcija**; njena domena je skup

$$\mathcal{D} = \{x \in \mathbb{R} \mid g(x) \neq 0\}.$$

Primjer 16.1. *(a) Racionalna funkcija*

$$f(x) = \frac{5}{x+1}$$

ima domenu $\mathcal{D}(f) = \{x \in \mathbb{R} \mid x + 1 \neq 0\} = \mathbb{R} \setminus \{-1\}$.

(b) Racionalna funkcija

$$g(x) = \frac{2x-7}{x^2+4x+9}$$

ima domenu $\mathcal{D}(g) = \{x \in \mathbb{R} \mid x^2 + 4x + 9 \neq 0\} = \mathbb{R}$ *jer kvadratna jednadžba* $x^2 + 4x + 9 = 0$ *nema realnih rješenja.*

Neka je $m \in \mathbb{R}[x]$ najveća zajednička mjera polinoma f i g; prisjetimo se, ona se određuje Euklidovim algoritmom (vidite kraj 13. poglavlja). Tada postoje relativno prosti polinomi $f_1, g_1 \in \mathbb{R}[x]$ takvi da je $f = m \cdot f_1$ i $g = m \cdot g_1$. Slijedi

$$\frac{f}{g} = \frac{m \cdot f_1}{m \cdot g_1} = \frac{f_1}{g_1}.$$

Kažemo da je racionalna funkcija $x \mapsto \frac{f(x)}{g(x)}$ **prava racionalna funkcija** ako je f **nulpolinom ili deg(f) $<$ deg(g)**.

Ako je $\deg(f) \geq \deg(g)$, tada prema teoremima 13.8 i 13.9 (o dijeljenju s ostatkom) postoje polinomi g_1 i r takvi da je $f = g \cdot g_1 + r$ i $\deg(r) < \deg(g)$. Slijedi

$$\frac{f}{g} = \frac{g \cdot g_1 + r}{g} = g_1 + \frac{r}{g}.$$

Pritom je g_1 polinom, a $\frac{r}{g}$ prava racionalna funkcija.

Primjer 16.2. *Neka je*

$$f(x) = \frac{x^3+2x+1}{x^2+1}.$$

Dijeljenjem polinoma $x^3 + 2x + 1$ *sa* $x^2 + 1$ *dobivamo kvocijent* x *i ostatak* $x + 1$. *Dakle,*

$$f(x) = x + \frac{x+1}{x^2+1}.$$

Primjer 16.3. *Neka je*

$$f(x) = \frac{2x^2 + 7x - 8}{x + 5}.$$

U ovom slučaju je nazivnik oblika $x - \alpha$ za $\alpha = -5$, pa ostatak pri dijeljenju polinoma $2x^2 + 7x - 8$ sa $x + 5$ možemo odrediti Hornerovom shemom:

	2	7	−8
$\alpha = -5$	2	−3	7

Kvocijent je polinom prvog stupnja, a njegove koeficijente redom pročitamo iz donjeg retka: to su 2 i −3. Brojnik prave racionalne funkcije je $f(-5) = 7$. Slijedi

$$f(x) = 2x - 3 + \frac{7}{x + 5}.$$

Prisjetimo se teorema 15.6: Svaki polinom $g \in \mathbb{R}[x]$ stupnja $n \geq 1$ se može na jedinstven način zapisati u obliku

$$g(x) = (x - x_1)^{n_1} \cdots (x - x_k)^{n_k} (x^2 + p_1 x + q_1)^{m_1} \cdots (x^2 + p_l x + q_l)^{m_l},$$

gdje su $x_1, \ldots, x_k \in \mathbb{R}$, $n_1, \ldots, n_k \in \mathbb{N}$, $p_1, \ldots, p_l \in \mathbb{R}$, $q_1, \ldots, q_l \in \mathbb{R}$, $m_1, \ldots, m_l \in \mathbb{N}$, $p_i^2 - 4q_i < 0$ za $i = 1, \ldots, l$; $n = n_1 + \cdots + n_k + 2m_1 + \cdots + 2m_l$ i svi $x - x_i$ (za $i = 1, \ldots, k$) te svi $x^2 + p_i x + q_i$ (za $i = 1, \ldots, l$) su međusobno različiti.

Oslanjajući se na takav prikaz polinoma, pravu racionalnu funkciju možemo rastaviti na **parcijalne razlomke**:

Teorem 16.4. *Neka je*

$$g(x) = (x - x_1)^{n_1} \cdots (x - x_k)^{n_k} (x^2 + p_1 x + q_1)^{m_1} \cdots (x^2 + p_l x + q_l)^{m_l},$$

pri čemu je $p_i^2 - 4q_i < 0$ za $i = 1, \ldots, l$. Neka je $f \in \mathbb{R}[x]$ te neka je deg(f) < deg(g). Tada je

$$\begin{aligned}
\frac{f(x)}{g(x)} \quad = \quad & \frac{A_{11}}{x - x_1} + \frac{A_{12}}{(x - x_1)^2} + \cdots + \frac{A_{1n_1}}{(x - x_1)^{n_1}} + \cdots \\
& + \frac{A_{k1}}{x - x_k} + \frac{A_{k2}}{(x - x_k)^2} + \cdots + \frac{A_{kn_k}}{(x - x_k)^{n_k}} \\
& + \frac{B_{11}x + C_{11}}{x^2 + p_1 x + q_1} + \cdots + \frac{B_{1m_1}x + C_{1m_1}}{(x^2 + p_1 x + q_1)^{m_1}} + \cdots \\
& + \frac{B_{l1}x + C_{l1}}{x^2 + p_l x + q_l} + \cdots + \frac{B_{lm_l}x + C_{lm_l}}{(x^2 + p_l x + q_l)^{m_l}},
\end{aligned}$$

gdje su $A_{ij} \in \mathbb{R}$ ($i = 1, \ldots, k$; $j = 1, \ldots, n_k$), $B_{uv}, C_{uv} \in \mathbb{R}$ ($u = 1, \ldots, l$; $v = 1, \ldots, m_l$) konstante.

Dokaz. Zapišimo

$$g(x) = (x - x_1)^{n_1} g_1(x).$$

Uočimo da je $g_1(x_1) \neq 0$. Neka je $A_{1n_1} = \frac{f(x_1)}{g_1(x_1)}$. Tada je

$$\begin{aligned}\frac{f(x)}{g(x)} &= \frac{A_{1n_1}}{(x-x_1)^{n_1}} + \frac{f(x)}{g(x)} - \frac{A_{1n_1}}{(x-x_1)^{n_1}} \\ &= \frac{A_{1n_1}}{(x-x_1)^{n_1}} + \frac{f(x) - A_{1n_1}g_1(x)}{g(x)}.\end{aligned}$$

Kako je

$$(f - A_{1n_1}g_1)(x_1) = f(x_1) - A_{1n_1}g_1(x_1) = 0,$$

to $x - x_1 \mid f - A_{1n_1}g_1$, pa postoji $h_1 \in \mathbb{R}[x]$ takav da je

$$(f - A_{1n_1}g_1)(x) = (x - x_1)h_1(x).$$

Sada je jasno zašto smo A_{1n_1} definirali baš kao $\frac{f(x_1)}{g_1(x_1)}$. Ideja je bila da se za tu konstantu izabere ona vrijednost za koju polinom $f(x) - A_{1n_1}g_1(x)$ ima x_1 za nultočku. Slijedi

$$\frac{(f - A_{1n_1}g_1)(x)}{g(x)} = \frac{(x-x_1)h_1(x)}{(x-x_1)^{n_1}g_1(x)} = \frac{h_1(x)}{(x-x_1)^{n_1-1}g_1(x)}.$$

Sada postupak nastavimo tako da ulogu polinoma f preuzima polinom h_1, a ulogu polinoma g polinom $x \mapsto (x-x_1)^{n_1-1}g_1(x)$ kojemu je x_1 nultočka kratnosti $n_1 - 1$. Tako ćemo doći do sumanda $\frac{A_{1,n_1-1}}{(x-x_1)^{n_1-1}}$. Nastavljajući postupak, nakon konačno koraka dolazimo do sumanda $\frac{A_{11}}{x-x_1}$ i tada će ulogu polinoma g preuzeti polinom g_1 kojemu su realne nultočke $x_2, \ldots, x_k$. Kada iskoristimo sve realne nultočke, dobili smo sve linearne članove u prikazu. Tada prelazimo na kompleksne nultočke. Znamo da se kompleksne nultočke polinoma pojavljuju kao parovi konjugirano kompleksnih brojeva, pa se polinom g_k (koji je nakon iscrpljivanja svih realnih nultočaka preuzeo ulogu polinoma g) može zapisati u obliku

$$g_k(x) = (x^2 + p_1x + q_1)^{m_1}g_{k+1}(x),$$

a to možemo shvatiti kao

$$g_k(x) = \big((x - z_1)(x - \overline{z_1})\big)^{m_1}g_{k+1}(x),$$

gdje su $z_1, \overline{z_1}$ parovi kompleksnih nultočaka polinoma g_k. Postupak za kompleksne nultočke nastavimo na isti način kako smo to radili za realne, s tim da ovog puta uvrštavamo bilo koju od dvije kompleksno konjugirane nultočke. Točnije, imamo

$$\begin{aligned}\frac{h(x)}{g_k(x)} &= \frac{B_{1m_1}x + C_{1m_1}}{(x^2+p_1x+q_1)^{m_1}} + \frac{h(x)}{g_k(x)} - \frac{B_{1m_1}x + C_{1m_1}}{(x^2+p_1x+q_1)^{m_1}} \\ &= \frac{B_{1m_1}x + C_{1m_1}}{(x^2+p_1x+q_1)^{m_1}} + \frac{h(x) - (B_{1m_1}x + C_{1m_1})g_{k+1}(x)}{g_k(x)}\end{aligned}$$

i sada se B_{1m_1} i C_{1m_1} odrede tako da brojnik drugog sumanda bude nula za z_1, tj.

$$h(z_1) - (B_{1m_1}z_1 + C_{1m_1})g_{k+1}(z_1) = 0.$$

Obzirom da kompleksno konjugiranje čuva tu jednadžbu, brojnik drugog sumanda je nula i za $\overline{z_1}$. Znači da je taj brojnik djeljiv sa

$$(x - z_1)(x - \overline{z_1}) = x^2 + p_1x + q_1,$$

pa nakon kraćenja u nazivniku ostaje

$$(x^2 + p_1x + q_1)^{m_1-1}g_{k+1}(x).$$

Postupak nastavimo. Kada iskoristimo sve kompleksne nultočke, dobili smo sve kvadratne članove u prikazu. □

Primjer 16.5. *Pravu racionalnu funkciju*

$$\frac{x^3-2}{x(x+1)^3}$$

rastavimo na parcijalne razlomke:

$$\frac{x^3-2}{x(x+1)^3} = \frac{A}{x} + \frac{B}{x+1} + \frac{C}{(x+1)^2} + \frac{D}{(x+1)^3}.$$

Treba odrediti konstante $A, B, C, D \in \mathbb{R}$. Množenjem gornje jednadžbe sa $x(x+1)^3$ dobivamo redom:

$$\begin{aligned} x^3-2 &= A(x+1)^3 + Bx(x+1)^2 + Cx(x+1) + Dx, \\ x^3-2 &= A(x^3+3x^2+3x+1) + B(x^3+2x^2+x) + C(x^2+x) + Dx, \\ x^3-2 &= (A+B)x^3 + (3A+2B+C)x^2 + (3A+B+C+D)x + A. \end{aligned}$$

Primjenom korolara 13.3 (o jednakosti polinoma) dolazimo do sustava:

$$\begin{aligned} A+B &= 1 \\ 3A+2B+C &= 0 \\ 3A+B+C+D &= 0 \\ A &= -2 \end{aligned}$$

čija su rješenja $A=-2,\ B=3,\ C=0,\ D=3$. Dakle,

$$\frac{x^3-2}{x(x+1)^3} = \frac{-2}{x} + \frac{3}{x+1} + \frac{3}{(x+1)^3}.$$

Primjer 16.6. *Pravu racionalnu funkciju*

$$\frac{2x^4+2x^2-5x+1}{x(x^2+x+1)^2}$$

rastavimo na parcijalne razlomke:

$$\frac{2x^4+2x^2-5x+1}{x(x^2+x+1)^2} = \frac{A}{x} + \frac{Bx+C}{x^2+x+1} + \frac{Dx+E}{(x^2+x+1)^2}.$$

Slijedi

$$\begin{aligned} 2x^4+2x^2-5x+1 &= A(x^2+x+1)^2 + (Bx+C)x(x^2+x+1) \\ &\quad +(Dx+E)x, \\ 2x^4+2x^2-5x+1 &= A(x^4+x^2+1+2x^3+2x^2+2x) \\ &\quad +(Bx^4+Cx^3+Bx^3+Cx^2+Bx^2+Cx) \\ &\quad +Dx^2+Ex, \\ 2x^4+2x^2-5x+1 &= (A+B)x^4 + (2A+B+C)x^3 \\ &\quad +(3A+B+C+D)x^2 + (2A+C+E)x + A. \end{aligned}$$

Uspoređivanje odgovarajućih koeficijenata daje:

$$\begin{aligned} A+B &= 2 \\ 2A+B+C &= 0 \\ 3A+B+C+D &= 2 \\ 2A+C+E &= -5 \\ A &= 1. \end{aligned}$$

Rješenja ovog sustava su $A=1,\ B=1,\ C=-3,\ D=1,\ E=-4$. *Dakle,*

$$\frac{2x^4+2x^2-5x+1}{x(x^2+x+1)^2} = \frac{1}{x} + \frac{x-3}{x^2+x+1} + \frac{x-4}{(x^2+x+1)^2}.$$