Relacije ekvivalencije i cijeli brojevi

Kovačić, Iva

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Iva Kovačić

RELACIJA EKVIVALENCIJE I CIJELI BROJEVI

Diplomski rad

Voditelj rada:
prof.dr.sc. Goran Muić

Zagreb, rujan 2023.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem Gospodinu Bogu koji me vodio kroz cijelo moje školovanje te mi dao pamet, snagu i volju da svoje fakultetsko obrazovanje uspješno privedem kraju. Zahvaljujem obitelji, posebno roditeljima, koji su mi ovo sve omogućili i bili podrška tijekom svih ovih godina. Zahvaljujem dečku Ivanu koji je uvijek bio uz mene i nije mi dopustio da posustanem. Hvala didi i baki čije molitve su me dizale i vodile i kad mi je bilo najteže. Veliko hvala i mom mentoru, prof.dr.sc. Goranu Muiću, na volji i strpljenju tijekom pisanja mog diplomskog rada. Hvala svima koji su na bilo koji način bili dio ovog mog "matematičkog putovanja".

Sadržaj

Uvod

Pojam ”relacija” se često rabi u svakodnevnom životu označavajući neki odnos ili vezu. Slično značenje taj pojam ima i u matematici. Ako kažemo da su neka dva elementa u relaciji, to znači da između njih postoji izvjesna veza. U ovom radu proučavamo upravo jednu takvu vezu, odnosno relaciju, a to je relacija ekvivalencije. Pomoću relacije ekvivalencije konstruirat ćemo i skup cijelih brojeva.

Sa skupom prirodnih brojeva se upoznajemo još u osnovnoj školi, no tada smatramo da svojstva koja imaju neki prirodni brojevi imaju i svi prirodni brojevi. Znamo da, ako zbrojimo ili pomnožimo dva prirodna broja, rezultat će opet biti prirodan broj. Zato kažemo da je skup prirodnih brojeva zatvoren u odnosu na zbrajanje i množenje. No, problem se pojavljuje već kod oduzimanja dvaju prirodnih brojeva kod kojih je umanjenik manji od umanjitelja, npr. $1 - 2$. Tada za rezultat dobivamo broj koji ne postoji u skupu prirodnih brojeva. Možemo reći da tada skup prirodnih brojeva postaje ”premali” ili ”preuzak” pa ga je potrebno ”proširiti”. Takvim ”proširivanjem” skupa prirodnih brojeva zapravo postupno konstruiramo skup cijelih brojeva. Tom problematikom bavimo se u ovom radu. Rad je podijeljen u dva pogavlja.

U prvom poglavlju definiramo sam pojam relacije i navodimo njihov primjer. Također, navodimo i Peanove aksiome na osnovi kojih je izgrađen skup prirodnih brojeva.

U drugom poglavlju najprije proučavamo jednu binarnu relaciju, relaciju ekvivalencije. Zatim, pomoću relacije ekvivalencije, na skupu $\mathbb{N} \times \mathbb{N}$, konstruiramo skup cijelih brojeva $\mathbb{Z}$ te potom proučavamo svojstva osnovnih računskih operacija na tom skupu. Također, proučavamo i algebarsku strukturu skupa $\mathbb{Z}$ te pokazujemo da uređena trojka $(\mathbb{Z}, +, \cdot)$ čini prsten s jedinicom.

Poglavlje 1

Preliminarni rezultati

U ovom poglavlju definiramo pojmove koji su nam potrebni za daljnje proučavanje ovog rada.

1.1 Pojam relacije

Najprije definiramo pojam relacije, jedan od najvažnijih pojmova matematike uopće, koji kao specijalan slučaj sadrži pojam funkcije.

Kod pojma funkcije imamo u prvom redu dva skupa, E i F, te svakom elementu $x \in E$ pridružujemo jedinstveni element $f(x)$ iz skupa F. Zapravo, zadajemo izvjestan odnos između elemenata skupova E i F. Taj odnos je specijalne prirode jer je svaki element $x \in E$ u odnosu (u funkcionalnoj vezi, u relaciji) s jedinstvenim elementom $f(x)$ iz skupa F. Takav odnos je previše specijalan pa nastaje potreba da se između elemenata dvaju skupova E i F uspostavi odnos pri kojem jednom elementu iz E odgovara više elemenata skupa F.

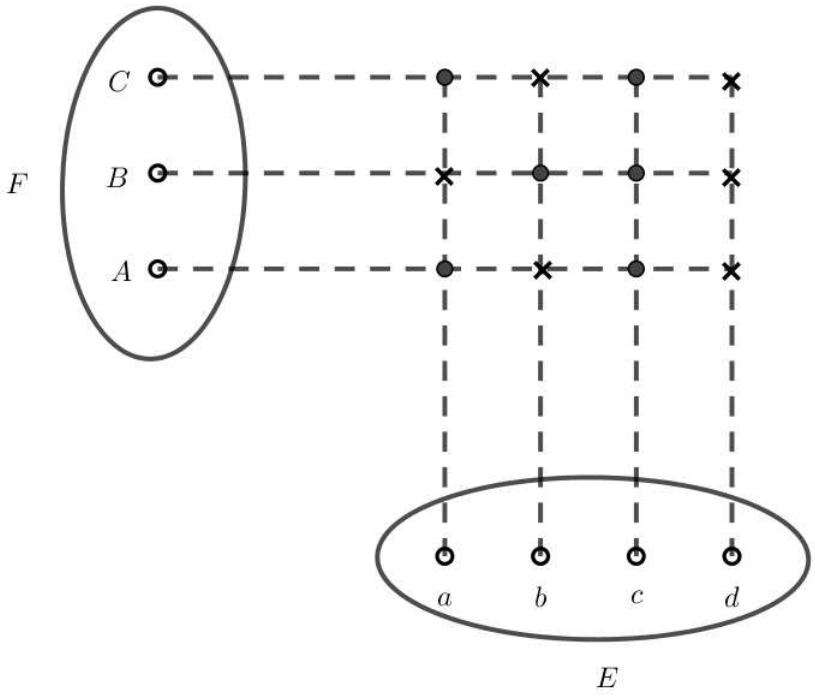
Mi zapravo želimo proučavati najopćenitije odnose elemenata skupova E i F koje ćemo nazivati relacijama. Prije nego napišemo formalnu definiciju relacije, uzmimo jednostavan primjer kojim ćemo ilustrirati taj matematički pojam.

Primjer 1.1.1. Neka je $E = \{a, b, c, d\}$ društvo od četiri osobe, a $F = \{A, B, C\}$ drugo društvo od tri osobe. Između ta dva društva možemo uspostaviti odnos "poznavanja", tj. može se dogoditi da npr. pripadnik b društva E pozna nijednu, jednu ili više osoba iz društva F.
Uzmimo ovu mogućnost

$a \in E$ pozna osobe A i C
$b \in E$ pozna osobu B
$c \in E$ pozna osobe A, B, C

$d \in E$ ne pozna ni A ni B ni C.

Na ovaj način je putem "poznavanja" uočen, odnosno ustanovljen, odnos između skupova E i F. Na Slici 1.1 prikazan je taj odnos. Prirodno je promatrati Kartezijev produkt skupova E i F jer se tu pojavljuju sve mogućnosti poznavanja. Na Slici 1.1 prikazani su skupovi E, F, njihov produkt $E \times F$, a s krugovima je označen odnos poznavanja naveden gore.



Slika 1.1: Relacije

Tako je npr. uređeni par (c, B) označen krugom jer osoba c iz društva E pozna osobu B iz društva F. Naprotiv, uređeni par (b, C) označen je samo križićem jer osoba $b \in E$ ne

pozna osobu $C \in F$.

Označimo li s ρ skup svih ispunjenih krugova na Slici 1.1, tj.

$$\rho = \{(a, A), (a, C), (b, B), (c, A), (c, B), (c, C)\}$$

vidimo da je ρ podskup Kartezijevog produkta $E \times F$ i to točno onaj koji sadrži elemente koji su u navedenom odnosu "poznavanja".

Podskup $\rho \subseteq E \times F$ kojeg smo opisali u prethodnom primjeru nije funkcijski, tj. nema funkcije iz E u F (niti iz F u E) za koji bi ρ bio graf. To upućuje na potrebu proučavanja proizvoljnih podskupova Kartezijeva produkta $E \times F$.

Definicija 1.1.2. *Neka su E i F skupovi. Svaki podskup ρ Kartezijeva produkta $E \times F$ zove se **relacija**.*

*Za element $x \in E$ kažemo da je **u relaciji** ρ s elementom $y \in F$ ako i samo ako je $(x, y) \in \rho$.*

Činjenicu $(x, y) \in \rho$ često pišemo u obliku $x \rho y$ ili $y = \rho(x)$ i kažemo x ima svojstvo da je u relaciji ρ s y.

Prva projekcija skupa ρ zove se područje definicije ili domena relacije ρ, a druga projekcija skupa ρ zove se slika relacije ρ.

Na sličan način kažemo da su elementi $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$ u relaciji ρ ako je $(a_1, \ldots, a_n) \in \rho$ i ρ podskup od $A_1 \times \cdots \times A_n$. Ovakva relacija se zove $n-$**arna**. U slučaju $n = 2$ **relacija** se zove **binarna**, a u slučaju $n = 1$ **unarna**. Prema tome, unarna relacija ρ na skupu E je svaki podskup $\rho \subseteq E$, a binarna relacija na skupu E je svaki podskup $\rho \subseteq E \times E$. Nama su najvažnije binarne relacije, i to oblika $\rho \subseteq E \times E$. Jednu specifičnu binarnu relaciju proučavamo upravo u sljedećem poglavlju.

Navedimo sada i neka važna svojstva koja binarna relacija može imati.

Definicija 1.1.3. *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*

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

(iii) ***antisimetrična*** *ako*

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

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

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

Kako smo već i spomenuli, funkcija je poseban slučaj relacije. Preciznije, **funkcija** ili **preslikavanje** $f : D \to K$ je svaka relacija $f \subseteq D \times K$ sa svojstvom da za svaki $x \in D$ postoji jedinstveni $y \in K$ takav da je $(x, y) \in f$. Pišemo

$$y = f(x),$$

a samo pridruživanje označavamo s

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

Prema tome, vrijedi

$$y = f(x) \Leftrightarrow (x, y) \in f.$$

Za daljnje proučavanje ovog rada, potrebna nam je i sljedeća definicija.

Definicija 1.1.4. *Dana je funkcija* $f : D \to K$.

Kažemo da je f ***injekcija (injektivno preslikavanje)*** *ako*

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

Kažemo da je f ***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.*

1.2 Peanovi aksiomi skupa prirodnih brojeva

S prirodnim brojevima upoznali smo se još i prije osnovne škole. Od ranije znamo da, zbog svoje važnosti u matematici, skup prirodnih brojeva ima svoju posebnu, stalnu oznaku. Pišemo: $\mathbb{N} = \{1, 2, 3, \dots\}$. Na skupu prirodnih brojeva imamo uobičajene operacije zbrajanja i množenja čija svojstva dobro znamo još iz osnovne škole.

Strogu aksiomatsku izgradnju skupa prirodnih brojeva moguće je napraviti na osnovi tzv. **Peanovih aksioma**.

Definicija 1.2.1. *Neprazan skup $\mathbb{N}$ zove se **skup prirodnih brojeva**, a njegovi elementi **prirodni brojevi**, ako vrijede ovi uvjeti (aksiomi):*

Aksiom A: Postoji funkcija $s : \mathbb{N} \longrightarrow \mathbb{N}$.
Aksiom B: Postoji bar jedan element u $\mathbb{N}$, označimo ga s 1, takav da je $s(n) \neq 1$ za svako $n \in \mathbb{N}$.
Aksiom C: Ako je $s(m) = s(n)$ za $m, n \in \mathbb{N}$, onda je $m = n$.
Aksiom D: Ako je M podskup od $\mathbb{N}$ i ako vrijedi

$$\begin{aligned} &(i) \quad 1 \in M \\ &(ii) \quad (\forall n \in \mathbb{N})\ (n \in M \Rightarrow s(n) \in M) \end{aligned}$$

onda je $M = N$.

Navedeni aksiomi poznati su pod imenom *Peanovi aksiomi skupa prirodnih brojeva* prema talijanskom matematičaru G. Peanu (1858. - 1931.). Skup $\mathbb{N}$, koji zadovoljava sva četiri navedena aksioma, ima sva ona svojstva za koja vjerujemo da ih ima skup prirodnih brojeva s kojim se služimo u svakodnevnom životu, no to ovdje nećemo dokazivati.

Poglavlje 2

Relacija ekvivalencije. Cijeli brojevi.

Nakon uvodnih i elementarnih primjera i definicija slijedi glavna tema ovog rada pa u ovom dijelu promatramo jednu specifičnu binarnu relaciju, relaciju ekvivalencije, te konstrukciju skupa cijelih brojeva.

2.1 Relacija ekvivalencije

Definicija 2.1.1. *Neka je E neprazan skup i $\sim \subseteq E \times E$ binarna relacija na E. Za relaciju $\sim$ kažemo da je **relacija ekvivalencije (relacija klasifikacije)** ako su ispunjena ova **tri** uvjeta:*

(a) $x \sim x\ (\forall\, x \in E)$ *(refleksivnost)*

(b) $x \sim y \Rightarrow y \sim x$ *(simetričnost)*

(c) $(x \sim y\ \&\ y \sim z) \Rightarrow x \sim z$ *(tranzitivnost).*

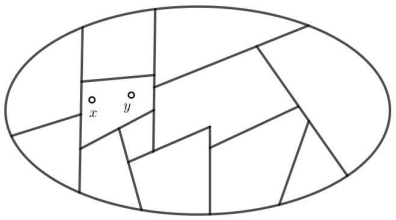
Primjer 2.1.2. Neka je E skup svih trokuta koji se nalaze u ravnini Π. Za dva trokuta $x, y \in E$ reći ćemo da su ekvivalentni, ako su oni kongruentni u smislu kongruencije naučene u osnovnoj školi (tj., oni se mogu jedan na drugoga "položiti").

Primjer 2.1.3. Neka E ima značenje kao u Primjeru 2.1.2 Sada za dva trokuta kažemo da su ekvivalentni, ako su slični u smislu sličnosti naučene u osnovnoj školi. Vidimo da je i sličnost relacija ekvivalencije.

Primjer 2.1.4. Sa E označimo skup svih pravaca ravnine Π. Za dva pravca $x, y \in E$ reći ćemo da su ekvivalentni ako su oni paralelni. Ponovno se uviđa da je paralelnost relacija ekvivalencije na skupu E.

Primjer 2.1.5. Neka je F skup svih država koje su bile članice UN (Ujedinjeni narodi) 1.11.1960. Sa E označimo skup svih ljudi sa svojstvom "$x \in E$ ako i samo ako je x

državljanin samo jedne države i ta je članica UN". Na taj način je zadana relacija ekvivalencije na skupu F. Ovaj primjer možemo skicirati (vidi sliku 2.1): skup E zamišljamo kao sve točke unutar zatvorene crte, a pojedini dijelovi tako podijeljenog skupa E predstavljaju pojedine države (njih je samo nekoliko skicirano). Vjernija slika dobiva se pomoću atlasa, odnosno globusa. Elementi x, y na Slici 2.1 su ekvivalentni.



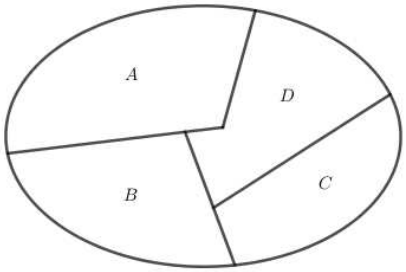
Slika 2.1: Države članice UN

Primjer 2.1.5 omogućava sljedeću generalizaciju:

Primjer 2.1.6. Neka je npr. skup E unija 4 skupa A, B, C, D (slika 2.2) za koja uzimamo da su disjunktni i da ni jedan nije prazan. Za dva elementa $x, y \in E$ stavimo $x \sim y$, ako i samo ako je ispunjena samo jedna od ovih mogućnosti

$$x, y \in A; \qquad x, y \in B; \qquad x, y \in C; \qquad x, y \in D,$$

tj. ako i samo ako su oni elementi istog skupa na koji je E podijeljeno.



Slika 2.2: Unija 4 skupa

Sada se lako vidi da je $\sim$ relacija ekvivalencije na E. No, *prirodno* je promatrati i skup $\mathfrak{F} = \{A, B, C, D\}$, čiji su elementi oni skupovi na koje je E podijeljeno. Za dva elementa $a, b \in E$ imamo $a \sim b$, ako i samo ako postoji X u $\mathfrak{F}$ takvo da je $a, b \in X$.

Primjer 2.1.6 možemo ovako generalizirati:

Neka je $E = \bigcup A$ $(A \in \mathfrak{F})$ unija skupova neke množine $\mathfrak{F}$. Pretpostavimo da nijedan element $A \in \mathfrak{F}$ nije prazan i da za bilo koja dva elementa $A, B \in \mathfrak{F}$ vrijedi

$$A = B \qquad ili \qquad A \cap B = \emptyset.$$

Drugim riječima, skup E je rastavljen (podijeljen) na pune disjunktne skupove. Za množinu $\mathfrak{F}$ s navedenim svojstvima kažemo da je *particija skupa E*. Prema tome, *skup* $\mathfrak{F}$ *je* ***particija skupa*** *E, ako i samo ako za svaki element* $x \in E$ *postoji jedan i samo jedan element* $A \in \mathfrak{F}$ *takav da je* $x \in A$.

Pomoću particije $\mathfrak{F}$ skupa E, slično kao u Primjeru 2.1.6., može se definirati relacija ekvivalencije na skupu E. Dovoljno je staviti $x \sim y$, ako i samo ako postoji $A \in \mathfrak{F}$ takvo da je $x, y \in A$. Odmah se vidi da je $\sim$ relacija ekvivalencije na E. Elementi skupa $\mathfrak{F}$ mogu se opisati pomoću tako dobivene relacije $\sim$. Naime, za $X \in \mathfrak{F}$ postoji $a \in X$. Sada je

$$X = \{x \in E : x \sim a\} .$$

Elementi skupa $\mathfrak{F}$ zovu se *razredi* ili klase ekvivalencije relacije $\sim$.

Napomena 2.1.7. *Elementi skupa* $\mathcal{F}$ *su podskupovi od E, tj.* $\mathcal{F} \subseteq \mathcal{P}(E)$*; dakle* $\mathcal{F} \in \mathcal{P}[\mathcal{P}(E)]$. Ovdje su u pitanju tri skupa: E, $\mathcal{P}(E)$ i $\mathcal{P}[\mathcal{P}(E)]$.

Uloga particije $\mathcal{F}$ vrlo je slična ulozi UN jer su UN stvoreni od različitih država. Svaka država tamo je zastupljena svojim predstavnikom (za UN nije važno tko je taj predstavnik, važno je samo da je on državljanin dotične države). Problemi koji su važni za cijeli svijet rješavaju se u okvirima UN, a ne u okvirima pojedinih država. Pojedine države sudjeluju samo preko svojih predstavnika.

Sada se prelazi na opisivanje jednog od osnovnih postupaka matematike kojim se pomoću relacije ekvivalencije na skupu E konstruira particija $\mathcal{F}$ skupa E i sasvim određena funkcija iz E u $\mathcal{F}$. Preostali dio ovog potpoglavlja su ustvari ilustracije tog postupka u nekim konkretnim situacijama.

Polazimo od nepraznog skupa E i relacije ekvivalencije $\sim$ na E.

Prvi korak: Za $a \in E$ sa E_a označimo skup svih elemenata $y \in E$ koji su ekvivalentni s a, tj.

$$E_a = \{y \in E : y \sim a\} .$$

Time smo u E_a skupili sve elemente koji su ekvivalentni s a i dobili potpuno određen element $E_a \in \mathcal{P}(E)$. To učinimo za svako $a \in$ E.

Drugi korak: Neka je $\mathcal{F}$ skup svih tako dobivenih elemenata iz $\mathcal{P}$ (E), tj.

$$\mathcal{F} = \{E_x : x \in E\}.$$

Time smo okupili sve skupove E_x.
Sada tvrdimo da je $\mathcal{F}$ particija skupa E.

U prvom redu, relacija $\sim$ je *refleksivna* pa je $x \sim x$ za svako $x \in E$. No,

$$(x \sim x) \Rightarrow (x \in E_x);$$

dakle

$$E = \cup E_x \qquad (x \in E).$$

Ako su $x, y \in E_a$ onda je $x \sim a$ i $y \sim a$. Budući da je $\sim$ *simetrična* relacija, to $y \sim a$ povlači $a \sim y$. Sada $x \sim a$ i $a \sim y$ te tranzitivnost relacije $\sim$ povlače $x \sim y$. Prema tome, *svaka dva elementa iz E_a međusobno su ekvivalentna.*

Pretpostavimo da skupovi E_a i E_b nisu disjunktni, tj. da postoji bar jedan element $c \in E_a \cap E_b$. Odavde je $(c \sim a$ i $c \sim b) \Rightarrow (a \sim b)$. Ako je $x \in E_a$, onda je $x \sim a$, a kako je $a \sim b$, to je $x \sim b$. No, $x \sim b$ povlači $x \in E_b$. Budući da $x \in E_a \Rightarrow x \in E_b$, to je $E_a \subseteq E_b$. Iz istih razloga je $E_b \subseteq E_a$. Prema tome, $(E_a \cap E_b \neq \emptyset) \Rightarrow (E_a = E_b)$.
Time je dokazano da je $\mathcal{F}$ particija skupa E.

Elementi skupa $\mathcal{F}$ zovu se *razredi* ili *klase ekvivalencije* relacije $\sim$; $\mathcal{F}$ se zove **kvocijentni skup** skupa E po relaciji $\sim$ (odnosno modulo $\sim$) i označava s

$$\mathcal{F} = E/\sim .$$

Ako je $A \in E/\sim$, onda za svako $a \in A$ imamo $E_a = A$. Svaki element $a \in A$ zove se **reprezentant razreda** (klase) A.

Particija $\mathcal{F}$ skupa E proizvodi relaciju ekvivalencije ρ na E. Budući da $(x, y) \in \rho$ znači da su x i y iz istog elementa A skupa $\mathcal{F}$, to je $x \sim y$. Kako vrijedi i obrat, relacije ρ i $\sim$ su jednake.

Treći korak: Svakom elementu $x \in E$ pridružili smo (prvi korak) element $E_x \in \mathcal{P}(E)$ za koji znamo da je $E_x \in \mathcal{F}$ (drugi korak). Time je definirana funkcija

$$x \longmapsto E_x$$

s E u $E/\sim$. Ta funkcija je surjekcija i zove se **projekcija** *skupa* E na kvocijentni skup $E/\sim$. Neka je $\tau : E \to E/\sim$ ta projekcija. Projekcija τ elementu $x \in E$ pridružuje njegovu klasu ekvivalencije E_x. Kada x varira po skupu A, $A \in E/\sim$ onda $\tau(x)$ prima uvijek istu vrijednost A, a $\tau(x)$ se mijenja jedino kada varijabla x prelazi iz jedne u drugu klasu ekvivalencije. Prema tome imamo

$$(x \sim y) \Leftrightarrow (\tau(x) = \tau(y)).$$

Važnost projekcije τ sastoji se u tome da se izvjesne funkcije s E u proizvoljan skup F *mogu faktorizirati pomoću* τ *kroz* $E/\sim$.

Neka je $f: E \to F$ zadana funkcija i

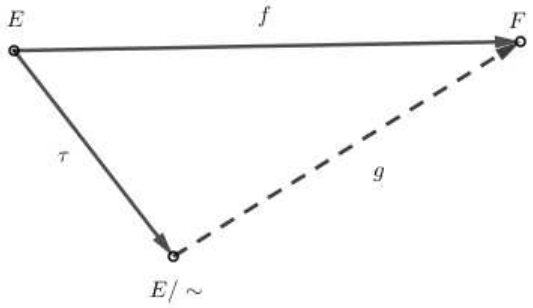
$$\rho = \{(x, x') \in E \times E : f(x) = f(x')\}.$$

S ρ je zadana relacija ekvivalencije na E. Skup ρ zove se **jezgro ekvivalencije funkcije** f jer je ρ relacija ekvivalencije na E.

Za funkciju f kažemo da je u harmoniji s relacijom $\sim$ ako i samo ako vrijedi

$$(x \sim y) \Rightarrow (f(x) = f(y)),$$

tj., ako i samo ako je $\sim$ poskup skupa ρ. Vrijednost funkcije f može se, dakle, promijeniti samo tako da varijabla x prolazi iz jedne u drugu klasu ekvivalencije (u odnosu na $\sim$). Sada ćemo pomoću funkcija f i τ definirati funkciju $g: E/\sim \to F$ takvu da dijagram komutira, tj. da bude $f = g \circ \tau$.



Slika 2.3: Kompozicija funkcija g i τ

S obzirom na važnost navedene faktorizacije funkcije f, slijede dva dokaza.

I. dokaz: Želimo svakom elementu A iz $E/\sim$ pridružiti element $g(A)$ iz F. U tu svrhu uzmemo nekog reprezentanta $a \in A$. Sada znamo da je $A = \tau(a)$ i znamo element $f(a)$.

Je li $A \mapsto f(a)$ tražena funkcija?
Najprije treba provjeriti je li to funkcija, tj. da je $f(a)$ potpuno određeno s A. Svakako s A a nije jednoznačno određeno jer A može imati mnogo predstavnika. Ako je a' drugi predstavnik od A, tj. $\tau(a') = A$, onda $\tau(a) = \tau(a')$ povlači $a \sim a'$. Budući da je f u harmoniji s $\sim$, to je $f(a) = f(a')$. Time je dokazano da rezultat navedenog postupka ne zavisi o reprezentantu skupa A. Prema tome, $A \mapsto f(a)$ je funkcija, tj. sa $g(A) = f(a)$ je definirana funkcija iz $E/\sim$ u F. Sada za $x \in E$ imamo

$$(g \circ \tau)(x) = g[\tau(x)] = f(x)$$

što povlači $f = g \circ \tau$.

II. dokaz: Promotrimo podskup

$$g = \{(\tau(a), f(a)) : a \in E\}$$

od $E/\sim \times F$. Tvrdimo da je g funkcijska relacija po drugoj varijabli. Treba dokazati da za $(x, y), (x', y') \in g$ $x = x'$ povlači $y = y'$. No, $x = \tau(a)$, $x' = \tau(a')$, $y = f(a)$ i $y' = f(a')$. Sada $x = x'$ povlači $a \sim a'$ iz čega je $f(a) = f(a')$; dakle $y = y'$. Time je dokazano da je g funkcija sa $E/\sim$ u F i da je $f(a) = g(\tau(a))$, $\forall\, a \in E$.

U nastavku gornje diskusije lako bi dokazali idući teorem.

Teorem 2.1.8. *Koristeći gornju notaciju imamo:*

I. Za relaciju ekvivalencije $\sim$ na skupu E postoji jedinstven podskup $E/\sim$ skupa $\mathcal{P}(E)$ (tzv. particija od E) i jedinstvena surjekcija $\tau : E \to E/\sim$ takvi da je:

$$(x \sim y) \Leftrightarrow (\tau(x) = \tau(y));$$

II. Za svaki skup F *i svaku funkciju $f : E \to F$ sa svojstvom da*

$$(x \sim y) \Rightarrow (f(x) = f(y))$$

postoji jedinstvena funkcija $g : E/\sim \to F$ takva da je

$$f = g \circ \tau.$$

Ako k tome $(f(x) = f(y)) \Rightarrow (x \sim y)$ (tj. $\sim$ je jezgro ekvivalentnosti funkcije f*), onda i samo onda je g injekcija.*
Ako je još i f surjekcija, onda je g bijekcija.

2.2 Cijeli brojevi

Cijeli brojevi se uvode zbog toga što je oduzimanje općenito neizvedivo u skupu $\mathbb{N}$.

Svaki cijeli broj je oblika m - n, gdje su m i n prirodni brojevi. Pri tome za cijele brojeve m - n i p - q imamo

$$\begin{cases} (m-n=p-q) \Leftrightarrow (m+q=p+n), \\ (m-n)+(p-q)=(m+p)-(n+q), \\ (m-n)(p-q)=(mp+nq)-(mq+np). \end{cases} \tag{2.1}$$

Odavde proizlazi da cijele brojeve treba dovoditi u vezu s uređenim parovima prirodnih brojeva, odnosno s podskupovima od $\mathbb{N}\times\mathbb{N}$. U ovom potpoglavlju, polazeći od skupa $\mathbb{N}$ i motivirani s (2.1), na $\mathbb{N}\times\mathbb{N}$ uvodimo relaciju ekvivalencije $\sim$ i u vezi s tim kvocijentni skup $\mathbb{Z}$ za koji ćemo dokazati da ima sva svojstva cijelih brojeva koje smo naučili u osnovnoj školi. Ta konstrukcija se oslanja na sljedeći teorem.

Teorem 2.2.1. *Za dva uređena para* $(m,n),(p,q)\in\mathbb{N}\times\mathbb{N}$ *definiramo*

$$(m,n)\sim(p,q) \tag{2.2}$$

ako i samo ako je

$$m+q=p+n.$$

Tada vrijedi:

I. $\sim$ *je relacija ekvivalencije na* $\mathbb{N}\times\mathbb{N}$.

II. Iz

$$(m,n)\sim(m',n') \quad \text{i} \quad (p,q)\sim(p',q') \tag{2.3}$$

slijedi

$$(m+p,n+q)\sim(m'+p',n'+q') \tag{2.4}$$

$$(mp+nq,mq+np)\sim(m'p'+n'q',m'q'+n'p'). \tag{2.5}$$

Dokaz. I. Budući da je zbrajanje na $\mathbb{N}$ komutativno, to je $m+n=n+m$; dakle $(m,n)\sim(m,n)$. Ako je $(m,n)\sim(p,q)$, tj. $m+q=p+n$, onda $p+n=q+m$ pokazuje da je $(p,q)\sim(m,n)$.

Neka je $(m,n)\sim(p,q)$ i $(p,q)\sim(r,s)$. Tada

$(m+q=p+n \text{ i } p+s=r+q)\Rightarrow(m+s)+(p+q)=(n+r)+(p+q)$.

Budući da je zbrajanje na $\mathbb{N}$ regularno, to je $m + s = r + n$, tj. $(m, n) \sim (r, s)$. Dakle, $\sim$ je relacija ekvivalencije.

II. Prema (2.3) je

$$m + n = n + m', \qquad p + q' = q + p'. \tag{2.6}$$

Koristeći (2.6) dobivamo

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

iz čega slijedi (2.4).
Tranzitivnost relacije $\sim$ i

$$(mp + nq, mq + np) \sim (m'p + n'q, m'q + n'p) \tag{2.7}$$
$$(m'p' + n'q', m'q' + n'p') \sim (m'p + n'q, m'q + n'p) \tag{2.8}$$

povlače (2.5). Dokažimo da (2.6) povlači (2.7). Iz

$$(mp + nq) + (m'q + n'p) = (m + n')p + (n + m')q = (m + n')(p + q),$$

$$(mq + np) + (m'p + n'q) = (m + n')q + (n + m')p = (m + n')(p + q)$$

slijedi (2.7), a iz

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

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

slijedi (2.8). □

Definicija 2.2.2. *Neka je $\sim$ relacija ekvivalencije na $\mathbb{N} \times \mathbb{N}$ opisana u Teoremu 2.2.1. Skup*

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$$

*zove se **skup cijelih brojeva**, a njegovi elementi **cijeli brojevi**. S τ označavamo projekciju sa $\mathbb{N} \times \mathbb{N}$ na $\mathbb{Z}$.*

2.3 Zbrajanje i množenje na $\mathbb{Z}$

Kako koristeći algebarsku strukturu (zbrajanje i množenje) na skupu $\mathbb{N}$ definirati algebarsku strukturu (zbrajanje i množenje) na skupu $\mathbb{Z}$? Postupamo heuristički. Do relacije ekvivalencije $\sim$ na $\mathbb{N} \times \mathbb{N}$ došli smo tako da smo u formuli (2.1) *m - n* zamijenili uređenim parom *(m, n)*. Sada ćemo to isto učiniti i u preostale dvije formule u (2.1). Dobivamo

$$(m, n) \oplus (p, q) = (m + p, n + q) \tag{2.9}$$

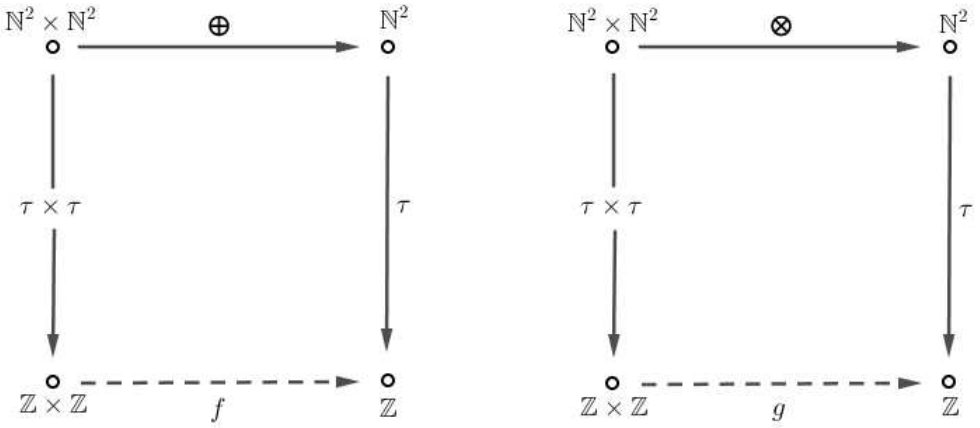
$$(m, n) \otimes (p, q) = (mp + nq, mq + np) \tag{2.10}$$

gdje $\oplus$ i $\otimes$ predstavljaju zbrajanje i množenje uređenih parova. Dakle, $\oplus$ i $\otimes$ su funkcije sa $\mathbb{N}^2 \times \mathbb{N}^2$ u $\mathbb{N}^2$. Prisjetimo se da je $\tau \times \tau$ također funkcija sa $\mathbb{N}^2 \times \mathbb{N}^2$ takva da je $(\tau \times \tau)(x, y) = (\tau(x), \tau(y)), \quad (x, y) \in \mathbb{N}^2 \times \mathbb{N}^2$.

Ako sada pogledamo dijagrame (pune linije), postavlja se pitanje kako te dijagrame upotpuniti funkcijama f, g tako da dobijemo komutativne dijagrame, tj. da bude

$$f \circ (\tau \times \tau) = \tau \circ \oplus, \qquad g \circ (\tau \times \tau) = \tau \circ \oplus. \tag{2.11}$$

Dakle, mi želimo funkcije $\oplus$ i $\otimes$ "spustiti" pomoću projekcije τ sa $\mathbb{N}^2$ na $\mathbb{Z}$. Ako je to moguće, onda je razumno funkciju f nazvati zbrajanje na $\mathbb{Z}$ i pisati $f(a, b) = a + b$, a funkciju g nazvati množenjem na na $\mathbb{Z}$ i pisati $g(a, b) = a \cdot b = ab$ za sve $a, b \in \mathbb{Z}$.



Slika 2.4: Zbrajanje i množenje na $\mathbb{Z}$

Očekujemo da f i g imaju bar ona svojstva zbrajanja i množenja koja te operacije imaju na $\mathbb{N}$. Uzmimo uređen par $z = ((m, n), (p, q))$ iz $\mathbb{N}^2 \times \mathbb{N}^2$ i na njega primijenimo (2.11).
Tada je

$$(\tau \circ \oplus)(z) = \tau[\oplus(z)] = \tau(m + p, n + q)$$

$$(f \circ \tau \times \tau)(z) = f[(\tau \times \tau)(z)] = f(\tau(m,n), \tau(p,q)),$$
$$(\tau \circ \oplus)(z) = \tau[\oplus(z)] = \tau(mp + nq, mq + np).$$

Prema tome, (2.11) prelazi u

$$f(\tau(m,n), \tau(p,q)) = \tau(m + p, n + q), \tag{2.12}$$

$$g(\tau(m,n), \tau(p,q)) = \tau(mp + nq, mq + np). \tag{2.13}$$

Sada napuštamo heuristička razmatranja i tvrdimo da su s (2.12) i (2.13) definirane funkcije sa $\mathbb{Z} \times \mathbb{Z}$ u $\mathbb{Z}$. Zaista, neka su $a, b \in \mathbb{Z}$. Tada postoje prirodni brojevi m, n, p, q takvi da je

$$a = \tau(m,n), \qquad b = \tau(p,q). \tag{2.14}$$

Pomoću zbrajanja i množenja na $\mathbb{N}$ formirajmo uređene parove

$$(m + p, n + q), \qquad (mp + nq, mq + np).$$

Neka je c razred ekvivalencije prvog, a d razred ekvivalencije drugog para. Dakle, tada je

$$c = \tau(m + p, n + q), \qquad d = \tau(mp + nq, mq + np). \tag{2.15}$$

Ako je $a = \tau(m', n')$ i $b = \tau(p', q')$, onda vrijedi formula (2.3). No, tada vrijede i formule (2.4) i (2.5), što pokazuje da je

$$c = \tau(m' + p', n' + q'), \qquad d = \tau(m'p' + n'q', m'q' + n'p').$$

Na taj način, oslanjajući se na Teorem 2.2.1, dokazano je da brojevi c, d definirani sa (2.15) ovise samo o brojevima a i b, a ne o njihovim reprezentantima. Drugim riječima, s

$$(a,b) \mapsto c, \qquad (a,b) \mapsto d$$

definirane su funkcije f, g sa $\mathbb{Z} \times \mathbb{Z}$ u $\mathbb{Z}$.

No, $c = f(a,b)$ i $d = g(a,b)$ nije ništa drugo nego (2.12) i (2.13) napisano pomoću reprezentanata. Pišemo $c = a + b$ i $d = a \cdot b$, tj.

$$\tau(m,n) + \tau(p,q) = \tau(m + p, n + q), \qquad (\forall m, n, p, q \in \mathbb{N}), \tag{2.16}$$

$$\tau(m,n) \cdot \tau(p,q) = \tau(mp + nq, mq + np), \qquad (\forall m, n, p, q \in \mathbb{N}). \tag{2.17}$$

Dokažimo da je τ ne samo "spustilo" zbrajanje i množenje na $\mathbb{Z}$, nego i njihova "dobra"

svojstva.

Za $a = \tau(m,n)$, $b = \tau(p,q)$, $c = \tau(r,s)$ imamo

$$\left.\begin{aligned} a+b &= \tau(m,n)+\tau(p,q) = \tau(m+p, n+q) \\ b+a &= \tau(p,q)+\tau(m,n) = \tau(p+m, q+n) \end{aligned}\right\} \Rightarrow$$

$a + b = b + a$, jer je zbrajanje na $\mathbb{N}$ komutativno;

$$\left.\begin{aligned} ab &= \tau(m,n)\cdot\tau(p,q) = \tau(mp+nq, mq+np) \\ ba &= \tau(p,q)\cdot\tau(m,n) = \tau(pm+qn, pn+qm) \end{aligned}\right\} \Rightarrow$$

$ab = ba$, jer je množenje na $\mathbb{N}$ komutativno;

$$\left.\begin{aligned} (a+b)+c &= \tau(m+p, n+q)+\tau(r,s) = \tau((m+p)+r, (n+q)+s) \\ a+(b+c) &= \tau(m,n)+\tau(p+r, q+s) = \tau(m+(p+r), n+(q+s)) \end{aligned}\right\} \Rightarrow$$

$(a + b) + c = a + (b + c)$, jer je zbrajanje na $\mathbb{N}$ asocijativno;

$$\begin{aligned} (ab)c &= \tau(mp+nq, mq+np)\cdot\tau(r,s) \\ &= \tau([mp+nq]r + [mq+np]s, [mp+nq]s + [mq+np]r) \\ &= \tau(mpr+nqr+mqs+nps, mps+nqs+mqr+npr), \end{aligned}$$

$$\begin{aligned} a(bc) &= \tau(m,n)\cdot\tau(pr+qs, ps+qr) \\ &= \tau(m[pr+qs]+n[ps+qr], m[ps+qr]+n[pr+qs]) \\ &= \tau(mpr+mqs+nps+nqr, mps+mqr+npr+nqs). \end{aligned}$$

Dakle,

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

je posljedica asocijativnosti množenja na $\mathbb{N}$ i distributivnosti množenja prema zbrajanju u $\mathbb{N}$.

Dokažimo distributivnost zbrajanja i množenja na $\mathbb{Z}$.

$$\begin{aligned} a(b+c) &= \tau(m,n)\cdot\tau(p+r, q+s) \\ &= \tau(m(p+r)+n(q+s), m(q+s)+n(p+r)) \\ &= \tau(mp+mr+nq+ns, mq+ms+np+nr) \\ &= \tau(mp+nq, mq+np)+\tau(mr+ns, ms+nr) \\ &= ab+ac. \end{aligned}$$

Stavimo $e = \tau(1,1)$ i $e' = \tau(2,1)$. Iz $(m,n) \sim (m+1, n+1)$ dobivamo

$$a + e = \tau(m,n)+\tau(1,1) = \tau(m+1, n+1) = \tau(m,n) = a,$$

$$a \cdot e' = \tau(m,n) \cdot \tau(2,1) = \tau(2m+n, 2n+m)$$
$$= \tau(m+n, m+n) + \tau(m,n) = e + a = a.$$

Prema tome je

$$a + e = e + a = a,$$
$$a \cdot e' = e' \cdot a = a$$

za svako $a \in \mathbb{Z}$.

Odatle slijedi da je $\mathbb{Z}$ aditivna polugrupa s neutralnim elementom e. Također, $\mathbb{Z}$ je multiplikativna polugrupa s neutralnim elementom e'.

Definicija 2.3.1. *Kažemo da je polugrupa $(S, \circ)$* ***monoid****, ako u S postoji bar jedan element e takav da je*

$$a \circ e = e \circ a = a$$

za svako $a \in S$.
Svaki takav element e zove se ***neutralni*** *ili* ***jedinični*** *element monoida S.*

Neutralni element u monoidu je jedinstven.

Zaista, uzmimo da su e_1 i e_2 neutralni elementi u monoidu S. Tada je $a \circ e_1 = a, e_2 \circ b = b$ za sve $a, b \in S$.
Uzmemo li $a = e_2$ i $b = e_1$, dobivamo

$$e_2 \circ e_1 = e_2, \quad e_2 \circ e_1 = e_1$$

od kuda je

$$e_1 = e_2.$$

Prema ovoj definiciji, slijedi da je $(\mathbb{Z}, +)$ aditivni monoid s neutralnim elementom $e = \tau(1,1)$ i da je $(\mathbb{Z}, \cdot)$ multiplikativni monoid s neutralnim elementom $e' = \tau(2,1)$.

Dakle, rezimiramo:

Teorem 2.3.2. *Neka je $\mathbb{Z}$ skup cijelih brojeva i τ projekcija sa $\mathbb{N} \times \mathbb{N}$ na $\mathbb{Z}$.*

Tada je s (2.16)*, odnosno s* (2.17)*, definirana funkcija sa $\mathbb{Z} \times \mathbb{Z}$ u $\mathbb{Z}$ koja se zove* ***zbrajanje****, odnosno* ***množenje*** *na $\mathbb{Z}$.*

$\mathbb{Z}$ je komutativni monoid u odnosu na zbrajanje. Neutralni element je $\tau(1,1)$.

$\mathbb{Z}$ je komutativni monoid u odnosu na množenje. Neutralni element je $\tau(2,1)$.

Množenje u $\mathbb{Z}$ je distributivno prema zbrajanju, tj. vrijedi $a(b+c) = ab + ac$ za sve $a, b, c \in Z$.

2.4 Pojam grupe

Iz prošlog potpoglavlja znamo da je $\mathbb{Z}$ aditivni monoid s neutralnim elementom $e = \tau(1,1)$. Taj element se označava s 0 i zove **nula** u $\mathbb{Z}$. Dakle, vrijedi

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

za svako $a \in \mathbb{Z}$ i 0 je jedini element iz $\mathbb{Z}$ s tim svojstvom.

Monoid $(\mathbb{Z}, +)$ ima još jedno novo svojstvo koje nije imala polugrupa $(\mathbb{N}, +)$. Vrijedi:

Za svaki element $a \in \mathbb{Z}$ postoji jedan i samo jedan element a' $\in \mathbb{Z}$ takav da je

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

Neka je $a = \tau(m,n)$. Tada za cijeli broj $a' = \tau(n,m)$ imamo

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

jer je $(m+n, m+n) \sim (1,1)$.

Dokažimo jedinstvenost broja a':

Neka za $b \in \mathbb{Z}$ vrijedi

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

Tada je

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

tj. $b = a'$, čime smo dokazali jedinstvenost broja $a' \in \mathbb{Z}$.

Element $a' \in \mathbb{Z}$ sa svojstvom $a + a' = 0$ zove se **suprotan** ili **simetričan element** od a i dalje ćemo ga označavati s $-a$ [minus a]. Dakle, po definiciji, $-a \in \mathbb{Z}$ je je element za koji vrijedi

$$a + (-a) = (-a) + a = 0.$$

Primijetimo da je $\tau(m,n) = -\tau(n,m)$.

Zbroj $b + (-a)$ piše se u obliku $b - a$ i zove **razlika** od b i a.

Skup $\mathbb{Z}$ u odnosu na zbrajanje ima ova svojstva:

1) Svakom uređenom paru $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ pridružen je jedinstveni element $a + b \in \mathbb{Z}$, tj. $\mathbb{Z}$ je *grupoid*.

2) Zbrajanje na $\mathbb{Z}$ je asocijativno:

$$(a + b) + c = a + (b + c) \qquad (\forall a, b, c, \in \mathbb{Z}),$$

tj. $\mathbb{Z}$ je *polugrupa*.

3) U $\mathbb{Z}$ postoji jedinstveni element 0 takav da je

$$a + 0 = 0 + a = a \qquad (\forall a \in \mathbb{Z}),$$

tj. $\mathbb{Z}$ je *monoid*.

4) Za svaki element $a \in \mathbb{Z}$ postoji jedinstveni element $-a \in \mathbb{Z}$ takav da je

$$a + (-a) = (-a) + a = 0.$$

5) Zbrajanje u $\mathbb{Z}$ je komutativno, tj. vrijedi

$$a + b = b + a \qquad (\forall a, b \in \mathbb{Z}).$$

Sada se prisjetimo Teorema 11 iz [1, str. 43] u kojem su dokazana neka svojstva kompozicije permutacija na nepraznom skupu E.
Neka je, dakle, $G(E)$ skup svih permutacija skupa E, tj. skup svih bijekcija s E na E. Tada $G = G(E)$ u odnosu na kompoziciju zadovoljava sljedeće uvjete:

1) Svakom uređenom paru $(a,b) \in G \times G$ pridružen je jedinstveni element $a \circ b \in G$, tj. G je *grupoid*.

2) Kompozicija u G je asocijativna.

$$(a \circ b) \circ c = a \circ (b \circ c) \qquad (\forall a, b, c \in G),$$

tj. G je *polugrupa*.

3) U G postoji jedinstveni element e (jedinična permutacija) takav da vrijedi

$$a \circ e = e \circ a = a \qquad (\forall a \in G),$$

tj. G je *monoid*.

4) Za svaki element $a \in G$ postoji jedinstveni element a^{-1} (inverzna permutacija) takav da je

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Napomenimo da može biti $a \circ b \neq b \circ a$ za $a, b \in G$.

Već iz ova dva primjera vidimo da je korisno promatrati neprazan skup G, čiji su elementi po svojoj prirodi proizvoljni, ali takav da je na G zadana algebarska operacija i da u odnosu na tu operaciju G zadovoljava uvjete 1, 2, 3 i 4. Na taj način dolazimo do strukture grupe, jedne od osnovnih struktura matematike.

Definicija 2.4.1. *Neprazan skup $G = \{a, b, \dots\}$ zove se **grupa** ako su ispunjeni ovi uvjeti:*

1) Zadana je funkcija koja se zove "množenje" i označava sa $\circ$, sa $G \times G$ u G, tj. svakom uređenom paru $(a, b) \in G \times G$ pridružen je jedinstveni element $a \circ b \in G$.

2) Množenje na G je asocijativno, tj.

$$(a \circ b) \circ c = a \circ (b \circ c) \qquad (\forall a, b, c \in G).$$

3) U G postoji barem jedan neutralni element *e takav da je*

$$a \circ e = e \circ a = a \qquad (\forall a \in G).$$

4) Za svaki element $a \in G$ postoji barem jedan element $b \in G$, tzv. inverzni element *od a, takav da je*

$$a \circ b = b \circ a = e.$$

Kraće: Grupa je monoid u kojem svaki element ima inverzni element.

Teorem 2.4.2.

I. Neutralni element u grupi je jedinstven.

II. Inverzni element je jedinstven za svaki element $a \in G$.

Dokaz.

I. Budući da je svaka grupa monoid, neutralni je element jedinstven.

II. Neka je $a \in G$ dani element i $b, c \in G$ dva za a inverzna elementa. Tada je

$$a \circ b = b \circ a = e,$$

$$a \circ c = c \circ a = e.$$

Sada je

$$c = c \circ e = c \circ (a \circ b) \text{ (radi asocijativnosti množenja u } G)$$

$$= (c \circ a) \circ b = e \circ b = b,$$

tj. $c = b$, pa je time dokazana jedinstvenost inverznog elementa.

□

Definicija 2.4.3. *Kažemo da je **grupa** G **komutativna** ili **Abelova,** ako vrijedi*

$$a \circ b = b \circ a \qquad (\forall a, b \in G).$$

Ako je grupna operacija $\circ$ u G pisana pomoću znaka množenja, onda se kaže da je G **multiplikativna grupa**. Neutralni element multiplikativne grupe zove se jedinični element ili jedinica, a inverzni element elementa $a \in G$ piše se u obliku a^{-1}.
Ako je grupa G komutativna i grupna operacija pisana pomoću simbola +, kaže se da je G **aditivna grupa**. Neutralni element aditivne grupe zove se **nula** i označava s 0. Inverzni element od $a \in G$ zove se **suprotni** ili **simetrični** element od a i označava s $-a$. Za aditivnu grupu G definira se funkcija $- : G \times G \to G$ koja uređenom paru $(a, b) \in G \times G$ pridružuje element $a - b = a + (-b)$. Ta funkcija se zove *odbijanje* ili *oduzimanje* na G.

Primijetimo razliku simbola "$-$" na lijevoj i desnoj strani u $a - b = a + (-b)$. Dok "$-$" na lijevoj strani označava algebarsku operaciju, na desnoj strani, u $(-b)$, "$-$" ulazi u sastav

broja. Dok -3 znači broj suprotan broju 3, dotle npr. $+3$ nema nikakvog smisla jer je $+$ funkcija sa $\mathbb{Z}\times\mathbb{Z}$ u $\mathbb{Z}$.

Prema ovoj terminologiji vidimo da skup $G(E)$ svih permutacija skupa E čini grupu s obzirom na kompoziciju permutacija kao grupnu operaciju. Ta grupa se zove **grupa permutacija skupa** E i ukoliko E ima barem tri elementa, $G(E)$ nije komutativna grupa. Nadalje, skup $\mathbb{Z}$ svih cijelih brojeva u odnosu na zbrajanje čini komutativnu grupu. To je **aditivna grupa cijelih brojeva**.

2.5 Uređajna relacija na $\mathbb{Z}$

Uređajnu relaciju na $\mathbb{Z}$ uvodimo na osnovu sljedećeg teorema:

Teorem 2.5.1. *Skup $\mathbb{Z}$ je unija od ova tri međusobno disjunktna skupa:*

$$\begin{aligned}\mathbb{Z}_+ &= \{\tau(n+1,1) : n\in\mathbb{N}\},\\ \mathbb{Z}_- &= \{\tau(1,n+1) : n\in\mathbb{N}\},\\ \mathbb{Z}_0 &= \{0\}.\end{aligned}$$

Dokaz. Neka je $a=\tau(p,q)$. Za prirodne brojeve p i q imamo samo jednu od ove tri mogućnosti:

$$p=q+n,\qquad p=q,\qquad q=p+n\qquad (n\in\mathbb{N}\text{, teorem 11 iz [1, str. 88].})$$

Ako je $p=q+n$, onda je $(p,q)\sim(n+1,1)$; dakle, $a=\tau(n+1,1)\in\mathbb{Z}_+$. Ako je $q=p+n$, onda je $(p,q)\sim(1,n+1)\Rightarrow a=\tau(1,n+1)\in\mathbb{Z}_-$. Ako je $p=q$, onda je $(p,q)\sim(1,1)\Rightarrow a=0\in\mathbb{Z}_0$. Prema tome je $\mathbb{Z}=\mathbb{Z}_+\cup\mathbb{Z}_0\cup\mathbb{Z}_-$. Za svako $n\in\mathbb{N}$ je $\tau(n+1,1)\neq 0, \tau(1,n+1)\neq 0$; dakle, $\mathbb{Z}_+\cap\mathbb{Z}_0=\varnothing, \mathbb{Z}_-\cap\mathbb{Z}_0=\varnothing$. Isto tako, nema prirodnih brojeva n i m takvih da je $(n+1,1)\sim(1,m+1)$. Dakle, $\mathbb{Z}_+\cap\mathbb{Z}_-=\varnothing$. □

Teorem 2.5.2. *Skup*

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

je uređajna relacija na $\mathbb{Z}$.

Dokaz. Iz $a,b\in\mathbb{Z}$ imamo $b-a\in\mathbb{Z}$. Sada imamo ove mogućnosti:

$$b-a\in\mathbb{Z},\qquad b-a\in\mathbb{Z}_0,\qquad b-a\in\mathbb{Z}_+.$$

Ako je $b-a\in\mathbb{Z}_-$, onda prema Teoremu 2.5.1 postoji $n\in\mathbb{N}$ takvo da je $b-a=\tau(1,n+1)$. Odavde je $a-b=\tau(n+1,1)$, tj. $a-b\in\mathbb{Z}_+$. Dakle, $(b,a)\in\rho$. Ako je $a=b$, onda je $b-a=0$, tj. $b-a\notin\mathbb{Z}_+$. Dakle, $(a,a)\notin\rho$. Ako je $b-a\in\mathbb{Z}_+$, onda je, prema definiciji,

$(a, b) \in \rho$.

Neka je sada $(a, b) \in \rho$ i $(b, c) \in \rho$. Tada je

$$b - a \in \mathbb{Z}_+ \Rightarrow b - a = \tau(n + 1, 1),$$

$$c - b \in \mathbb{Z}_+ \Rightarrow c - b = \tau(m + 1, 1).$$

Odavde je

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

dakle,

$$((a, b) \in \rho \text{ i } (b, c) \in \rho) \Rightarrow (a, c) \in \rho.$$

□

Prema tome je ss ρ definirana uređajna relacija na $\mathbb{Z}$. Tu relaciju označavamo sa $<$. Dakle, za $a, b \in \mathbb{Z}$ imamo samo jednu od ove tri mogućnosti: $a = b, a < b$ ili $a > b$. Nadalje, $a < b$ i $b < c$ povlači $a < c$.

Definicija 2.5.3. *Elementi skupa $\mathbb{Z}_+$ zovu se **strogo pozitivni cijeli brojevi**, a elementi skupa $\mathbb{Z}_-$ **strogo negativni cijeli brojevi**.*

Očigledno je $a \in \mathbb{Z}_+ \Leftrightarrow (a > 0), (b \in \mathbb{Z}_-) \Leftrightarrow (b < 0)$.

Teorem 2.5.4. *Za elemente skupa $\mathbb{Z}$ vrijede ove izreke:*

1) $(a > 0 \quad \& \quad b > 0) \Rightarrow (a + b > 0, \quad ab > 0)$*;*

2) $(a > 0 \quad \& \quad b < 0) \Rightarrow (ab < 0)$;

3) $(a < 0 \quad \& \quad b < 0) \Rightarrow (ab > 0)$;

4) $(a < b) \Rightarrow (a + c < b + c) \quad (\forall c \in \mathbb{Z})$;

5) $a \neq 0 \Rightarrow a^2 = a \cdot a > 0$;

6) $ab = 0 \Rightarrow (a = 0$ *ili* $b = 0$ *ili* $a = b = 0)$;

7) $(ab = ac \quad \& \quad a \neq 0) \Rightarrow (b = c)$.

2.6 Ulaganje prirodnih u cijele brojeve. Homomorfizam

Za svaki $a \in \mathbb{Z}_+$, postoji jedan i samo jedan prirodni broj n takav da je $a = \tau(n+1,1)$. Na taj način je zadan niz $j : \mathbb{N} \to \mathbb{Z}$, gdje je $j(n) = \tau(n+1,1)$. Lako se pokaže da niz j ima ova svojstva:

1) j injektivno preslikava $\mathbb{N}$ na $\mathbb{Z}_+$,

2) $j(m+n) = \tau(m+n+1,1) = \tau(m+1,1) + \tau(n+1,1) = j(m) + j(n)$, tj. j zbrajanje s $\mathbb{N}$ prenosi u zbrajanje u $\mathbb{Z}$ elemenata skupa $\mathbb{Z}_+$,

3) $j(m \cdot n) = \tau(m \cdot n + 1, 1) = \tau(m+1,1) \cdot \tau(n+1,1) = j(m) \cdot j(n)$, tj. j množenje s $\mathbb{N}$ prenosi u množenje u $\mathbb{Z}$ elemenata skupa $\mathbb{Z}_+$,

4) $(n < m) \Leftrightarrow (j(n) < j(m))$, tj. j prenosi uređaj s $\mathbb{N}$ u uređaj u $\mathbb{Z}$, elemenata skupa $\mathbb{Z}_+$.

Ovdje je *s':* $\mathbb{Z}_+ \to \mathbb{Z}_+$ definirano sa $s'[j(n)] = j(n+1)$ $(\forall n \in \mathbb{N})$. Može se pokazati da uređena trojka $(\mathbb{Z}_+, s', j(1))$ zadovoljava Peanove aksiome A1-A4. Prema tome, $\mathbb{Z}_+$ je skup prirodnih brojeva isto toliko koliko i $\mathbb{N}$.

Zahvaljujući svojstvima funkcije j, skupove $\mathbb{N}$ i $\mathbb{Z}_+$, tj. sliku od j, na neki način možemo poistovijetiti. Svaki teorem dokazan u $\mathbb{N}$ pomoću j prelazi u teorem u $\mathbb{Z}_+$ i obratno.
Ukratko: kažemo da smo s j $\mathbb{N}$ *uložili* u $\mathbb{Z}$. Skupove $\mathbb{N}$ i $\mathbb{Z}_+$ identificiramo tako da identificiramo $n \in \mathbb{N}$ i $j(n) = \tau(n+1,1)$ pa s n označavamo cijeli broj $\tau(n+1,1)$. Tada npr. umjesto $\tau(2,1)$ pišemo 1, umjesto $\tau(3,1)$ pišemo 2 itd. Također, umjesto $\tau(1,n+1) = -\tau(n+1,1)$ pišemo $-n$. Dakle, cijeli broj $-n$ je suprotni broj od n i vrijedi $(-n) + n = 0$. Iz $-1 = \tau(1,2) < 0$ dobivamo

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

Dakle, vrijedi

$$(-1)(-1) = 1.$$

Također, imamo

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

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

tj. vrijedi

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

Sada možemo reći da definirani skup $\mathbb{Z}$ ima sva svojstva skupa cijelih brojeva s kojima smo se upoznali još u osnovnoj školi.
Uočimo sada neka svojstva funkcije $j : \mathbb{N} \to \mathbb{Z}$. Umjesto da kažemo da je $j : \mathbb{N} \to \mathbb{Z}$ zbrajanje, množenje i uređaj prenijelo na zbrajanje, množenje i u uređaj u $\mathbb{Z}$, reć ćemo da funkcija *j poštuje* strukture na $\mathbb{N}$ i $\mathbb{Z}$. To je jedna od redovnih situacija koja prati aksiomatski i strukturalni pristup u matematici.

Radi boljeg shvaćanja, generalizirajmo. Neka su $(A, \circ)$ i $(A', \circ')$ dva grupoida. To znači da je $\circ$ funkcija s $A \times A$ u A. Isto tako, $\circ'$ je funkcija s $A' \times A'$ u A'.

Za funkciju $f : A \to A'$ kažemo da je **homomorfizam** grupoida $(A, \circ)$ u grupoid $(A', \circ')$ ako ona algebarsku operaciju $\circ$ s A prenosi u algebarsku operaciju $\circ'$ na A', tj. ako vrijedi

$$f(a \circ b) = f(a) \circ' f(b) \tag{2.18}$$

za sve $a, b \in A$.

Ako je $g : A' \to A''$ homomorfizam grupoida $(A', \circ')$ u grupoid $(A'', \circ'')$, onda je $h = g \circ f$ homomorfizam grupoida $(A, \circ)$ u grupoid $(A'', \circ'')$, tj. *kompozicija homomorfizama* je *homomorfizam*.

U ovom smislu je j homomorfizam grupoida $(\mathbb{N}, +)$ u grupoid $(\mathbb{Z}, +)$. Isto tako, j je homomorfizam grupoida $(\mathbb{N}, \cdot)$ u grupoid $(\mathbb{Z}, \cdot)$.

Ako na skupu A imamo više binarnih operacija, npr. $\circ, \boxdot$ te na A', imamo binarne operacije $\circ', \boxdot'$ onda je $f : A \to A'$ homomorfizam strukture $(A, \circ, \boxdot)$ u strukturu $(A', \circ', \boxdot')$, ako pored (2.18) još vrijedi i

$$f(a \boxdot b) = f(a) \boxdot' f(b) \qquad (\forall a, b \in A). \tag{2.19}$$

Ako A ima neutralni element e u odnosu na operaciju $\circ$, a A' neutralni element e' u odnosu na $\circ'$, zahtijeva se da bude $e' = f(e)$.

Prema tome, kod homomorfizma algebarske strukture $(A, \dots)$ u algebarsku strukturu $(A', \dots)$ zahtijeva se da f čuva odgovarajuće operacije i neutralne elemente.

Tako je $j : \mathbb{N} \to \mathbb{Z}$ bio aditivan i multiplikativan homomorfizam i uređajan homomorfizam.

*Homomorfizam $f : A \to A'$ zove e **izomorfizam** ako je f bijekcija.* Neka su npr. $(G, \circ)$ i $(G, \circ')$ grupe. Ako postoji bijekcija $f : G \to G'$ takva da je

$$f(a \circ b) = f(a) \circ' f(b) \qquad (\forall a, b \in G)$$

$$f(e) = e',$$

gdje su e i e' jedinice u G i G' onda se takva bijekcija zove **izomorfizam grupa**.

2.7 Pojam prstena

Definicija 2.7.1. *Skup P koji ima barem dva elementa zovemo **prsten** ako su na P definirane dvije algebarske operacije: zbrajanje "+" i množenje "·" i ako one imaju ova svojstva:*

1) $(P, +)$ *je aditivna grupa*

2) $(P, \cdot)$ *je multiplikativna polugrupa*

3) množenje je distributivno s obje strane u odnosu na zbrajanje, tj.

$$a(b + c) = ab + ac \text{ (distribucija slijeva)}$$
$$(a + b)c = ac + bc \text{ (distribucija zdesna).}$$

*Prsten P je **prsten s jedinicom** ako postoji barem jedan element $e \in P$ takav da je $ae = ea = a$ za svako $a \in P$.*

*Prsten P s jedinicom je **integralna domena** ako $a \neq 0$ i $b \neq 0$ povlači $ab \neq 0$ $(a, b \in P)$.*

Primjer prstena je skup $\mathbb{Z}$ sa zbrajanjem na $\mathbb{Z}$ kao grupnom operacijom, množenjem na $\mathbb{Z}$ kao množenjem u prstenu. Taj prsten ima jedinicu 1 i on je integralna domena.

Mi ćemo pretpostavljati da prsten ima jedinicu. **Homomorfizam** f **prstena** P u prsten P' je funkcija $f : P \to P'$ koja je homomorfizam u odnosu na zbrajanje, u odnosu na množenje i $f(e) = e'$, gdje su e i e' jedinice prtsena P i P'. Prema tome, vrijedi

$$f(x + y) = f(x) + f(y)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$f(e) = e'$$

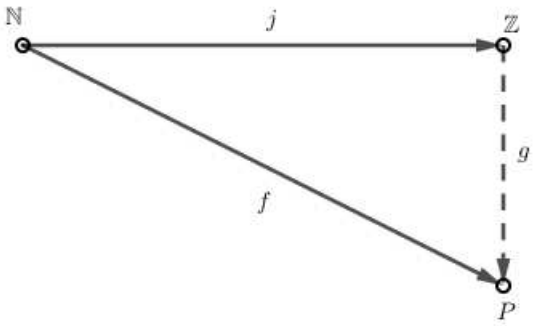
za sve $x, y \in P$.

Sada želimo dati karakterizaciju prstena $\mathbb{Z}$ kojeg smo dobili proširivanjem skupa $\mathbb{N}$ prirodnih brojeva.

Teorem 2.7.2.

I. Za svaki prsten P s jedinicom e postoji jedinstveni homomorfizam prstena $\mathbb{Z}$ u P.

II. Za svaki prsten P s jedinicom e i za svaki aditivni i multiplikativni homomorfizam $f : \mathbb{N} \to P$ za koji je $f(1) = e$, homomorfizam g koji je dan u I ima svojstvo da je $f = g \circ j$. Pri tome je $j : \mathbb{N} \to \mathbb{Z}$ ulaganje iz prethodnog potpoglavlja.



Slika 2.5: Homomorfizam

Dokaz.

I. Neka je $g : \mathbb{Z} \to P$ homomorfizam prstena sa svojstvom $g(1) = e$. Tada je $g(2) = g(1+1) = g(1)+g(1) = 2e$ i općenito $g(n) = ne (n \in \mathbb{N})$. Iz $g(0) = g(0+0) = g(0)+g(0)$ slijedi $g(0) = 0$. Odavde je $g(-n) + g(n) = g(-n + n) = 0$. Dakle,

$$g(-n) = -g(n) = -(ne) = (-n)e.$$

Prema tome, $g(m) = m \cdot e\, (\forall m \in \mathbb{Z})$. S druge strane, $m \mapsto m \cdot e$ je homomorfizam prstena $\mathbb{Z}$ u P.

II. Iz $f(1) = e$ i činjenice da je f homomorfizam zbrajanja na $\mathbb{N}$ slijedi $f(n) = n \cdot e$ za svako $n \in \mathbb{N}$.

No, $f(n) = n \cdot e = g[\tau(n+1, 1)] = g[j(n)]$. Dakle, vrijedi

$$f = g \circ j.$$

□

S II je opisano *univerzalno svojstvo prstena* $\mathbb{Z}$. Time je taj prsten karakteriziran do izomorfizma.

2.8 Djeljivost u $\mathbb{Z}$

Osnovni rezultat ovog potpoglavlja je sljedeći teorem.

Teorem 2.8.1. *Ako je* (a, b) *uređeni par cijelih brojeva i* $b > 0$*, onda postoji jedinstveni uređeni par* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ *takav da je*

$$a = bq + r \qquad (0 \leq r < b). \tag{2.20}$$

r se zove ***ostatak pri dijeljenju*** *broja a na b, a q* ***kvocijent*** *pri tom dijeljenju.*

Ako je $r = 0$ *kaže se da je a djeljivo s b, odnosno da je b* ***djelitelj*** *(ili* ***mjera, divizor****) od a.*

Dokaz. Ako je $a > 0$ i $b > a$, onda je (2.20) zadovoljeno s $r = a, q = 0$. Ako je $b \leq a$, onda skup $\mathbb{N}' = \{n \in \mathbb{N} : nb \geq a\}$ nije prazan. Neka je $m = \min \mathbb{N}'$. Ako je $mb = a$, onda je (2.20) zadovoljeno s $r = 0, q = m$. Ako je $mb > a$, onda je (2.20) zadovoljeno s $q = m - 1, r = a - qb$. Prema tome, (2.20) vrijedi za $a > 0$.

Ako je $a < 0$, onda prema već dokazanom imamo

$$-a = q'b + r' \qquad (0 \leq r' < b).$$

Odavde je $a = (-1-q')\,b + (b-r'), 0 < b-r' \leq b$ pa je (2.20) zadovoljeno s $q = -1-q', r = b - r' < b$ ili s $q = -q', r = r' = 0$.
Dokažimo jedinstvenost.
Uzmimo da je

$$a = bq + r = bq_1 + r_1 \qquad (0 \leq r, r_1 < b).$$

Ako je $r_1 < r$, onda $0 < b(q_1 - q) < b$ povlači $0 < q_1 - q < 1$ što je nemoguće jer u $\mathbb{Z}$ iza nule dolazi 1. Isto tako, i $r < r_1$ vodi na kontradikciju. Prema tome, $r = r_1$, odnosno $b(q - q_1) = 0$. Odavde slijedi $q = q_1$. □

Ako su $a, b \in \mathbb{N}$, onda skup S svih prirodnih brojeva s kojima su djeljivi i a i b nije prazan ($1 \in S$). Budući da je S konačan skup, on ima maksimalan element. Označimo ga s $M(a, b)$. Broj $M(a, b)$ se zove **najveća zajednička mjera** brojeva a, b. Jasno je da vrijedi $M(a, b) = M(b, a)$.

Vrijednost funkcije $M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ na uređenom paru (a, b), tj. broj $M(a, b)$ dobiva se iz brojeva a i b tzv. *Euklidovim algoritmom*

$$\begin{aligned} a &= b\,q_1 + r_1 & 0 < r_1 < b \\ b &= r_1\,q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 &= r_2\,q_3 + r_3 & 0 < r_3 < r_2 \\ &\vdots & \vdots \\ r_{n-1} &= r_n\,q_{n+1} + r_{n+1} & r_{n+1} = 0 \end{aligned}$$

Prema tome, ako je $a > b$, a dijelimo na b i dobivamo broj r_1. Ako je $r_1 \neq 0$ b dijelimo na r_1 i dobivamo r_2 itd. Budući da je $b > r_1 > r_2 > \ldots$ proces završava nakon konačno koraka, tj. postoji $n \in \mathbb{N}_0$ takvo da je $r_{n+1} = 0, r_n \neq 0$. No, tada je $r_{n-1} = r_n\,q_{n+1}$. Iz $M(a, b) = M(b, r_1) = \cdots = M(r_{n-1}, r_n) = r_n$ slijedi da je r_n najveća zajednička mjera brojeva a i b.

Recimo da je $r_2 \neq 0, r_3 = 0$. Tada imamo

$$r_2 = b - r_1\,q_2 = b - q_2\,(a - b\,q_1) = (-q_2)\,a + (1 + q_1\,q_2)\,b,$$

tj.

$$M(a, b) = ac + bd \tag{2.21}$$

gdje su c i d cijeli brojevi. Na sličan način, ako je $r_{n+1} = 0$, dobiva se (2.21) s tim da se r_n izrazi pomoću r_{n-1}, r_{n-1} pomoću r_{n-2} itd.

Ako je $M(a, b) = 1$, kažemo da su a i b **relativno prosti brojevi**.

Prosti brojevi

Definicija 2.8.2. *Kažemo da je prirodan broj p **prost** ili **prim-broj** ako vrijedi:*

(i) $p > 1$

(ii) $(\forall n \in \mathbb{N})\,(n \mid p \Rightarrow n \in \{1, p\})$

Prirodan broj p koji nije prost, a strogo je veći od 1, naziva se ***složen***.

Primjeri prvih nekoliko prostih brojeva su: $2, 3, 5, 7, 11, 13, 17, 19, 23 \ldots$

Svaki prirodni broj $a > 1$ je produkt prostih brojeva. Zaista, neka je p_1 najveći prost broj na koji je a djeljivo. Tada je $a = p_1\, a_1$. Ako je $a_1 > 1$, onda s p_2 označavamo najveći prost broj na koji je a_1 djeljivo, $a_1 = p_2\, a_2$ itd. Budući da je $a > a_1 > \ldots$ to dolazimo do prostog broja $a_{n-1} = p_n$. Recimo da je $a_2 = p3$. Tada je $a = p_1\, a_1 = p_1\, (p_2\, a_2) = p_1\, p_2\, p_3$.

U općem slučaju je analogno

$$a = p_1\, p_2 \cdots p_n. \tag{2.22}$$

Stavimo, $q_1 = p_1$ i neka k_1 pokazuje koliko puta p_1 u (2.22) dolazi kao faktor. Ako je $k_1 = n$, onda je $a = q_1^n$. Ako je $k_1 < n$, onda stavljamo $q_2 = p_{1+k_1}$ i s k_2 označavamo koliko puta se q_2 kao faktor pojavljuje u (2.22). Na taj način dolazimo do

$$a = q_1^{k_1}\, q_2^{k_2} \cdots q_m^{k_m} \qquad (q_1 > q_2 > \cdots > q_m;\, k_1, \ldots, k_m \in \mathbb{N}). \tag{2.23}$$

Prikaz broja a u obliku (2.23) je jedinstven.

Odavde slijedi teorem:

Teorem 2.8.3. *Svaki prirodni broj $a > 1$ je produkt prostih brojeva. Ako je*

$$p_1\, p_2 \cdots p_n = q_1\, q_2 \cdots q_m$$

gdje su p_i, q_j prosti brojevi, onda je $n = m$ i postoji permutacija s skupa $\{1, \ldots, n\}$ takva da je $q_i = p_{s(i)}, i \in \{1, \ldots, n\}$.

Sljedeći teorem, kojeg nazivamo Osnovnim teoremom artimetike, je reformulacija Teorema 2.8.3 i njega navodimo bez dokaza.

Teorem 2.8.4. *(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*

$$n = q_1^{\alpha_1}\, q_2^{\alpha_2} \cdots q_l^{\alpha l}.$$

Ako su $p_1, \ldots, p_n$ prosti brojevi, onda je $a = 1 + p_1 \cdots p_n$ prost broj ili u faktorizaciji $a = q_1 \cdots q_m$ (teorem 2.8.3) na proste brojeve nijednog od brojeva $p_1, \ldots, p_n$ ne ulazi kao faktor. Dakle, postoji prost broj koji nije u skupu $\{p_1, \ldots, p_n\}$. Odavde slijedi da je **skup prostih brojeva beskonačan**.

Bibliografija

[1] S. Kurepa, *Uvod u matematiku*, Tehnička knjiga Zagreb, Zagreb, 1984.

[2] D. Ilišević, G. Muić, *Uvod u matematiku*, skripta Prirodoslovno-matematičkog fakulteta, Zagreb, 2022.

Sažetak

U ovom radu se najprije prisjećamo pojma relacije te aksioma na temelju kojih je izgrađen skup prirodnih brojeva. Potom proučavamo jednu specifičnu relaciju, relaciju ekvivalencije i njezina svojstva te način na koji konstruiramo i izgrađujemo skup cijelih brojeva $\mathbb{Z}$. Također, proučavamo algebarsku strukturu i svojstva osnovnih računskih operacija na skupu cijelih brojeva.

Summary

In this thesis, firstly, we introduce the notion of relation and the Peano axioms on which the set of natural numbers was built. Then, we study one specific relation, which is the relation of equivalence, used in our construction of the set of integers $\mathbb{Z}$. Also, we study the algebraic structure and properties of elementary arithmetic operations on a set of integers.

Životopis

Rođena sam 6. veljače 1998. godine u Novoj Gradiški. Odrasla sam i živim u Orubici, nedaleko od Nove Gradiške. Prva četiri razreda osnovne škole pohađala sam u Orubici, u Područnoj školi "Fra Marijan Lanosović". Svoje daljnje školovanje nastavljam u Osnovnoj školi "Matija Antun Relković" u Davoru. Nakon završene osnovne škole s odličnim uspjehom upisujem Gimnaziju Nova Gradiška. Godine 2016. s odličnim uspjehom završavam četvrti razred gimnazije te uspješno polažem državnu maturu. Iste godine upisujem preddiplomski sveučilišni studij Matematika, smjer nastavnički, na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Nakon završenog preddiplomskog studija upisujem diplomski sveučilišni studij Matematika, smjer nastavnički na istom odsjeku. Tijekom školovanja bila sam članica Kulturno umjetničke udruge "Marijan Lanosović" iz Orubice. Danas sam aktivna članica zbora mladih Župe sv. Ilije proroka u Orubici.