**MILGOR - serija univerzitetski udžbenici**

**Ž. Mijajlović**

# ALGEBRA

# 1

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

MILGOR - serija univerzitetski udžbenici

Ž. Mijajlović

# ALGEBRA

# 1

Suplement: rešenja zadataka,
napisali Ž. Mijajlović i I. Farah

Beograd, Москва
1993

**ALGEBRA, 1 deo** UDC 512.5, 511.11, 510.65
Serija: univerzitetski udžbenici

Recenzenti:
prof. dr. Branka Alimpić, *PMF, Beograd*
doc. dr. Aleksandar Lipkovski, *PMF, Beograd*

ISBN

Izdaje: MILGOR
Mate Jerkovića 1/c, 11001 Beograd
Za izdavača: Goran Kilibarda

Redakcija:
акад. проф. Валерий Борисович Кудрявцев, predsednik Redakcije, *МГУ, Москва*
проф. Алкесандр Егорович Андреев, *МГУ, Москва*
prof. Boško Jovanović, *PMF, Beograd*
doc. Goran Kilibrada, *TMF, Beograd*
проф. Вадим Александрович Малышев, *МГУ, Москва*
prof. Žarko Mijajlović *PMF, Beograd*
prof. Šćepan M. Ušćumlić, *TMF, Beograd*

U TEX-u tekst knjige složio: Žarko Mijajlović.
U TeX-u tekst suplementa (rešenja zadataka) složio: Ilijas Farah.

Štampanje završeno aprila 1993.
Štampa:
Московский научный центр культуры и информационных технологии

---

**Agebra, 1 deo.** Knjiga predstavlja prvi deo udžbenika iz algebre sa ciljem da se prikažu osnovne oblasti i relevantne teorije savremene algebre. U ovoj prvoj knjizi izlažu se glavni algebarski pojmovi. Stavlja se poseban naglasak na zasnivanje algebarskih pojmova, tako da izlaganje o algebarskim strukturama počinje od univerzalnih algebarskih struktura sa njihovim generalnim svojstvima, a zatim dalje izlaganje teče razmatranjem konkretnih algebarskih struktura. Strogo i konzistentno se uvode osnove algebre, bazirane na pojmu algebarskog jezika, terma i interpretacije. Izlažu se elementi teorije algebri sa relacijama u okvirima predikatskog računa prvog reda. Poseban naglasak stavljen je na zasnivanje brojevnih struktura, od prirodnih brojeva pa do polja kompleksnih brojeva, imajući u vidu da su brojevi glavni izvor nastanka specijalnih algebarskih teorija. Istovremeno se detaljno izlaže induktivni metod i daju osnove konačne kombinatorike, važnih polazišta u izučavanju konačnih algebarskih struktura. Ovaj deo može biti od koristi studentima i u drugim kursevima, na primer u zasnivanju matematičke analize, zatim u računarstvu i diskretnoj matematici. U knjizi ima veći broj primera i (rešenih) zadataka koji treba da pomognu studentu da lakše usvoji izloženo gradivo, ali i da se znatiželjnom čitaocu daju dopune van glavnog toka izlaganja.

1. izdanje
Tiraž 600 primeraka

# SADRŽAJ

# Uvod

Jedan od najstarijih delova matematike je algebra. Prvi opisi računskih operacija sa razlomcima, kao i opisi rešavanja nekih jednostavnih algebarskih jednačina pojavljuju se već 2000 godina pre nove ere. Na primer, u Egiptu u vreme Srednjeg carstva u *Londonskom papirusu* (poznatom i kao *Ahmesova računica*), ili na Vavilonskim pločicama u približno isto vreme. U 19. veku, postavljanjem temelja klasičnih algebarskih disciplina: teorije grupa, teorije polja i teorije prstena, kao i nastankom teorije skupova, stvorene su osnove i preduslovi za razvoj savremene algebre. Možemo reći da savremena algebra, kao aksiomatski zasnovana nauka doživljava potpuni razvoj u ovom veku. Tada se utvrđuje shvatanje da su osnovni objekti izučavanja u algebri algebarske operacije nad elementima proizvoljne prirode. Precizira se jezik, kao na primer značenje reči "proizvoljne prirode" stavljanjem algebre u okvir kantorovske teorije skupova. Razvijaju se veze i ostvaruje uticaj algebre na druge matematičke discipline, na primer na geometriju, analizu i topologiju. Pojavom digitalnih računara dolazi do izražaja i računski aspekt algebre, kako na numeričkom tako i na simboličkom planu. Zato algebra danas drugačije izgleda nego početkom veka, pa i u odnosu na sredinu ovog veka.

Pored već pomenutih klasičnih algebarskih disciplina nastaju nove oblasti. Spomenimo neke od njih: teorija mreža i Bulovih algebri sa primenama od analize i konstrukcije elemenata digitalnih računara pa do raspravljanja najdubljih pitanja iz zasnivanja matematike. Metode homološke algebre dale su mnoge rezultate u topologiji i algebarskoj geometriji, dok se zahvaljujući teoriji diferencijalnih prstena i polja raspravljaju pitanja iz teorije diferencijalnih jednačina. Generalizacijom teorije grupa nastaje teorija semigrupa i teorija kvazigrupa sa primenama, na primer, u kombinatorici i konačnim geometrijama. Teorija kategorija ili "račun strelica" daje nov, u osnovi algebarski formalizam za izučavanje mnogih matematičkih disciplina, od algebre i topologije, pa sve do matematičke logike i računarstva. Najzad, nastaju teorija univerzalnih algebri i opštija teorija modela (algebre sa relacijama), blisko povezane sa matematičkom logikom. S druge strane, u klasičnim oblastima algebre pojavljuju se duboki rezultati. Na primer u teoriji grupa uvrđuje se potpuna klasifikacija konačnih grupa, dok u kristalografiji i teorijskoj fizici ova teorija nailazi na fundamentalne primene.

Ova knjiga predstavlja prvi deo udžbenika iz algebre sa ciljem da se prikažu osnovne oblasti i relevantne teorije savremene algebre. U ovoj prvoj knjizi izlažu se osnovni algebarski pojmovi. Stavlja se poseban naglasak na zasnivanje algebarskih pojmova, tako da izlaganje o algebarskim strukturama počinje od univerzalnih algebarskih struktura sa njihovim generalnim svojstvima, a zatim dalje izlaganje teče razmatranjem konkretnih algebarskih struktura. Strogo i konzistentno se uvode osnove algebre, bazirane na pojmu algebarskog jezika, terma i interpretacije. Izlažu se elementi teorije algebri sa relacijama u okvirima predikatskog računa prvog reda. Poseban naglasak stavljen je na zasnivanje brojevnih struktura, od prirodnih brojeva pa do polja kompleksnih brojeva, imajući u vidu da su brojevi glavni izvor nastanka specijalnih algebarskih teorija. Istovremeno se detaljno izlaže induktivni metod i daju osnove konačne kombinatorike, važnih aspekata u izučavanju konačnih algebarskih struktura. Verujem da ovaj deo može biti od koristi studentima i u drugim kursevima, na primer u zasnivanju matematičke analize, zatim u računarstvu i diskretnoj matematici. U knjizi ima veći broj primera i (rešenih) zadataka koji treba da pomognu studentu da lakše usvoji izloženo gradivo, ali i da se znatiželjnom čitaocu daju dopune van glavnog toka izlaganja.

Prvi deo udžbenika namenjen je studentima druge godine za predmet algebra, prvi semester. Dakle, pretpostavlja se da je čitalac već upoznat sa elementima linearne algebre, da je imao prvi kurs analize, pa i da zna neke od elementarnih pojmova iz algebre, na primer da poznaje pojam grupe, prstena i polja. Istina, svi ti pojmovi ovde se ponovo razmatraju, ali, kao što je već rečeno, sa apstraktnijeg nivoa, odnosno sa stanovišta univerzalnih algebarskih struktura. Na ovaj način omogućava se da se kompaktno prikažu pojedine oblasti algebre i izbegne u osnovi nepotrebno ponavljanje definicija ključnih pojmova kod konkretnih algebarskih struktura. I što je važnije, student može da stekne uvid u suštinske algebarske pojmove i konstrukcije, zajedničke svim algebarskim strukturama (kao, na primer, pojmovi i konstrukcije: term, algebarski zakon, algebarski varijetet, homomorfizam, proizvod algebri, kongruencija i količnička algebra). Evo nekoliko reči o drugoj knjizi udžbenika. Ta knjiga odnosi se na klasične algebarske teorije: teoriju grupa, teoriju prstena i modula, i teoriju polja.

Knjiga je nastala iz nekoliko kurseva algebri koje sam predavao od 1978. godine na matematičkim grupama prirodnomatematičkih fakulteta u Beogradu, Nišu i Kragujevcu. Neke delove rukopisa počeo sam da pišem 1987. godine, a sadašnju formu knjiga je dobila 1992. godine. Izbor zadataka, osim što služi osnovnom cilju, da student uvežba gradivo iz knjige, delom reflektuje ukus pisca ove knjige. Teži zadaci, kao i oni u kojima se pretpostavlja detaljnije znanje iz drugih oblasti, označeni su zvezdicom. Rešenja zadataka napisao sam zajedno sa kolegom Ilijas Farahom.

Pošto je ova knjiga prevashodno udžbenik, nije uvek navedena referenca na literaturu za svaku pomenutu teoremu. Citirana dela uglavnom predstavljaju dopunsku literaturu, ili knjige koje se predlažu studentu za dalje čitanje. Pretpostavlja se da je čitalac upoznat sa osnovama elementarne teorije skupova. Pored znanja o skupovnim operacijama, podrazumeva se poznavanje definicije kardinalnog broja, uređenog skupa, Aksime izbora i njene varijante, Kuratowski-Zornove leme. Osim izuzetaka, u ovoj knjizi biće malo reči iz teorije skupova, ali se student može detaljnije upoznati sa ovom teorijom iz literature na srpskom jeziku, na primer, iz knjige A. Krona, *Elementarna teorija skupova.*

Što se tiče notacije u ovoj knjizi, $f : A \to B$ označava činjenicu da je $f$ preslikavanje iz skupa $A$ u skup $B$. Isto značenje imaju oznake $f = \langle f(x) \,|\, x \in A \rangle$, i $f : x \mapsto f(x)$, $x \in A$. U ovom slučaju $f(x)$ može biti zamenjeno nekim konkretnim izrazom. Restrikcija funkcije $f$ na skup $X$ označena je simbolom $f \restriction X$, ili $f|X$, dok je $f(X) = \{f(x) \,|\, x \in X\}$. Kardinalni broj skupa $X$ označen je sa $|X|$, dok za partitivni skup (skup svih podskupova) skupa $X$ koristimo simbol $P(X)$ ili $\mathbf{P}(X)$.

Metateorija na kojoj je zasnovano izlaganje u ovoj knjizi je ZFC teorija skupova (Zermelo-Fraenkel teorija skupova sa Aksiomom izbora), ali nećemo u svim prilikama eksplicitno pominjati koršćenje, na primer, Askiome izbora ili njenih ekvivalenata. Ipak, svi izuzeci ili dodatne hipoteze biće naznačene, kao Kontinuum hipoteza ili slabije forme Aksiome izbora (Stav kompaktnosti, na primer).

Želim da izrazim zahvalnost svojim kolegama koji su pročitali rukopis knjige i dali korisne primedbe i sugestije: prof. Branki Alimpić, dr Aleksandru Lipkovskom, Dragani Todorić, Ilijas Farahu i prof. Aleksandru Kronu.

Najzad, nekoliko reči o skraćenicama. Reč *akko* je skraćenica za frazu "ako i samo ako". Kraj dokaza označavaćemo pomoću simbola $\diamondsuit$.

U Beogradu, Žarko Mijajlović
Februara 1993

# 1. Algebre

Pojam algebre ili algebarske strukture svakako se nalazi među najvažnijim pojmovima predmeta algebra. S druge strane, u definiciji algebarske strukture učestvuje pojam algebarske operacije i stoga ćemo ovaj pojam detaljnije razmotriti.

## 1.1 Algebarske operacije i strukture

Neka je $A$ neprazan skup. Pod algebarskom operacijom dužine $n$ skupa $A$, n je pozitivan ceo broj, podrazumevamo svako preslikavanje $f : A^n \to A$. Za takvo preslikavanje $f$ kažemo da je dužine $n$, odnosno da je $f$ $n$–arna ili $n$-mesna operacija. Ako je $n = 1$ onda kažemo da je $f$ unarna operacija, a ukoliko je $n = 2$ onda $f$ nazivamo binarnom operacijom. Za $n = 3$ koristi se i termin ternarna operacija.

**1.1.1 Primer** Aritmetičke operacije sabiranja i množenja prirodnih brojeva su primeri binarnih operacija skupa prirodnih brojeva.

**1.1.2 Primer** Neka je $A^B$ skup svih preslikavanja skupa $B$ u skup $A$, tj. $A^B = \{f|\ f : B \to A\}$. Tada je $A^A$ skup svih preslikavanja skupa $A$ u $A$. Slaganje (kompozicija) funkcija $\circ$ određuje jednu binarnu operaciju skupa $A^A$.

**1.1.3 Primer** Preslikavanje $f : (x, y, z) \mapsto x^2 + y^2 - z^2$, $x, y, z \in Z$, jeste jedna ternarna operacija skupa celih brojeva.

**1.1.4 Primer** Preslikavanje $f : x \mapsto 1/x$, $x \in Q^+$, je primer unarne operacije skupa pozitivnih racionalnih brojeva.

U slučaju binarnih operacija vrlo često se koristi posebna notacija. Naime, ako je $f : A^2 \to A$ binarna operacija, onda se umesto $f(x, y)$ takođe piše $(xfy)$. Za označavanje binarnih operacija između ostalog se koriste simboli: $*$, $\circ$, $+$, $-$, $/$.

**1.1.5 Tvrđenje** *Ako je $A$ konačan skup od $m$ elemenata, onda na skupu $A$ postoji tačno $m^{m^n}$ operacija dužine $n$.*

**Dokaz** Skup svih operacija dužine $n$ skupa A je skup $A^{A^n}$, odakle
$$|A^{A^n}| = |A|^{|A|^n} = m^{m^n}. \qquad \diamondsuit$$

**1.1.6 Definicija** *Algebarska struktura ili algebra je svaka n-torka*

$$\mathbf{A} = (A, f_1, f_2, ..., f_k, a_1, a_2, ..., a_m)$$

*gde je $A$ je neprazan skup, $m$ i $k$ su prirodni brojevi i $n = m + k + 1$, $f_1, ..., f_k$ su operacije skupa $A$ i $a_1, ..., a_m \in A$.*

Pri ovakvoj definiciji algebre skup $A$ se naziva *domenom*, dok se elementi $a_1, a_2, \ldots, a_m$ nazivaju *konstantama* algebre **A**. Inače, nije obavezno da se u svakom primeru algebre pojavljuju konstante, pa ni operacije; drugim rečima nizovi $f_1, f_2, \ldots, f_k$ i $a_1, a_2, \ldots, a_m$ mogu biti prazni.

**1.1.7 Primer** Uz uobičajena značenja brojevnih operacija $+$ i $\cdot$ imamo ove primere algebri:

$\mathbf{N} = (N, +, \cdot, 0, 1)$, $N = \{0, 1, 2, ...\}$ je skup prirodnih brojeva.
$\mathbf{Z} = (Z, +, \cdot, 0, 1)$, $Z = \{..., -2, -1, 0, 1, 2, ...\}$ je skup celih brojeva.
$\mathbf{Q} = (Q, +, \cdot, 0, 1)$, $Q$ je skup racionalnih brojeva.
$\mathbf{R} = (R, +, \cdot, 0, 1)$, $R$ je skup realnih brojeva.
$\mathbf{C} = (C, +, \cdot, 0, 1)$, $C$ je skup kompleksnih brojeva.

**1.1.8 Primer** $(A^A, \circ, i_A)$ je algebra funkcija, gde je $\circ$ slaganje funkcija, a $i_A$ identično preslikavanje skupa $A$, tj. $i_A : x \mapsto x,\ x \in A$. Dakle, ovde je $(f \circ g)(x) = f(g(x))$. Primetimo da je za $A = \emptyset$, $A^A = \{\emptyset\}$.

**1.1.9 Primer** Neka je $P(X)$ skup svih podskupova skupa X, i neka su $\cup, \cap, {}^c$ uobičajene skupovne operacije unije, preseka i komplementiranja u odnosu na skup $X$. Tada je $\mathbf{P}(X) = (P(X), \cup, \cap, {}^c, \emptyset, X)$ algebra.

**1.1.10 Primer** Neka je niz skupova $V_n$ definisan na sledeći način:

$$V_0 = \emptyset, \quad V_{n+1} = P(V_n), \quad n \in N.$$

Dalje, neka je $V = \cup_n V_n$. Tada važi:

1. $V_0 \subseteq V_1 \subseteq V_2 \subseteq ... \subseteq V$.
2. $x, y \in V \Rightarrow \{x, y\} \in V$, tj. operacija formiranja dvočlanog skupa je jedna binarna operacija skupa V.
3. Ako za definiciju uređenog para elemenata uzmemo skup $\{\{x\}, \{x, y\}\}$, dakle $(x, y) = \{\{x\}, \{x, y\}\}$, onda takođe važi $x, y \in V \Rightarrow (x, y) \in V$, tj. formiranje uređenog para je jedna operacija domena $V$. Primetimo da je onda $V \times V \subseteq V$.

**1.1.11 Primer** Neka je $n$ pozitivan prirodan broj, $x \in Z$ i $Z_n = \{0, 1, \ldots, n-1\}$. Dalje, neka je $r$ ostatak dobijen deljenjem broja $x$ sa $n$, tj. za neki $q \in Z$ važi $x = qn + r$ i $0 \leq r < n$. Primetimo da je $r$ *jedinstven* ceo broj, v. Lemu 3.4.1, sa osobinom

$$\exists q \in Z\, (x = qn + r \wedge 0 \leq r < n).$$

Ovim je dobro definisano preslikavanje rest $: Z \times N \to N$. To preslikavanje nazivamo funkcijom ostatka. Ova funkcija ima sledeću osobinu:

$$r = \mathrm{rest}(x, n) \Leftrightarrow \exists q \in Z\, (x = qn + r \wedge 0 \leq r < n), \quad x \in Z, n \in N.$$

Dalje, neka su $+_n$ i $\cdot_n$ operacije domena $Z_n$ definisane jednakostima:

$$x +_n y = \mathrm{rest}(x + y, n), \quad x \cdot_n y = \mathrm{rest}(xy, n)$$

Tada je $\mathbf{Z}_n = (Z_n, +_n, \cdot_n, 0, 1)$ algebra, tzv. *prsten ostataka po modulu* $n$. Operacije $+_n$ i $\cdot_n$ su redom operacije sabiranja i množenja po modulu $n$.

## 1.2 Jezik

Najjednostavnija klasifikacija algebri je prema jeziku, tj. prema broju i vrsti algebarskih operacija i konstanti koje učestvuju u njihovoj definiciji. Pod *algebarskim jezikom* podrazumevamo svaki konačan skup simbola

$$L = \mathrm{Const}_L \cup \mathrm{Fun}_L, \qquad \mathrm{Const}_L \cap \mathrm{Fun}_L = \emptyset,$$

gde je svakom simbolu $F \in \mathrm{Fun}_L$ pridružen neki prirodan broj $\mathrm{ar}(F)$, takozvana *arnost* ili *dužina* simbola $F$. Elemente skupa $\mathrm{Const}_L$ nazivamo simbolima konstanti, dok elemente skupa $\mathrm{Fun}_L$ nazivamo operacijskim ili funkcijskim znacima. Dogovorno simbolima konstanti dodeljujemo kao arnost broj 0. Bilo koji od skupova $\mathrm{Const}_L$, $\mathrm{Fun}_L$ može biti prazan.

Neka je $L = \mathrm{Const}_L \cup \mathrm{Fun}_L$ algebarski jezik, gde su $\mathrm{Const}_L = \{c_1, \ldots, c_m\}$ i $\mathrm{Fun}_L = \{F_1, \ldots, F_k\}$. *Algebra jezika* $L$ je svaka algebarska struktura

$$\mathbf{A} = (A, f_1, \ldots, f_k, a_1, \ldots, a_m)$$

gde je dužina operacije $f_i$ upravo $\mathrm{ar}(F_i)$, $1 \le i \le k$. U takvom slučaju kažemo da je operacija $f_i$ *interpretacija* operacijskog simbola $F_i$, dok je konstanta $a_j$, $(1 \le j \le m)$, interpretacija simbola $c_j$. Za interpretacije simbola jezika $L$ koristimo i ove oznake:

$$F_i^{\mathbf{A}} = f_i, \ \ (1 \le i \le k); \qquad c_j^{\mathbf{A}} = a_j, \quad (1 \le j \le m).$$

Dakle, interpretacija jezika $L$ u algebri $\mathbf{A}$ je neko preslikavanje vida

$$J : s \mapsto s^{\mathbf{A}}, \ \ s \in L, \qquad J : L \to A \cup A^A \cup A^{A^2} \cup A^{A^3} \cup \cdots .$$

**1.2.1 Primer** Neka je $\mathrm{Const}_L = \{0, 1\}$, $\mathrm{Fun}_L = \{+, \cdot, -\}$ gde su $+$ i $\cdot$ binarni operacijski znaci a $-$ unarni operacijski znak. Algebre

$$\mathbf{Z} = (Z, +, \cdot, -, 0, 1), \qquad \mathbf{P}(X) = (P(X), \cup, \cap, {}^c, \emptyset, X)$$

su dve interpretacije jezika $L$. U $\mathbf{Z}$ smo uzeli da je $-$ unarna operacija promene znaka.

Kao što prethodni primer pokazuje, moguće je da se isti znaci koriste za simbole jezika $L$, kao i za njihove interpretacije u datoj algebri jezika $L$.

*Signatura algebre* $\mathbf{A} = (A, f_1, f_2, \ldots, f_k, a_1, \ldots, a_m)$ je

$$\sigma\mathbf{A} = (\mathrm{ar}(f_1), \mathrm{ar}(f_2), \ldots, \mathrm{ar}(f_k), 0, 0, \ldots).$$

Dakle, najjednostavnija klasifikacija algebri je prema signaturi. Na primer sve algebre iz Primera 1.1.7 su iste signature (2,2,0,0).

Uslov konačnosti za algebarske jezike može se izostaviti. Naime, moguće je generalisati pojam algebarske strukture kao uređene trojke

$$\mathbf{A} = (A, \mathcal{F}, \mathcal{C}) \tag{1.1-1}$$

gde je $\mathcal{F} = \langle f_i |\ i \in I\rangle$ familija operacija domena $A$, dok je $\mathcal{C} = \langle a_j |\ j \in J\rangle$ familija elemenata iz $A$, $I$ i $J$ su neki skupovi indeksa. Tada se interpretacija proizvoljnog algebarskog jezika $L$, pa i beskonačnog, definiše na sličan način kao i kod konačnih jezika: Ako je $\mathrm{Const}_L = \langle c_j |\ j \in J\rangle$ i $\mathrm{Fun}_L = \langle F_i |\ i \in I\rangle$, $\mathbf{A}$ je algebra jezika $L$ ako je za sve $i \in I$, $\mathrm{ar}(f_i) = \mathrm{ar}(F_i)$. Umesto zapisa 1.1-1 koristi se i notacija $\mathbf{A} = (A, f_i, a_j)_{i\in I, j\in J}$. Na primer, za prebrojive skupove $\mathcal{F}$ i $\mathcal{C}$ imali bismo $\mathbf{A} = (A, f_i, a_j)_{i\in N, j\in N}$, ali možemo pisati takođe $\mathbf{A} = (A, f_0, f_1, \dots, a_0, a_1, \dots)$. Za algebre konačnog jezika kažemo da su konačne signature, dok za algebre beskonačnog jezika kažemo da su beskonačne signature. U ovoj knjizi bavićemo se uglavnom algebrama konačne signature.

## 1.3. Termi

U izgradnji algebarskih izraza nekog algebarskog jezika $L$ pored simbola iz $L$ ključnu ulogu imaju *promenljive*. Pod promenljivama podrazumevamo neki prebrojiv niz simbola, recimo $v_0, v_1, v_2, \dots$. Skup svih promenljivih obeležićemo sa Var, dakle $\mathrm{Var} = \{v_0, v_1, v_2, \dots\}$. Videćemo da su domeni ovih promenljivih, tj. skupovi u kojima one uzimaju vrednosti, zapravo domeni algebri. S druge strane pod metapromenljivama podrazumevaćemo promenljive čiji su domeni neki drugi skupovi promenljivih (uglavnom će to biti upravo skup Var). U takvom smislu koristimo i druge simbole, na primer $x, y, z, x_0, y_0, z_0, x_1, y_1, z_1, \dots$, za oznake promenljivih, tj. to su metapromenljive čiji je domen skup Var. Uz ove napomene neformalna definicija algebarskih izraza jezika L izgleda ovako:

(1) Promenljive, dakle $v_0, v_1, \dots$, su termi jezika $L$. Simboli konstanti jezika $L$ su termi jezika $L$.
(2) Ako je $F \in \mathrm{Fun}_L$ operacijski znak dužine $n$, i ako su $u_1, u_2, \dots, u_n$ termi jezika $L$, tada je i $F(u_1, u_2, \dots, u_n)$ term jezika $L$.
(3) Svaki term jezika $L$ dobija se konačnom primenom pravila (1) i (2).

U slučaju unarnih i binarnih operacijskih simbola, uslov (2) može da izgleda nešto drugačije:

(2') Ako je $\alpha$ unarni operacijski znak i $u$ je term, onda je $(\alpha u)$ (odnosno $(u^\alpha)$) term. Ako je $*$ binarni operacijski znak onda je $(u * v)$ takođe term za bilo koje terme $u, v$ jezika $L$.

Ubuduće nećemo posebno razlikovati slučajeve (2) i (2'). U smislu prethodne definicije sledeći izrazi su termi jezika $L$ iz Primera 1.2.1:

$$x,\ y,\ 0,\ 1,\ (x+0),\ (((x \cdot y) + ((-1) \cdot x_0)) + 0).$$

Formalna definicija terma nekog jezika $L$ je induktivnog karaktera. Naime, najpre definišemo niz skupova $T_n$ induktivno na sledeći način:

$$T_0 = \mathrm{Const}_L \cup \mathrm{Var}$$

$$T_{n+1} = T_n \cup \{F(u_1, \dots, u_k) |\ k \in N,\ \ F \in \mathrm{Fun}_L,\ \mathrm{ar}(F) = k,\ \ u_1, \dots, u_k \in T_n\}$$

**1.3.1 Definicija** $\mathrm{Term}_L = \cup_n T_n$.

Uobičajeno je da se koriste dogovori o kraćim zapisima algebarskih izraza. Na primer, spoljne zagrade kod terma se mogu izostaviti, a i neke unutrašnje ukoliko je uveden prioritet u skupu operacijskih simbola jezika $L$. S obzirom na induktivnu definiciju terma, dokazi većine tvrđenja o termima izvode se indukcijom, kao što vidimo na sledećem primeru.

**1.3.2 Teorema** *Za skupove $T_n$ i $\mathrm{Term}_L$ važi:*
1. $T_0 \subseteq T_1 \subseteq T_2 \subseteq \cdots \subseteq \mathrm{Term}_L$.
2. $\mathrm{Term}_L$ *sadrži promenljive i simbole konstanti jezika* $L$.
3. *Ako je* $F \in \mathrm{Fun}_L$ *dužine* $k$ *i* $u_1, \ldots, u_k \in \mathrm{Term}_L$, *onda* $F(u_1, \ldots, u_k) \in \mathrm{Term}_L$.
4. $\mathrm{Term}_L$ *je najmanji skup koji ima osobine 2. i 3.*

Primetimo da 2., 3. i 4. odgovaraju redom uslovima (1), (2) i (3) neformalne definicije terma. Prema ovoj teoremi skup terma jezika $L$ moguće je definisati kao najmanji skup $T$ koji sadrži Var i $\mathrm{Const}_L$ kao podskupove i koji je zatvoren za operaciju formiranja terma:

Ako je $F \in \mathrm{Fun}_L$, $\mathrm{ar}(F) = k$ i $u_1, \ldots, u_k \in T$, onda je $F(u_1, \ldots, u_k) \in T$.

**Dokaz** Teoreme 1.3.2 Tvrđenja 1. i 2. neposredno slede na osnovu definicije niza $T_n$ i skupa $\mathrm{Term}_L$.

3. Neka je $F \in \mathrm{Fun}_L$, $\mathrm{ar}(F) = k$ i neka su $u_1, \ldots, u_k \in \mathrm{Term}_L$. Tada za neke $n_i$, $1 \leq i \leq k$, $u_i \in T_{n_i}$, pa s obzirom da je niz $\langle T_n |\ n \in N\rangle$ monotono rastući, za $n = \max_{i \leq k} n_i$ imamo $u_1, \ldots, u_k \in T_n$. Prema definiciji skupa $T_{n+1}$ tada sledi $F(u_1, \ldots, u_k) \in T_{n+1}$, odakle $F(u_1, \ldots, u_k) \in \mathrm{Term}_L$ jer $T_{n+1} \subseteq \mathrm{Term}_L$.

4. Neka je $T$ bilo koji skup koji sadrži Var i $\mathrm{Const}_L$ kao podskupove i neka je $T$ zatvoren za operaciju formiranja terma. Indukcijom po $n$ dokazujemo da je za svaki $n \in N$, $T_n \subseteq T$: $T_0 \subseteq T$ jer je $T_0 = \mathrm{Var} \cup \mathrm{Const}_L$. Pretpostavimo da tvrđenje važi za neki fiksiran prirodan broj $n$, tj. $T_n \subseteq T$. S obzirom da je $T$ zatvoren za operaciju formiranja terma, sledi $T_{n+1} \subseteq T$, čime je dokazan induktivan korak. $\diamondsuit$

*Složenost terma* je preslikavanje $\mathrm{sl} : \mathrm{Term}_L \to N$ definisano na sledeći način:

Ako je $u \in T_0$ onda je $\mathrm{sl}(u) = 0$.

Neka je $u \in \mathrm{Term}_L$ i $u \notin T_0$. Tada je $\mathrm{sl}(u)$ najmanji prirodan broj $n$ takav da je $u \in T_n - T_{n-1}$.

**1.3.3 Primer** Ako su $+$ i $\cdot$ binarni znaci, i ako su $x, y, z$ promenljive, onda $\mathrm{sl}(x + y) = 1$ i $\mathrm{sl}((x \cdot y) + z) = 2$.

Vrednost terma u algebri $\mathbf{A}$ za zadate vrednosti promenljivih takođe je induktivnog karaktera i definiše se indukcijom po složenosti terma. Pri tome je pogodno da se za term $u$ koristi oznaka $u(x_1, x_2, \ldots, x_n)$ koja znači da su *sve* promenljive koje imaju pojavljivanja u termu $u$ neke od promenljivih $x_1, x_2, \ldots, x_n$.

**1.3.4 Definicija** *Neka je* $\mathbf{A} = (A, \mathcal{F}, \mathcal{C})$ *algebra jezika* $L = \mathrm{Fun}_L \cup \mathrm{Const}_L$. *Dalje, neka je* $\alpha$ *valuacija domena* $A$, *tj.* $\alpha$ *je funkcija koja svakoj promenljivoj* $v_i \in \mathrm{Var}$ *dodeljuje neku vrednost* $a_i$, *dakle* $\alpha : \mathrm{Var} \to A$. *Tada se vrednost terma* $u$, *u oznaci* $u^{\mathbf{A}}[\alpha]$, *određuje ovako:*

*Ako je* $\mathrm{sl}(u) = 0$ *onda razlikujemo dva slučaja.*

(1) *Ako je* $u$ *promenljiva* $v_i$, *onda je* $u^{\mathbf{A}}[\alpha] = a_i$.

(2) *Ako je* $u$ *simbol konstante* $c \in \mathrm{Const}_L$, *onda je* $u^{\mathbf{A}}[\alpha] = c^{\mathbf{A}}$.

*Neka je* $\mathrm{sl}(u) = n + 1$. *Tada za neki* $F \in \mathrm{Fun}_L$, $\mathrm{ar}(F) = k$, *imamo*

$$u = F(u_1, \dots, u_k)$$

*gde su* $u_1, \dots, u_k$ *neki termi složenosti* $\leq n$. *Tada je*

$$u^{\mathbf{A}}[\alpha] = F^{\mathbf{A}}[u_1^{\mathbf{A}}[\alpha], \dots, u_k^{\mathbf{A}}[\alpha]].$$

Neka je $u = u(x_1, x_2, \dots, x_n)$ term jezika $L$ i pretpostavimo da su promenljivama $x_1, x_2, \dots, x_n$ redom dodeljene vrednosti $a_1, a_2, \dots, a_n$. Tada se umesto $u^{\mathbf{A}}[\alpha]$ koriste i oznake $u^{\mathbf{A}}[a_1, \dots, a_n]$, ili $u^{\mathbf{A}}(a_1, a_2, \dots, a_n)$, odnosno $u[a_1, a_2, \dots, a_n]$, ili $u(a_1, a_2, \dots, a_n)$ ako je jasno o kojoj je algebri **A** reč. U prethodnoj definiciji vrednosti terma koristili smo implicitno pretpostavku da se svaki term može prikazati na samo jedan način. Naime, važi sledeće tvrđenje koje navodimo bez dokaza.

**1.3.5 Teorema** *Neka je* $u$ *term algebarskog jezika* $L$. *Tada je* $u$ *ili promenljiva, ili simbol konstante, ili postoji tačno jedan funkcijski znak* $F \in \mathrm{Fun}_L$ *i jedinstveni termi* $t_1, t_2, \dots, t_n$ *jezika* $L$, *gde je* $n = \mathrm{ar}(F)$, *tako da je* $u = F(t_1, t_2, \dots, t_n)$. $\diamondsuit$

## 1.4 Algebarski zakoni

Algebarskim zakonima mogu se izraziti razne algebarske osobine algebarskih struktura. Kao što ćemo videti to je zapravo posebna vrsta formula, zapisanih na jeziku razmatrane algebre.

**1.4.1 Definicija** *Algebarski zakon ili identitet jezika* $L$ *je svaka formula oblika* $u = v$ *gde su* $u$ *i* $v$ *termi jezika* $L$

Evo nekoliko primera algebarskih zakona.

1. Neka je $L = \{*, e\}$ gde je $*$ simbol binarne operacije, a $e$ simbol konstante. U važnije algebarske zakone jezika $L$ spadaju ovi identiteti:

| | |
|---|---|
| $x * (y * z) = (x * y) * z,$ | Zakon asocijacije, |
| $x * y = y * x,$ | Zakon komutacije, |
| $x * e = x, e * x = x,$ | Zakoni jediničnog elementa, |
| $x * x = x,$ | Zakon idempotencije, |
| $x * x = e,$ | Zakon involucije. |

2. Neka su $*$ i $\circ$ simboli binarnih operacija jezika $L$. Tada imamo ove algebarske identitete jezika $L$:

| | |
|---|---|
| $x \circ (y * z) = (x \circ y) * (x \circ z),$ | Levi distributivni zakon ($\circ$ prema $*$), |
| $(y * z) \circ x = (y \circ x) * (z \circ x),$ | Desni distributivni zakon ($\circ$ prema $*$), |
| $x \circ (x * y) = x,$ | Zakon apsorpcije ($\circ$ prema $*$), |
| $(x \circ y) * (y \circ z) * (z \circ x) = (x * y) \circ (y * z) \circ (z * x),$ | Dedekindov zakon. |

Neka je $\mathbf{A}$ algebarska struktura jezika $L$ i neka je $u(x_1, ..., x_n) = v(x_1, ..., x_n)$ algebarski zakon jezika $L$. Kažemo da algebra $\mathbf{A}$ *zadovoljava* zakon $u = v$, ili da identitet $u = v$ *važi* u algebri $\mathbf{A}$ akko (ako i samo ako):

Za sve $a_1, ..., a_n \in A$, $\quad u^{\mathbf{A}}[a_1, ..., a_n] = v^{\mathbf{A}}[a_1, ..., a_n]$.

Simbol $\models$ se koristi da se označi relacija važenja identiteta u algebri. Naime, za algebru $\mathbf{A}$ i zakon $u = v$ jezika $L$ imamo:

$\mathbf{A} \models u = v \quad$ akko $\quad$ u algebri $\mathbf{A}$ važi zakon $u = v$.

Algebarske teorije i algebarski varijeteti su fundamentalni pojmovi algebre. Evo njihovih definicija.

**1.4.2 Definicija** *Algebarska teorija jezika $L$ je svaki skup $T$ identiteta jezika $L$. U takvom slučaju članovi skupa $T$ nazivaju se aksiomama teorije $T$.*

**1.4.3 Definicija** *Neka je $T$ algebarska teorija jezika $L$. Varijetet teorije $T$ je klasa $\mathfrak{M}(T)$ svih algebri jezika $L$ koje zadovoljavaju sve zakone teorije $T$. Klasa $\mathfrak{M}$ algebri jezika $L$ je algebarski varijetet ako postoji algebarska teorija $T$ jezika $L$ takva da je $\mathfrak{M} = \mathfrak{M}(T)$.*

Primetimo da je svaki varijetet $\mathfrak{M}(T)$ neprazan jer sadrži sve *trivijalne algebre* jezika $L$, tj. algebre čiji je domen jednočlan skup. To sledi iz činjenice da trivijalna algebra jezika $L$ zadovoljava sve zakone jezika $L$, dakle i aksiome teorije $T$. Odavde sledi da je $\mathfrak{M}(T)$ ne samo neprazna klasa, već prava klasa. Naime $\mathfrak{M}(T)$ nije skup, jer klasa svih jednočlanih skupova je prava klasa. Navodimo neke važnije primere algebarskih teorija i varijeteta. U svakom primeru istovremeno dajemo jezik na koji se dotična teorija ili varijetet odnosi.

**1.** *Teorija grupoida* $G$. $\quad L_G = \{\cdot\}$, $\cdot$ je simbol binarne operacije. Ova teorija nema aksioma, tj. $G = \emptyset$, dok je $\mathfrak{M}(G)$ klasa svih grupoida, tj. algebri vida $\mathbf{A} = (A, \cdot)$. Ovaj primer pokazuje da teorija može biti prazan skup.

**2.** *Teorija semigrupa* $S$. $\quad$ U ovom slučaju jezik je $L_S = L_G$ dok $S$ ima jednu aksiomu, $S = \{x \cdot (y \cdot z) = (x \cdot y) \cdot z\}$. $\mathfrak{M}(S)$ je klasa svih semigrupa, tj. asocijativnih grupoida.

**3.** *Teorija monoida* Mon. $\quad L_{\mathrm{Mon}} = L_S \cup \{1\}$, 1 je simbol konstante, dok su aksiome teorije Mon:

zakon asocijacije,
$x \cdot 1 = x, \quad 1 \cdot x = x.$

$\mathfrak{M}(\mathrm{Mon})$ je klasa svih monoida, dakle algebri vida $\mathbf{A} = (A, \cdot, 1)$ koje zadovoljavaju navedene zakone.

**4.** *Teorija grupa* Gp. $\quad L_{\mathrm{Gp}} = L_{\mathrm{Mon}} \cup \{^{-1}\}$, gde je $^{-1}$ simbol unarne operacije. Aksiome teorije grupa su:

Aksiome teorije monoida,
$x \cdot x^{-1} = 1, \quad x^{-1} \cdot x = 1.$

$\mathfrak{M}(\mathrm{Gp})$ je klasa svih grupa, tj. algebri vida $\mathbf{A} = (A, \cdot, ^{-1}, 1)$ koje zadovoljavaju navedene aksiome.

**5.** *Teorija komutativnih grupa* Ab. $L_{\mathrm{Ab}} = \{+, -, 0\}$, gde je $+$ simbol binarne operacije, $-$ je simbol unarne operacije, $0$ je simbol konstante, a aksiome ove teorije su:

$$x + (y + z) = (x + y) + z, \qquad x + y = y + x,$$
$$x + 0 = x, \qquad x + (-x) = 0.$$

$\mathfrak{M}(\mathrm{Ab})$ je klasa svih komutativnih grupa, algebri vida $\mathbf{A} = (A, +, -, 0)$ koje zadovoljavaju navedene aksiome.

**6.** *Teorija prstena* $P$. U ovom slučaju $L_P = L_G \cup L_{\mathrm{Ab}}$, dok su aksiome:

aksiome teorije Ab,
aksiome teorije $S$,
$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \qquad (x + y) \cdot z = (x \cdot z) + (y \cdot z).$

$\mathfrak{M}(P)$ je klasa svih prstena, dakle algebri vida $\mathbf{P} = (P, +, -, \cdot, 0)$ koje zadovoljavaju aksiome teorije $P$.

**7.** *Teorija prstena sa jedinicom* $P_1$. Jezik ove teorije je $L_{P_1} = L_{\mathrm{Mon}} \cup L_{\mathrm{Ab}}$, dok su aksiome:

aksiome teorije prstena,
$x \cdot 1 = x, \qquad 1 \cdot x = x.$

Varijetet $\mathfrak{M}(P_1)$ je klasa svih prstena sa jedinicom od kojih je svaki oblika $\mathbf{P} = (P, +, -, \cdot, 0, 1)$.

**8.** *Teorija komutativnih prstena sa jedinicom* Pk. $L_{\mathrm{Pk}} = L_{P_1}$, aksiome teorije Pk su aksiome teorije $P_1$ i komutativni zakon $x \cdot y = y \cdot x$. Varijetet $\mathfrak{M}(\mathrm{Pk})$ je klasa svih komutativnih prstena sa jedinicom.

**9.** *Teorija mreža* $M$. $L_M = \{\vee, \wedge\}$, $\vee$, $\wedge$ su simboli binarnih operacija, dok su aksiome teorije $M$:

| | | | |
|---|---|---|---|
| M1. | $x \wedge (y \wedge z) = (x \wedge y) \wedge z,$ | M2. | $x \vee (y \vee z) = (x \vee y) \vee z,$ |
| M3. | $x \wedge y = y \wedge x,$ | M4. | $x \vee y = y \vee x,$ |
| M5. | $x \wedge x = x,$ | M6. | $x \vee x = x,$ |
| M7. | $x \wedge (x \vee y) = x,$ | M8. | $x \vee (x \wedge y) = x.$ |

Varijetet $\mathfrak{M}(M)$ je klasa svih mreža, dakle algebri vida $\mathbf{D} = (D, \vee, \wedge)$ koje zadovoljavaju aksiome M1-M8.

Ako je $\mathbf{D}$ mreža onda nije teško dokazati da je binarna relacija $\leq$ domena D definisana pomoću $a \leq b$ akko $a = a \wedge b$ zapravo parcijalno uređenje i da je u tom uređenju $a \vee b = \sup\{a, b\}$, $a \wedge b = \inf\{a, b\}$. U klasi $\mathfrak{M}(M)$ posebno su interesantne sledeće mreže:

*Modularne* ili *Dedekindove* mreže. To su mreže koje zadovoljavaju uslov *modularnosti:*

Za sve $a, b, c \in L$, $\quad a \leq b \Rightarrow (c \vee a) \wedge b = (c \wedge b) \vee a.$

Ovaj uslov naziva se i *modularnim zakonom*, mada, strogo rečeno to nije algebarski zakon u smislu Definicije 1.4.1. Ipak, može se pokazati da je uslov modularnosti ekvivalentan algebarskom zakonu $y \wedge (z \vee x) = y \wedge ((z \wedge (y \vee x)) \vee x)$.

Drugu klasu predstavljaju *distributivne* mreže, tj. mreže koje zadovoljavaju *distributivne* zakone:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \qquad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Lako je videti da je svaka distributivna mreža modularna.

**10.** *Teorija Bulovih algebri* BA. $L_{\mathrm{BA}} = L_M \cup \{\,', 0, 1\}$ gde je $'$ simbol unarne operacije, a 0 i 1 su simboli konstanti. Aksiome ove teorije su:

aksiome teorije distributivnih mreža,

$x \wedge x' = 0,\;\; x \vee x' = 1,\;\; x \wedge 1 = x,\;\; x \vee 1 = 1,\;\; x \wedge 0 = 0,\;\; x \vee 0 = x.$

Varijetet $\mathfrak{M}(\mathrm{BA})$ je klasa svih Bulovih algebri, prema tome algebri oblika $\mathbf{B} = (B, \vee, \wedge, ', 0, 1)$ koje zadovoljavaju navedene aksiome.

## 1.5 Homomorfizmi

Najkraće rečeno homomorfizmi su preslikavanja koja održavaju algebarsku strukturu. Posledica ove činjenice je da homomorfne slike čuvaju mnoge algebarske osobine polazne algebre. U daljem izlaganju često ćemo za neku funkciju $h$, vrednost $h(x)$ obeležavati jednostavno pomoću $hx$.

**1.5.1 Definicija** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *algebre jezika* $L$. *Homomorfizam iz algebre* $\mathbf{A}$ *u algebru* $\mathbf{B}$ *je svako preslikavanje* $h : A \to B$ *sa osobinama:*

1. *Ako je* $c \in \mathrm{Const}_L$ *onda* $h(c^{\mathbf{A}}) = c^{\mathbf{B}}$.
2. *Ako je* $F \in \mathrm{Fun}_L$ *dužine* $n$, *onda za sve* $a_1, a_2, \ldots, a_n \in A$ *važi*

$$h(F^{\mathbf{A}}(a_1, a_2, \ldots, a_n)) = F^{\mathbf{B}}(ha_1, ha_2, \ldots, ha_n).$$

Neka su $\mathbf{A} = (A, f_1, \ldots, f_k, b_1, \ldots, b_m)$ i $\mathbf{B} = (B, g_1, \ldots, g_k, d_1, \ldots, d_m)$ algebre jezika $L$ i neka je $h$ homomorfizam ovih algebri. Tada prema definiciji homomorfizma imamo: Za svaki $1 \leq i \leq m$, $h(b_i) = d_i$. Ako su $f_i$ i $g_i$ operacije dužine $n$, onda je za sve $a_1, a_2, \ldots, a_n \in A$

$$h(f_i(a_1, a_2, \ldots, a_n)) = g_i(ha_1, ha_2, \ldots, ha_n).$$

U ovakvom slučaju takođe kažemo da je preslikavanje $h$ *saglasno* sa operacijama $f_i$ i $g_i$. Ako su $f_i$ i $g_i$ binarne operacije, na primer $*$ i $\circ$, onda prema posebnoj notaciji za binarne operacije uslov homomorfizma za $h$ izgleda ovako:

$$\text{Za sve } a_1, a_2 \in A, \quad h(a_1 * a_2) = h(a_1) \circ h(a_2).$$

Ako je $h : A \to B$ homomorfizam algebre $\mathbf{A}$ u algebru $\mathbf{B}$, onda koristimo oznaku $h : \mathbf{A} \to \mathbf{B}$. Skup svih homomorfizama iz $\mathbf{A}$ u $\mathbf{B}$ obeležavamo sa $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$.

**1.5.2 Primer** Preslikavanje $h : R^+ \to R$, gde je $h(x) = \ln(x)$, $x \in R^+$, je homomorfizam multiplikativne grupe pozitivnih realnih brojeva $(R^+, \cdot, 1)$ u aditivnu grupu realnih brojeva $(R, +, 0)$, jer $h(1) = 0$ i $h(xy) = \ln(xy) = \ln(x) + \ln(y) = h(x) + h(y)$, $x, y \in R^+$.

**1.5.3 Primer** Neka je $n \in N$, $n \geq 2$, $Z_n = \{0, 1, 2, ..., n-1\}$ i neka je preslikavanje $\rho_n : Z \to Z_n$ definisano sa $\rho_n(x) = \mathrm{rest}(x, n)$. U ovom primeru, dalje ćemo umesto $\rho_n$ jednostavno pisati $\rho$. Preslikavanje $\rho$ je homomorfizam prstena celih brojeva $\mathbf{Z} = (Z, +, \cdot, 0, 1)$ na $\mathbf{Z}_n = (Z_n, +_n, \cdot_n, 0, 1)$, prsten ostataka po modulu $n$. Zaista, neka su $r_1 = \rho(x)$ i $r_2 = \rho(y)$. Tada je za neke $q_1, q_2 \in Z$, $x = q_1 n + r_1$ i $y = q_2 n + r_2$ i takođe $0 \leq r_1, r_2 < n$. Prema definiciji operacija $+_n$ i $\cdot_n$, videti Primer 1.1.11, imamo

$$\begin{aligned} r_1 +_n r_2 &= \rho(r_1 + r_2), \quad 0 \leq r_1 +_n r_2 < n, \\ r_1 \cdot_n r_2 &= \rho(r_1 \cdot r_2), \quad\ \ 0 \leq r_1 \cdot_n r_2 < n. \end{aligned}$$

Otuda za neke $\alpha, \beta \in Z$, $r_1 + r_2 = \alpha n + (r_1 +_n r_2)$, $r_1 \cdot r_2 = \beta n + (r_1 \cdot_n r_2)$, dakle,

$$\begin{aligned} x + y &= (q_1 + q_2 + \alpha)n + (r_1 +_n r_2), & 0 \leq r_1 +_n r_2 < n \\ x \cdot y &= (q_1 q_2 n + q_1 r_2 + q_2 r_1 + \beta)n + (r_1 \cdot_n r_2), & 0 \leq r_1 \cdot_n r_2 < n \end{aligned}$$

što znači da je

$$\begin{aligned} \mathrm{rest}(x+y, n) &= r_1 +_n r_2, \quad \text{tj.} \quad \rho(x+y) = \rho(x) +_n \rho(y) \\ \mathrm{rest}(xy, n) &= r_1 \cdot_n r_2, \quad\ \ \text{tj.} \quad \rho(xy) = \rho(x) \cdot_n \rho(y) \end{aligned}$$

Očigledno je $\rho(0) = 0$ i $\rho(1) = 1$, prema tome $\rho : \mathbf{Z} \to \mathbf{Z}_n$. Kako je za $i \in Z_n$, $\rho(i) = i$, $\rho$ je preslikavanje *na*.

Sledećom definicijom daje se osnovna klasifikacija homomorfizama.

**1.5.4 Definicija** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *algebre jezika* $L$ *i neka je* $h : \mathbf{A} \to \mathbf{B}$ *homomorfizam. Tada*

1. *h je utapanje (monomorfizam) ako i samo ako je h* $1-1$ *preslikavanje, tj.*

$$\forall x, y \in A \quad (x \neq y \Rightarrow h(x) \neq h(y)).$$

*Ako je h utapanje onda koristimo oznaku* $h : \mathbf{A} \underset{1\text{-}1}{\longrightarrow} \mathbf{B}$.

2. *h je homomorfizam* **na** *(epimorfizam) ako i samo ako je h preslikavanje* **na**, *tj.*

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

*U takvom slučaju koristimo oznaku* $h : \mathbf{A} \xrightarrow{\text{na}} \mathbf{B}$. *Tada takođe kažemo da je* $\mathbf{B}$ *homomorfna slika algebre* $\mathbf{A}$ *i pišemo* $\mathbf{B} = h(\mathbf{A})$ *ili* $\mathbf{B} = h\mathbf{A}$.

3. *h je izomorfizam algebri* $\mathbf{A}$ *i* $\mathbf{B}$ *ako i samo ako je h* $1-1$ *i* **na**. *U takvom slučaju koristimo ove oznake:* $h : \mathbf{A} \cong \mathbf{B}$ *ili* $h : \mathbf{A} \xrightarrow{\sim} \mathbf{B}$ *i kažemo da su algebre* $\mathbf{A}$ *i* $\mathbf{B}$ *izomorfne. Oznaka* $\mathbf{A} \cong \mathbf{B}$ *znači da postoji izomorfizam iz algebre* $\mathbf{A}$ *u* $\mathbf{B}$.
4. *h je endomorfizam ili unutrašnji homomorfizam ako i samo ako je* $\mathbf{A} = \mathbf{B}$. *Skup svih endomorfizama algebre* $\mathbf{A}$ *obeležava se sa* $\mathrm{End}(\mathbf{A})$.
5. *h je automorfizam algebre* $\mathbf{A}$ *ako i samo ako je* $\mathbf{A} = \mathbf{B}$ *i h je izomorfizam. Skup svih automorfizama algebre* $\mathbf{A}$ *označavamo sa* $\mathrm{Aut}(\mathbf{A})$.

U Primeru 1.5.2, preslikavanje $h$ je izomorfizam, dakle $(R^+, \cdot, 1) \cong (R, +, 0)$. U Primeru 1.5.3, preslikavanje $\rho$ je epimorfizam prstena $\mathbf{Z}$ na algebru $\mathbf{Z}_n$. Konjugacija $h : z \mapsto \overline{z}$, $z \in C$, je primer jednog automorfizma polja kompleksnih brojeva $\mathbf{C} = (C, +, \cdot, 0, 1)$, jer za $z_1, z_2 \in C$ važi:

$$\begin{aligned} h(z_1 + z_2) &= \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 = h(z_1) + h(z_2), \\ h(z_1 \cdot z_2) &= \overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2 = h(z_1) \cdot h(z_2), \end{aligned}$$

$$\overline{z}_1 = \overline{z}_2 \Rightarrow \overline{\overline{z}}_1 = \overline{\overline{z}}_2 \Rightarrow z_1 = z_2, \quad \text{i} \quad \overline{z_1} = z_2 \Rightarrow z_1 = \overline{z_2}.$$

**1.5.5 Teorema** *Neka su* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *algebre jezika* $L$ *i neka su* $f : \mathbf{A} \to \mathbf{B}$, $g : \mathbf{B} \to \mathbf{C}$ *homomorfizmi. Tada je preslikavanje* $h = g \circ f$ *homomorfizam algebre* $\mathbf{A}$ *u algebru* $\mathbf{C}$. *Pri tome važi:*

1. *Ako su* $f$ *i* $g$ *utapanja onda je i* $h$ *utapanje.*
2. *Ako su* $f$ *i* $g$ *epimorfizmi onda je i* $h$ *epimorfizam.*
3. *Ako su* $f$ *i* $g$ *izomorfizmi onda je i* $h$ *izomorfizam.*
4. *Ako je* $f$ *izomorfizam onda je i* $f^{-1}$ *izomorfizam algebre* $\mathbf{B}$ *u algebru* $\mathbf{A}$.

**Dokaz** Dokazujemo da je $h$ homomorfizam. Neka je $e \in \mathrm{Const}_L$. Tada važi: $h(e^{\mathbf{A}}) = (g \circ f)(e^{\mathbf{A}}) = g(f(e^{\mathbf{A}})) = g(e^{\mathbf{B}}) = e^{\mathbf{C}}$. Neka je $F \in \mathrm{Fun}_L$ dužine $n$, i neka su $a_1, a_2, \dots, a_n \in A$. Tada

$$
\begin{aligned}
h(F^{\mathbf{A}}(a_1, a_2, \dots, a_n)) &= g(f(F^{\mathbf{A}}(a_1, a_2, \dots, a_n))) \\
&= g(F^{\mathbf{B}}(fa_1, fa_2, \dots, fa_n)) \\
&= F^{\mathbf{C}}(gfa_1, gfa_2, \dots, gfa_n) \\
&= F^{\mathbf{C}}(ha_1, ha_2, \dots, ha_n).
\end{aligned}
$$

Ovakva veza između algebri $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ i homomorfizama $g$, $f$ i $h$ prikazana je sledećim dijagramom, i u tom slučaju kažemo da dijagram komutira.

$$
\begin{tikzcd}
\mathbf{A} \arrow[r, "f"] \arrow[dr, phantom, "h"] & \mathbf{B} \arrow[d, "g"] \\
 & \mathbf{C}
\end{tikzcd}
\qquad h = g \circ f
$$

Tvrđenja $1 - 3$ slede na osnovu činjenica da je proizvod $1 - 1$ ($na$) preslikavanja takođe $1 - 1$ ($na$) preslikavanje.

Dokazujemo tvrđenje 4. Neka je $e \in \mathrm{Const}_L$. Kako je $f(e^{\mathbf{A}}) = e^{\mathbf{B}}$ to je onda $f^{-1}(e^{\mathbf{B}}) = e^{\mathbf{A}}$. Dalje, neka je $F \in \mathrm{Fun}_L$ dužine $n$ i neka su $b_1, b_2, \dots, b_n \in B$. Kako je $f$ preslikavanje **na**, postoje $a_1, a_2, \dots, a_n \in A$ takvi da je $b_i = f(a_i)$. Tada je $a_i = f^{-1}(b_i)$ i

$$
\begin{aligned}
f^{-1}(F^{\mathbf{B}}(b_1, ..., b_n)) &= f^{-1}(F^{\mathbf{B}}(fa_1, fa_2, \dots, fa_n)) \\
&= f^{-1}(f(F^{\mathbf{A}}(a_1, a_2, \dots, a_n))) \\
&= F^{\mathbf{A}}(a_1, a_2, \dots, a_n) \\
&= F^{\mathbf{A}}(f^{-1}b_1, f^{-1}b_2, \dots, f^{-1}b_n),
\end{aligned}
$$

tj. preslikavanje $f^{-1}$ je saglasno sa operacijama $F^{\mathbf{B}}$ i $F^{\mathbf{A}}$. $\diamondsuit$

Na osnovu tvrđenja 3 i 4 Teoreme, kao i činjenice da je identičko preslikavanje $i_A$ automorfizam bilo koje algebre sa domenom $A$, sledi da je $\cong$ relacija ekvivalencije u klasi svih algebri datog jezika.

**1.5.6 Posledica** Za svaku algebru $\mathbf{A}$, $\mathbf{End}(\mathbf{A}) = (\mathrm{End}(\mathbf{A}), \circ, i_A)$ je monoid.

**1.5.7 Posledica** Za svaku algebru $\mathbf{A}$, $\mathbf{Aut}(\mathbf{A}) = (\mathrm{Aut}(\mathbf{A}), \circ, ^{-1}, i_A)$ je grupa.

## 1.6 Homomorfizmi i termi

Neka je $\mathbf{A}$ algebra jezika L i $u \in \mathrm{Term}_L$. Term $u = u(x_1, x_2, \dots, x_n)$ određuje tzv. *term-preslikavanje* $U : A^n \to A$ algebre $\mathbf{A}$ na sledeći način:

$U(a_1, a_2, \dots, a_n) = u^{\mathbf{A}}[a_1, a_2, \dots, a_n], \quad a_1, a_2, \dots, a_n \in A.$

Ovako uvedeno term – preslikavanje $U$ označavaćemo sa $u^{\mathbf{A}}(x_1, x_2, \dots, x_n)$, ili $u(x_1, x_2, \dots, x_n)$ ako je jasno o kojoj je algebri reč. Ovo preslikavanje očigledno određuje jednu operaciju algebre $\mathbf{A}$ dužine $n$. Tu operaciju nazivamo *izvedenom operacijom* algebre $\mathbf{A}$. Sledeće tvrđenje kaže da su homomorfizmi algebri preslikavanja takođe saglasna za izvedene operacije.

**1.6.1 Teorema** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *algebre jezika* $L$ *i neka je* $h : \mathbf{A} \to \mathbf{B}$ *homomorfizam. Tada za svaki term* $u(x_1, x_2, \dots, x_n)$ *jezika* $L$ *važi*

$$\forall a_1, a_2, \dots, a_n \in A \;\; h(u^{\mathbf{A}}[a_1, a_2, \dots, a_n]) = u^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n]$$

**Dokaz** Dokaz izvodimo indukcijom po složenosti terma. Neka je $u \in \mathrm{Term}_L$ i neka su promenljivama $x_1, x_2, \dots, x_n$ dodeljene redom vrednosti $a_1, a_2, \dots, a_n$. Tada razlikujemo sledeće slučajeve:

(1) $u$ je simbol konstante $c \in L$. Tada

$$h(u^{\mathbf{A}}[a_1, a_2, \dots, a_n]) = h(c^{\mathbf{A}}) = c^{\mathbf{B}} = u^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n].$$

(2) $u$ je promenljiva $x_i$, $i \le n$. Tada

$$h(u^{\mathbf{A}}[a_1, a_2, \dots, a_n]) = h(a_i) = u^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n].$$

Pretpostavimo da tvrđenje važi za terme složenosti $\le m$, $m$ je neki utvrđen prirodan broj, (induktivna hipoteza) i neka je složenost terma $u$ jednaka $m+1$. Tada za neki $F \in \mathrm{Fun}_L$ dužine $k$ i neke $u_1, u_2, ..., u_k \in \mathrm{Term}_L$ imamo $u \equiv F(u_1, u_2, ..., u_k)$. Tada

$$\begin{aligned} h(u^{\mathbf{A}}[a_1, a_2, \dots, a_n]) &= h(F^{\mathbf{A}}(u_1^{\mathbf{A}}[a_1, a_2, \dots, a_n], \dots, u_k^{\mathbf{A}}[a_1, a_2, \dots, a_n])) \\ &= F^{\mathbf{B}}(hu_1^{\mathbf{A}}[a_1, a_2, \dots, a_n], \dots, hu_k^{\mathbf{A}}[a_1, a_2, \dots, a_n]) \\ &\text{(koristeći induktivnu hipotezu jer je } \mathrm{sl}(u_i) \le m) \\ &= F^{\mathbf{B}}(u_1^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n], \dots, u_k^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n]) \\ &= u^{\mathbf{B}}[ha_1, ha_2, \dots, ha_n]. \end{aligned}$$

Na osnovu matematičke indukcije tvrđenje sada sledi za svaki $m \in N$. $\diamondsuit$

Očigledno je da se prethodno tvrđenje može ovako iskazati:

Za svaku valuaciju $\mu : \mathrm{Var} \to A$ važi $h(u^{\mathbf{A}}[\mu]) = u^{\mathbf{B}}[h \circ \mu]$.

Otuda vidimo da homomorfizam $h$ i valuacija $\mu$ domena $A$ određuju novu valuaciju $\tau$ domena $B$ preko jednakosti $\tau = h \circ \mu$. Ova činjenica predstavljena je pomoću sledećeg komutativnog dijagrama:

$$\begin{tikzcd} \mathrm{Var} \arrow[r, "\mu"] \arrow[dr, phantom, "\tau"] & A \arrow[d, "h"] \\ & B \end{tikzcd} \qquad \tau = h \circ \mu$$

**1.6.2 Posledica** Neka su **A**, **B** algebre jezika $L$ i pretpostavimo da je **B** homomorfna slika algebre **A**. Tada svaki identitet koji važi u **A** takođe važi i u **B**.

**Dokaz** Neka je $h : \mathbf{A} \to \mathbf{B}$ epimorfizam i pretpostavimo $\mathbf{A} \models u = v$ Tada za proizvoljne elemente $b_1, b_2, \ldots, b_n \in B$ postoje $a_1, a_2, \ldots, a_n \in A$ takvi da je $h(a_i) = b_i$, $1 \leq i \leq n$, pa

$$\begin{aligned} u^{\mathbf{B}}[b_1, b_2, ..., b_n] &= u^{\mathbf{B}}[ha_1, ha_2, ..., ha_n] \\ &= h(u^{\mathbf{A}}[a_1, a_2, ..., a_n]) \\ &= h(v^{\mathbf{A}}[a_1, a_2, ..., a_n]) \\ &= v^{\mathbf{B}}[ha_1, ha_2, ..., ha_n] \\ &= v^{\mathbf{B}}[b_1, b_2, ..., b_n]. \end{aligned} \qquad \diamondsuit$$

**1.6.3 Posledica** Varijeteti su zatvoreni za homomorfne slike, tj. ako je $\mathfrak{M}$ varijetet jezika $L$ i algebra **B** istog jezika je homomorfna slika neke algebre $\mathbf{A} \in \mathfrak{M}$, onda je i $\mathbf{B} \in \mathfrak{M}$.

**1.6.4 Primer** Prema oznakama iz Primera 1.5.3 , važi $\mathbf{Z}_n = \rho_n \mathbf{Z}$, tj. $\mathbf{Z}_n$ je homomorfna slika prstena celih brojeva. Otuda je, prema prethodnoj posledici, i $\mathbf{Z}_n$ komutativan prsten sa jedinicom.

## 1.7 Podalgebre

Algebra **A** jezika L može da sadrži podskupove koji su takođe domeni algebri istog jezika $L$, a kod kojih su operacije nastale suženjem odnosno restrikcijom operacija polazne algebre **A**. Otuda imamo pojam podalgebre.

**1.7.1 Definicija** *Neka je* **A** *algebra jezika* $L$. *Podalgebra algebre* **A** *je svaka algebra* **B** *jezika* $L$ *za koju važi:*

1. $B \subseteq A$.
2. *Ako je* $c \in \mathrm{Const}_L$ *onda je* $c^{\mathbf{B}} = c^{\mathbf{A}}$.
3. *Ako je* $F \in \mathrm{Fun}_L$ *dužine* $n$, *onda za sve* $b_1, b_2, \ldots, b_n \in B$ *važi*

$$F^{\mathbf{B}}(b_1, b_2, \ldots, b_n) = F^{\mathbf{A}}(b_1, b_2, \ldots, b_n).$$

Činjenicu da je $\mathbf{B}$ podalgebra algebre $\mathbf{A}$ zapisujemo sa $\mathbf{B} \subseteq \mathbf{A}$. S obzirom da su vrednosti operacija u algebri i podalgebri jednake, podalgebra je u potpunosti odredjena svojim domenom. Naime, ako su $\mathbf{B}, \mathbf{C} \subseteq \mathbf{A}$ i $B = C$, onda je i $\mathbf{B} = \mathbf{C}$. Otuda umesto $\mathbf{B} \subseteq \mathbf{A}$ često kažemo da je $B$ podalgebra algebre $\mathbf{A}$. Dalje, ako je $F$ funkcijski znak dužine $k$, tada je prema definiciji podalgebre $F^{\mathbf{B}} = F^{\mathbf{A}} \mid B^k$, tj. $F^{\mathbf{B}}$ je restrikcija preslikavanja $F^{\mathbf{A}}$ na skup $B^k$. Ubuduće ćemo govoriti da je $F^{\mathbf{B}}$ restrikcija operacije $F^{\mathbf{A}}$ na domen $B$. Takođe, za oznake operacija u podalgebri $\mathbf{B}$ obično se zadržavaju oznake iz polazne algebre $\mathbf{A}$. Dakle, ako je $\mathbf{B} \subseteq \mathbf{A}$ i $\mathbf{A} = (A, f_1, f_2, \ldots, f_m, a_1, a_2, \ldots, a_n)$ tada takođe pišemo $\mathbf{B} = (B, f_1, f_2, \ldots, f_m, a_1, a_2, \ldots, a_n)$.

### 1.7.2 Primer

1. $(N, +, \cdot, 0) \subseteq (Z, +, \cdot, 0) \subseteq (Q, +, \cdot, 0) \subseteq (R, +, \cdot, 0) \subseteq (C, +, \cdot, 0)$ gde su $+$ i $\cdot$ uobičajene operacije sa brojevima, a $N, Z, Q, R, C$ redom označavaju skup prirodnih, celih, racionalnih, realnih i kompleksnih brojeva.
2. Neka je $S$ bilo koji skup i $\mathbf{A} = (S^S, \circ, i_S)$. Tada je skup svih permutacija skupa $S$ podalgebra algebre $\mathbf{A}$.

Za pojedine varijetete imamo posebne nazive za podalgebre. Na primer, umesto podalgebra kod grupa koristimo naziv podgrupa, kod prstena potprsten, kod mreža podmreža itd.

**1.7.3. Teorema** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *algebre jezika* $L$ *i neka je* $A \subseteq B$. *Tada je* $\mathbf{A}$ *podalgebra algebre* $\mathbf{B}$ *ako i samo ako je inkluziono preslikavanje* $i_A : A \longrightarrow B$, $i_A : x \mapsto x$, $(x \in A)$, *homomorfizam iz* $\mathbf{A}$ *u* $\mathbf{B}$.

**Dokaz** $(\Rightarrow)$ Neka je $\mathbf{A} \subseteq \mathbf{B}$ i pretpostavimo da je $F \in \mathrm{Fun}_L$ dužine $k$. Tada za $a_1, a_2, \ldots, a_k \in A$ važi:

$$\begin{aligned} i_A(c^{\mathbf{A}}) =& c^{\mathbf{A}} = c^{\mathbf{B}}, \\ i_A F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) =& F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) = F^{\mathbf{B}}(a_1, a_2, \ldots, a_k) = \\ & F^{\mathbf{B}}(i_A a_1, i_A a_2, \ldots, i_A a_k), \end{aligned}$$

tj. $i_A$ je homomorfizam.

$(\Leftarrow)$ Pretpostavimo da je $i_A : \mathbf{A} \longrightarrow \mathbf{B}$ homomorfizam. Tada je za $c \in \mathrm{Const}_L$, $i_A(c^{\mathbf{A}}) = c^{\mathbf{B}}$ tj. $c^{\mathbf{A}} = c^{\mathbf{B}}$. Dalje, imamo

$$\begin{aligned} F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) =& i_A(F^{\mathbf{A}}(a_1, a_2, \ldots, a_k)) = \\ & F^{\mathbf{B}}(i_A a_1, i_A a_2, \ldots, i_A a_k) = F^{\mathbf{B}}(a_1, a_2, \ldots, a_k), \end{aligned}$$

tj.

$$\forall a_1, a_2, \ldots, a_k \in A \;\; F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) = F^{\mathbf{B}}(a_1, a_2, \ldots, a_k).$$

dakle $\mathbf{A} \subseteq \mathbf{B}$. $\diamondsuit$

**1.7.4. Posledica** Neka je $\mathbf{B}$ algebra jezika $L$ i neka je $\mathbf{A} \subseteq \mathbf{B}$. Tada za svaki zakon $u = v$ jezika $L$ važi:

Ako je $\mathbf{B} \models u = v$ onda $\mathbf{A} \models u = v$.

**Dokaz** Pretpostavimo $\mathbf{B} \models u(x_1, x_2, \ldots, x_n) = v(x_1, x_2, \ldots, x_n)$. Tada prema prethodnim teoremama imamo

$$\begin{aligned} u^{\mathbf{A}}(a_1, a_2, \ldots, a_n) =& i_A u^{\mathbf{A}}(a_1, a_2, \ldots, a_n) = u^{\mathbf{B}}(i_A a_1, i_A a_2, \ldots, i_A a_n) = \\ & v^{\mathbf{B}}(i_A a_1, i_A a_2, \ldots, i_A a_n) = i_A v^{\mathbf{A}}(a_1, a_2, \ldots, a_n) = \\ & v^{\mathbf{A}}(a_1, a_2, \ldots, a_n). \end{aligned} \qquad \diamondsuit$$

Iz ove posledice neposredno vidimo da su algebarski varijeteti zatvoreni za podalgebre, tj. važi

**1.7.5. Posledica** Neka je $\mathfrak{M}$ algebarski varijetet i $\mathbf{A} \in \mathfrak{M}$. Tada je svaka podalgebra algebre $\mathbf{A}$ element varijeteta $\mathfrak{M}$.

## 1.8. Proizvod algebri

Proizvod algebri omogućava konstrukciju novih algebri polazeći od neke date konačne ili beskonačne familije algebri. Najpre ćemo razmotriti konačne proizvode.

**1.8.1 Definicija** *Neka su* $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ *algebre jezika* $L$. *Proizvod ovih algebri je algebra* $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$ *jezika* $L$ *gde je:*
1. $A = A_1 \times A_2 \times \ldots \times A_n$.
2. *Ako je* $c \in \mathrm{Const}_L$ *tada je* $c^{\mathbf{A}} = (c^{\mathbf{A}_1}, c^{\mathbf{A}_2}, \ldots, c^{\mathbf{A}_n})$.
3. *Neka je* $F \in \mathrm{Fun}_L$ *dužine* $k$ *i neka su* $a_1, a_2, \ldots, a_k \in A$, $a_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, $i = 1, 2, \ldots, k$. *Tada je*

$$\begin{aligned} & F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) = \\ & (F^{\mathbf{A}_1}(a_{11}, a_{21}, \ldots, a_{k1}), F^{\mathbf{A}_2}(a_{12}, a_{22}, \ldots, a_{k2}), \ldots, F^{\mathbf{A}_n}(a_{1n}, a_{2n}, \ldots, a_{kn})) \end{aligned}$$

Ako su algebre $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ međusobno jednake, recimo $\mathbf{A}_1 = \mathbf{A}_2 = \ldots = \mathbf{A}_n = \mathbf{C}$, tada se proizvod $\mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$ naziva *stepenom* algebre $\mathbf{C}$ i obeležava se sa $\mathbf{C}^n$.

**1.8.2 Primer** Neka su algebre $\mathbf{A} = (A, *_A, ^{-1_A}, 1_A)$, $\mathbf{B} = (B, *_B, ^{-1_B}, 1_B)$, $\mathbf{C} = (C, *_C, ^{-1_C}, 1_C)$ grupe. Ako je $\mathbf{D} = \mathbf{A} \times \mathbf{B} \times \mathbf{C}$, tada je $\mathbf{D} = (D, *, ^{-1}, 1)$ gde je $1 = (1_A, 1_B, 1_C)$, dok je $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 *_A a_2, b_1 *_B b_2, c_1 *_C c_2)$ i $(a, b, c)^{-1} = (a^{-1_A}, b^{-1_B}, c^{-1_C})$.

Neka je $1 \le i \le n$. Preslikavanje $\pi_i : A_1 \times A_2 \times \ldots \times A_n \to A_i$ definisano sa

$$\pi_i : (x_1, x_2, \ldots, x_n) \mapsto x_i, \qquad x_1 \in A_1, \ldots, x_n \in A_n$$

naziva se *i-tom projekcijom.* Prema definiciji projekcije $\pi_i$ odmah nalazimo da za $x, y \in A_1 \times A_2 \times \ldots \times A_n$ važi: $\quad x = y \Leftrightarrow \forall i \le n \;\; \pi_i(x) = \pi_i(y)$.

**1.8.3 Teorema** *Neka su $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ algebre jezika $L$. Tada je za svaki $1 \le i \le n$ projekcija $\pi_i$ homomorfizam algebre $\mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$ na algebru $\mathbf{A}_i$.*

**Dokaz** Neka je $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$. Prema definiciji constante $c^{\mathbf{A}}$ i projekcije $\pi_i$ za $c \in \mathrm{Const}_L$ imamo $\pi_i(c^{\mathbf{A}}) = c^{\mathbf{A}_i}$. Neka je $F \in \mathrm{Fun}_L$ dužine $k$, i neka su $a_1, a_2, \dots, a_k \in A$, gde je $a_i = (a_{i1}, a_{i2}, ..., a_{in})$. Tada je

$$\pi_i F^{\mathbf{A}}(a_1, a_2, \dots, a_k) = F^{\mathbf{A}_i}(a_{1i}, a_{2i}, \dots, a_{ki}) = F^{\mathbf{A}_i}(\pi_i a_1, \pi_i a_2, \dots, \pi_i a_k).$$

Dalje, neka je $a \in A_i$ i $a_j \in A_j$ za $j \neq i$. Tada iz $a_i = a$ sledi $\pi_i(a_1, a_2, \dots, a_n) = a_i = a$, tj. $\pi_i$ je preslikavanje *na*. Prema tome, $\pi_i$ je homomorfizam algebre $\mathbf{A}$ na algebru $\mathbf{A}_i$. ♢

**1.8.4 Posledica** Neka su $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ algebre jezika $L$. Zakon $u = v$ jezika $L$ važi na svakoj algebri $\mathbf{A}_i$ akko taj zakon važi na proizvodu algebri $\mathbf{A}_i$.

**Dokaz** Neka je $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n$ i pretpostavimo

$$\mathbf{A}_i \models u(x_1, x_2, \dots, x_m) = v(x_1, x_2, \dots, x_m), \quad 1 \le i \le n.$$

Dalje, neka su $a_1, a_2, \dots, a_m \in A$. Da bismo dokazali da je $u^{\mathbf{A}}(a_1, a_2, \dots, a_m) = v^{\mathbf{A}}(a_1, a_2, \dots, a_m)$, dovoljno je da proverimo da je za sve $1 \le i \le n$

(1) $$\pi_i u^{\mathbf{A}}(a_1, a_2, \dots, a_m) = \pi_i v^{\mathbf{A}}(a_1, a_2, \dots, a_m).$$

Pretpostavimo da je $1 \le i \le n$. Prema Teoremi 1.6.1 i s obzirom da je $\mathbf{A}_i \models u = v$, imamo

$$\begin{aligned}\pi_i(u^{\mathbf{A}}(a_1, a_2, \dots, a_m)) = & u^{\mathbf{A}_i}(\pi_i a_1, \pi_i a_2, \dots, \pi_i a_m) = \\ & v^{\mathbf{A}_i}(\pi_i a_1, \pi_i a_2, \dots, \pi_i a_m) = \\ & \pi_i(v^{\mathbf{A}}(a_1, a_2, \dots, a_m))\end{aligned}$$

prema tome (1) važi. Obrat važi prema Posledici 1.6.2 i Teoremi 1.8.3. ♢

**1.8.5 Posledica** Svaki algebarski varijetet $\mathfrak{M}$ zatvoren je za konačne proizvode algebri, tj. za svaki $n \in N$, $n \ge 2$, važi

$$\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n \in \mathfrak{M} \Rightarrow \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n \in \mathfrak{M}.$$

Prema ovoj posledici konačan proizvod semigrupa je semigrupa, konačan proizvod grupa je grupa, konačan proizvod prstena je prsten, konačan proizvod mreža je mreža, itd.

Sada ćemo razmotriti proizvode proizvoljno velikih, dakle i beskonačnih familija algebri. Najpre se podsetimo da pod familijom nekih objekata podrazumevamo svako preslikavanje vida $\mathcal{S} = \langle S_i |\ i \in I\rangle$. U takvom slučaju elemente skupa $I$ nazivamo *indeksima*. Familiju $\langle S_i |\ i \in I\rangle$ kraće zapisujemo $S_i, i \in I$, pa i samo $S_i$ ako je jasno o kojem skupu indeksa $I$ je reč. Prema prethodnom, familija algebri je svako preslikavanje $\mathcal{A}$ oblika $\mathcal{A} = \langle A_i | i \in I\rangle$, gde su $A_i$ neke algebre istog jezika.

U definiciji proizvoda algebri važnu ulogu ima pojam uopštenog direktnog proizvoda familije skupova. Ova konstrukcija omogućava da se generalizuje pojam konačnog proizvoda skupova i na beskonačne familije skupova. Podsetimo se te konstrukcije. Neka je $X_i, i \in I$, proizvoljna familija skupova. *Uopšten direktan proizvod* skupova $X_i$ je skup

$$X = \{f \mid\ f : I \to \bigcup_{i \in I} X_i, \forall i \in I\, f(i) \in X_i\}$$

Ovako uveden proizvod skupova obeležavamo sa $\prod_{i \in I} X_i$. U vezi sa ovom konstrukcijom od interesa su sledeće dve napomene.

Najpre, ako je za svaki $i \in I$ skup $X_i$ neprazan, onda prema Aksiomi izbora postoji izborna funkcija $f$ za familiju $X_i$, tj. funkcija $f$ sa svojstvom $\forall i \in I\ f(i) \in X_i$. Drugim rečima ako je $X_i$, $i \in I$, familija nepraznih skupova onda je uopšteni proizvod $\prod_{i \in I} X_i$ takođe neprazan skup. Ova činjenica je zapravo jedna moguća forma iskazivanja Aksiome izbora, o čemu će biti više reči u sledećem poglavlju.

Dalje, primetimo da su elementi skupa $\prod_{i \in I} X_i$ funkcije, dok su s druge strane elementi konačnog direktnog proizvoda skupova, recimo $X_1 \times X_2 \times \ldots \times X_n$, $n$-torke. Ako za indeksni skup izaberemo $I = \{1, 2, \ldots, n\}$, nije teško proveriti da je preslikavanje $\tau : \prod_{i=1}^{n} A_i \to \prod_{i \in I} A_i$ definisano sa

$$\tau:\ (a_1, a_2, \ldots, a_n) \longmapsto \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \tag{1.8-1}$$

bijekcija između $X_1 \times X_2 \times \ldots \times X_n$ i $\prod_{i \in I} X_i$. Dakle, ukoliko se identifikuju $a = (a_1, a_2, \ldots, a_n)$ i $\tau(a)$, $a \in X_1 \times X_2 \times \ldots \times X_n$, onda su ove dve konstrukcije proizvoda iste. Otuda u konačnom slučaju ubuduće nećemo razlikovati ove dve vrste proizvoda, a pod direktnim proizvodom skupova podrazumevaćemo i uopšten proizvod skupova.

Sledećom definicijom generalizuje se konstrukcija konačnog proizvoda algebri na proizvoljne, pa i beskonačne familije algebri.

**1.8.6. Definicija** *Neka je $\langle \mathbf{A}_i \mid\ i \in I\rangle$ familija algebri jezika $L$. Uopšten direktan proizvod $\prod_{i \in I} \mathbf{A}_i$ algebri $\mathbf{A}_i$, je algebra $\mathbf{A}$ definisana na sledeći način:*

(1) *Domen je $A = \prod_{i \in I} A_i$,*
(2) *Ako je $c \in \mathrm{Const}_L$ tada je $c^{\mathbf{A}} = \langle c^{\mathbf{A}_i} \mid\ i \in I\rangle$.*
(3) *Neka je $F \in \mathrm{Fun}_L$ dužine $n$. Tada je za $f_1, f_2, \ldots, f_n \in A$*

$$F^{\mathbf{A}}(f_1, f_2, \ldots, f_n) = \langle F^{\mathbf{A}_i}(f_1(i), \ldots, f_n(i)) \mid\ i \in I\rangle.$$

**1.8.7 Primer** 1. Neka je $\mathbf{Z}_n = (Z_n, +_n, \cdot_n, \mathbf{0}, \mathbf{1})$, $n \in N^+$ i $\mathbf{S} = (S, +, \cdot, 0^{\mathbf{S}}, 1^{\mathbf{S}})$ gde je

$$\mathbf{S} = \mathbf{Z}_1 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \ldots = \prod_{n \in N^+} \mathbf{Z}_n.$$

Tada je domen ove algebre skup $S = \{f \mid\ f : N^+ \longrightarrow Z,\ \forall n \in N^+\, 0 \le f_n < n\}$, dok je $0^{\mathbf{S}} = (0, 0, 0, \ldots)$, $1^{\mathbf{S}} = (0, 1, 1, \ldots)$. Za $f, g \in S$ važi

$$(f + g)_n = f_n +_n g_n, \qquad (f \cdot g)_n = f_n \cdot_n g_n.$$

2. Ako za sve $i \in I$ važi $\mathbf{A}_i = \mathbf{A}$, tada se proizvod $\prod_{i\in I}\mathbf{A}_i$ naziva *stepenom* algebre $\mathbf{A}$ i obeležava se sa $\mathbf{A}^I$. Na primer, uzmimo da je skup prirodnih brojeva $N$ indeksni skup. Tada je stepen polja realnih brojeva, $\mathbf{R}$, $\mathbf{R}^N = (R^N, +, \cdot, \mathbf{0}, \mathbf{1})$, prsten realnih nizova. Primetimo da je u ovoj algebri za $f, g \in R^N$,

$$(f+g)_n = f_n + g_n, \quad (f\cdot g)_n = f_n \cdot g_n, \quad n \in N. \tag{1.8-2}$$

dok je $\mathbf{0} = (0,0,0,\dots)$ i $\mathbf{1} = (1,1,1,\dots)$. Slično, ako je skup $R$ realnih brojeva indeksni skup, onda je $\mathbf{R}^R$ prsten realnih funkcija.

Ako je $I$ konačan skup, na primer $I = \{1,2,...,n\}$, postavlja se pitanje da li su proizvodi algebri u smislu Definicije 1.8.1. i Definicije 1.8.6. jednaki, odnosno da li je

$$\prod_{i=1}^{n}\mathbf{A}_i = \prod_{i\in I}\mathbf{A}_i.$$

Sa algebarskog stanovišta možemo smatrati da ove algebre jesu jednake s obzirom da su izomorfne. Zaista, jedan izomorfizam ovih algebri je bijekcija $\tau$ uvedena u 1.8-1.

Da bismo to proverili, neka su $\mathbf{A}_i$ algebre jezika $L$ i neka su $\mathbf{A} = \prod_{i=1}^{n}\mathbf{A}_i$ i $\mathbf{B} = \prod_{i\in I}\mathbf{A}_i$. Tada je za simbol konstante $c \in L$, $c^{\mathbf{A}} = (c^{\mathbf{A}_1}, c^{\mathbf{A}_2}, ..., c^{\mathbf{A}_n})$ i $c^{\mathbf{B}} = \langle c^{\mathbf{A}_i} |\ i \in I\rangle$, odakle je $\tau(c^{\mathbf{A}}) = c^{\mathbf{B}}$. Pretpostavimo da je $F \in \mathrm{Fun}_L$ dužine $k$. Onda za $a_1, a_2, \dots, a_k \in \prod_{i=1}^{n} A_i$, $a_i = (a_{i1}, a_{i2}, ..., a_{in})$, $1 \le i \le k$, važi

$$F^{\mathbf{A}}(a_1, a_2, \dots, a_k) = (F^{\mathbf{A}_1}(a_{11}, a_{21}, \dots, a_{k1}), \dots, F^{\mathbf{A}_k}(a_{1n}, a_{2n}, \dots, a_{kn}))$$

odakle je

$$\tau(F^{\mathbf{A}}(a_1, a_2, \dots, a_k)) = \langle F^{\mathbf{A}_i}(\tau a_1(i), \dots, \tau a_k(i)) |\ i \in I\rangle$$

tj. $\tau : \mathbf{A} \to \mathbf{B}$ je homomorfizam.

Prema prethodnom možemo smatrati da su konačni proizvodi algebri poseban slučaj uopštenog proizvoda algebri. Otuda, kao i u slučaju proizvoda skupova, ubuduće uglavnom nećemo posebno razlikovati ove dve vrste proizvoda algebri, tj. koristićemo isti termin, direktan proizvod algebri, za obe konstrukcije.

Kao i u slučaju konačnih proizvoda skupova i kod uopštenih proizvoda uvode se projekcijske funkcije. Neka je $\langle A_i |\ i \in I\rangle$ familija nepraznih skupova. Projekcijske funkcije $\pi_i$, $i \in I$, proizvoda familije ovih skupova definišemo na sledeci način:

$$\pi_i : f \mapsto f(i), \quad f \in \textstyle\prod_{i\in I} A_i.$$

Dakle, $\pi_i : \prod_{i\in I} A_i \to A_i$. Primetimo da za $f, g \in \prod_{i\in I} A_i$ važi

$$f = g \Leftrightarrow (\forall i \in I)\ \pi_i(f) = \pi_i(g).$$

S obzirom da je $f = \langle \pi_i f |\ i \in I\rangle$, ponekad se $\pi_i(f)$ naziva *i-tom koordinatom* funkcije $f$.

Većina tvrđenja koja se odnose na konačne proizvode algebri prenose se na uopšten proizvod algebri. Na primer, analogon Teoreme 1.8.3 izgleda ovako:

**1.8.8 Teorema** *Neka je $\langle \mathbf{A}_i |\ i \in I\rangle$ neprazna familija algebri jezika $L$. Tada je za svaki $i \in I$ preslikavanje $\pi_i$ homomorfizam algebre $\prod_{i\in I}\mathbf{A}_i$ na algebru $\mathbf{A}_i$.*

**Dokaz** Neka je $\mathbf{A} = \prod_{i\in I}\mathbf{A}_i$. Tada je interpretacija simbola konstante c, $c^{\mathbf{A}} = \langle c^{\mathbf{A}_i} |\ i \in I\rangle$ odakle je $\pi_i(c^{\mathbf{A}}) = c^{\mathbf{A}_i}$. Dalje, ako je $F \in \mathrm{Fun}_L$ dužine $n$, onda je za $f_1, f_2, \ldots, f_n \in A$,

$$F^{\mathbf{A}}(f_1, f_2, \ldots, f_n) = \langle F^{\mathbf{A}_i}(f_1(i), \ldots, f_n(i)) |\ i \in I\rangle,$$

prema tome

$$\begin{aligned}\pi_i F^{\mathbf{A}}(f_1, f_2, \ldots, f_n) =& F^{\mathbf{A}_i}(f_1(i), \ldots, f_n(i)) = \\ & F^{\mathbf{A}_i}(\pi_i f_1, \pi_i f_2, \ldots, \pi_i f_n)\end{aligned}$$

Dalje, neka je $a \in A_i$. Kako su $A_j$ neprazni skupovi, prema Aksiomi izbora postoji funkcija $f : I \to \bigcup_j A_j$ tako da je $f(i) = a$ i za $j \neq i$, $f(j) \in A_j$. Tada je $\pi_i f = a$, tj. $\pi_i$ je homomorfizam iz algebre $\mathbf{A}$ na algebru $\mathbf{A}_i$. $\diamondsuit$

Na sličan način kao u posledicama 1.8.4 i 1.8.5 dokazuje se da važi sledeće tvrđenje.

**1.8.9 Posledica** Neka su $\mathbf{A}_i$, $i \in I$, algebre jezika $L$. Zakon $u = v$ jezika $L$ važi na svim algebrama $\mathbf{A}_i$ akko $u = v$ važi na proizvodu $\prod_{i\in I}\mathbf{A}_i$.

**1.8.10 Posledica** Svaki algebarski varijetet $\mathfrak{M}$ zatvoren je za proizvoljne proizvode algebri, tj. ako je za sve $i \in I$, $\mathbf{A}_i \in \mathfrak{M}$, tada je i $\prod_{i\in I}\mathbf{A}_i \in \mathfrak{M}$.

Shodno prethodnom razmatranju možemo zaista da govorimo o prstenu realnih nizova $\mathbf{R}^N$ i prstenu realnih funkcija $\mathbf{R}^R$ (Primer 1.8.7.). Naime, prsten $\mathbf{R}^N$ je prebrojiv stepen polja realnih brojeva, te je prema Posledici 1.8.10. $\mathbf{R}^N$ takođe prsten. Primetimo da $\mathbf{R}^N$ nije polje jer ovaj prsten ima delitelje nule, na primer za $f = \langle 1, 0, 1, 0, \ldots\rangle$ i $g = \langle 0, 1, 0, 1, \ldots\rangle$ važi $f \cdot g = \mathbf{0}$, mada je $f, g \neq \mathbf{0}$. Slično bismo pokazali da je i $\mathbf{R}^R$ prsten. S obzirom na Posledicu 1.8.10 ovi primeri istovremeno pokazuju da klasa svih polja nije algebarski varijetet. Dakle, ne postoji algebarska teorija (u smislu Definicije 1.4.2) koja bi opisivala tačno klasu svih polja.

**1.8.11 Primer** Svaki netrivijalan algebarski varijetet $\mathfrak{M}$ sadrži beskonačnu algebru.

**Dokaz** Neka je $\mathbf{A} \in \mathfrak{M}$ netrivijalna algebra. Tada je prema Posledici 1.8.9 za svaki neprazan skup $I$, $\mathbf{A}^I \in \mathfrak{M}$. Neka je $I$ beskonačan skup i $|I| = \mu$. Ako je $|A| = k$ tada važi $|A^I| = k^\mu \geq 2^\mu > \mu$, jer je $k \geq 2$. Prema tome $\mathfrak{M}$ sadrži ne samo beskonačnu algebru već algebre proizvoljno velike kardinalnosti.

Neka je $\mathfrak{M}$ varijetet algebri jezika $L$ i neka je $\mathbf{A}_i \in \mathfrak{M}$, $i \in I$. Proizvod $\mathbf{A} = \prod_{i\in I}\mathbf{A}_i$ ima sledeću zanimljivu osobinu: Ako je $\mathbf{B} \in \mathfrak{M}$ i $\tau_i : \mathbf{B} \to \mathbf{A}_i$, $i \in I$, tada postoji *jedinstven* homomorfizam $\tau : \mathbf{B} \to \mathbf{A}$ tako da sledeći dijagram komutira za svaki $i \in I$:

(D)
$$\begin{tikzcd} \mathbf{A} \arrow[r, "\pi_i"] & \mathbf{A}_i \\ & \mathbf{B} \arrow[u, "\tau_i"'] \arrow[ul, "\tau"] \end{tikzcd} \qquad \pi_i \circ \tau = \tau_i$$

Zaista, definišimo $\tau : B \to A$ ovako: $\tau(b) = \langle \tau_i(b) | \ i \in I \rangle$, $b \in B$. Nije teško proveriti da je $\tau$ homomorfizam iz $\mathbf{B}$ u $\mathbf{A}$ kao i da je $\pi_i \circ \tau = \tau_i$. Dalje, ako je $\tau' : B \to A$ bilo koje preslikavanje tako da je $\pi_i \circ \tau' = \tau_i$, $i \in I$, onda za svaki $i \in I$ važi

$$\pi_i(\tau'(b)) = \tau_i(b) = \pi_i(\tau(b))$$

odakle je $\tau'(b) = \tau(b)$, prema tome $\tau$ je jedinstveno preslikavanje za koje dijagram (D) komutira za svaki $i \in I$.

Ovo svojstvo dijagrama je karakteristična svojstvo direktnog proizvoda algebri nekog varijeteta, jer omogućava da se proizvod algebri u algebarskim varijetetima definiše (do na izomorfizam), ne pominjući eksplicitno Dekartov proizvod skupova. Naime, važi sledeće tvrđenje.

**1.8.12 Teorema** *Neka je* $\mathfrak{M}$ *varijetet algebri jezika* $L$ *i* $\mathbf{A}_i \in \mathfrak{M}$, $i \in I$. *Pretpostavimo da* $\mathbf{C} \in \mathfrak{M}$ *i* $\alpha_i : \mathbf{C} \to \mathbf{A}_i$, $i \in I$, *imaju sledeću osobinu:*

*Ako je* $\mathbf{B} \in \mathfrak{M}$ *i* $\tau_i : \mathbf{B} \to \mathbf{A}_i$, $i \in I$, *tada postoji jedinstven* $\tau : \mathbf{B} \to \mathbf{C}$ *takav da sledeći dijagram komutira za svaki* $i \in I$*:*

(P)
$$\begin{tikzcd} \mathbf{C} \arrow[r, "\alpha_i"] & \mathbf{A}_i \\ & \mathbf{B} \arrow[u, "\tau_i"'] \arrow[ul, phantom, "\tau"] \end{tikzcd} \qquad \alpha_i \circ \tau = \tau_i$$

*Tada* $C \cong \prod_{i \in I} \mathbf{A}_i$.

**Dokaz**

$$\begin{tikzcd} \prod_{i\in I} \mathbf{A}_i \arrow[r, "\pi_i"] & \mathbf{A}_i \\ & \mathbf{C} \arrow[u, "\alpha_i = \pi_i \circ \alpha"'] \arrow[ul, phantom, "\alpha"] \end{tikzcd} \qquad \begin{tikzcd} \mathbf{C} \arrow[r, "\alpha_i"] & \mathbf{A}_i \\ & \prod_{i\in I} \mathbf{A}_i \arrow[u, "\pi_i = \alpha_i \circ \pi"'] \arrow[ul, phantom, "\pi"] \end{tikzcd}$$

Dijagram 1.8-3 Dijagram 1.8-4

Primetimo da je $\prod_{i \in I} \mathbf{A}_i \in \mathfrak{M}$. Otuda prema osobini (D) direktnog proizvoda postoji homomorfizam $\alpha : \mathbf{C} \to \prod_{i \in I} \mathbf{A}_i$ tako da Dijagram 1.8-3 komutira za svaki $i \in I$. Slično, prema osobini (P) algebre $\mathbf{C}$ postoji homomorfizam $\pi : \prod_{i \in I} \mathbf{A}_i \to \mathbf{C}$ takav da Dijagram 1.8-4 komutira.

$$\begin{tikzcd} \mathbf{C} \arrow[r, "\alpha_i"] & \mathbf{A}_i \\ & \mathbf{C} \arrow[u, "\alpha_i"'] \arrow[ul, phantom, "\pi \circ \alpha"] \end{tikzcd} \qquad \begin{tikzcd} \mathbf{C} \arrow[r, "\alpha_i"] & \mathbf{A}_i \\ & \mathbf{C} \arrow[u, "\alpha_i = \alpha_i \circ i_C"'] \arrow[ul, phantom, "i_C"] \end{tikzcd}$$

Dijagram 1.8-5 Dijagram 1.8-6

Iz komutativnosti dijagrama 1.8-3 i 1.8-4 sledi da je i Dijagram 1.8-5 komutativan za svaki $i \in I$. Najzad, za identičko preslikavanje $i_C : C \to C$, Dijagram 1.8-6 takođe komutira. Uzimajući u obzir uslov jedinstvenosti preslikavanja $\tau$ u (P) sledi

$$\pi \circ \alpha = i_C. \tag{1}$$

Na sličan način koristeći jedinstvenost preslikavanja $\tau$ u svojstvu (D) direktnog proizvoda, nalazimo

$$\alpha \circ \pi = i_A, \qquad \text{gde je } A = \prod_{i \in I} A_i. \tag{2}$$

Iz (1) i (2) sledi $\alpha : \mathbf{C} \cong \prod_{i \in I} \mathbf{A}_i$. ♢

## 1.9 Generatori algebri

Neka je $\mathbf{A}$ algebra jezika $L$. Skup $X \subseteq A$ *generiše* algebru $\mathbf{A}$ ako i samo ako je

$$A = \{u^{\mathbf{A}}(a_1, a_2, \ldots, a_n) \mid u \in \mathrm{Term}_L,\ a_1, a_2, \ldots, a_n \in X, n \in N\}.$$

Dakle, ako skup $X \subseteq A$ generiše algebru $\mathbf{A}$ onda za svaki $a \in A$ postoji term $u(x_1, x_2, \ldots, x_n)$ jezika $L$ i $a_1, a_2, \ldots, a_n \in X$ takvi da je $a = u^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$. Elemente skupa $X$ nazivamo *generatorima* algebre $\mathbf{A}$ i u tom slučaju koristimo oznaku $\mathbf{A} = \langle X \rangle_{\mathbf{A}}$. Sledeće tvrđenje pokazuje da je homomorfizam u potpunosti određen svojim vrednostima na generatorskom skupu domena.

**1.9.1 Teorema** *Neka su $\mathbf{A}$ i $\mathbf{B}$ algebre jezika $L$ i pretpostavimo da $X \subseteq A$ generiše algebru $\mathbf{A}$. Ako su $f, g : \mathbf{A} \to \mathbf{B}$ homomorfizmi onda važi implikacija*

$$f|X = g|X \Rightarrow f = g.$$

**Dokaz** Pretpostavimo da je $f|X = g|X$ i neka je $a \in A$. Tada postoji term $u(x_1, x_2, \ldots, x_n) \in \mathrm{Term}_L$ i $a_1, a_2, \ldots, a_n \in A$ tako da je $a = u^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$. Tada prema Teoremi 1.6.1 važi

$$f(a) = u^{\mathbf{B}}(fa_1, fa_2, \ldots, fa_n) = u^{\mathbf{B}}(ga_1, ga_2, \ldots, ga_n) = g(a),$$

dakle $(\forall x \in A)\ f(a) = g(a)$, tj. $f = g$. ♢

**1.9.2 Primer** 1. Jedan primer generatorskog skupa aditivne grupe celih brojeva $\mathbf{Z} = (Z, +, -, 0)$ je $X = \{1\}$. Ako je $h$ homomorfizam grupe $\mathbf{Z}$ u neku grupu $\mathbf{G}$, onda je preslikavanje $h$ određeno vrednošću $h(1)$. Naime, ako je $a = h(1)$, onda je za bilo koji $n \in Z$, $h(n) = n \cdot h(1) = a \cdot n$. Ovde je za $n > 0$

$$a \cdot n = \underbrace{a + a + \cdots + a}_{n\text{-puta}}$$

dok je za $n < 0$,

$$a \cdot n = \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n\text{-puta}}.$$

Specijalno $\mathrm{End}(\mathbf{Z}) = \{\langle a \cdot x|\ x \in Z\rangle|\ a \in Z\}$ i nije teško videti da je

$$\mathbf{End}(\mathbf{Z}, \circ, i_Z) \cong (Z, \cdot, 1).$$

2. Prsten celih brojeva generiše bilo koji podskup $\{a, b\} \subseteq Z$ takav da je $\mathrm{NZD}(a, b) = 1$ ($\mathrm{NZD}(a, b)$ je najveći zajednički delilac brojeva $a$ i $b$). Ova činjenica sledi prema Bézoutovoj teoremi, da jednačina $ax + by = 1$ u tom slučaju ima rešenja po $x$ i $y$ u skupu $Z$. Dakle, $n = a(nx) + b(ny)$ za bilo koji $n \in Z$.

Vrednost terma $t$ u nekoj algebri $\mathbf{A}$ zavisi jedino od promenljivih koje se pojavljuju u $t$. Otuda se u izračunavanju vrednosti terma možemo ograničiti na skoro konstantne valuacije, tj. takve valuacije $\mu$ domena $A$ za koje postoji $n$ tako da za $i, j > n$, $\mu(i) = \mu(j)$. Zato uvodimo sledeći skup:

$$A_\infty = \{\mu|\ \mu : \mathrm{Var} \to A, \exists a \in A\, \exists n \in N\ \ \forall i > n\, \mu(i) = a\}$$

Primetimo da za proizvoljnu valuaciju $\sigma$ domena $A$ postoji $\mu \in A_\infty$ tako da je $t^{\mathbf{A}}[\sigma] = t^{\mathbf{A}}[\mu]$. Prema sledećem tvrđenju svaki podskup $X$ algebre $\mathbf{A}$ generiše podalgebru algebre $\mathbf{A}$.

**1.9.3 Teorema** *Neka je $\mathbf{A}$ algebra jezika $L$ i $X$ neprazan podskup skupa $A$. Tada postoji najmanja podalgebra $\mathbf{B} \subseteq \mathbf{A}$ koja sadrži $X$.*

**Dokaz** Dokazujemo da je

$$B = \{t^{\mathbf{A}}[\mu]|\ t \in \mathrm{Term}_L,\ \ \mu \in X_\infty\}$$

tražena podalgebra. Najpre dokažimo

(1) $B$ je podalgebra algebre $\mathbf{A}$.

Zaista, ako je $c \in \mathrm{Const}_L$ onda je $c$ i term jezika $L$, pa za bilo koju valuaciju $\mu \in X_\infty$ važi $c^{\mathbf{A}} = c^{\mathbf{A}}[\mu]$, odakle sledi $c^{\mathbf{A}} \in B$.

Dalje, pretpostavimo da je $F$ funkcijski znak dužine $n$, zatim $b_1, b_2, \ldots, b_n \in B$ i neka su $t_1, t_2, \ldots, t_n \in \mathrm{Term}_L$ i $\mu_1, \mu_2, \ldots, \mu_n \in X_\infty$ takvi da je $b_1 = t_1[\mu_1]$, $b_2 = t_2[\mu_2]$, $\ldots$, $b_n = t_n[\mu_n]$. Za odgovarajuću supstituciju promenljivih u termima $t_1, t_2, \ldots, t_n$, možemo naći terme $u_i$ i valuaciju $\mu \in X_\infty$ tako da je $t_i[\mu_i] = u_i[\mu]$. Zaista, neka su $x_{i1}, x_{i2}, \ldots, x_{ik_i}$ promenljive koje se pojavljuju u termima $t_i$, tj. $t_i = t_i(x_{i1}, x_{i2}, \ldots, x_{ik_i})$, $1 \le i \le n$. S obzirom da promenljivih ima beskonačno mnogo, možemo izabrati različite promenljive $y_{ij}$, $1 \le i \le n$, $1 \le j \le k_i$. Neka su $u_1, u_2, \ldots, u_n$ termi dobijeni iz terma $t_1, t_2, \ldots, t_n$ supstitucijom promenljivih $x_{ij}$ promenljivama $y_{ij}$ i neka je $\mu$ bilo koja valuacija iz $X_\infty$ takva da je $\mu(y_{ij}) = \mu_i(x_{ij})$, $1 \le i \le n$, $1 \le j \le k_i$. Tada je $t_i^{\mathbf{A}}[\mu_i] = u_i^{\mathbf{A}}[\mu]$, odakle je

$$F^{\mathbf{A}}(b_1, b_2, \ldots, b_n) = F^{\mathbf{A}}(u_1^{\mathbf{A}}[\mu], u_2^{\mathbf{A}}[\mu], \ldots, u_n^{\mathbf{A}}[\mu]) = t^{\mathbf{A}}[\mu]$$

gde je $t = F(u_1, u_2, \ldots, u_n)$. Prema tome $F^{\mathbf{A}}(b_1, b_2, \ldots, b_n) \in B$, pa s obzirom da je $X$ neprazan skup to je i $B$ neprazan, tj. (1) važi.

Sada ćemo dokazati

(2) Svaka podalgebra algebre $\mathbf{A}$ koja sadrži $X$ takođe sadrži $B$.

Zaista, pretpostavimo da je $C$ podalgebra algebre $\mathbf{A}$ i neka je $X \subseteq C$. S obzirom da je $C$ domen zatvoren za operacije algebre $\mathbf{A}$, to za bilo koji term $t$ jezika $L$ i valuaciju $\mu \in X_\infty$ važi $t[\mu] \in C$ (ova činjenica mogla bi se strogo dokazati indukcijom po složenosti terma), tj. $B \subseteq C$. $\diamondsuit$

Podalgebru $B$ iz ove teoreme takođe ćemo obeležavati sa $\langle X \rangle_{\mathbf{A}}$. Prema tvrđenju (2) prethodne teoreme imamo ovaj korolar.

**1.9.4 Posledica** $\langle X \rangle_{\mathbf{A}} = \bigcap \{B \mid \mathbf{B} \subseteq \mathbf{A},\ X \subseteq B\}$.

Ako je $\mathrm{Const}_L$ neprazan skup nije teško videti da se uslov nepraznosti skupa $X$ u prethodnoj teoremi može izostaviti. Naime, u tom slučaju podalgebra algebre $\mathbf{A}$ generisana praznim skupom je najmanja podalgebra koja sadrži skup $\{c^{\mathbf{A}} \mid c \in \mathrm{Const}_L\}$. Sada ćemo razmotriti detaljnije kardinalni broj domena algebre generisane skupom $X$ u zavisnosti od kardinalnih brojeva $|X|$ i $|L|$. U toj analizi koristićemo sledeća tvrđenja teorije skupova.

**1.9.5 Lema** *Neka je $X$ beskonačan skup i $k = |X|$. Tada važi:*
1. *$k^2 = k$. Ako je $\lambda > 0$ kardinalni broj onda $k \cdot \lambda = \max(k, \lambda)$.*
2. *Ako je $P_{\aleph_0}(X)$ skup svih konačnih podskupova skupa $X$, onda je $|P_{\aleph_0}(X)| = k$.*
3. *Ako je $P_\infty(X)$ skup svih konačnih nizova elemenata iz $X$, onda je takođe $|P_\infty(X)| = k$.*

Nije teško videti da su poslednja dva iskaza jednostavne posledice prvog tvrđenja. Ovde dajemo jedan neposredan dokaz drugog i trećeg tvrđenja Leme za prebrojive skupove. Očigledno je da se u dokazu bez gubljenja opštosti možemo ograničiti na skup prirodnih brojeva, tj. uzećemo $X = N$. Evo jednog nabrajanja svih konačnih podskupova skupa $N$:

(1.9-1) $$\underbrace{\underbrace{\emptyset, \{0\}, \{0,1\}, \{1\}}_{P(\{0,1\})}, \{1,2\}, \{0,1,2\}, \{0,2\}, \{2\}}_{P(\{0,1,2\})}, \{2,3\}, \{0,2,3\}, \ldots$$

Ovaj niz, označimo ga sa $\langle S_n \mid n \in N \rangle$, definisan je rekurentnom jednakošću

(1.9-2) $$S_{2^n+k} = S_{2^n-k-1} \cup \{n\}, \quad n \in N^+,\ 0 \le k < 2^n$$

Nije teško proveriti, na primer matematičkom indukcijom, da ovaj niz ima sledeće osobine:
- Svaka dva uzastopna člana niza razlikuju se za tačno jedan element.
- Prvih $2^{n+1}$ članova niza je jednoznačno nabrajanje svih podskupova skupa $\{0, 1, \ldots, n\}$.

Polazeći od ovih osobina niza $S_n$, imamo sledeće posledice.

**1.9.6 Posledica** Neka je $X$ prebrojiv skup. Tada su prebrojivi i ovi skupovi:

$$P_{\aleph_0}(X),\ \ P_{\aleph_0}(P_{\aleph_0}(X)),\ \ P_{\aleph_0}(P_{\aleph_0}(P_{\aleph_0}(X))).$$

Podsetimo se da je za proizvoljne elemente $x$, $y$ važi $(x,y)=\{\{x\},\{x,y\}\}$, kao i da je svaki konačan niz nekih elemenata oblika

$$\{(0,a_0),(1,a_1),(2,a_2),\dots,(k,a_k)\}.$$

Odavde odmah sledi

$$P_\infty(N)\subseteq P_{\aleph_0}(P_{\aleph_0}(P_{\aleph_0}(N)))$$

te je prema Posledici 1.9.6 skup svih konačnih nizova skupa prirodnih brojeva, ili bilo kojeg prebrojivog skupa, prebojiv skup.

Koristeći ovo tvrđenje možemo izbrojati terme prebrojivog jezika i skoro konstantne valuacije prebrojivog domena.

**1.9.7 Lema** 1. *Terma prebrojivog jezika ima prebrojivo mnogo, tj. važi implikacija:* $|L|\le\aleph_0\Rightarrow|\mathrm{Term}_L|\le\aleph_0$.
2. *Ako je $A$ najviše prebrojiv skup tada je i $A_\infty$ najviše prebrojiv skup.*

**Dokaz** (1) Primetimo da je svaki term jezika $L$ konačan niz elemenata (prebrojivog) skupa $L\cup\mathrm{Var}\cup\{(,),,\}$, te je $|\mathrm{Term}_L|\le\aleph_0$.

2. Svaki član $\mu\in A_\infty$ je oblika $\mu=\langle a_1,a_2,\dots,a_n,b,b,b,\dots\rangle$ za neki $n$, pa možemo uzeti da je $A_\infty=P_\infty(A)\times A$. Otuda je

$$|A_\infty|=|P_\infty(A)\times A|=|P_\infty(A)|\cdot|A|\le\aleph_0\cdot\aleph_0=\aleph_0 \qquad \diamondsuit$$

**1.9.8 Teorema** *Neka je $\mathbf{A}$ algebra najviše prebrojivog jezika $L$ i neka je $X\subseteq A$ najviše prebrojiv skup. Tada je $|\langle X\rangle_{\mathbf{A}}|\le\aleph_0$.*

**Dokaz** Preslikavanje $\sigma:\mathrm{Term}_L\times X_\infty\to\langle X\rangle_{\mathbf{A}}$ definisano sa

$$\sigma:(t,\mu)\mapsto t^{\mathbf{A}}[\mu],\qquad t\in\mathrm{Term}_L,\ \ \mu\in X_\infty,$$

je preslikavanje *na*, odakle sledi

$$|\langle X\rangle_{\mathbf{A}}|\le|\mathrm{Term}_L\times X_\infty|=|\mathrm{Term}_L|\cdot|X_\infty|\le\aleph_0\cdot\aleph_0=\aleph_0. \qquad \diamondsuit$$

Prethodnu teoremu dokazali smo koristeći poseban slučaj Leme 1.9.5, tj. slučaj $|X|=\aleph_0$. Koristeći ovu lemu bez ograničenja na sličan način kao u Teoremi 1.9.8 dokazuje se sledeća generalizacija Teoreme 1.9.8

**1.9.9 Teorema** *Neka je $\mathbf{A}$ algebra proizvoljnog jezika $L$ i $X\subseteq A$. Tada važi:*

$$|\langle X\rangle_{\mathbf{A}}|\le\max\{\aleph_0,|L|,|X|\}.$$

Prema sledećoj posledici svaki netrivijalan algebarski varijetet ima veoma mnogo neizomorfnih algebri. Podsetimo se da je algebarski varijetet netrivijalan ako sadrži algebru koja ima bar dva elementa.

**1.9.10 Teorema** *Neka je $L$ najviše prebrojiv algebarski jezik. Ako je varijetet $\mathfrak{M}$ neke teorije jezika $L$ netrivijalan, onda za svaki beskonačan kardinalni broj $k$, $\mathfrak{M}$ sadrži algebru kardinalnosti $k$.*

*Ako $\mathfrak{M}$ ima bar jednu netrivijalnu konačnu algebru, onda $\mathfrak{M}$ sadrži beskonačno mnogo neizomorfnih konačnih algebri.*

**Dokaz** Pretpostavimo da je $\mathbf{A} \in \mathfrak{M}$ netrivijalna algebra, $k$ beskonačan kardinalan broj, $S$ skup kardinalnosti $k$ i $\mathbf{B} = \mathbf{A}^S$. Primetimo da je domen algebre $\mathbf{B}$ Dekartov stepen $A^S$, kao i da za njega važi:

$$|B| = |A^S| = |A|^{|S|} \geq 2^{|S|}.$$

Prema Kantorovoj teoremi, $2^{|S|} > |S|$, tj. $|B| > k$ pa $B$ sadrži podskup od $k$ elemenata. Neka je $X \subseteq B$, $|X| = k$ i $\mathbf{C} = \langle X \rangle_{\mathbf{B}}$. Prema prethodnoj teoremi imamo $|C| = k$ i takođe ovaj niz implikacija

$$\mathbf{A} \in \mathfrak{M} \Rightarrow \mathbf{A}^S \in \mathfrak{M} \Rightarrow \mathbf{C} \in \mathfrak{M}.$$

Dakle, $\mathfrak{M}$ sadrži algebru kardinalnosti $k$, i to je $\mathbf{C}$.

Ako je $\mathbf{A} \in \mathfrak{M}$ konačna netrivijalna algebra, onda je za svaki prirodan broj $n$, $\mathbf{A}^n \in \mathfrak{M}$. S obzirom da su za različite $m$ i $n$ domeni $A^m$ i $A^n$ različite kardinalnosti, to algebre $\mathbf{A}^m$ i $\mathbf{A}^n$ nisu izomorfne, pa je ovim dokazan i drugi deo teoreme. $\diamondsuit$

Specijalan slučaj prethodne teoreme je da svaki netrivijalan algebarski varijetet prebrojivog jezika sadrži prebrojivu algebru. Dalje, ako je $\mathfrak{N}$ bilo koji podskup algebri netrivijalnog varijeteta $\mathfrak{M}$, onda postoji algebra $\mathbf{A} \in \mathfrak{M}$ koja nije izomorfna ni jednoj algebri iz $\mathfrak{N}$; to će biti bilo koja algebra $\mathbf{A}$ iz $\mathfrak{M}$ čija je kardinalnost veća od kardinalnosti svake od algebri iz $\mathfrak{N}$, a takva algebra postoji prema prethodnoj teoremi.

## 1.10 Kongruencije i količničke algebre

Do sada smo razmotrili nekoliko mogućnosti pomoću kojih se polazeći od date algebre mogu dobiti neke druge algebre. Takve konstrukcije su, na primer, Dekartov stepen algebre i podalgebre generisane podskupovima. Pojam *količničke algebre* je još jedna konstrukcija ove vrste. U definiciji količničkih algebri ključnu ulogu ima pojam relacije kongruencije tj. relacija ekvivalencije domena koja je saglasna sa operacijama algebre. Podsetimo se da je relacija ekvivalencija skupa $A$ binarna relacija $\sigma$ skupa $A$ koja zadovoljava ove uslove za sve $x, y, z \in A$:

1. $x\sigma x$, $\quad$ $\sigma$ je refleksivna relacija.
2. $x\sigma y \Rightarrow y\sigma x$, $\quad$ $\sigma$ je simetrična relacija.
3. $x\sigma y \wedge y\sigma z \Rightarrow x\sigma z$, $\quad$ $\sigma$ je tranzitivna relacija.

Podsetimo se da je $x\sigma y$ drugi zapis za $(x, y) \in \sigma$. U ovoj skupovnoj notaciji prethodni uslovi se mogu ovako izraziti. Relacija $\sigma \subseteq A^2$ je relacija ekvivalencije skupa $A$ akko

- $\triangle_A \subseteq \sigma$, $\quad$ uslov refleksivnosti za $\sigma$.

- $\sigma^{-1} = \sigma$, uslov simetričnosti za $\sigma$.
- $\sigma \circ \sigma \subseteq \sigma$, uslov tranzitivnosti za $\sigma$.

$\triangle_A = \{(x,x)|\ x \in A\}$ je *dijagonala* skupa $A$, $\sigma^{-1} = \{(x,y)|\ (y,x) \in \sigma\}$ je *inverzna relacija* relaciji $\sigma$, dok je simbol $\circ$ oznaka za *proizvod* (kompoziciju) relacija. Napomenimo da je proizvod binarnih relacija $\alpha \subseteq A \times B$ i $\beta \subseteq B \times C$ binarna relacija $\tau \subseteq A \times C$, u oznaci $\alpha \circ \beta$, gde je

$$\alpha \circ \beta = \{(x,y) \in A \times C|\ \exists u \in B\ \ (x,u) \in \alpha \wedge (u,y) \in \beta\}$$

Neka je $\sigma$ relacija ekvivalencije. *Klasa ekvivalencije* elementa $a \in A$ je $a/\sigma = \{x \in A|\ x\sigma a\}$, dok je količnički skup $A/\sigma = \{a/\sigma|\ a \in A\}$. Najzad, napomenimo da je uobičajeno da se simbol $\sim$ koristi kao oznaka za relaciju ekvivalencije.

**1.10.1 Primer** Neka je $f : A \longrightarrow B$ bilo koje preslikavanje. Tada možemo definisati sledeću relaciju ekvivalencije $\sim$ domena $A$

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

U ovom slučaju je $A/{\sim} = \{f^{-1}[\{b\}]|\ b \in f(A)\}$, gde je $f^{-1}[\{b\}] = \{x \in A|\ f(x) = b\}$, $b \in B$. Dakle, ako je $f$ preslikavanje *na*, onda je $A/{\sim} = \{f^{-1}[\{b\}]|\ b \in B\}$.

**1.10.2 Primer** Kongruencija po modulu prirodnog broja $m$, koja je definisana ekvivalencijom

$$x =_m y \Leftrightarrow m|x - y, \quad x, y \in Z$$

je relacija ekvivalencije skupa celih brojeva. Klasa ekvivalencije elementa $r \in Z$ je $r/{\sim} = \{km + r|\ k \in Z\}$. Ovaj skup obeležavamo takođe sa $mZ + r$. Ako je $m = 0$, tada se $=_n$ poklapa sa jednakošću i prema tome $r/{\sim} = \{r\}$. Ako je $m = 1$, tada je $=_n$ puna relacija, tj. svaka dva cela broja su u relaciji, dakle $r/{\sim} = Z$ za svaki ceo broj $r$. Ako je $m > 1$, tada ima konačno mnogo klasa ekvivalencija; to su $mZ, mZ + 1, \ldots, mZ + (m-1)$.

**1.10.3 Primer** Neka je $\mathfrak{M}$ algebarski varijetet jezika $L$ i neka je $u = v$ algebarski zakon jezika $L$. Ako za svaku algebru $\mathbf{A} \in \mathfrak{M}$ važi $\mathbf{A} \models u = v$, onda pišemo $\mathfrak{M} \models u = v$. Relacija $\sim$ definisana pomoću

$$u \sim v \ \text{ akko } \ \mathfrak{M} \models u = v, \quad u, v \in \mathrm{Term}_L,$$

je primer jedne relacije ekvivalencije skupa $\mathrm{Term}_L$.

U bliskoj vezi sa pojmom relacije ekvivalencije je pojam *particije*, ili *razbijanja* skupa.

**1.10.4 Definicija** *Mnoštvo skupova $\mathcal{X} = \{X_i|\ i \in I\}$ je particija ili razbijanje skupa $A$ akko su zadovoljeni sledeći uslovi:*

*1.* $\forall i \in I\ \ X_i \neq \emptyset$.
*2.* $\bigcup_{i \in I} X_i = A$.
*3.* $\forall i, j \in I\ \ i \neq j \Rightarrow X_i \cap X_j = \emptyset$.

Ako ne koristimo indekse, prema prethodnoj definiciji, $\mathcal{X}$ je particija domena $A$ akko $\mathcal{X}$ zadovoljava sledeće uslove:

$\forall X \in \mathcal{X}\ \ X \neq \emptyset$,

$\bigcup \mathcal{X} = A$,
$\forall X, Y \in \mathcal{X} \;\; X \neq Y \Rightarrow X \cap Y = \emptyset$.

Sledeća teorema ukazuje na postojanje bliske veze između pojmova relacije ekvivalencije i particije skupa.

**1.10.5 Teorema** 1. *Ako je $\sim$ relacija ekvivalencije skupa $A$, onda je $A/\sim$ particija skupa $A$.*
*2. Ako je $\mathcal{X}$ particija skupa $A$, onda je relacija $\sim$ skupa $A$ definisana pomoću*

$$x \sim y \Leftrightarrow (\exists X \in \mathcal{X}) \;\; x, y \in X, \qquad x, y \in A$$

*relacija ekvivalencije skupa $A$ i pritom je $A/\!\sim = \mathcal{X}$.*

**Dokaz** 1. Iz refleksivnosti relacije $\sim$ sledi $a \in a/\sim$, pa je ispunjen prvi uslov Definicije 1.10.4, a takođe i $A \subseteq \bigcup_{a\in A} a/\sim$. Iz $a/\sim \subseteq A$ sledi $\bigcup_{a\in A} a/\sim \subseteq A$, tj. ispunjen je i drugi uslov Definicije 1.10.4. Najzad, pretpostavimo da je $a/\sim \cap\, b/\sim \neq \emptyset$, i neka je $c \in a/\sim \cap\, b/\sim$, tj. $c \sim a$ i $c \sim b$, dakle i $a \sim b$. Iz $x \in a/\sim$ sledi $x \sim a$, pa prema uslovu tranzitivnosti za $\sim$, važi $x \sim b$, dakle $x \in b/\sim$, tj. $a/\sim \subseteq b/\sim$. Slično je $b/\sim \subseteq a/\sim$, dakle $a/\sim = b/\sim$, što znači da je ispunjen i treći uslov Definicije 1.10.4.

2. Iz uslova $\bigcup \mathcal{X} = A$ za proizvoljan $a \in A$ postoji $X \in \mathcal{X}$ tako da je $a \in X$, dakle važi $a \sim a$. Uslov simetričnosti za $\sim$ je očigledan, dok iz $a \sim b$, $b \sim c$ sledi da postoje $X, Y \in \mathcal{X}$ takvi da je $a, b \in X$, $b, c \in Y$, tj. $X \cap Y \neq \emptyset$. Prema tome $X = Y$, pa $a, c \in X$, tj. $a \sim c$, što znači da je $\sim$ i tranzitivna relacija.

Dalje, neka je $a \in X$. Za proizvoljan $b \in a/\sim$ postoji $Y \in \mathcal{X}$ tako da je $a, b \in Y$. Iz uslova disjunktnosti za članove iz $\mathcal{X}$, sledi $X = Y$ i $b \in X$. Dakle, pokazali smo da je $a/\sim \;\subseteq X$. Za bilo koji $c \in X$ iz uslova $a \in X$ sledi $a \sim c$, tj. $c \in a/\sim$, pa je $X \subseteq a/\sim$ i otuda $X = a/\sim$. Prema tome važi

(1) $$A/\sim \;\subseteq \mathcal{X}.$$

Ako je $X \in \mathcal{X}$, onda iz uslova nepraznosti članova mnoštva $\mathcal{X}$ možemo izabrati neki element $a \in X$ i prema prethodnom onda je $X = a/\sim$, dakle $\mathcal{X} \subseteq A/\sim$, što prema (1) daje $\mathcal{X} = A/\sim$. $\diamondsuit$

Važan pojam u vezi sa pojmom relacije ekvivalencije je *kanonsko preslikavanje* $k : A \to A/\sim$ koje se definiše na sledeći način: $k : a \mapsto a/\sim, \;\; a \in A$. Prema tome kanonsko preslikavanje svakom elementu domena $A$ pridružuje njegovu klasu ekvivalencije. Primetimo sledeća svojstva kanonskog preslikavanja:

- $k : A \xrightarrow{\text{na}} A/\sim$ .
- $a \sim b \Leftrightarrow k(a) = k(b), \quad a, b \in A$.

**1.10.6 Primer** Za relaciju ekvivalencije iz Primera 1.10.2 količnički skup je $Z/\!\sim = \{nZ + i \mid i \in Z_n\}$.

Jedan od fundamentalnih pojmova algebre je pojam *relacije kongruencije*. Naime, reč je o relacijama ekvivalencije neke algebre koje su saglasne sa operacijama te algebre. Evo i stroge definicije tog pojma.

**1.10.7 Definicija** *Neka je* $\mathbf{A}$ *algebra jezika* $L$. *Binarna relacija* $\sim$ *domena* $A$ *je kongruencija algebre* $\mathbf{A}$ *akko važi:*

1. Relacija $\sim$ je relacija ekvivalencije skupa $A$.
2. Relacija $\sim$ je *saglasna* sa operacijama algebre $\mathbf{A}$, tj. za sve $F \in \mathrm{Fun}_L$ dužine $k$ i sve $a_1, a_2, \ldots, a_k \in A$, $k$ važi:

$$a_1 \sim b_1 \wedge \cdots \wedge a_k \sim b_k \Rightarrow F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) \sim F^{\mathbf{A}}(b_1, b_2, \ldots, b_k).$$

Ako je $F^{\mathbf{A}}$ binarna operacija algebre $\mathbf{A}$, na primer $*$, tada se uslov iz definicije svodi na ovaj uslov:

$$a_1 \sim b_1 \wedge a_2 \sim b_2 \Rightarrow a_1 * a_2 \sim b_1 * b_2, \quad a_1, a_2, b_1, b_2 \in A$$

U slučaju kongruencija, $a/\sim$ naziva se *klasom kongruencije* elementa $a$.

**1.10.8 Primer** 1. Jednakost na skupu $A$ je kongruencija bilo koje algebre $\mathbf{A}$ sa domenom $A$. Primetimo da je $\sim = \Delta_A$, dok je $A/\sim = \{\{a\} |\ a \in A\}$.
2. Drugi primer kongruencije koja je takođe definisana na proizvoljnoj algebri je tzv. puna kongruencija, kod koje su svi elementi domena $A$ uzajamno kongruentni. U ovom slučaju je $\sim = A^2$, dok je $A/\sim = \{A\}$.

Algebre koje imaju jedino ove dve vrste kongruencija nazivaju se *prostim*.
3. Neka su $A$ i $B$ algebre jezika $L$ i neka je $h : \mathbf{A} \to \mathbf{B}$. Relacija $\sim$ definisana pomoću:

$$x \sim y \Leftrightarrow h(x) = h(y), \quad x, y \in A$$

je kongruencija algebre $\mathbf{A}$ (vidi Primer 1.10.1). Dokažimo da je relacija $\sim$ saglasna sa operacijama algebre $\mathbf{A}$. Neka je $F \in \mathrm{Fun}_L$ dužine $k$ i pretpostavimo da elementi $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ pripadaju domenu $A$. Tada:

$$a_1 \sim b_1, \ldots, a_k \sim b_k \Rightarrow ha_1 = hb_1, \ldots, ha_k = hb_k,$$

a s obzirom da je $h$ homomorfizam onda je

$$\begin{aligned} hF^{\mathbf{A}}(a_1, a_2, \ldots, a_k) &= F^{\mathbf{B}}(ha_1, ha_2, \ldots, ha_k) \\ &= F^{\mathbf{B}}(hb_1, hb_2, \ldots, hb_k) = hF^{\mathbf{A}}(a_1, a_2, \ldots, a_k) \end{aligned}$$

tj. $F^{\mathbf{A}}(a_1, a_2, \ldots, a_k) \sim F^{\mathbf{A}}(b_1, b_2, \ldots, b_k)$.

Ovu kongruenciju nazivamo *jezgrom* homomorfizma $h$, i obeležavamo je sa $\ker(h)$. Dakle $\ker(h) = \{(x, y) \in A^2 |\ hx = hy\}$. Videćemo kasnije da je *svaka* kongruencija algebre $\mathbf{A}$ ustvari jezgro nekog homomorfizma.
4. Relacija $=_n$ je kongruencija prstena celih brojeva (vidi Primer 1.10.2). Na primer, za $x_1, x_2, y_1, y_2 \in Z$ važi ovaj niz implikacija:

$$\begin{aligned} x_1 =_n y_1, x_2 =_n y_2 &\Rightarrow n | x_1 - y_1, x_2 - y_2 \\ &\Rightarrow n | (x_1 + x_2) - (y_1 + y_2) \Rightarrow x_1 + x_2 =_n y_1 + y_2, \end{aligned}$$

tj. $=_n$ saglasna je sa operacijom $+$ prstena $\mathbf{Z}$. Dalje, ako je $x_1 =_n y_1$, $x_2 =_n y_2$, onda za neke $\alpha, \beta \in Z$, $x_1 = y_1 + \alpha n$, $x_2 = y_2 + \beta n$, odakle je

$$x_1 x_2 - y_1 y_2 = n(y_1 \beta + y_2 \alpha + \alpha \beta n)$$

tj. $x_1x_2 =_n y_1y_2$, što znači da je $=_n$ saglasna i sa operacijom množenja u $\mathbf{Z}$.

Primetimo i ove osobine kongruencije $=_n$. Neka je $x$ ceo broj. Tada važi:

- $x/_{=_0} = \{x\}$, tj, $=_0$ je jednakost.
- $x/_{=_1} = Z$, tj, $=_1$ je puna kongruencija strukture $\mathbf{Z}$.
- Ako je $n > 1$ onda postoji jedinstven $k \in \{0, 1, \ldots, n-1\}$ tako da je $x =_n k$.

Zaista, neka je $k$ najmanji prirodan broj za koji postoji $q \in Z$ tako da je $x = qn + k$. Nije teško videti da je $0 \leq k < n$. Ako je $r \in \{0, 1, \ldots, n-1\}$ takav da je $r =_n x$, onda na osnovu tranzitivnosti relacije $=_n$ sledi $k =_n r$, tj. $n|k - r$, a s obzirom da je $|k - r| < n$, sledi $|k - r| = 0$, tj. $k = r$. Vidimo da je zapravo $k = \mathrm{rest}(x, n) = \rho_n(x)$. Prema tome, skup klasa kongruencija relacije $=_n$ za $n > 1$ izgleda ovako:

- $Z/_{=_n} = \{nZ, nZ + 1, \ldots, nZ + (n-1)\}$
- Lako je proveriti da su celi brojevi $x, y$ kongruentni po modulu $n$ akko imaju iste ostatke dobijene deljenjem sa $n$, tj. važi ekvivalencija

$$x =_n y \Leftrightarrow \mathrm{rest}(x, n) = \mathrm{rest}(y, n),$$

dakle $x =_n y \Leftrightarrow \rho_n(x) = \rho_n(y)$. Prema tome relacija $=_n$ je jezgro homomorfizma $\rho_n : \mathbf{Z} \to \mathbf{Z}_n$.

**1.10.9 Teorema** *Neka su $q_i$, $i \in I$, kongruencije algebre $\mathbf{A}$. Tada je $q = \bigcap_{i \in I} q_i$ takođe kongruencija algebre $\mathbf{A}$.*

**Dokaz** Neka su $x, y, z \in Z$. Tada važi:

(1) $q$ je refleksivna relacija:
$(x, x) \in q$ jer $(x, x) \in q_i$ za sve $i \in I$.

(2) $q$ je simetrična relacija:
$(x, y) \in q \Rightarrow \forall i \ (x, y) \in q_i \Rightarrow \forall i \ (y, x) \in q_i \Rightarrow (y, x) \in q$.

(3) Najzad, $q$ je tranzitivna relacija:

$$\begin{aligned}(x, y) \in q \wedge (y, z) \in q \Rightarrow & \forall i \ (x, y) \in q_i \wedge (y, z) \in q_i \\ \Rightarrow & \forall i \ (x, z) \in q_i \Rightarrow (x, z) \in q.\end{aligned}$$

(4) Dokažimo da je $q$ saglasna sa operacijama algebre. Neka je $F^{\mathbf{A}}$ operacija algebre $\mathbf{A}$ dužine $n$ i neka su $x_1, \ldots, x_n \in A$. Tada za $(x_1, y_1), \ldots, (x_n, y_n) \in q$ važi:

$$\begin{aligned}\forall i \ (x_1, y_1), \ldots, (x_n, y_n) \in q_i \Rightarrow & \forall i \ (F^{\mathbf{A}}(x_1, \ldots, x_n), F^{\mathbf{A}}(y_1, \ldots, y_n)) \in q_i \\ \Rightarrow & (F^{\mathbf{A}}(x_1, \ldots, x_n), F^{\mathbf{A}}(y_1, \ldots, y_n)) \in q.\end{aligned}$$ $\diamondsuit$

**1.10.10 Posledica** Ako je $r$ binarna relacija domena $A$ algebre $\mathbf{A}$, onda postoji najmanja kongruencija algebre $\mathbf{A}$ koja sadrži $r$.

**Dokaz** $q = \bigcap\{s| \ s$ je kongruencija algebre $\mathbf{A}$ i $r \subseteq s\}$ je najmanja kongruencija algebre $\mathbf{A}$ koja sadrži $r$. $\diamondsuit$

Neka je $\mathbf{A}$ algebra jezika $L$, i označimo sa $\mathcal{C}(\mathbf{A})$ skup svih kongruencija algebre $\mathbf{A}$; tada je $(\mathcal{C}(\mathbf{A}), \subseteq)$ parcijalno uređen skup. Neka su $p, q \in \mathcal{C}(\mathbf{A})$. S obzirom na Teoremu 1.10.9 važi $p \cap q = \inf\{p, q\}$, dok prema Posledici 1.10.10 u ovom parcijalno uređenom skupu postoji i $\sup\{p,q\}$, to je presek svih kongruencija algebre $\mathbf{A}$ koje sadrže $p$ i $q$. Nije teško videti da je $p\circ q=\sup\{p,q\}$. Zaista, kako je $\triangle_A\subseteq p,q$, onda $p=p\circ\triangle_A\subseteq p\circ q$, i slično $q\subseteq p\circ q$, tj. $p\circ q$ je gornja granica skupa $\{p,q\}$. Pretpostavimo da je $r$ neka gornja granica skupa $\{p,q\}$; tada $p,q\subseteq r$. Neka su $a,b\in A$ takvi da je $a(p\circ q)b$. Onda postoji $c\in A$ tako da je $a\,p\,c$ i $c\,q\,b$, dakle $a\,r\,c$ i $c\,r\,b$, pa $a(r\circ r)b$. S obzirom na tranzitivnost relacije $r$, sledi $r\circ r\subseteq r$, prema tome $a\,r\,b$, tj. $p\circ q\subseteq r$. Dakle $p\circ q$ je najmanja gornja granica skupa $\{p,q\}$. Prema prethodnom, algebra $(\mathcal{C}(\mathbf{A}),\circ,\cap)$ je mreža, tzv. *mreža kongruencija algebre* $\mathbf{A}$.

**1.10.11 Primer** Neka su $m$ i $n$ pozitivni prirodni brojevi i neka je $\sim$ presek kongruencija $=_m$ i $=_n$. Tada za cele brojeve $x,y$ važi

$$x\sim y\Leftrightarrow x=_m y\wedge x=_n y\Leftrightarrow m,n|\ x-y\Leftrightarrow \mathrm{NZS}(m,n)|\ x-y,$$

gde je $\mathrm{NZS}(m,n)$ najmanji zajednički sadržalac brojeva $m,n$. Dakle, relacija $\sim$ je $=_k$, gde je $k=\mathrm{NZS}(m,n)$.

Kongruencija $\sim$ algebre $\mathbf{A}$ određuje na prirodan način konstrukciju količničke algebre $\mathbf{A}/\!\sim$. Sledeća lema obezbeđuje korektnost definicije ovog pojma.

**1.10.12 Lema** *Neka je* $\mathbf{A}$ *algebra jezika* $L$, $F$ *funkcijski znak jezika* $L$ *dužine* $n$ *i* $\sim$ *relacija kongruencije algebra* $\mathbf{A}$. *Tada za sve* $a_1,\ldots,a_n,b_1,\ldots,b_n\in A$ *važi:*

$$a_1/\!\sim=b_1/\!\sim,\ldots,a_n/\!\sim=b_n/\!\sim\ \Rightarrow F^{\mathbf{A}}(a_1,\ldots,a_n)/\!\sim=F^{\mathbf{A}}(b_1,\ldots,b_n)/\!\sim$$

**Dokaz** Ako je za sve $1\le i\le n$, $a_i/\!\sim=b_i/\!\sim$, onda je takođe za sve $1\le i\le n$, $a_i\sim b_i$, pa kako je $\sim$ kongruencija, to je $F^{\mathbf{A}}(a_1,\ldots,a_n)\sim F^{\mathbf{A}}(b_1,\ldots,b_n)$, odakle sledi $F^{\mathbf{A}}(a_1,\ldots,a_n)/\!\sim=F^{\mathbf{A}}(b_1,\ldots,b_n)/\!\sim$. ♢

**1.10.13 Definicija** *Neka je* $\mathbf{A}$ *algebra jezika* $L$ *i pretpostavimo da je* $\sim$ *kongruencija algebre* $\mathbf{A}$. *Količnička algebra algebre* $\mathbf{A}$ *po kongruenciji* $\sim$ *je algebra* $\mathbf{A}/\!\sim$ *jezika* $L$ *kod koje su domen i operacije definisani na sledeći način:*

(1) *Domen je* $A/\!\sim$.
(2) *Ako je* $c\in\mathrm{Const}_L$, *onda je* $c^{\mathbf{A}/\sim}=c^{\mathbf{A}}/\!\sim$.
(3) *Ako je* $F\in\mathrm{Fun}_L$ *dužine* $n$ *i* $a_1,\ldots,a_n\in A$, *onda je*

$$F^{\mathbf{A}/\sim}(a_1/\!\sim,\ldots,a_n/\!\sim)=F^{\mathbf{A}}(a_1,\ldots,a_n)/\!\sim.$$

Definicija količničke algebre je korektna jer prema prethodnoj lemi vidimo da vrednost operacije $F^{\mathbf{A}/\sim}$ ne zavisi od izbora predstavnika iz klasa ekvivalencija $a_i/\!\sim$.

**1.10.14 Teorema** *Neka je* $\mathbf{A}$ *algebra jezika* $L$ *i* $\sim$ *kongruencija algebre* $\mathbf{A}$. *Tada je* $\mathbf{A}/\!\sim$ *homomorfna slika algebre* $\mathbf{A}$.

Dokaz Neka je $k:A\longrightarrow A/\!\sim$ kanonsko preslikavanje, tj. $k:x\mapsto x/\!\sim$, $x\in A$. Dokazujemo da je $k:\mathbf{A}\xrightarrow{\text{na}}\mathbf{A}/\!\sim$

Zaista, ako je $c\in\mathrm{Const}_L$, onda je $k(c^{\mathbf{A}})=c^{\mathbf{A}}/\!\sim=c^{\mathbf{A}/\sim}$.

Ako je $F \in L$ funkcijski znak dužine $n$, i $a_1, \ldots, a_n \in A$, onda je

$$\begin{aligned} k(F^{\mathbf{A}}(a_1, \ldots, a_n)) &= F^{\mathbf{A}}(a_1, \ldots, a_n)/\sim \\ &= F^{\mathbf{A}/\sim}(a_1/\sim, \ldots, a_n/\sim) \\ &= F^{\mathbf{A}/\sim}(ka_1, \ldots, ka_n). \end{aligned}$$

Dakle, $k$ je homomorfizam iz algebre $\mathbf{A}$ u algebru $\mathbf{A}/\sim$. S obzirom da je svaki element domena $A/\sim$ oblika $a/\sim = k(a)$, to je $k$ epimorfizam. $\diamondsuit$

**1.10.15 Posledica** Algebarski varijeteti zatvoreni su za konstrukciju količničkih algebri, tj. ako je $\mathfrak{M}$ algebarski varijetet onda

$$\mathbf{A} \in \mathfrak{M} \Rightarrow \mathbf{A}/\sim \in \mathfrak{M}.$$

**1.10.16 Primer** 1. Neka su $\mathbf{A}$ i $\mathbf{B}$ algebre algebarskog varijeteta $\mathfrak{M}$ i neka je $h : \mathbf{A} \to \mathbf{B}$. Tada je $\mathbf{A}/\ker(h) \in \mathfrak{M}$.
2. Neka je $\sim$ kongruencija algebre $\mathbf{A}$ i $k : \mathbf{A} \to \mathbf{A}/\sim$ kanonski homomorfizam. Tada za sve $x, y \in A$ važi $x \sim y$ akko $k(x) = k(y)$, tj. $\sim$ je jezgro homomorfizma $k$ (videti napomenu u Primeru 1.10.8.3).

**1.10.17 Primer** Neka je $\rho_n : \mathbf{Z} \to \mathbf{Z}_n$ homomorfizam iz Primera 1.5.3. Tada je $=_n$ jezgro homomorfizma $\rho_n$, dakle $Z_n/\ker(\rho_n) = Z_n/_{=_n} = \{nZ, nZ+1, \ldots, nZ+(n-1)\}$. Za operacije količničke algebre $\mathbf{Z}_n/_{=_n} = (Z_n/_{=_n}, \oplus, \odot, \mathbf{0}, \mathbf{1})$ i $0 \leq a, b < n$ važi

$$(nZ+a) \oplus (nZ+b) = nZ + (a +_n b), \quad (nZ+a) \odot (nZ+b) = nZ + (a \cdot_n b),$$

dok je $\mathbf{0} = nZ$ i $\mathbf{1} = nZ + 1$.

U daljem izlaganju takođe ćemo koristiti sledeće tvrđenje koje se odnosi na binarne operacije i kongruencije.

**1.10.18 Lema** *Neka je $A$ neprazan skup i neka je $\sim$ relacija ekvivalencije domena $A$. Ako je $*$ binarna operacija domena $A$ i ako važi:*

$$x \sim y \Rightarrow a * x \sim a * y, \;\; x * a \sim y * a, \quad a, x, y \in A$$

*tada je $\sim$ saglasna sa $*$.*

**Dokaz** Neka su $x_1, y_1, x_2, y_2 \in A$, i pretpostavimo $x_1 \sim y_1$, $x_2 \sim y_2$. Tada,

$$x_1 * x_2 \sim y_1 * x_2, \quad y_1 * x_2 \sim y_1 * y_2$$

odakle nalazimo $x_1 * x_2 \sim y_1 * y_2$. $\diamondsuit$

Neka je $h : \mathbf{A} \to \mathbf{B}$ homomorfizam. Nije teško videti da je $h(A)$ podalgebra algebre $\mathbf{B}$, i tu ćemo algebru označiti sa $h\mathbf{A}$. Homomorfizam $h$ može se razložiti na proizvod jednog epimorfizma, jednog izomorfizma i jednog monomorfizma. To tvrdi sledeća teorema.

**1.10.19 *Teorema o razlaganju homomorfizma*** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *algebre jezika* $L$*, neka je* $h : \mathbf{A} \to \mathbf{B}$ *homomorfizam i neka je* $k : \mathbf{A} \to \mathbf{A}/\mathrm{ker}(h)$ *kanonski homomorfizam. Tada je inkluziono preslikavanje* $i : x \mapsto x, x \in h(A)$*, homomorfizam iz algebre* $h\mathbf{A}$ *u algebru* $\mathbf{B}$ *i postoji izomorfizam* $h' : \mathbf{A}/\mathrm{ker}(h) \cong h\mathbf{A}$ *tako da je* $h = i \circ h' \circ k$*. Drugim rečima (D) je korektno definisan i komutativan dijagram.*

(D)
$$\begin{tikzcd} \mathbf{A} \arrow[r, "h"] \arrow[d, "k"] & \mathbf{B} \\ \mathbf{A}/\mathrm{ker}(h) \arrow[r, "h'"] & h\mathbf{A} \arrow[u, "i"] \end{tikzcd}$$

Razlaganje homomorfizma $h$

$$h = i \circ h' \circ k$$

**Dokaz** S obzirom da je $h\mathbf{A} \subseteq \mathbf{B}$, prema Teoremi 1.7.3 inkluziono preslikavanje $i : h\mathbf{A} \to \mathbf{B}$ je utapanje. Dalje, označimo sa $\sim$ kongruenciju $\mathrm{ker}(h)$, tj. $x \sim y \Leftrightarrow h(x) = h(y)$ za sve $x, y \in A$. Dakle, $k(x) = x/\!\sim$ za $x \in A$. Najzad definišimo preslikavanje $h' : A/\!\sim \to h(A)$ pomoću $h' : x/\!\sim \mapsto h(x), x \in A$. S obzirom na

$$x/\!\sim = y/\!\sim \;\Leftrightarrow x \sim y \Leftrightarrow h(x) = h(y)$$

odmah nalazimo da je $h'$ dobro definisano i $1-1$ preslikavanje. Dalje,

$$(i \circ h' \circ k)(x) = (i \circ h')(k(x)) = (i \circ h')(x/\!\sim) = i(h'(x/\!\sim)) = i(h(x)) = h(x),$$

pa $h = i \circ h' \circ k$. Dokažimo da je $h' : \mathbf{A}/\mathrm{ker}(h) \cong h\mathbf{A}$. Ako je $c$ simbol konstante jezika $L$, onda $h'(c^{\mathbf{A}/\sim}) = h(c^{\mathbf{A}}) = c^{\mathbf{B}}$. Neka je $F \in L$ funkcijski znak dužine $n$. S obzirom da je za $a_1, a_2, \ldots, a_n \in A$:

$$F^{\mathbf{A}/\sim}(a_1/\!\sim, a_2/\!\sim, \ldots, a_n/\!\sim) = F^{\mathbf{A}}(a_1, a_2, \ldots, a_n)/\!\sim,$$

imamo

$$\begin{aligned} &h'(F^{\mathbf{A}/\sim}(a_1/\!\sim, a_2/\!\sim, \ldots, a_n/\!\sim)) = h(F^{\mathbf{A}}(a_1, a_2, \ldots, a_n)) = \\ &\quad F^{\mathbf{B}}(ha_1, ha_2, \ldots, ha_n) = F^{\mathbf{B}}(h'(a_1/\!\sim), h'(a_2/\!\sim), \ldots, h'(a_n/\!\sim)). \end{aligned}$$

Dakle $h'$ je utapanje algebre $\mathbf{A}/\!\sim$ u algebru $\mathbf{B}$. Kako je $h'(A/\!\sim) = \{h(x) | \, x \in A\} = h(A)$, to je $h' : \mathbf{A}/\!\sim \,\cong h\mathbf{A}$. $\diamondsuit$

**1.10.20 Primer** Neka je $n \in N$ i $f : \mathbf{Z} \to \mathbf{Z}_n$ homomorfizam iz prstena celih brojeva $\mathbf{Z}$ u prsten ostataka $\mathbf{Z}_n$, gde je $f(x) = \mathrm{rest}(x, n)$, $x \in Z$, funkcija ostatka. Tada je $=_n$ jezgro homomorfizma $f$, dok je $f(Z) = Z_n$, a $f' : x/\!=_n \mapsto \mathrm{rest}(x, n)$, $x \in Z$. Dakle, razlaganje homomorfizma $f$ izgleda ovako:

$$\begin{tikzcd} \mathbf{Z} \arrow[r, "f"] \arrow[d, "k"] & \mathbf{Z}_n \\ \mathbf{Z}/\!=_n \arrow[r, "f'"] & \mathbf{Z}_n \arrow[u, "i_{Z_n}"] \end{tikzcd} \qquad f = i_{Z_n} \circ f' \circ k$$

# Zadaci

**1.1** Neka je uređen par $(x, y)$ elemenata $x, y$ definisan kao u Primeru 1.1.10. Dokazati da važi: $(x, y) = (x', y') \Rightarrow x = x', y = y'$.

**1.2** Proveriti da je algebra $\mathbf{A}$ monoid, gde:
**a.** $\mathbf{A} = (S^S, \circ, i_A)$, operacija $\circ$ je slaganje funkcija i $i_A : x \mapsto x$, $x \in A$.
**b.** $\mathbf{A} = (M_n, \cdot, I)$, $M_n$ je skup kvadratnih matrica reda $n$ nad nekim poljem, $I$ je identička matrica i $\cdot$ je operacija množenja matrica.
**c.** $\mathbf{A} = (S^*, \cdot, e)$, gde je $S^*$ skup reči nad nekom azbukom $S$, $\cdot$ je operacija dopisivanja (konkatenacija) reči i $e$ je prazna reč.

**1.3** Proveriti da je algebra $\mathbf{A}$ grupa, gde:
**a.** $\mathbf{A} = (\mathbf{P}X, \triangle, ^{-1}, \emptyset)$, $U \triangle V$ je simetrična razlika skupova $U$ i $V$, $U^{-1} = U$.
**b.** $\mathbf{A} = (A, \cdot, ^{-1}, 1)$, gde je $A = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \,|\, x, y, z \in Q, x^2 + y^2 + z^2 \neq 0\}$.
**c.** $\mathbf{A} = (S_X, \circ, ^{-1}, i_X)$, $S_X = \{f \,|\, f : X \xrightarrow[\text{1-1}]{\text{na}} X\}$, i $\circ$ je slaganje fukcija.

**1.4** Proveriti da je algebra $\mathbf{A}$ prsten sa jedinicom, gde:
**a.** $\mathbf{A} = (P, +, \cdot, 0, 1)$, gde je $P$ skup svih kompleksnih brojeva koji se mogu konstruisati u kompleksnoj ravni uz pomoć lenjira i šestara, pretpostavljajući da se jedinična duž može konstruisati, dok su $+$ i $\cdot$ uobičajene operacije sabiranja i moženja kompleksnih brojeva. **b.** $\mathbf{A} = (\mathbf{P}X, \triangle, \cap, \emptyset, X)$.
**c.** $\mathbf{A} = (M_n, +, \cdot, \mathbf{0}, I)$, $M_n$ je skup kvadratnih matrica reda $n$ nad nekim poljem, dok su $+$ i $\cdot$ uobičajene matrične operacije, $I$ je jedinična matrica reda $n$.

**1.5** Proveriti da je algebra $\mathbf{A}$ Bulova algebra, gde:
**a.** $\mathbf{A}$ je iskazna algebra $(\{0, 1\}, \vee, \wedge, ', 0, 1)$. **b.** $\mathbf{A} = (\mathbf{P}X, \cup, \cap, ^c, \emptyset, X)$.
**c.** $\mathbf{A} = (S, \cup, \cap, ^c, \emptyset, X)$, $S$ je mnoštvo svih otvoreno–zatvorenih podskupova nekog topološkog prostora $X$.
**d.** $\mathbf{A} = (S, \cup, \cap, ^{-1}, \emptyset, X)$, $S$ je mnoštvo svih regularno otvorenih podskupova nekog topološkog prostora $X$, a za $U^{-1}$ se uzima unutrašnjost skupa $U^c$. (Podskup $U$ topološkog prostora $X$ je *regularno otvoren* akko je jednak unutrašnjosti svog zatvorenja).

**1.6** (*Term algebra*) Neka je $L = \{F_1, F_2, \dots, F_m, c_1, c_2, \dots, c_n\}$ algebarski jezik. Dokazati da je $(\mathrm{Term}_L, f_1, f_2, \dots, f_m, c_1, c_2, \dots, c_n)$ algebra jezika $L$ ako je:
$f_i(t_1, t_2, \dots, t_{k_i}) = F_i(t_1, t_2, \dots, t_{k_i})$, $1 \leq i \leq m$, $k_i = \mathrm{ar}(f_i)$.

**1.7** Neka je $\mathbf{G}$ grupoid sa neutralnim elementom. Dokazati da $\mathbf{G}$ sadrži maksimalan podgrupoid $S$ koji:
**a.** zadovoljava komutativan zakon, **b.** zadovoljava asocijativan zakon,
**c.** zadovoljava i asocijativan i komutativan zakon.

**1.8*** Algebarski zakon $u = v$ jezika $L$ je *netrivijalan* ako su termi $u$ i $v$ različiti. Dokazati da svaka konačna algebra jezika $L$, kod kojeg je $\mathrm{Fun}_L \neq \emptyset$, zadovoljava neki netrivijalan zakon.

**1.9** Neka je $\mathbf{M} = (M, \vee, \wedge)$ mreža, i neka je $\leq$ binarna relacija domena $M$ definisana pomoću $x \leq y \Leftrightarrow x = x \wedge y$. Dokazati da je **a.** $(M, \leq)$ parcijalno uređen skup, **b.** $x \leq y$ akko $y = x \vee y$, **c.** $x \vee y = \sup\{x, y\}$, $x \wedge y = \inf\{x, y\}$, kao i **d.** $(x \vee y) \wedge z \geq (x \wedge z) \vee (y \wedge z)$.

**1.10** Dokazati da je $(N, \mathrm{NZS}, \mathrm{NZD})$ mreža. Dokazati da je relacija $\leq$ definisana u prethodnom zadatku zapravo relacija deljivosti. Dokazati da je 1 najmanji, a 0 najveći element ove mreže u odnosu na to uređenje.

**1.11*** Neka je $\mathbf{A} = (A, \vee, \wedge)$ mreža. Dokazati da su sledeća tri uslova ekvivalentna:
**a.** Za sve $x, y, z \in A$ važi: iz $x \wedge y \leq z, x \leq y \vee z$ sledi $x \leq z$,
**b.** Za sve $x, y, z \in A$ važi $(x \vee y) \wedge z \leq (x \wedge z) \vee y$,
**c.** Mreža $\mathbf{A}$ je distributivna.

**1.12** Neka je $\mathbf{A}$ komutativna grupa i neka je $\mathbf{EndA} = (\mathrm{End}\mathbf{A}, +, \circ, \mathbf{0}, i_A)$, gde je $(\forall x \in A)\mathbf{0}(x) = 0$, $(\forall f, g \in \mathrm{End}A)(\forall x \in A)(f+g)(x) = f(x) +^{\mathbf{A}} g(x)$. Dokazati da je $\mathbf{EndA}$ prsten sa jedinicom.

**1.13** Neka je $(G, \cdot, 1)$ monoid. Algebru $\mathbf{A} = (A, f_a)_{a \in A}$ definišemo na sledeći način: $A = G$, i za svako $a \in A$, $f_a : A \to A$ je desna translacija, tj. $\forall x \in A\, f_a(x) = x \cdot a$. Slično definišemo levu translaciju $h_a : A \to A$, gde $\forall x \in A\, h_a(x) = a \cdot x$. Dokazati: **a.** Za sve $a \in A$, $h_a$ je endomorfizam algebra $\mathbf{A}$.
**b.** $(\mathrm{End}\mathbf{A}, \circ, i_A) \cong (G, \cdot, 1)$.

**1.14** Neka su $f : X \to Y$ i $g : X' \to Y'$ proizvoljna preslikavanja. *Dekartov proizvod* preslikavanja $f$ i $g$ je funkcija $h : X \times X' \to Y \times Y'$ definisana pomoću $h(x, x') = (f(x), g(x'))$. Ovo preslikavanje označavamo i sa $(f, g)$. Neka su $\mathbf{A}, \mathbf{A}', \mathbf{B}, \mathbf{B}'$ algebre jezika $L$, i neka su $f : \mathbf{A} \to \mathbf{A}'$, $g : \mathbf{B} \to \mathbf{B}'$. Dokazati da je $(f, g)$ homomorfizam iz algebre $\mathbf{A} \times \mathbf{A}'$ u algebru $\mathbf{B} \times \mathbf{B}'$.

**1.15** Neka su $\mathbf{A}$ i $\mathbf{B}$ algebre jezika $L$. Dokazati da postoji monomorfizam grupe $\mathbf{AutA} \times \mathbf{AutB}$ u $\mathbf{Aut}(\mathbf{A} \times \mathbf{B})$.

**1.16** Neka su $\mathbf{A}_i$, $\mathbf{B}_i$ algebre jezika $L$, $i \in I$. Dokazati:
**a.** Ako je za svaki $i \in I$, algebra $\mathbf{B}_i$ homomorfna slika algebre $\mathbf{A}_i$, tada je $\prod_{i \in I} \mathbf{B}_i$ homomorfna slika algebre $\prod_{i \in I} \mathbf{A}_i$.
**b.** Ako je za sve $i \in I$, $\mathbf{A}_i \cong \mathbf{B}_i$, tada $\prod_{i \in I} \mathbf{A}_i \cong \prod_{i \in I} \mathbf{B}_i$.

**1.17** Navesti primer beskonačne algebre (grupoida) $\mathbf{A}$ tako da za svaki prirodan broj $n > 0$ važi $\mathbf{A}^n \cong \mathbf{A}$.

**1.18** Netrivijalna algebra $\mathbf{A}$ je *dekompozibilna* ako postoji algebra $\mathbf{B}$ tako da je $\mathbf{A} \cong \mathbf{B} \times \mathbf{B}$. Dokazati da svaka dekomposibilna algebra ima netrivijalan (tj. različit od $i_A$) automorfizam.

**1.19** Neka je $\mathbf{A}$ netrivijalna algebra. Dokazati da je $\mathrm{Aut}\mathbf{A}^N$ beskonačan skup, tačnije $|\mathrm{Aut}\mathbf{A}^N| \geq 2^{\aleph_0}$.

**1.20** **a.** Neka je $n \in N^+$. Dokazati da postoji grupoid koji ima tačno $n$ elemenata i koji nema pravi podgrupoid.
**b.** Dokazati da postoji prebrojiv grupoid koji nema pravi podgrupoid.

**c.** Dokazati da svaka neprebrojiva algebra najviše prebrojivog jezika sadrži pravu podalgebru.

**1.21** Dokazati da je svaka beskonačna grupa generisana jednim elementom izomorfna aditivnoj grupi celih brojeva.

**1.22** Dokazati da aditivna grupa racionalnih brojeva $(Q, +, -, 0)$ nije konačno generisana.

**1.23** Neka je $\mathbf{A}$ konačno generisana algebra najviše prebrojivog jezika. Dokazati da je End$\mathbf{A}$ najviše prebrojiv skup.

**1.24*** Neka je $\mathbf{A}$ konačno generisana algebra i $\mathbf{B}$ prava podalgebra algebre $\mathbf{A}$ (dakle $B \neq A$). Dokazati da postoji maksimalna prava podalgebra $\mathbf{C} \subseteq \mathbf{A}$ koja sadrži $\mathbf{B}$.

**1.25*** Neka je $\mathbf{A}$ prebrojiva algebra konačnog jezika. Dokazati da je $|\mathrm{Aut}\mathbf{A}| \leq \aleph_0$ ili $|\mathrm{Aut}\mathbf{A}| = 2^{\aleph_0}$.

**1.26** Dokazati da nabrajanje 1.9.–1 konačnih podskupova prirodnih brojeva ima pobrojana svojstva kod 1.9.-2.

**1.27** Neka je $p_n$ broj svih relacija ekvivalencije skupa od $n$ elemenata. Dokazati da važi $p_{n+1} = \sum_{i=0}^{n} \binom{n}{i} p_i$, gde $p_0 = 1$. Izračunati $p_{100}$.

**1.28** Dokazati da je svaka kongruencija prstena celih brojeva oblika $=_n$ za neki prirodan broj $n$.

**1.29** Dokazati da je mreža kongruencija prstena celih brojeva izomorfna mreži $(N, \mathrm{NZD}, \mathrm{NZS})$.

**1.30** Neka je $S$ skup algebri jezika $L$ takav da je za sve $A, B \in S$, $A \times B \in S$. Dokazati da je $\cong$ kongruencija grupoida $(S, \times)$ i da je $(S, \times)/\cong$ komutativna semigrupa.

**1.31** Dokazati da je proizvod $q \circ r$ kongruencija $q, r$ algebre $\mathbf{A}$, takođe kongruencija ako i samo ako važi $q \circ r = r \circ q$.

**1.32** **a.** Neka je $\mathbf{M} = (M, \vee, \wedge)$ mreža. Dokazati da je $\mathbf{M}$ modularna mreža akko u $\mathbf{M}$ važi: $y \leq z \Rightarrow (x \vee y) \wedge z \leq (x \wedge z) \vee y$.
**b.** Neka je $\mathbf{A}$ algebra sa svojstvom: Za bilo koje dve kongruencije $q, r$ važi $q \circ r = r \circ q$. Dokazati da je $(\mathcal{Q}_A, \circ, \wedge)$ modularna mreža, gde je $\mathcal{Q}_A$ skup svih kongruencija algebre $\mathbf{A}$.

**1.33** Neka je $\langle \mathbf{A}_i | \, i \in N \rangle$ proizvoljna familija algebri jezika $L$ i pretpostavimo $\mathcal{S} \subseteq \mathbf{P}N$, gde je $N$ skup prirodnih brojeva. Dalje, neka je za $f, g \in \prod_{i \in N} A_i$ relacija $\sim$ definisana pomoću $f \sim g \Leftrightarrow \{i \in N | \, f(i) = g(i)\} \in \mathcal{S}$. Dokazati da je $\sim$ kongruencija algebre $\prod_{i \in N} \mathbf{A}_i$ ako je:
**a.** $\mathcal{S} = \{X \subseteq N | \, X^c \text{ je konačan}\}$.
**b.** $\mathcal{S} = \{X \subseteq N | \, m \in X\}$, $m$ je neki fiksiran prirodan broj.
**c.** $\mathcal{S} = \{X \subseteq N | \text{ red } \sum_{n \in X^c} 1/n \text{ konvergira}\}$.

**d.** $\mathcal{S}$ ima sledeća svojstva: (i) $N \in \mathcal{S}$, (ii) $X \in \mathcal{S}$, $X \subseteq Y \subseteq N \Rightarrow Y \in \mathcal{S}$, (iii) $X, Y \in \mathcal{S} \Rightarrow X \cap Y \in \mathcal{S}$.

# 2. Algebre sa relacijama

Algebarski varijeteti predstavljaju jednu moguću klasifikaciju algebri datog jezika. S druge strane, mnoge značajne klase algebri ne mogu se u tom formalizmu na pogodan način predstaviti. Na primer, videli smo da ne postoji algebarska teorija, v. Posledicu 1.8.10, koja opisuje tačno klasu svih algebarskih polja. Isto tako ima važnih primera algebri na kojima su definisane određene relacije koje su vezi sa operacijama date algebre kao što su, na primer, uređena polja. Takve proširene strukture nisu obuhvaćene formalnom definicijom algebre. Stoga su razvijeni formalni sistemi koji između ostalog dopuštaju izučavanje i takvih primera algebarskih struktura. Ovom prilikom spomenimo dva takva formalizma: teoriju modela i teoriju kategorija. Za teoriju modela smatra se da je to oblast smeštena između algebre i logike. Jedan deo ove oblasti, takozvani sintaksni deo, zasnovan je na predikatskom računu. Zato ćemo najpre izložite neke osnovne konstrukcije predikatskog računa.

## 2.1 Teorije prvog reda

Predikatski račun omogućava dalju i finiju klasifikaciju algebri, opštije algebri sa relacijama. Dok ključno mesto u definiciji algebarskog varijeteta ima pojam algebarskog zakona, to mesto u predikatskom računu ima pojam predikatske formule. Slično termima, predikatske formule su dobro definisani izrazi nekog jezika $L$, u ovom slučaju nekog algebarskog jezika proširenog skupom relacijskih simbola. Dakle,

$$L = \mathrm{Const}_L \cup \mathrm{Fun}_L \cup \mathrm{Rel}_L$$

gde su $\mathrm{Const}_L$, $\mathrm{Fun}_L$ i $\mathrm{Rel}_L$ uzajamno disjunktni skupovi simbola, a $\mathrm{Const}_L \cup \mathrm{Fun}_L$ je algebarski jezik. Elemente skupa $\mathrm{Rel}_L$ nazivamo relacijskim simbolima i kao kod funkcijskih simbola svakom $R \in \mathrm{Rel}_L$ pridružena je *arnost*, ili dužina, $\mathrm{ar}(R)$. To je prirodan broj koji govori koliko argumentnih mesta ima simbol $R$.

U definiciji formula jezika $L$ predikatskog računa prvog reda, pored simbola jezika $L$, skupa promenljivih Var, pomoćnih simbola (,),, i simbola jednakosti $=$, učestvuju i ovi logički znaci:

*Logički veznici*:
$\neg$ - znak negacije,
$\wedge$ - znak konjunkcije (*i*), $\vee$ - znak disjuncije (*ili*),
$\Rightarrow$ - znak implikacije, $\Leftrightarrow$ - znak ekvivalencije.
*Kvantifikatori*:
$\exists$ - egzistencijalni kvantifikator, $\forall$ - univerzalni kvantifikator.

U izgradnji formula najpre se definišu atomične formule. To su formule oblika

$$u = v, \quad \text{i} \quad R(u_1, u_2, \ldots, u_n)$$

gde su $u, v, u_1, u_2, \ldots, u_n \in \mathrm{Term}_L$ i $R \in \mathrm{Rel}_L$ je dužine $n$. Ako je $R$ binarni relacijski simbol, dakle dužine 2, onda $R(x, y)$ zapisujemo takođe u *infiksnoj* notaciji, $xRy$. Na primer, u slučaju specijalnih binarnih relacijskih simbola, kao što su $<, \sim$, u formulama uglavnom pišemo $x < y$, $x \sim y$ umesto $<(x, y)$, odnosno $\sim(x, y)$. Isto tako, kod binarnih relacijskih znakova, kao što su na primer $=, \in$, umesto $\neg(x = y)$, $\neg(x \in y)$ pišemo kraće $x \neq y$, $x \notin y$.

Neka je $\mathrm{At}_L$ skup svih atomičnih formula jezika $L$. Formalna definicija formula nekog jezika $L$ je induktivnog karaktera. Naime, najpre induktivno definišemo niz skupova $F_n$ na sledeći način:

$$\begin{aligned} F_0 &= \mathrm{At}_L \\ F_{n+1} &= F_n \cup \{\neg\varphi \mid \varphi \in F_n\} \cup \\ &\qquad \{(\varphi \wedge \psi) \mid \varphi, \psi \in F_n\} \cup \{(\varphi \vee \psi) \mid \varphi, \psi \in F_n\} \cup \\ &\qquad \{(\varphi \Rightarrow \psi) \mid \varphi, \psi \in F_n\} \cup \{(\varphi \Leftrightarrow \psi) \mid \varphi, \psi \in F_n\} \cup \\ &\qquad \{\exists v\varphi \mid \varphi \in F_n, v \in \mathrm{Var}\} \cup \{\forall v\varphi \mid \varphi \in F_n, v \in \mathrm{Var}\}, \qquad n \in N. \end{aligned}$$

Neka je $\mathrm{For}_L = \bigcup_n F_n$. Tada se formule jezika $L$ definišu kao elementi skupa $\mathrm{For}_L$. Nije teško proveriti da formule zadovoljavaju sledeće uslove:

- Atomične formule su formule.
- Ako su $\varphi$ i $\psi$ formule jezika $L$, $x$ promenljiva, tada su $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$, $\exists x\varphi$, $\forall x\varphi$ takođe formule jezika $L$.
- Svaka formula jezika $L$ dobija se konačnom primenom prethodna dva pravila.

Da bi se mogla meriti složenost formula, modifikovaćemo funkciju složenosti terma sl. Dakle, preslikavanje $\mathrm{sl} : \mathrm{For}_L \to N$ definisano je induktivno na sledeći način:

Ako je $\varphi \in \mathrm{At}_L$, tada $\mathrm{sl}(\varphi) = 0$,
Ako je $\varphi \in F_n - F_{n-1}$, $n \in N - \{0\}$, tada $\mathrm{sl}(\varphi) = n$.

U pisanju formula primenjuju se razni dogovori radi jednostavnijeg i preglednijeg zapisa. Tako, kao i u slučaju terma, pretpostavljamo da je čitalac upoznat sa osnovnim konvencijama o pisanju formula, kao što su pravila o brisanju zagrada, izostavljanje univerzalnih kvantifikatora na početku formule, prioriteti logičkih veznika, itd. Pored toga, blok kvantora skupićemo pod jedan kvantor, na primer, umesto formule $\forall x_1 \forall x_2 \ldots \forall x_n \varphi$ pisaćemo jednostavno $\forall x_1 x_2 \ldots x_n \varphi$. Napomenimo da je $u \neq v$ skraćeni zapis za $\neg(u = v)$. Gde je uputno, na primer da bismo razlikovali logički znak $=$ od jednakosti dva objekta, koristićemo $\equiv$ za oznaku meta-jednakosti, i tada $a \equiv b$ čitamo *"a je identički jednako b"*.

Pojam slobodnog pojavljivanja promenljive dopušta da se precizno opišu one promenljive u formuli koje nisu pod dejstvom kvantifikatora.

**2.1.1 Definicija** *Skup* $\mathrm{Fv}(\varphi)$ *promenljivih koje imaju slobodna pojavljivanja u formuli* $\varphi$ *jezika* $L$ *uvodi se induktivno po složenosti formule* $\varphi$ *na sledeći način:*
1. *Ako je* $\varphi \in \mathrm{At}_L$, *tada je* $\mathrm{Fv}(\varphi)$ *skup promenljivih koje se pojavljuju u* $\varphi$.
2. *Ako je* $\varphi = \neg\psi$, *tada* $\mathrm{Fv}(\varphi) = \mathrm{Fv}(\psi)$.
3. *Ako je* $\varphi = \psi * \theta$, *gde je* $* \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, *tada* $\mathrm{Fv}(\varphi) = \mathrm{Fv}(\psi) \cup \mathrm{Fv}(\theta)$.
4. *Ako je* $\varphi = \exists x\psi$, *ili* $\varphi = \forall x\psi$, *tada* $\mathrm{Fv}(\varphi) = \mathrm{Fv}(\psi) - \{x\}$.

Elementi skupa $\mathrm{Fv}(\varphi)$ nazivaju se slobodnim promenljivama formule $\varphi$, dok se ostale promenljive koje imaju pojavljivanja u $\varphi$ nazivaju vezanim. Na primer, ako je $\varphi \equiv (x \neq 0 \Rightarrow \exists y(x \cdot y = 1))$, tada je $\mathrm{Fv}(\varphi) = \{x\}$. Dakle, $x$ je slobodna promenljiva formule $\varphi$, dok je $y$ vezana promenljiva.

Ako je $\varphi \in \mathrm{For}_L$, tada se notacija $\varphi(x_1, x_2, \ldots, x_n)$, ili $\varphi x_1 x_2 \ldots x_n$, koristi da se označi činjenica da su sve slobodne promenljive formule $\varphi$ neke od promenljivih $x_1, x_2, \ldots, x_n$.

Formule $\varphi$ koje nemaju slobodnih promenljivih, tj. za koje je $\mathrm{Fv}(\varphi) = \emptyset$, nazivaju se *rečenicama*. Dakle, formule

$$0 = 1, \quad \forall x(x \neq 0 \Rightarrow \exists y(x \cdot y = 1))$$

su rečenice jezika $L = \{\cdot, 0, 1\}$, gde je $\cdot$ binarni operacijski simbol. Skup svih rečenica jezika $L$ označavaćemo sa $\mathrm{Sent}_L$. Definicija teorije prvog reda je jednostavna.

**2.1.2 Definicija** *Teorija prvog reda jezika* $L$ *je svaki skup rečenica jezika* $L$.

Dakle, skup $T$ je teorija jezika $L$ akko $T \subseteq \mathrm{Sent}_L$. U takvom slučaju elemente teorije $T$ nazivamo *aksiomama* teorije $T$. Glavni pojmovi u vezi sa pojmom teorije koje ćemo i mi u daljem koristiti su pojmovi dokaza i teoreme. Ovde nećemo ulaziti u formalnu definiciju ovih pojmova, već znatiželjnog čitaoca upućujemo na bilo koji udžbenik iz logike. Ipak, s obzirom na značaj koji u algebri ima logička jednakost $=$, navodimo glavna svojstva ovog znaka.

**2.1.3** ***Aksiome jednakosti.*** Neka je $u(x_1, x_2, \ldots, x_n)$ term jezika $L$ i neka je $\varphi(x_1, x_2, \ldots, x_n)$ formula jezika $L$. Tada
1. $x = x$.
2. $x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow u(x_1, x_2, \ldots, x_n) = u(y_1, y_2, \ldots, y_n)$.
3. Ako promenljive $y_1, y_2, \ldots, y_n$ nemaju slobodnih pojavljivanja u formuli $\varphi(x_1, x_2, \ldots, x_n)$, onda
   $x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow (\varphi(x_1, x_2, \ldots, x_n) \Leftrightarrow \varphi(y_1, y_2, \ldots, y_n))$.

Odavde se izvode sledeće teoreme:
- $x = y \Rightarrow y = x$, *simetričnost* logičke jednakosti.
- $x = y \wedge y = z \Rightarrow x = z$, *tranzitivnost* logičke jednakosti.

**2.1.4** ***Primeri teorija prvog reda.*** Navodimo nekoliko primera teorija prvog reda. U svakom primeru naveden je i odgovarajući jezik $L$ u kojem su aksiome teorije $T$ zapisane.

**1.** *Teorija linearnog uređenja*, LO. U ovom slučaju je $L_{\mathrm{LO}} = \{\leq\}$, gde je $\leq$ binarni relacijski simbol. Aksiome:

| | | |
|---|---|---|
| LO.1 | $x \leq x$ | refleksivnost, |
| LO.2 | $x \leq y \wedge y \leq z \Rightarrow x \leq z$ | tranzitivnost, |
| LO.3 | $x \leq y \wedge y \leq x \Rightarrow x = y$ | antisimetričnost, |
| LO.4 | $x \leq y \vee y \leq x$ | linearnost. |

Primetimo da navedene aksiome nisu rečenice jer imaju slobodnih promenljivih. Radi jednostavnijeg zapisa, u ispisivanju ovih aksioma primenili smo konvenciju o brisanju spoljnih univerzalnih kvantifikatora. Tako, na primer, aksioma LO.2 u neskraćenom zapisu glasi $\forall xyz(x \leq y \wedge y \leq z \Rightarrow x \leq z)$. Dakle, ukoliko se u spisku aksioma neke teorije $T$ nalazi formula $\varphi(x_1, x_2, \ldots, x_n)$ sa slobodnim promenljivama $x_1, x_2, \ldots, x_n$, aksioma teorije $T$ je zapravo *univerzalno zatvorenje* ove formule, tj. $\forall x_1 x_2 \ldots x_n \varphi$.

Binarni relacijski simbol $<$ uvodimo pomoću definicione aksiome $x < y \Leftrightarrow x \leq y \wedge \neg x = y$, dok dualne relacijske znake $\geq$ i $>$ uvodimo pomoću $x \geq y \Leftrightarrow y \leq x$, odnosno $x > y \Leftrightarrow y < x$.

Ima više primera teorija u vezi sa teorijom LO. Evo nekih:

**2.** *Teorija parcijalnog uređenja*, koju označavamo sa PO, ima aksiome LO.1-3.

**3.** *Teorija gustog linearnog uređenja bez krajeva.* Jezik ove teorije jednak je jeziku teorije LO, dok su aksiome – aksiome teorije LO kao i sledeće rečenice:

$$\forall xy \exists z(x < y \Rightarrow x < z \wedge z < y), \quad \forall x \exists y \ x < y, \quad \forall x \exists y \ y < x.$$

**4.** *Teorija polja*, F. Jezik ove teorije jednak je jeziku teorije Ab, teorije Abelovih (komutativnih) grupa, zajedno sa nekim dodatnim simbolima, tj. $L_F = L_{\mathrm{Ab}} \cup \{\cdot, 1\}$, gde je $\cdot$ binarni operacijski simbol, a 1 simbol konstante. Aksiome teorije F su aksiome teorije Ab kao i sledeće aksiome:

$$\begin{array}{lll} (x \cdot y) \cdot z = x \cdot (y \cdot z) & x \cdot y = y \cdot x & x \cdot 1 = x, \\ x \neq 0 \Rightarrow \exists y(x \cdot y = 1) & x \cdot (y + z) = (x \cdot y) + (x \cdot z), & 0 \neq 1. \end{array}$$

Novi funkcijski simbol $^{-1}$ uvodi se u teoriju F pomoću definicione aksiome: $\forall xy(x \neq 0 \Rightarrow (x \cdot y = 1 \Leftrightarrow y = x^{-1}))$. Tada je u F moguće dokazati:

$\forall x(x \neq 0 \Rightarrow x \cdot x^{-1} = 1)$.

Definicionom aksiomom za $^{-1}$ u poljima se zapravo uvodi parcijalna operacija, s obzirom da ta aksioma ne određuje vrednost $0^{-1}$. Ukoliko želimo da izbegnemo uvođenje pojma parcijalne operacije, možemo uzeti da je $^{-1}$ bilo koja operacija polja, tačnije interpretacija ovog simbola u datom polju, koja zadovoljava tu definicionu aksiomu, pa i ona za koju je, na primer, $0^{-1} = 1$. Aksiome polja i u tom slučaju ostaju nenarušene.

**5.** *Teorija uređenih polja*, FO. Jezik ove teorije je $L_{\mathrm{FO}} = L_{\mathrm{LO}} \cup L_F$. Aksiome ove teorije su aksiome teorije polja, aksiome teorije linearnog uređenja kao i aksiome saglasnosti $\leq$ sa $+$ i $\cdot$:

$$x \leq y \Rightarrow x + z \leq y + z, \qquad x \leq y \wedge 0 \leq z \Rightarrow x \cdot z \leq y \cdot z.$$

Primetimo da je formula $x_1^2 + \ldots + x_n^2 = 0 \Rightarrow x_1 = 0 \wedge \ldots \wedge x_n = 0$ teorema ove teorije .

**6.** Bilo koja algebarska teorija algebarskog jezika $L$ je teorija prvog reda.

**7.** *Zermelo-Fraenkelova teorija skupova*, ZF. Od nelogičkih simbola ova teorija ima samo binarni relacijski znak $\in$. Aksiome ove teorije su:

1. Aksioma ekstenzionalnosti: $x = y \Leftrightarrow \forall z(z \in x \Leftrightarrow x \in y)$.
   Prema ovoj aksiomi, dva skupa su jednaka akko imaju iste elemente.
2. Aksioma praznog skupa: $\exists x \forall y(y \notin x)$.
   Ova aksioma tvrdi da postoji prazan skup. Na osnovu ove aksiome možemo uvesti konstantu $\emptyset$ pomoću $\emptyset = \{x \mid x \neq x\}$.
3. Aksioma para: $\exists z \forall u(u \in z \Leftrightarrow u = x \vee u = y)$.
   Prema ovoj aksiomi, za svaka dva skupa $x, y$ postoji neuređen par, odnosno dvočlan skup $\{x, y\}$.
4. Aksioma unije: $\exists z \forall u(u \in z \Leftrightarrow \exists v(u \in v \wedge v \in x))$.
   Pomoću ove aksiome uvodi se skupovna operacija unije. Naime, prema ovoj aksiomi za svaki skup $x$ postoji unija članova tog skupa, koju označavamo sa $\bigcup x$. Specijalno, ako izaberemo $x = \{u, v\}$, onda postoji $u \cup v = \bigcup x$.
5. Aksioma partitivnog skupa: $\exists z \forall u(u \in z \Leftrightarrow \forall v(v \in u \Rightarrow v \in x))$.
   Ovom aksiomom se tvrdi da za svaki skup postoji skup čiji su elementi tačno podskupovi skupa $x$. Taj skup se naziva partitivnim skupom skupa $x$ i obično se obeležava pomoću $P(x)$.
6. Aksioma beskonačnosti: $\exists x(\emptyset \in x \wedge \forall y(y \in x \Rightarrow y \cup \{y\} \in x))$.
   Prema ovoj aksiomi postoji beskonačan skup, specijalno skup $x$ sa osobinom da $\emptyset \in x$, $\emptyset' \in x$, $\emptyset'' \in x \ldots$, gde je $y' = y \cup \{y\}$.
7. Aksioma regularnosti: $x \neq \emptyset \Rightarrow \exists y(y \in x \wedge \neg \exists z(z \in x \wedge z \in y))$.
   Prema ovoj aksiomi, svaki neprazan skup ima $\in$–minimalan element.
8. Shema – aksioma podskupa: $\exists y \forall z(z \in y \Leftrightarrow z \in x \wedge \varphi(z, u_1, \ldots, u_n))$,
   gde je $\varphi$ formula koja ne sadrži promenljivu $y$. Ova aksioma intutitivno tvrdi da za svaki skup $x$ i svako svojstvo $\varphi$ postoji podskup skupa $x$ čiji su elementi tačno oni koji imaju svojstvo $\varphi$. Taj skup obeležavamo pomoću $\{z \in x \mid \varphi(z, u_1, \ldots, u_n)\}$. Primetimo da je ovom shemom opisan beskonačan skup aksioma; svaka formula $\varphi$ daje jednu instancu aksiome podksupa. Pomoću ove aksiome možemo definisati nove skupovne operacije odnosno objekte. Na primer, presek skupova $x, y$ biće $x \cap y = \{z \in x \mid z \in y\}$, dok će presek članova iz skupa $x$ biti $\bigcap x = \{z \in \cup x \mid \forall y \in x(z \in y)\}$.
9. Shema – aksioma kolekcije:

$$\begin{aligned}\forall x(x \in u \Rightarrow &\exists z \varphi(x, z, u, v_1, \ldots, v_n)) \Rightarrow \\ &\exists y \forall x(x \in u \Rightarrow \exists z(z \in y \wedge \varphi(x, z, u, v_1, \ldots, v_n))),\end{aligned}$$

gde je $\varphi$ formula koja ne sadrži promenljivu $y$. Ova aksioma intuitivno tvrdi da ako je za svako $x \in u$ klasa $U_x = \{z \mid \varphi(x, z, \ldots)\}$ neprazna, onda postoji skup koji ima neprazan presek sa svakom klasom $U_x$, $x \in u$. Primetimo da i ova shema daje beskonačan skup aksioma teorije ZF.

10. Aksioma izbora:
$\forall x \exists f (f$ je funkcija sa domenom $x$ $\wedge \forall z \in x(z \neq \emptyset \Rightarrow f(z) \in z))$.

    Prema ovoj aksiomi svaki skup $x$ nepraznih skupova ima funkciju izbora, tj. funkciju $f$ definisanu na $x$ tako da za sve $z \in x$, $f(z) \in z$. Ova aksioma zapravo tvrdi da je skupovni proizvod $\prod_{i \in I} z_i$ nepraznih skupova $z_i$, $i \in I$, neprazan; dovoljno je primeniti Aksiomu izbora na $x = \{z_i \mid i \in I\}$. Prethodni zapis aksiome izbora nije dat u jeziku $L_{\mathrm{ZF}}$ teorije ZF. Ipak, nije teško videti da se iskaz "$f$ je funkcija sa domenom $x$" može zapisati formulom u $L_{\mathrm{ZF}}$, na primer uvodeći predikat koji definiše pojam funkcije i skupovnu operaciju koja datoj funkciji pridružuje njen domen, za detalje videti Teoremu 3.5.1. Aksioma izbora ima više ekvivalentnih formulacija. Jedna od njih je da svaka familija $x$ disjunktnih i nepraznih skupova ima *transverzalu*, ili izborni skup, tj. skup koji sadrži tačno po jedan element iz svakog člana familije $x$. Drugi ekvivalent koji se često koristi je *Zornova lema* ili *Lema Kuratovskog* koja tvrdi da svaki parcijalno uređen skup $(A, \leq_A)$ ima maksimalan lanac, tj. maksimalan podskup koji je linearno uređen u odnosu na $\leq_A$.

ZF označava teoriju sa aksiomama 1-9, dok sa ZFC obeležavamo teoriju ZF zajedno sa aksiomom izbora. Ova teorija je važna jer se u njoj može izgraditi – zasnovati najveći deo matematičkih pojmova, počev od apstraktnih pojmova kao što su uređen par i funkcija, pa do složenih konstrukcija kao što je izgradnja prirodnih, ili realnih brojeva. Istovremeno, ova teorija predstavlja formalizaciju tzv. Kantorove teorije skupova. G. Kantor je uveo i razvijao teoriju skupova sedamdesetih i osamdesetih godina prošlog veka, a danas je ta teorija opšte prihvaćena kao univerzalan jezik za izučavanje drugih matematičkih teorija i disciplina. Mi se u ovoj knjizi nećemo posebno baviti ovom teorijom, pa čitaoca upućujemo na bogatu literaturu, koja postoji i na našem jeziku, posvećenu teoriji skupova.

U vezi sa relacijom pripadanja uvode se *ograničeni kvantor* $\forall x \in A$ i $\exists x \in A$: formula $(\forall x \in A)\varphi x$ je kraći zapis za $\forall x(x \in A \Rightarrow \varphi(x))$, dok je $(\exists x \in A)\varphi x$ kraći zapis za $\exists x(x \in A \wedge \varphi x)$. Na sličan način se uvode ograničeni kvantori i u odnosu na binarne relacijske simbole $\leq, <, \geq$ i $>$. Spomenimo i kvantor "postoji tačno jedno x" kojeg zapisujemo $\exists_1 x$, a uvodi se pomoću $\exists_1 x \varphi x \Leftrightarrow \exists x(\varphi x \wedge \forall y(\varphi y \Rightarrow y = x))$.

## 2.2 Modeli

U prethodnom poglavlju razmatrali smo uglavnom sintaksne pojmove predikatskog računa. S druge strane, najvažniji pojam u ovom kontekstu je pojam algebarsko-relacione strukture, ili jednostavno *model* nekog jezika $L$. Uobičajene strukture kao što su grupe, prsteni, polja, uređena polja, kao i struktura prirodnih brojeva su primeri modela. U izučavanju svojstava modela, istaknutu ulogu ima pojam formalnog jezika, jer se pomoću simbola jezika izgrađuje precizan pojam formule, a time i pojam aksiome neke teorije. Ipak, glavni razlog za uvođenje pojma formule je što se pomoću njih mogu opisivati svojstva operacijsko-relacijskih struktura.

**2.2.1 Definicija** *Model je svaka struktura* $\mathbf{A} = (A, \mathcal{F}, \mathcal{R}, \mathcal{C})$, *gde je* $A$ *neprazan skup,* $(A, \mathcal{F}, \mathcal{C})$ *je algebra i* $\mathcal{R}$ *je je skup relacija domena* $A$.

Pojmove operacija i konstanata u algebri smo ranije definisali. Ako je $R$ relacija modela $\mathbf{A}$, tj. $R \in \mathcal{R}$, onda postoji pozitivan prirodan broj $n$ tako da je $R \subseteq A^n$. Tada za $R$ kažemo da je relacija dužine $n$. Činjenicu $(a_1, a_2, \ldots, a_n) \in R$ zapisujemo takođe pomoću $R(a_1, a_2, \ldots, a_n)$.

Svakom jeziku prvog reda $L$ odgovaraju određene algebarske strukture sa relacijama. Ukoliko je, na primer,

$\mathrm{Const}_L = \{c_1, c_2, \ldots, c_n\}$, $\mathrm{Fun}_L = \{F_1, F_2, \ldots, F_m\}$, $\mathrm{Rel}_L = \{S_1, S_2, \ldots, S_k\}$,

gde je $\mathrm{ar}(F_i) = \alpha_i$, $\mathrm{ar}(S_i) = \sigma_i$, onda je

$$\mathbf{A} = (A, f_1, \ldots, f_m, R_1, \ldots, R_k, a_1, \ldots, a_n)$$

algebarsko relacijska struktura, ili jednostavno model jezika $L$, ako su dužine operacija $f_i$ i relacija $R_i$ jednake redom $\alpha_i$ i $\sigma_i$. Takođe kažemo da je $\mathbf{A}$ *interpretacija* jezika $L$, dok su $f_i$, $R_i$, $a_i$ redom interpretacije simbola $F_i$, $S_i$, $c_i$.

Mnogi pojmovi definisani za operacije i algebre neposredno se prenose i na relacije odnosno modele, pa ukoliko je jasno o kakvoj je definiciji reč, nećemo je posebno uvoditi. Na primer, kao što je već rečeno, binarna relacija je relacija dužine 2 i umesto $S(a,b)$ uobičajeno pišemo $aSb$. Neki od standardnih relacijskih simbola u upotrebi su, na primer, $\sim, \leq, \geq, \in$.

**2.2.2 Primer** 1° Uređeno polje realnih brojeva $\mathbf{R} = (R, +, \cdot, -, \leq, 0, 1)$. U ovom slučaju operacije su $+, \cdot, -$ redom dužine 2,2,1, relacija je $\leq$ dužine 2, dok su konstante $0, 1$. Dakle, $\mathbf{R}$ je model jezika $L = \{+, \cdot, -, \leq, 0, 1\}$, gde su $\mathrm{Rel}_L = \{\leq\}$, $\mathrm{Fun}_L = \{+, \cdot, -\}$, $\mathrm{Const}_L = \{0, 1\}$, $\mathrm{ar}(+) = \mathrm{ar}(\cdot) = 2$, $\mathrm{ar}(-) = 1$, $\mathrm{ar}(\leq) = 2$.
2° Struktura prirodnih brojeva $\mathbf{N} = (N, +, \cdot, ', \leq, 0)$.
3° Polje (Bulova algebra) svih podskupova skupa $X$: $\mathbf{P}(X) = (P(X), \cup, \cap, ^c, \emptyset, X)$. Primetimo da ova algebra nije polje u uobičajenom smislu, tj. ne zadovoljava aksiome teorije polja.
4° Algebre su specijalne vrste modela; to su modeli jezika $L$ kod kojih je $\mathrm{Rel}_L = \emptyset$.

Ako je reč o modelima, ubuduće slova $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$ označavaće modele, dok će $A, B, C, \ldots$ označavati redom njihove domene. Ako je $\mathbf{A}$ model jezika $L$ i $s \in L$, tada ćemo pomoću $s^{\mathbf{A}}$ označiti interpretaciju simbola $s$ u modelu $\mathbf{A}$. Primetimo da su $s$ i $s^{\mathbf{A}}$ objekti potpuno različite prirode; $s$ je simbol, znak, dok je $s^{\mathbf{A}}$ skupovni objekt. Ipak, ako to kontekst dopušta, koristićemo isti znak da označimo simbol jezika $L$, kao i njegovu interpretaciju u nekom modelu jezika $L$. To zapravo znači da će indeks $^{\mathbf{A}}$ biti izostavljen iz $s^{\mathbf{A}}$. Tada će se iz konteksta videti da li je $s \in L$ ili je, ustvari, $s$ interpretacija nekog simbola jezika $L$. Često će biti reči o nekoj strukturi $\mathbf{A}$ bez eksplicitnog navođenja pridruženog jezika. Iz definicije modela biće jasno o kojem je jeziku reč. Slična situacija može se pojaviti i za neku teoriju $T$. U tom slučaju odgovarajući jezik obeležićemo sa $L_T$.

Pretpostavimo da su $L \subseteq L'$ jezici prvog reda, i neka je $\mathbf{A}$ model jezika $L'$. Ispuštanjem $s^{\mathbf{A}}$ za $s \in L' - L$, iz spiska relacija (operacija, konstanti) modela $\mathbf{A}$, dobijamo nov model $\mathbf{B}$, gde je $B = A$. U tom slučaju $\mathbf{A}$ se naziva *ekspanzijom* modela $\mathbf{B}$, dok se $\mathbf{B}$ naziva *reduktom* modela $\mathbf{A}$. Na primer, ako je $\mathbf{R} = (R, +, \cdot, -, \leq, 0, 1)$ uređeno polje realnih brojeva, onda je $\mathbf{S} = (R, +, \cdot, -, 0, 1)$ redukt modela $\mathbf{R}$, dok je $\mathbf{R}$ ekspanzija strukture $\mathbf{S}$. Pod algebarskim reduktom modela $\mathbf{A}$ jezika $L$ podrazumevaćemo redukt modela $\mathbf{A}$ na algebarski deo jezika $L$. Ako je $L'' = L' - L$ i model $\mathbf{A}$ jezika $L'$ je ekspanzija modela $B$ jezika $L$, onda ćemo tu činjenicu zapisivati takođe pomoću $\mathbf{A} = (\mathbf{B}, s^{\mathbf{A}})_{s \in L''}$, ili $\mathbf{A} = (\mathbf{B}, s_1^{\mathbf{A}}, s_2^{\mathbf{A}}, \ldots, s_n^{\mathbf{A}})$ ako je $L'' = \{s_1, s_2, \ldots, s_n\}$.

**2.2.3 Definicija** *Neka su* $\mathbf{A}$, $\mathbf{B}$ *modeli jezika* $L$ *i* $\mathbf{A}'$, $\mathbf{B}'$ *redom njihovi algebarski redukti. Tada je* $\mathbf{B}$ *podmodel (podstruktura) modela* $\mathbf{A}$ *akko* $\mathbf{B}' \subseteq \mathbf{A}'$ *i za svaki relacijski znak* $R \in L$, $R^{\mathbf{B}} = R^{\mathbf{A}} \cap B^k$, *gde je* $\mathrm{ar}(R) = k$.

Ako je $\mathbf{B}$ podmodel modela $\mathbf{A}$, pisaćemo $\mathbf{B} \subseteq \mathbf{A}$. Na primer, $(N, +, \cdot, \leq, 0) \subseteq (R, +, \cdot, \leq, 0)$, ali za $X \subseteq Y$, $X \neq Y$, nije $(P(X), \cup, \cap, {}^c, \emptyset, X) \subseteq (P(Y), \cup, \cap, {}^c, \emptyset, Y)$.

Slično kao kod algebri uvodi se pojam homomorfizma.

**2.2.4 Definicija** *Neka su* $\mathbf{A}$, $\mathbf{B}$ *modeli jezika* $L$ *i* $\mathbf{A}'$, $\mathbf{B}'$ *redom njihovi algebarski redukti. Neka su* $a_1, a_2, \ldots, a_n \in A$ *proizvoljno izabrani. Preslikavanje* $h : A \to B$ *je homomorfizam iz modela* $\mathbf{A}$ *u model* $\mathbf{B}$ *akko je* $h : \mathbf{A}' \to \mathbf{B}'$ *i za svaki* $R \in \mathrm{Rel}_L$ *dužine* $n$, $R^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$ *povlači* $R^{\mathbf{B}}(ha_1, ha_2, \ldots, ha_n)$. *Preslikavanje* $h$ *je jak homomorfizam iz* $\mathbf{A}$ *u* $\mathbf{B}$ *ako je* $h$ *homomorfizam iz* $\mathbf{A}$ *u* $\mathbf{B}$ *i za svaki* $R \in \mathrm{Rel}_L$ *dužine* $n$, $R^{\mathbf{B}}(ha_1, ha_2, \ldots, ha_n)$ *povlači* $R^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$.

Na primer, ako su $\mathbf{A}$ i $\mathbf{B}$ parcijalno uređeni skupovi, onda su homomorfizmi iz $\mathbf{A}$ u $\mathbf{B}$ tačno monotona preslikavanja iz $\mathbf{A}$ u $\mathbf{B}$.

Pomoću $h : \mathbf{A} \to \mathbf{B}$ zapisujemo činjenicu da je $h$ homomorfizam iz modela $\mathbf{A}$ u model $\mathbf{B}$. Kao i u slučaju algebri, uvode se razne vrste homomorfizama: utapanja, izomorfizmi, endomorfizmi i automorfizmi, kao i pridruženi pojmovi. Ako je $h : \mathbf{A} \to \mathbf{B}$ homomorfizam *na*, kažemo da je $\mathbf{B}$ homomorfna slika modela $\mathbf{A}$ i pišemo $\mathbf{B} = h(\mathbf{A})$. Utapanje modela $\mathbf{A}$ u model $\mathbf{B}$ biće svaki jak i 1–1 homomorfizam $f : \mathbf{A} \to \mathbf{B}$, dok će izomorfizam iz $\mathbf{A}$ na $\mathbf{B}$ biti svako utapanje iz $\mathbf{A}$ *na* $\mathbf{B}$. Dalje, $\mathrm{Aut}\mathbf{A}$ biće skup svih automorfizama modela $\mathbf{A}$, tj. izomorfizama iz $\mathbf{A}$ u $\mathbf{A}$, dok je $\mathbf{AutA} = (\mathrm{Aut}\mathbf{A}, \circ, {}^{-1}, i_A)$ odgovarajuća grupa automorfizama.

U algebri je čest slučaj da se neka struktura $\mathbf{A}$ dograđuje do neke strukture $\mathbf{B}$. Deo konstrukcije sastoji se u tome da se nađu algebre $\mathbf{B}$ i $\mathbf{A}' \subseteq \mathbf{B}$, tako da je $\mathbf{A} \cong \mathbf{A}'$. Tada kažemo da je struktura $\mathbf{A}$ *identifikovana* sa podmodelom strukture $\mathbf{B}$. O tome preciznije govori sledeća teorema, koja se odnosi na prenos i identifikaciju struktura.

**2.2.5 Teorema** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *modeli jezika* $L$ *i neka je* $f : \mathbf{A} \to \mathbf{B}$ *utapanje. Tada:*

1. *Postoji model* $\mathbf{A}' \subseteq \mathbf{B}$ *i izomorfizam* $\mathbf{A} \xrightarrow{\approx} \mathbf{A}'$ *tako da dijagram* D-1 *komutira.*
2. *Postoji model* $\mathbf{B}' \supseteq \mathbf{A}$ *i izomorfizam* $\mathbf{B} \xrightarrow{\approx} \mathbf{B}'$ *tako da dijagram* D-2 *komutira.*

$$\begin{tikzcd} \mathbf{A} \arrow[r, "\approx"] \arrow[dr, "f"'] & \mathbf{A}' \arrow[d, "i_{A'}"] \\ & \mathbf{B} \end{tikzcd} \qquad\qquad \begin{tikzcd} \mathbf{B} \arrow[r, "\approx"] & \mathbf{B}' \\ & \mathbf{A} \arrow[u, "i_A = f' \circ f"'] \arrow[ul, "f"] \end{tikzcd}$$

D-1 D-2

Ovde su $i_A : A \to B'$ i $i_{A'} : A' \to B$ inkluziona preslikavanja.

**Dokaz** 1. Neka je domen modela $\mathbf{A}'$ skup $A' = f[A]$, dok interpretacije simbola jezika $L$ biramo na sledeći način. Ako je $c \in \mathrm{Const}_L$ uzećemo $c^{\mathbf{A}'} = c^{\mathbf{B}}$. Neka su $H \in \mathrm{Fun}_L$ i $R \in \mathrm{Rel}_L$ dužine $n$, $b_1, b_2, \ldots, b_n \in A'$, i $a_1, a_2, \ldots, a_n \in A$ takvi da je $b_i = fa_i, i \leq n$. Tada ćemo uzeti da je $H^{\mathbf{A}'}(b_1, b_2, \ldots, b_n) = fH^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$, i $R^{\mathbf{A}'}(b_1, b_2, \ldots, b_n)$ akko $R^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$. Za tako izabran model $\mathbf{A}'$ nije teško videti da je $f : \mathbf{A} \overset{\approx}{\to} \mathbf{A}'$, kao i da dijagram D-1 komutira.
2. Neka je $S$ bilo koji skup iste kardinalnosti kao $B - f[A]$, disjunktan sa A i neka je $B' = A \cup S$. Tada postoji bijekcija $\sigma : B - f[A] \to S$, dok je $f' = f^{-1} \cup \sigma$ bijekcija između skupova $B$ i $B'$. Model $\mathbf{B}'$ određujemo na sledeći način. Za domen modela $\mathbf{B}'$ uzećemo $B'$. Ako je $c \in \mathrm{Const}_L$, biramo $c^{\mathbf{B}'} = c^{\mathbf{A}}$. Neka su $b'_1, b'_2, \ldots, b'_n \in B'$ i $b_1, b_2, \ldots, b_n \in B$ takvi da je $b'_i = f'(b_i), i \leq n$. Ako su $H \in \mathrm{Fun}_L$ i $R \in \mathrm{Rel}_L$ dužine $n$ tada ćemo uzeti da je $H^{\mathbf{B}'}(b'_1, b'_2, \ldots, b'_n) = f'H^{\mathbf{B}}(b_1, b_2, \ldots, b_n)$, i $R^{\mathbf{B}'}(b'_1, b'_2, \ldots, b'_n)$ akko $R^{\mathbf{B}}(b_1, b_2, \ldots, b_n)$. Za tako izabran model $\mathbf{B}'$ nije teško videti da je $f' : \mathbf{B} \xrightarrow{\approx} \mathbf{B}'$, kao i da dijagram D-2 komutira. $\diamondsuit$

Za ovako konstruisane strukture $\mathbf{A}'$ i $\mathbf{B}'$ reći ćemo da su dobijene *prenosom*, kao i da se modeli $\mathbf{A}$ i $\mathbf{B}$ redom identifikuju sa tim strukturama (tj. ne razlikuju od njih). Prema tome, ako je $f : \mathbf{A} \to \mathbf{B}$ utapanje, identifikacija modela $\mathbf{A}$ sa podmodelom modela $\mathbf{B}$ znači konstrukciju odgovarajućeg izomorfizma, kako je već opisano u prethodnoj teoremi.

## 2.3 Relacija zadovoljenja

Jedan od fundamentalnih pojmova matematike uopšte je pojam matematičke istine. Definicija relacije zadovoljenja $\models$ koju je uveo A.Tarski određuje precizno taj pojam. Naime, rečenica $\varphi$ biće tačna, ili istinita, u modelu $\mathbf{A}$ akko $\mathbf{A} \models \varphi$. Formalizacijom matematičke istine omogućava se matematička analiza metamatematičkih pojmova, ali isto tako primena novih metoda u algebri i drugim oblastima matematike.

U definiciji relacije zadovoljenja koristićemo sledeću oznaku. Neka je $\mu$ valuacija domena $A$, $k \in N$ i $a \in A$. Pomoću $\mu(k/a)$ označićemo valuaciju $\tau$ domena $A$ definisanu sa $\tau(v_i) = \mu(v_i)$ za $i \neq k$, i $\tau(v_k) = a$. Dakle, valuacija $\mu(k/a)$ dodeljuje iste vrednosti promenljivama $v_i$ kao valuacija $\mu$, osim promenljivoj $v_k$, kojoj dodeljuje vrednost $a$.

**2.3.1 Definicija** *Neka je* $\mathbf{A}$ *model jezika* $L$. *Relacija* $\mathbf{A} \models \varphi[\mu]$ *definiše se induktivno prema složenosti formule* $\varphi$ *za sve formule* $\varphi$ *jezika* $L$ *i valuacije* $\mu$ *domena* $A$ *na sledeći način:*

Ako je $\varphi$ formula $u = v$, $u, v \in \mathrm{Term}_L$, tada $\mathbf{A} \models \varphi[\mu]$ akko $u^{\mathbf{A}}[\mu] \equiv v^{\mathbf{A}}[\mu]$, tj. $u^{\mathbf{A}}[\mu]$ i $v^{\mathbf{A}}[\mu]$ imaju identički jednake vrednosti.

Ako je $\varphi$ formula $R(u_1, u_2, \ldots, u_n)$, $R \in \mathrm{Rel}_L$ dužine $n$, i $u_1, u_2, \ldots, u_n \in \mathrm{Term}_L$, tada je $\mathbf{A} \models \varphi[\mu]$ akko $(u_1^{\mathbf{A}}[\mu], u_2^{\mathbf{A}}[\mu], \ldots, u_n^{\mathbf{A}}[\mu]) \in R^{\mathbf{A}}$, odnosno $R^{\mathbf{A}}(u_1^{\mathbf{A}}[\mu], u_2^{\mathbf{A}}[\mu], \ldots, u_n^{\mathbf{A}}[\mu])$.
Ako je $\varphi$ formula $\neg\psi$, tada $\mathbf{A} \models \varphi[\mu]$ akko *nije* $\mathbf{A} \models \psi[\mu]$.
Ako je $\varphi$ formula $\psi \wedge \theta$, tada $\mathbf{A} \models \varphi[\mu]$ akko $\mathbf{A} \models \psi[\mu]$ *i* $\mathbf{A} \models \theta[\mu]$.
Ako je $\varphi$ formula $\psi \vee \theta$, tada $\mathbf{A} \models \varphi[\mu]$ akko $\mathbf{A} \models \psi[\mu]$ *ili* $\mathbf{A} \models \theta[\mu]$.
Ako je $\varphi$ formula $\psi \Rightarrow \theta$, tada $\mathbf{A} \models \varphi[\mu]$ akko *nije* $\mathbf{A} \models \psi[\mu]$ *ili* $\mathbf{A} \models \theta[\mu]$.
Ako je $\varphi$ formula $\psi \Leftrightarrow \theta$, tada $\mathbf{A} \models \varphi[\mu]$ akko $\mathbf{A} \models \psi[\mu]$ *ako i samo ako* $\mathbf{A} \models \theta[\mu]$.
Ako je $\varphi$ formula $\exists v_k \psi(v_1, v_2, \ldots, v_n)$, $k \leq n$, tada $\mathbf{A} \models \varphi[\mu]$ akko *postoji* $a \in A$ tako da je $\mathbf{A} \models \psi[\mu(k/a)]$.
Ako je $\varphi$ formula $\forall v_k \psi(v_1, v_2, \ldots, v_n)$, $k \leq n$, tada $\mathbf{A} \models \varphi[\mu]$ akko *za svaki* $a \in A$ važi $\mathbf{A} \models \psi[\mu(k/a)]$.

Prema definiciji zadovoljenja vidimo da vrednost $\mathbf{A} \models \varphi[\mu]$ zavisi jedino od slobodnih promenljivih formule $\varphi$. Strog dokaz ove činjenice može se izvesti indukcijom po složenosti formule $\varphi$. To nam omogućava da uvedemo sledeće dogovore.

Ako je $\varphi = \varphi(v_1, v_2, \ldots, v_n)$ i $\mu(v_i) = a_i, i \in N$, tada ćemo jednostavno pisati $\mathbf{A} \models \varphi[a_1, a_2, \ldots, a_n]$ umesto $\mathbf{A} \models \varphi[\mu]$. Rečenice nemaju slobodnih promenljivih, prema tome njihove vrednosti u strukturi ne zavise od izbora valuacije. Drugim rečima, ako je $\varphi \in \mathrm{Sent}_L$ i $\mathbf{A} \models \varphi[\mu]$, tada je za *sve* valuacije $\sigma$, $\mathbf{A} \models \varphi[\sigma]$. Otuda ćemo u tom slučaju pisati $\mathbf{A} \models \varphi$ umesto $\mathbf{A} \models \varphi[\mu]$.

Definicija relacije zadovoljenja omogućava da se uvedu novi pojmovi. Jedan od tih je *teorija modela* $\mathbf{A}$ jezika $L$: $\mathrm{Th}\mathbf{A} = \{\varphi \in \mathrm{Sent}_L : \mathbf{A} \models \varphi\}$. Za svaku formulu $\varphi$ jezika $L$ i svaku valuaciju $\mu$ važi $\mathbf{A} \models \varphi[\mu]$ ili $\mathbf{A} \models \neg\varphi[\mu]$. Dakle, za svaku rečenicu $\varphi \in \mathrm{Sent}_L$ važi $\varphi \in \mathrm{Th}\mathbf{A}$ ili $\neg\varphi \in \mathrm{Th}\mathbf{A}$, tj. $\mathrm{Th}\mathbf{A}$ je *kompletna* teorija.

Neka je $T$ teorija jezika $L$. Struktura $\mathbf{A}$ jezika $L$ je *model* teorije $T$ ukoliko svaka aksioma teorije $T$ važi u modelu $\mathbf{A}$, tj. $T \subseteq \mathrm{Th}\mathbf{A}$. U takvom slučaju pišemo $\mathbf{A} \models T$. Na primer, svako uređeno polje, kao što je polje racionalnih brojeva ili polje realnih brojeva je model teorije uređenih polja FO. Dalje, reći ćemo da je $T$ *sintaksno neprotivurečna* teorija ako se iz $T$ ne može dobiti kontradikcija. S druge strane, $T$ je *semantički neprotivurečna* ako postoji model teorije $T$.

Pomoću $\mathfrak{M}(T)$ označavaćemo klasu svih modela teorije $T$. Klasa struktura $\mathfrak{M}$ jezika $L$ je *aksiomatska* ako postoji teorija $T$ jezika $L$ tako da je $\mathfrak{M} = \mathfrak{M}(T)$. Na primer, klasa svih uređenih polja je aksiomatska.

Spomenimo ovde bez dokaza fundamentalnu teoremu karakterizacije predikatskog računa prvog reda.

**2.3.2** ***Teorema potpunosti*** *(K. Gödel) Neka je $T$ teorija jezika prvog reda $L$. Rečenica $\varphi$ jezika $L$ je teorema teorije $T$ ako i samo ako $\varphi$ važi na svim modelima teorije $T$.*

Nešto drugačiji oblik ove teoreme glasi:

**2.3.3** ***Teorema potpunosti - druga forma*** *Neka je $T$ teorija jezika $L$. Teorija $T$ je sintaksno neprotivurečna teorija akko je $T$ semantički neprotivurečna, tj. $T$ ima model.*

Dakle, teorema potpunosti tvrdi da je za neprotivurečne teorije $T$, $\mathfrak{M}(T) \neq \emptyset$. Jedna važna posledica ove teoreme je Stav kompaktnosti. Kao što ćemo videti, teorema kompaktnosti ima zanimljive primene u algebri. U jednom od kasnijih poglavlja daćemo direktan dokaz ove teoreme.

**2.3.4** ***Stav kompaktnosti*** *Neka je $T$ teorija jezika $L$. Ako svaki konačan podskup $S \subseteq T$ ima model, onda $T$ ima model.*

**Dokaz** Pretpostavimo da svaki konačan podskup od $T$ ima model, ali da $T$ nema model. Tada je prema Stavu potpunosti T protivrečna teorija, tj. postoji konačan niz aksioma $\sigma_1, \sigma_2, \ldots, \sigma_n \in T$ koji daje dokaz za kontradikciju. Tada je $S = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ konačan protivurečan podksup od $T$, pa $S$ nema model, suprotno pretpostavci. $\diamondsuit$

Naziv prethodne teoreme potiče iz formulacije ove teoreme koja podseća na neke topološke iskaze. U vezi sa tim zanimljivo je da Stav kompaktnosti ima i topološku reformulaciju. Spomenimo ovde značajnu istorijsku činjenicu da su prve primene matematičke logike u ostalim delovima matematike bile, ustvari, primene teoreme kompaktnosti u algebri (Malcev 1936 godine). Dokaz ove teoreme prvi je dao Malcev za teorije prebrojivog jezika, dok je Gödel dokazao opšti slučaj. Evo nekih jednostavnih primena ove teoreme. Prva teorema je jedna vrsta generalizacije teoreme 1.9.10 na elementarne klase struktura.

**2.3.5** **Teorema** *Neka teorija $T$ jezika $L$ ima beskonačan model ili konačne modele proizvoljno velike kardinalnosti. Tada $T$ ima beskonačne modele proizvoljno velike kardinalnosti.*

**Dokaz** Dokazujemo da za svaki beskonačan kardinalni broj $k$, $T$ ima model čija je kardinalnost bar $k$. Neka je $C = \{c_i | \, i \in I\}$ skup *novih* simbola konstanata, tj. $L \cap C = \emptyset$ i neka je jezik $L_C = L \cup C$. Ovde smo uzeli da je kardinalnost skupa indeksa $I$ jednaka $k$. Dalje, uvedimo teoriju $S$ jezika $L_C$ pomoću $S = T \cup \{c_i \neq c_j | \, i \neq j\}$. Proverimo sada uslove teoreme kompaktnosti za teoriju $S$.

Neka je $\Delta \subseteq S$ konačan. Dokazujemo da $\Delta$ ima model. Kako je $\Delta$ konačan skup, i svaka formula je konačan niz simbola, to postoji konačan $C' \subseteq C$, recimo $C' = \{c_1, c_2, \ldots, c_n\}$ takav da je svaki od simbola iz $C$ koji se pojavljuje u $\Delta$ neki od simbola iz $C'$. Neka je $\Delta' = T \cup \{c_i \neq c_j | \, 1 \leq i < j \leq n\}$. Kako je $\Delta \subseteq \Delta'$, dovoljno je dokazati da $\Delta'$ ima model. Prema pretpostavci $T$ ima model kardinalnosti $\geq n$, neka je to $\mathbf{A}$. Dalje, neka su $a_1, a_2, \ldots, a_n \in A$ različiti. Ako simbole konstanata $c_1, c_2, \ldots, c_n$ interpretiramo redom sa $a_1, a_2, \ldots, a_n$, tada je ekspanzija modela $\mathbf{A}$, $(\mathbf{A}, a_1, a_2, \ldots, a_n)$ model za $\Delta'$, i tim pre model za $\Delta$.

Kako svaki konačan podskup teorije $S$ ima model, prema Stavu kompaktnosti $S$ ima neki model $(\mathbf{A}, a_i)_{i \in I}$, gde su simboli $c_i$ interpretirani sa $a_i$, i gde je $\mathbf{A}$ model teorije $T$. S obzirom na aksiome $c_i \neq c_j$ za $i \neq j$, elementi $a_i$ su uzajamno različiti, što znači da je $|A| \geq k$. $\diamondsuit$

Pogledajmo sledeća dva primera. S obzirom da je uređeno polje racionalnih brojeva beskonačno, prema prethodnoj teoremi postoje uređena polja proizvoljno velike beskonačne kardinalnosti, kao i gusto linearno uređeni skupovi. S druge strane, prema istoj teoremi, s obzirom da za svaki prirodan broj $n$ postoji grupa reda $n$, klasa svih konačnih grupa nije aksiomatska klasa.

Drugi primer primene Stava kompaktnosti odnosi se na uređene skupove.

**2.3.6 Teorema** *Neka je* $\mathbf{A} = (A, \preceq)$ *parcijalno uređen skup. Tada se* $\mathbf{A}$ *može proširiti do linearno uređenog skupa, tj. postoji linearno uređenje* $\preceq'$ *domena* $A$ *tako da za sve* $a, b \in A$, $a \preceq b$ *povlači* $a \preceq' b$.

Pre dokaza ove teoreme dokažimo tu teoremu u slučaju konačnih skupova.

**Dokaz** teoreme ako je $A$ konačan skup. Dokaz izvodimo potpunom indukcijom po broju elemenata skupa $A$. Neka je $|A| = n$. Ako je $n = 1$ tvrđenje očigledno važi, pa pretpostavimo da je $n > 1$. Kako je $A$ konačan skup, postoji minimalan element $a \in A$ u odnosu na uređenje $\preceq$. Neka je $B = A - \{a\}$ i $(B, \preceq_B)$ restrikcija uređenja $\preceq$ na domen $B$. Kako je $|B| < |A|$, prema induktivnoj hipotezi postoji linearno uređenje $\leq_B$ koje proširuje $\preceq_B$. Tada $\leq_A = \{a\} \times A \cup \leq_B$ linearno uređuje skup $A$ i proširuje parcijalno uređenje $\preceq$.

**Dokaz** teoreme za proizvoljne skupove. Neka je $C = \{\underline{a} : a \in A\}$ skup novih simbola konstanti. Ovde je svakom simbolu $a \in A$ pridružen simbol $\underline{a}$, takozvano *ime* elementa $a$, s tim da različitim elementima skupa $A$ odgovaraju različita imena kao i da $\underline{a} \notin L$. Dalje, neka je jezik $L = \{\leq\} \cup C$, gde je $\leq$ binarni relacijski znak, i neka je $T$ teorija jezika $L$ definisana pomoću

$$T = \mathrm{LO} \cup \{\underline{a} \neq \underline{b} : a, b \in A, a \not\equiv b\} \cup \{\underline{a} \leq \underline{b} : a \preceq b, a, b \in A\}.$$

Podsetimo se da je LO teorija linearnog uređenja.

Dokazujemo da svaki konačan podskup teorije $T$ ima model. Neka je $\Delta \subseteq T$ konačan. Tada postoji konačan $S \subseteq A$ tako da svaki simbol konstanti iz $C$ koji se javlja u $\Delta$ jeste neki element iz $\{\underline{a} : a \in S\}$. Bez gubljenja opštosti možemo uzeti da je tada

$$\Delta = \mathrm{LO} \cup \{\underline{a} \neq \underline{b} : a, b \in S, a \not\equiv b\} \cup \{\underline{a} \leq \underline{b} : a \preceq b, a, b \in S\}.$$

Prema dokazu teoreme za konačne skupove postoji linearno uređenje $\leq^S$ domena $S$ koje proširuje restrikciju uređenja $\preceq$ na domen $S$. Tada je $(S, \leq^S)$ model teorije $\Delta$, dakle svaki konačan podskup teorije $T$ ima model.

Prema teoremi kompaktnosti teorija $T$ ima model $\mathbf{B} = (B, \leq^{\mathbf{B}}, \underline{a}^{\mathbf{B}})_{a \in A}$. S obzirom da je $\mathbf{B} \models \mathrm{LO}$, to je $\mathbf{B}$ linearno uređen skup. Neka je $h : A \to B$ preslikavanje definisano pomoću $h : a \mapsto \underline{a}^{\mathbf{B}}$, $a \in A$. Nije teško videti da je $h$ utapanje:

Pretpostavimo da je $a \not\equiv b$, $a, b \in A$. Tada je $(\underline{a} \neq \underline{b}) \in T$, pa kako je $\mathbf{B} \models T$, to je $\mathbf{B} \models \underline{a} \neq \underline{b}$, dakle $\underline{a}^{\mathbf{B}} \not\equiv \underline{b}^{\mathbf{B}}$, tj. $h$ je $1-1$.

Pretpostavimo sada da je $a \preceq b$, $a, b \in A$. Tada je $(\underline{a} \leq \underline{b}) \in T$, pa kako je $\mathbf{B} \models T$, to je $\mathbf{B} \models \underline{a} \leq \underline{b}$, dakle $\underline{a}^{\mathbf{B}} \leq^{\mathbf{B}} \underline{b}^{\mathbf{B}}$, tj. $h$ je homomorfizam.

Definišimo uređenje $\preceq'$ domena $A$ pomoću $a \preceq' b$, $a, b \in A$, akko $\underline{a}^{\mathbf{B}} \leq^{\mathbf{B}} \underline{b}^{\mathbf{B}}$. Nije teško videti da $\preceq'$ zadovoljava uslove teoreme. $\diamondsuit$

Deo osobina neke elementarne klase struktura proističe iz oblika aksioma koje definišu tu klasu. Pre formulacija odgovarajućih teorema evo definicija posebnih vrsta formula koje se koriste u tim tvrđenjima.

**2.3.7 Definicija** *Formula $\varphi$ jezika $L$ je univerzalna ako i samo ako je oblika $\forall x_1 x_2 \dots x_n \psi$, gde je $\psi$ formula jezika $L$ bez kvantora.*

Formula $\varphi$ jezika $L$ je *univerzalno-egzistencijalna* akko je oblika

$$\forall x_1 x_2 \dots x_n \exists y_1 y_2 \dots y_m \psi,$$

gde je $\psi$ formula jezika $L$ bez kvantora. Primetimo da je svaka univerzalna formula takođe univerzalno-egzistencijalna.

Sledeće tvrđenje je uopštenje Teoreme 1.7.5.

**2.3.8 Teorema** *Neka je $T$ teorija jezika $L$ čije su sve aksiome univerzalne. Tada je klasa $\mathfrak{M}(T)$ zatvorena za podmodele, tj. ako su $\mathbf{A}$ i $\mathbf{B}$ modeli jezika $L$ takvi da je $\mathbf{A} \models T$ i $\mathbf{B} \subseteq \mathbf{A}$, onda je i $\mathbf{B} \models T$.*

**Dokaz** Neka je $\mathbf{A} \models T$ i $\mathbf{B} \subseteq \mathbf{A}$, gde su $\mathbf{A}$ i $\mathbf{B}$ modeli jezika $L$. Najpre dokazujemo:

(1) Neka formula $\varphi$ jezika $L$ ne sadrži kvantore, i neka je $\mu$ valuacija domena $B$. Tada $\mathbf{A} \models \varphi[\mu]$ akko $\mathbf{B} \models \varphi[\mu]$.

Dokaz tvrđenja (1) izvešćemo indukcijom po dužini formule $\varphi$. Prvo razmotrimo slučaj atomičnih formula. Ako je $\varphi$ formula $u = v$, s obzirom da je $\mathbf{B} \subseteq \mathbf{A}$ to je $u^{\mathbf{A}}[\mu] = u^{\mathbf{B}}[\mu]$ i $v^{\mathbf{A}}[\mu] = v^{\mathbf{B}}[\mu]$, pa $\mathbf{A} \models (u = v)[\mu]$ akko $u^{\mathbf{A}}[\mu] = v^{\mathbf{A}}[\mu]$ akko $u^{\mathbf{B}}[\mu] = v^{\mathbf{B}}[\mu]$ akko $\mathbf{B} \models (u = v)[\mu]$. Slično, ako su $u_1, u_2, \dots, u_n \in \mathrm{Term}_L$, onda $(u_1^{\mathbf{A}}[\mu], \dots, u_n^{\mathbf{A}}[\mu]) = (u_1^{\mathbf{B}}[\mu], \dots, u_n^{\mathbf{B}}[\mu])$, pa ako je $R \in Rel_L$ dužine $n$, sledi $R^{\mathbf{A}}(u_1^{\mathbf{A}}[\mu], \dots, u_n^{\mathbf{A}}[\mu])$ akko $R^{\mathbf{B}}(u_1^{\mathbf{B}}[\mu], \dots, u_n^{\mathbf{B}}[\mu])$. Dakle, tvrđenje (1) važi za atomične formule.

Neka je $\varphi$ oblika $\neg\psi$. Tada

| | | | |
|---|---|---|---|
| $\mathbf{A} \models \varphi[\mu]$ | akko | *nije* $\mathbf{A} \models \psi[\mu]$, | prema induktivnoj hipotezi |
| | akko | *nije* $\mathbf{B} \models \psi[\mu]$, | |
| | akko | $\mathbf{B} \models \varphi[\mu]$. | |

Neka je $\varphi$ oblika $\psi \wedge \theta$. Tada

| | | | |
|---|---|---|---|
| $\mathbf{A} \models \varphi[\mu]$ | akko | $\mathbf{A} \models \psi[\mu]$ *i* $\mathbf{A} \models \theta[\mu]$, | prema induktivnoj hipotezi |
| | akko | $\mathbf{B} \models \psi[\mu]$ *i* $\mathbf{B} \models \theta[\mu]$, | |
| | akko | $\mathbf{B} \models \varphi[\mu]$. | |

Dokaz za ostale logičke veznike teče na isti način, pa je ovim (1) dokazano.

Nastavimo sada sa dokazom teoreme. Neka je $\mathbf{A} \models \varphi$, gde je $\varphi$ univerzalna rečenica $\forall x_1 x_2 \dots x_n \psi x_1 x_2 \dots x_n$ i $\psi x_1 x_2 \dots x_n$ je bez kvantora. Za $b_1, b_2, \dots, b_n \in B$ tada je $\mathbf{A} \models \psi[b_1, b_2, \dots, b_n]$, pa prema (1) takođe je $\mathbf{B} \models \psi[b_1, b_2, \dots, b_n]$. S obzirom da su $b_1, b_2, \dots, b_n \in B$ proizvoljni, sledi $\mathbf{B} \models \varphi$. Prema tome sve aksiome teorije $T$ važe u $\mathbf{B}$, dakle $\mathbf{B}$ je model teorije $T$. $\diamondsuit$

**2.3.9 Primer** Neka je

$$u_1(x_1, x_2, \dots, x_n) = b_1, u_2(x_1, x_2, \dots, x_n) = b_2, \dots, u_m(x_1, x_2, \dots, x_n) = b_m, \qquad (S)$$

sistem linearnih jednačina sa koeficijentima u polju racionalnih brojeva. Tada sistem $(S)$ ima rešenje nad poljem racionalnih brojeva $\mathbf{Q}$ akko $(S)$ ima rešenje nad poljem realnih brojeva $\mathbf{R}$.

Najpre primetimo da se $(S)$ može zapisati kao neka formula $\psi x_1 x_2 \dots x_n$ bez kvantora u jeziku teorije linearno uređenih polja:

$$u_1(x_1, x_2, \dots, x_n) = b_1 \wedge \dots \wedge u_m(x_1, x_2, \dots, x_n) = b_m \qquad (S)$$

Uzeli smo da racionalnim brojevima odgovaraju termi (razlomci) izgrađeni od $0, 1, +, -, /$. Ako je $q_1, q_2, \dots, q_n \in Q$ rešenje sistema $(S)$, to znači da je $\mathbf{Q} \models \psi[q_1, q_2, \dots, q_n]$, pa prema tvrđenju (1) u dokazu prethodne teoreme takođe je $\mathbf{R} \models \psi[q_1, q_2, \dots, q_n]$, tj. $q_1, q_2, \dots, q_n$ je rešenje sistema $(S)$ i u polju $\mathbf{R}$. Dakle, ako je sistem $(S)$ neprotivurečan nad poljem $\mathbf{Q}$, onda je $(S)$ neprotivurečan i nad poljem $\mathbf{R}$.

Pretpostavimo sada da je sistem $(S)$ neprotivurečan nad poljem $\mathbf{R}$. Tada je prema Kroneker-Kapelijevoj teoremi u polju $\mathbf{R}$, $\mathrm{rang}A = \mathrm{rang}[A, b]$, gde je $A$ matrica sistema $(S)$ i $b = (b_1, b_2, \dots, b_n)$. S obzirom da su elementi matrica $A$ i $[A, b]$ racionalni brojevi i koristeći činjenicu da se rang matrice može sračunati, na primer, pomoću minora matrice, vidimo da je identitet $\mathrm{rang}A = \mathrm{rang}[A, b]$ ekvivalentan nekoj formuli bez kvantora $\theta$ jezika teorije polja. Dakle $\mathbf{R} \models \theta$, odakle je prema prethodnoj teoremi $\mathbf{Q} \models \theta$, tj. $\mathrm{rang}A = \mathrm{rang}[A, b]$ i u polju $\mathbf{Q}$. Opet primenjujući Kroneker-Kapelijevu teoremu nalazimo da je $(S)$ neprotivurečan sistem nad poljem $\mathbf{Q}$.

Sličnim razmatranjem i polazeći od Furie-Mockinovog algoritma za rešavanje sistema jednačina i nejednačina nad uređenim poljima, može se dokazati da je neki sistem $(S)$ jednačina i nejednačina sa koeficijentima u $Q$ neprotivurečan nad uređenim poljem $\mathbf{Q}$ akko je $(S)$ neprotivurečan nad uređenim poljem $\mathbf{R}$.

*Lanac* modela jezika $L$ je niz modela $\mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \dots$ jezika $L$. *Unija* lanca modela $\mathbf{A}_i$ je model $\mathbf{A}$ jezika $L$ definisan na sledeći način. Domen je $A = \cup_i A_i$. Ako je $c \in L$ simbol konstante, onda je $c^{\mathbf{A}} = c^{\mathbf{A}_0}$. Neka je $F \in \mathrm{Fun}_L$ dužine n, i neka su $a_1, a_2, \dots, a_n \in A$. Tada za svaki $i \leq n$ postoji $k_i$ takav da je $a_i \in A_{k_i}$. S obzirom da je $A_0 \subseteq A_1 \subseteq \dots$, za $k = \max\{k_1, k_2, \dots, k_n\}$ sledi $a_1, a_2, \dots, a_n \in A_k$. Neka je $F^{\mathbf{A}}(a_1, a_2, \dots, a_n) = F^{\mathbf{A}_k}(a_1, a_2, \dots, a_n)$. Slično, ako je $R \in \mathrm{Rel}_L$ dužine $n$, uzećemo da je $R^{\mathbf{A}}(a_1, a_2, \dots, a_n)$ akko $R^{\mathbf{A}_k}(a_1, a_2, \dots, a_n)$. Nije teško videti da je ovako definisana struktura $\mathbf{A}$ dobro definisan model jezika $L$, kao i da je svaki $\mathbf{A}_n$ podmodel modela $\mathbf{A}$. Ovaj model označavaćemo pomoću $\bigcup_n \mathbf{A}_n$. U vezi sa unijama lanaca modela imamo sledeću teoremu.

**2.3.10 Teorema** *Neka je $T$ teorija koja ima univerzalno-egzistencijalne aksiome. Tada je $\mathfrak{M}(T)$ zatvorena za unije lanaca modela, tj. ako je $\mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \dots$ niz modela teorije $T$, tada je i unija $\mathbf{A}$ lanca ovih modela takođe model ove teorije.*

**Dokaz** Neka je $\mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \dots$ lanac modela teorije $T$, i neka je $\mathbf{A}$ unija ovih modela. Dalje, neka je $\varphi \in T$. Dokazujemo da $\varphi$ važi u modelu $\mathbf{A}$. S obzirom da je $\varphi$ univerzalno-egzistencijalna, postoji formula $\psi(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$ tako da je $\varphi = \forall x_1 x_2 \dots x_n \exists y_1 y_2 \dots y_m \psi(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$, i takođe za sve $i$, $\mathbf{A}_i \models \varphi$. Neka su $a_1, a_2, \dots, a_n \in A$ proizvoljni. Kao u opisu unije modela, nalazimo $k$ tako da je $a_1, a_2, \dots, a_n \in A_k$. S obzirom da je $\mathbf{A}_k \models \varphi$, postoje $b_1, b_2, \dots, b_m \in A_k$ tako da je $\mathbf{A}_k \models \psi[a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m]$. S obzirom da je $\mathbf{A}_k \subseteq \mathbf{A}$, sledi $\mathbf{A} \models \psi[a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m]$. Prema tome $\mathbf{A} \models \varphi$. $\diamondsuit$

**2.3.11 Primer** $1^\circ$ Aksiome svake algebarske teorije su univerzalno–egzistencijalne, prema tome algebarski varijeteti su zatvoreni za unije algebri. Dakle, unija lanca grupa je grupa, unija lanca prstena je prsten, itd.

2° Aksiome linearno uređenih polja su takođe univerzalno-egzistencijalne, dakle unija lanca uređenih polja je uređeno polje.

**2.3.12 Primer** Lanac utapanja i modela jezika $L$ je niz

$$\mathbf{A}_0 \xrightarrow{h_0} \mathbf{A}_1 \xrightarrow{h_1} \mathbf{A}_2 \xrightarrow{h_2} \cdots .$$

modela jezika $L$ i utapanja kako je prikazano na dijagramu. Prema Teoremi 2.2.5 postoji lanac modela

$$\mathbf{A}'_0 \subseteq \mathbf{A}'_1 \subseteq \mathbf{A}'_2 \subseteq \cdots .$$

i niz izomorfizama $p_i : \mathbf{A}_i \to \mathbf{A}'_i$, tako da je sledeći dijagram komutativan:

(D-1)
$$\begin{tikzcd}
\mathbf{A}_0 \arrow[r, "h_0"] \arrow[d, "p_0"] & \mathbf{A}_1 \arrow[r, "h_1"] \arrow[d, "p_1"] & \mathbf{A}_2 \arrow[r, "h_2"] \arrow[d, "p_2"] & \ldots \\
\mathbf{A}'_0 \arrow[r, "i_0"] & \mathbf{A}'_1 \arrow[r, "i_1"] & \mathbf{A}'_2 \arrow[r, "i_2"] & \ldots
\end{tikzcd}$$

gde su $i_n$ inkluziona preslikavanja. Neka je $\mathbf{A} = \cup_n \mathbf{A}'_n$. Model $\mathbf{A}$ zvaćemo *graničnom vrednošću* modela $\mathbf{A}_i$, i taj model obeležavaćemo pomoću $\lim_n \mathbf{A}_n$. Homomorfizmi $p_i$ : $\mathbf{A}_i \to \mathbf{A}$ su utapanja, kao i $h_{ij} : \mathbf{A}_i \to \mathbf{A}_j$, gde su $h_{ij} = h_{j-1} \circ \ldots \circ h_{i+1} \circ h_i$, $i < j$. Za tako izabrana preslikavanja, za sve $i, j$ dijagram D-2 komutira.

$$\begin{tikzcd}
\mathbf{A}_i \arrow[r, "h_{ij}"] & \mathbf{A}_j \arrow[d, "p_j"] \\
p_i & \mathbf{A}
\end{tikzcd}$$
D-2

$$\begin{tikzcd}
\mathbf{A}_i \arrow[r, "h_{ij}"] & \mathbf{A}_j \arrow[d, "q_j"] \\
q_i & \mathbf{B}
\end{tikzcd}$$
D-3

$$\begin{tikzcd}
\mathbf{A}_i \arrow[r, "p_i"] & \mathbf{A} \arrow[d, "g"] \\
q_i & \mathbf{B}
\end{tikzcd}$$
D-4

Model $\mathbf{A}$ ima interesantno svojstvo minimalnosti. Naime, ako je $\mathbf{B}$ bilo koji model jezika $L$ sa istom osobinom, tj. ako dijagram D-3 komutira za sve $i, j$, gde su $q_i : \mathbf{A}_i \to \mathbf{B}$ utapanja, onda se $\mathbf{A}$ utapa u $\mathbf{B}$. Zaista, utapanje $g : \mathbf{A} \to \mathbf{B}$ definišemo na sledeći način. Za $a \in A$ postoji $i$ tako da je $a \in A_i$. Neka je $g(a) = q_i p_i^{-1}(a)$. Nije teško proveriti da je preslikavanje $g$ dobro definisano, kao i da dijagram D-4 komutira.

Obrati teorema 2.3.8 i 2.3.10 takođe važe. Ovde ćemo dati skicu dokaza obrata teoreme 2.3.8. U tom dokazu koristićemo se *dijagramima* modela. Neka je $\mathbf{A}$ model jezika $L$ i neka je $L_A = L \cup \{\underline{a} \mid a \in A\}$. Dijagram modela $\mathbf{A}$ je skup $\Delta_{\mathbf{A}}$ atomičnih i negacija atomičnih rečenica jezika $L_A$, tačnih u $(\mathbf{A}, a)_{a \in A}$. Primetimo da su formule iz $\Delta_{\mathbf{A}}$ rečenice.

**2.3.13 Lema**

1. *Svaka konačna konjunkcija formula iz* $\Delta_{\mathbf{A}}$ *je tačna u modelu* $(\mathbf{A}, a)_{a \in A}$.
2. *Ako je* $\mathbf{B}$ *model jezika* $L$, *tada se* $\mathbf{A}$ *utapa u* $\mathbf{B}$ *akko postoji ekspanzija modela* $\mathbf{B}$ *do strukture* $(\mathbf{B}, b_a)_{a \in A}$ *koja je model teorije* $\Delta_{\mathbf{A}}$.

**Dokaz** Dokažimo tvrđenje 2. Ako je $f : \mathbf{A} \to \mathbf{B}$ utapanje, tada je $(\mathbf{B}, f(a))_{a \in A} \models \Delta_{\mathbf{A}}$. S druge strane, ako je $(\mathbf{B}, b_a)_{a \in A} \models \Delta_{\mathbf{A}}$, tada je preslikavanje $g : A \to B$, definisano sa $g : a \mapsto b_a$, utapanje modela $\mathbf{A}$ u $\mathbf{B}$. $\diamondsuit$

U dokazu teoreme koja sledi, koristićemo takođe sledeće tvrđenje iz logike.

**2.3.14** ***Lema o promenljivoj konstanti*** *Neka je $T$ teorija jezika $L$ i neka je $\varphi(x)$ formula jezika $L$. Dalje, pretpostavimo da je $c$ simbol konstante koji nije u $L$. Ako je $\varphi(c)$ teorema teorije $T$, tada je $\forall x\varphi(x)$ takođe teorema teorije $T$.*

**Dokaz** Ako je $\varphi_1(c), \dots, \varphi_n(c)$ dokaz u $T$ formule $\varphi_n(c) \equiv \varphi(c)$, neka je $x$ promenljiva koja se ne pojavljuje u formulama tog niza. Tada je i $\varphi_1(x), \dots, \varphi_n(x)$ dokaz u $T$ formule $\varphi(x)$. Primenom pravila izvođenja generalizacije, nalazimo da je $\forall x\varphi(x)$ takođe teorema teorije $T$. $\diamondsuit$

**2.3.15 Teorema** *Neka je $\mathfrak{M}$ aksiomatska klasa struktura jezika $L$. Ako je klasa $\mathfrak{M}$ zatvorena za podmodele, onda $\mathfrak{M}$ ima aksiomatizaciju pomoću univerzalnih aksioma.*

**Dokaz** Neka je $T$ teorija jezika $L$ koja opisuje klasu $\mathfrak{M}$, tj. $\mathfrak{M} = \mathfrak{M}(T)$. Dalje, neka je

$$S = \{\varphi \mid \varphi \text{ je univerzalna rečenica jezika } L \text{ i } \varphi \text{ važi na svim modelima iz } \mathfrak{M}\}.$$

Neka je $\mathbf{A}$ proizvoljan model jezika $L$ koji zadovoljava sve aksiome iz $S$. Dokazujemo da svaki konačan podskup $S'$ teorije $T \cup \Delta_{\mathbf{A}}$ ima model. Bez gubljenja opštosti možemo uzeti $S' = T \cup \{\varphi_1, \varphi_2, \dots, \varphi_n\}$, gde su $\varphi_1, \varphi_2, \dots, \varphi_n \in \Delta_{\mathbf{A}}$. Pretpostavimo da $S'$ *nema* model. Neka je $\psi = \wedge_i \varphi_i$. Po pretpostavci $S'$ nema model, dakle, $T \cup \{\psi\}$ je protivrečna teorija, pa $T \vdash \neg\psi$. Primetimo da je formula $\psi$ bez kvantora, kao i da je $\psi \equiv \psi(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_m)$ za neke $a_1, a_2, \dots, a_m \in A$, pa s obzirom da $\underline{a}_1, \underline{a}_2, \dots, \underline{a}_m$ ne pripadaju $L$, prema Lemi 2.3.14, $T \vdash \forall x_1 \dots x_m \neg\psi(x_1, \dots, x_m)$. U $\mathbf{A}$ važe sve univerzalne posledice teorije $T$, pa u $\mathbf{A}$ važi $\forall x_1 \dots x_m \neg\psi(x_1, \dots, x_m)$ odnosno $\forall x_1 \dots x_m \neg \wedge_i \varphi_i(x_1, \dots, x_m)$. Dakle, u $(\mathbf{A}, a)_{a\in A}$ važi $\neg \wedge_i \varphi_i(\underline{a}_1, \dots, \underline{a}_m)$, suprotno Lemi 2.3.13.1. Prema tome $S'$ ima model.

Prema Stavu kompaktnosti, dakle, teorija $T \cup \Delta_{\mathbf{A}}$ ima model, neka je to $(\mathbf{B}, b_a)_{a\in A}$. Tada je $\mathbf{B} \in \mathfrak{M}$, dok prema Lemi 2.3.13 onda model $\mathbf{B}$ sadrži izomorfnu kopiju modela $\mathbf{A}$, pa je $\mathbf{A}$ podmodel strukture iz $\mathfrak{M}$. Prema pretpostavci teoreme onda je $\mathbf{A} \in \mathfrak{M}$. Dakle, dokazali smo da je svaki model teorije $S$ takođe model teorije $T$, dok je očigledno svaki model teorije $T$ model i teorije $S$. Otuda je $\mathfrak{M} = \mathfrak{M}(T) = \mathfrak{M}(S)$. $\diamondsuit$

## 2.4 Modeli sa dva domena

Podsetimo se da je svaki vektorski prostor oblika $\mathcal{V} = (\mathbf{V}, \mathbf{F}, \bullet)$, gde je $\mathbf{V} = (V, +, -, \mathbf{0})$ Abelova grupa, $\mathbf{F} = (F, +, \cdot, 0, 1)$ je polje i $\bullet : F \times V \to V$ tzv. spoljašna operacija množenja vektora skalarima. Ovo je primer strukture u kojoj se pojavljuju dva domena: skup vektora $V$ i skup skalara $F$ sa pripadnim algebarskim strukturama. Ovako definisana struktura očigledno ne zadovoljava definiciju algebre, odnosno modela, kako smo te pojmove definisali u ovoj knjizi. Ima nekoliko načina da se i ovako prošireni pojmovi algebarskih struktura svedu na standardne pojmove algebri odnosno modela.

Prvu mogućnost daje nam tzv. *dvosortna logika*. Ova logika se razlikuje od predikatskog računa prvog reda u tome što se uvode dve vrste promenljivih, recimo:

$x, y, z, \ldots$ i $\alpha, \beta, \gamma, \ldots$ koje uzimaju vrednosti u dva različita domena. U tom slučaju modeli ove logike su oblika $\mathcal{A} = (\mathbf{A}, \mathbf{B}, \mathcal{F}, \mathcal{R})$ gde su $\mathbf{A}$ i $\mathbf{B}$ modeli redom disjunktnih jezika $L_1$ i $L_2$, dok je $\mathcal{F}$ neki skup spoljašnjih operacija, a $\mathcal{R}$ je neki skup spoljašnjih relacija strukture $\mathcal{A}$. Dakle, za svaki $F \in \mathcal{F}$ postoje $m, n \in N^+$ tako da je $F : A^m \times B^n \to A$ ili $F : A^m \times B^n \to B$. Slično, za svaki $R \in \mathcal{R}$ postoje $m, n \in N^+$ tako da je $R \subseteq A^m \times B^n$. Onda vektorski prostor $\mathcal{V} = (\mathbf{V}, \mathbf{F}, \bullet)$ možemo smatrati strukturom dvosortne logike jezika $L_1 = \{\oplus, \ominus, \mathbf{0}\}$ i $L_2 = \{+, -, \cdot, 0, 1\}$, gde je $\mathcal{F} = \{\bullet\}$, $\bullet : F \times V \to V$ i $\mathcal{R} = \emptyset$. Slično predikatskom računu 1. reda mogu se i za dvosortnu logiku izgraditi pojmovi algebarskih terma, formula, rečenica, teorija itd. U matematičkoj logici dokazuje se da se ova logika može svesti na običan predikatski račun 1. reda. Mogu se uvesti strukture i sa više domena (3, 4, ...), koje nisu od nekog značaja za algebru, ali imaju primenu u računarstvu i matematičkoj lingvistici u definisanju tzv. *denotacijskih (skupovnih) semantika* programskih i prirodnih jezika.

Drugi način svođenja je odgovarajuća adaptacija uopštene algebarske strukture do modela ili algebre predikatskog računa 1. reda. Prikazaćemo taj metod na primeru vektorskih prostora, definišući vektorski prostor kao algebru sa operatorima.

**2.4.1 Primer** *Algebarski varijetet vektorskih prostora nad datim poljem* $\mathbf{F}$. Neka je $\mathbf{F} = (F, +, -, \cdot, 0, 1)$ neko algebrasko polje, fiksirano u daljem razmatarnju, $L = \{\oplus, \ominus, \mathbf{0}\}$ algebarski jezik gde je $\oplus$ simbol binarne operacije, $\ominus$ simbol unarne operacije i $\mathbf{0}$ je simbol konstante. Dalje, neka je $L_F = \{f_\alpha | \, \alpha \in F\}$ skup unarnih operacijskih simbola. Najzad, za jezik vektorskih prostora biramo $L_V = L \cup L_F$, dok će aksiome vektorskih prostora biti:

(1) Aksiome Abelovih grupa za L:
$x \oplus (y \oplus z) = (x \oplus y) \oplus z, \;\; x \oplus y = y \oplus x, \;\; x \oplus \mathbf{0} = x, \;\; x \oplus (-x) = \mathbf{0}$

(2) Za sve $\alpha, \beta \in F$:
$f_{\alpha+\beta}(x) = f_\alpha(x) \oplus f_\beta(x), \; f_\alpha(x + y) = f_\alpha(x) \oplus f_\alpha(y), \; f_\alpha(f_\beta(x)) = f_{\alpha\beta}(x), \; f_1(x) = x.$

Dakle, vektorski prostor u smislu ove definicije biće algebra $\mathbf{V} = (V, +, -, \mathbf{f}_\alpha, 0)_{\alpha \in F}$ koja zadovljova navedene algebarske zakone. Unarne operacije $\mathbf{f}_\alpha$, $\alpha \in F$, nazivamo *operatorima* algebre $\mathbf{V}$. Primetimo, ako je $F$ beskonačno polje, onda je $\mathbf{V}$ algebra beskonačne signature. Prema tome klasa svih vektorskih prostora nad datim poljem je algebarski varijetet, što znači da je podalgebra vektorskog prostora nad poljem $\mathbf{F}$ vektorski prostor nad poljem $\mathbf{F}$, proizvod vektorskih prostora nad poljem $\mathbf{F}$ je vektorski prostor nad poljem $\mathbf{F}$, itd.

Ako je vektorski prostor $\mathcal{V} = (\mathbf{V}, \mathbf{F}, \bullet)$ dat kao dvodomenska algebra, nije teško proveriti da algebra $\mathcal{V}' = (V, +, -, \mathbf{f}_\alpha, 0)_{\alpha \in F}$ zadovoljava navedene aksiome, ako su operatori $\mathbf{f}_\alpha : V \to V$, $\alpha \in F$ definisani pomoću $\mathbf{f}_\alpha(x) = \alpha \bullet x$, $x \in V$. Obrnuto, ukoliko je vektorski prostor dat kao algebra sa operatorima, na primer $\mathbf{V} = (V, +, -, \mathbf{f}_\alpha, 0)_{\alpha \in F}$, onda je $\mathbf{V}^* = ((V, +, -, 0), \mathbf{F}, \bullet)$ vektorski prostor predstavljen kao dvodomenska algebra. Pri tome važi $\mathbf{V}^{*\prime} = \mathbf{V}$, i obrnuto, ako je vektorski prostor dat kao dvodomenska algebra $\mathcal{V}$, onda $\mathcal{V}'^* = \mathcal{V}$.

**2.4.2 Primer** *Algebarski varijetet levih modula nad datim prstenom* $\mathbf{P}$. Neka je $\mathbf{P} = (P, +, -, \cdot, 0, 1)$ neki prsten sa jedinicom, fiksiran u daljem razmatranju. *Levi modul* nad prstenom $\mathbf{P}$ je svaka algebarska struktura $\mathbf{M} = (M, +, -, \mathbf{f}_\alpha, 0)_{\alpha \in P}$ koja zadovoljava algebarske zakone (1) i (2) iz prethodnog primera. Dakle, razlika u odnosu na pojam vektorskog prostora je što se umesto polja $\mathbf{F}$ uzima prsten, u ovom slučaju $\mathbf{P}$, i prema tome $(M, +, -, 0)$ je Abelova grupa. Shodno prethodnom primeru, jasno je kako se levi moduli nad prstenom $\mathbf{P}$ mogu predstaviti kao dvodomenske algebre. Primetimo da je svaki vektorski prostor nad poljem $\mathbf{F}$ jedan primer modula nad $\mathbf{F}$.

## Zadaci

**2.1** Za jezik $L$ prvog reda, neka je $||L||$ kardinalni broj skupa svih formula jezika $L$. Neka je $L$ najviše prebrojiv jezik. Dokazati da je $||L|| = \aleph_0$. Ako je $L$ beskonačan skup, dokazati da je $||L|| = |L|$.

**2.2** Neka je $\mathfrak{M}$ klasa modela jezika $L$ i neka je binarna relacija $\sim$ skupa $\mathrm{Sent}_L$ uvedena pomoću $\varphi \sim \psi$ ako i samo ako $\varphi \Leftrightarrow \psi$ važi na svim modelima iz $\mathfrak{M}$. Dokazati da je $\sim$ relacija ekvivalencije, kao i da je $(\mathrm{Sent}_L/\sim, +, \cdot, ', \mathbf{0}, \mathbf{1})$ Bulova algebra, gde je $\varphi/\sim + \psi/\sim = (\varphi \vee \psi)/\sim$, $\varphi/\sim \cdot \psi/\sim = (\varphi \wedge \psi)/\sim$, $\mathbf{0} = \varphi \wedge \neg\varphi$, $\mathbf{1} = \varphi \vee \neg\varphi$, $\varphi, \psi \in \mathrm{Sent}_L$.

**2.3** Neka je $(X, \leq)$ parcijalno uređen skup i neka je binarna relacija $<$ na $X$ definisana pomoću $x < y \Leftrightarrow x \leq y \wedge x \neq y$. Dokazati da $<$ zadovoljava aksiome *striktnog* uređenja: $x < y \Rightarrow \neg y < x$, i $x < y \wedge y < z \Rightarrow x < z$. Ako definišemo binarnu relaciju $\leq'$ na $X$ pomoću $x \leq' y \Leftrightarrow x < y \vee x = y$, dokazati da se relacije $\leq$ i $\leq'$ poklapaju.

**2.4** Neka je $V$ skup iz Primera 1.1.10. Dokazati da $(V, \in)$ zadovoljava sve aksiome teorije ZFC, osim aksiome beskonačnosti.

**2.5** Formula $\varphi$ jezika $L$ je *pozitivna* ako se od logičkih znakova u $\varphi$ javljaju jedino $=$, $\vee$, $\wedge$, $\exists$ i $\forall$. Dokazati da homomorfizmi modela održavaju pozitivne formule, tj. ako je $\varphi$ pozitivna, $\mathbf{A} \models \varphi$ i $h : \mathbf{A} \xrightarrow{\text{na}} \mathbf{B}$, onda i $\mathbf{B} \models \varphi$.

**2.6** Abelova grupa $\mathbf{A} = (A, +, -, 0)$ je grupa sa deljenjem ako za svaki $n \in N^+$, za svaki $a \in A$ postoji $b \in A$ tako da je $n \cdot b = a$. Dokazati da je klasa Abelovih grupa sa deljenjem aksiomatska.

**2.7** Polje $\mathbf{F}$ je algebarski zatvoreno ako svaki polinom stepena $\geq 1$ sa koeficijentima u $F$ ima koren u $\mathbf{F}$. Dokazati da je klasa algebarski zatvorenih polja aksiomatska.

**2.8** Navesti primer modela $\mathbf{A}$ i $\mathbf{B}$ i $1-1$ i *na* homomorfizma $h : \mathbf{A} \to \mathbf{B}$ koji nije izomorfizam.

**2.9** Neka je $\mathbf{A}$ model. Dokazati da je $(\mathrm{Aut}\mathbf{A}, \circ, ^{-1}, i_A)$ grupa.

**2.10** Neka je $Q(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in Q\}$. Dokazati:
**a.** $|\mathrm{Aut}(Q(\sqrt{2}), \leq)| = 2^{\aleph_0}$.
**b.** $\mathrm{Aut}(Q(\sqrt{2}), +, \leq, 0) = \{f_a \,|\, a \in Q^+(\sqrt{2})\}$, gde $f_a(x) = ax, x \in Q(\sqrt{2})$.
**c.** $\mathrm{Aut}(Q(\sqrt{2}), +, \leq, 0, 1) = \{i_Q\}$.

**2.11** Odrediti sve automorfizme uređenog polja realnih brojeva.

**2.12** Pretpostavimo da aksiomatska klasa $\mathfrak{M}$ ima beskonačan model. Dokazati da $\mathfrak{M}$ ima modele proizvoljno velike kardinalnosti. Otuda izvesti da postoje (uređena) polja proizvoljno velike kardinalnosti.

**2.13** Dokazati da sledeće klase modela nisu aksiomatske:
**a.** Klasa cikličnih grupa. **b.** Klasa konačnih grupa.
**c.** Klasa dobro uređenih skupova.

**2.14** Klasa modela $\mathfrak{M}$ istog jezika je konačno aksiomatska ako postoji konačan skup aksioma $T$ tako da je $\mathfrak{M} = \mathfrak{M}(T)$. Dokazati da sledeće klase nisu konačno aksiomatske:
**a.** Klasa Abelovih grupa sa deljenjem. **b.** Klasa polja karakterisitke 0.
**c.** Klasa svih beskonačnih grupa.

**2.15** Neka je $\mathfrak{M}_n$, $n \in N$ niz aksiomatskih klasa modela jezika $L$ tako da je $\mathfrak{M}_0 \supseteq \mathfrak{M}_1 \supseteq \mathfrak{M}_2 \supseteq \ldots$, i za svaki $n \in N$ postoji $\mathbf{A} \in \mathfrak{M}_n$, $\mathbf{A} \notin \mathfrak{M}_{n+1}$. Neka je $\mathfrak{M}$ klasa svih modela jezika $L$ koji pripadaju svakoj klasi $\mathfrak{M}_n$. Dokazati da je $\mathfrak{M}$ aksiomatska, ali ne i konačno aksiomatska klasa.

**2.16*** Dva modela $\mathbf{A}$ i $\mathbf{B}$ jezika $L$ su elementarno ekvivalentna ako zadovoljavaju iste rečenice jezika $L$. Dokazati: konačni, elementarno ekvivalentni modeli su izomorfni.

**2.17*** Neka je (S) konačan sistem linearnih jednačina i nejednačina sa racionalnim koeficijentima od nepoznatih $x_1, x_2, \ldots, x_n$. Dokazati da je (S) neprotivurečan sistem (ima beskonačno mnogo rešenja po $x_1, x_2, \ldots, x_n$) nad poljem racionalnih brojeva ako i samo ako je (S) neprotivurečan sistem (ima beskonačno mnogo rešenja po $x_1, x_2, \ldots, x_n$) nad poljem realnih brojeva.

**2.18** Predstaviti algebru kvadratnih matrica reda $n$ nad datim poljem $\mathbf{F}$ kao dvodomensku algebru, odnosno algebru sa operatorima.

**2.19** Neka je $\mathbf{A}$ Abelova grupa. Dokazati da je $\mathbf{EndA} = (\mathrm{End}\mathbf{A}, +, -, \circ, \mathbf{0}, \mathbf{1})$ prsten, gde je $\mathbf{0}(x) = 0$, $\mathbf{1}(x) = x$, $x \in A$, dok je za $f \in \mathrm{End}\mathbf{A}$ i $x \in A$: $(f+g)(x) = f(x) + g(x)$, $(-f)(x) = -f(x)$ i $\circ$ je slaganje funkcija. Dokazti da je $(\mathbf{A}, \mathbf{EndA}, \bullet)$ modul, gde je $f \bullet \alpha = f(\alpha)$, za $\alpha \in A$, $f \in \mathrm{End}\mathbf{A}$.

# 3. Brojevi

Brojevi su polazni objekti pomoću kojih se izgrađuju ostale osnovne matematičke strukture. O tome kakav značaj imaju, na primer, prirodni brojevi u zasnivanju matematike i u matematici uopšte, govori i sledeća Kronekerova (L. Kronecker) sentencija: "Bog je stvorio prirodne brojeve, a ljudi sve ostalo". Zaista, polazeći od prirodnih brojeva mogu se izgraditi celi i racionalni brojevi, od ovih realni, a opet od realnih kompleksni brojevi. Mnoga svojstva prirodnih brojeva se nasleđuju u tom nizu, ali se javljaju i neka druga o kojima nema smisla govoriti ukoliko je reč samo o prirodnim brojevima. Šireći pojam broja nastaju nova sredstva i ideje za izučavanje kako samih brojeva, tako i drugih struktura. U ovom poglavlju razmotrićemo sa algebarskog stanovišta izgradnju i zasnivanje pomenutih brojevnih struktura.

## 3.1 Prirodni brojevi

Prirodni brojevi spadaju sigurno u najstarije matematičke pojmove. O tome kako je nastala reč *broj*, Anton Bilimović u svojoj knjizi *Elementi više matematike*, I knj., str. 11 iz 1961 g. piše:

*Da li znate poreklo reči broj? Evo odgovora jednog filologa. Reč "broj" je staroslovenska reč; sačuvana je u srpskom jeziku; ona je u etimološkoj vezi sa glagolom – "brijati" – seći. Reč "broj" značila bi, prema tome, zasek ili zarez.*

*Pa kakva je veza između pojma "broj" i pojma "zasek"? Biće nam jasno, ako predstavimo sebi ovu sliku iz života starih Slovena. Pastir želi da prebroji svoje stado; uzima drveni štapić – raboš – i, prelazeći pogledom sa jedne na drugu ovcu, pravi na štapiću zaseke: koliko zaseka, toliko i ovaca. Zasek na štapiću je broj. Takav primitivan način brojanja, neposredno upoređivanje jedne množine sa drugom, leži u osnovi svakog brojanja.*

*Iz potrebe za prebrojavanjem nastao je niz prirodnih brojeva:* 1, 2, 3, ... *kao osnovna množina za upoređivanje.*

Ipak, prva aksiomatika prirodnih brojeva potiče tek od Dedekinda i Peana s kraja 19. veka. Te aksiome nisu date u formalizmu predikatskog računa 1. reda, ali sadrže primitivne simbole: simbol konstanti 0 i unarni funkcijski znak $'$. Tada Peanove aksiome glase:

P.1. 0 je prirodan broj.
P.2. Ako je $x$ prirodan broj, onda je i $x'$ prirodan broj.
P.3. Ako su $x$ i $y$ prirodni brojevi i $x' = y'$, onda $x = y$.
P.4. Za svaki prirodan broj $x$, $x' \neq 0$.

P.5. Neka je $\Phi$ bilo koje svojstvo takvo da 0 ima to svojstvo, i ako $x$ ima svojstvo $\Phi$ onda $x'$ ima svojstvo $\Phi$. Tada svaki prirodan broj ima svojstvo $\Phi$.

Aksioma P.5 naziva se *Aksiomom indukcije.* U toj aksiomi $\Phi$ može biti bilo koje svojstvo koje se odnosi na prirodne brojeve. Ako sa $N$ označimo skup prirodnih brojeva, onda svakom takvom svojstvu odgovara neki podskup $S$ skupa $N$, pa je $S = \{x \in N \mid \Phi(x)\}$. U tom slučaju aksioma indukcije glasi:

P$'$.5. Ako je $0 \in S$ i za svaki $x$, $x \in S$ povlači $x' \in S$, onda $S = N$.

*Numerali* su specijalna vrsta terma definisanih u jeziku Peanove aritmetike. Obeležavaju se pomoću prirodnih brojeva podvučenih crtom:

$$\underline{0} = 0,\ \ \underline{1} = \underline{0}' = 0',\ \ \underline{2} = \underline{1}' = (0')',\ \ \underline{3} = \underline{2}' = ((0')')', \ldots$$

Kao što ćemo se uveriti, numerali imaju mnoga svojstva prirodnih brojeva.

S gledišta teorije modela, Peanove aksiome samo opisuju svojstva prirodnih brojeva, ali ne daju odgovor na to, na koju se tačno strukturu one odnose. Ukoliko se za osnovu uzme klasična teorija skupova (recimo ZF sistem), prirodni brojevi se prema Fon Nojmanu (Von Neumann) mogu definisati na sledeći način:

(N) $$0 = \emptyset,\ \ 1 = \{0\},\ \ 2 = \{0, 1\},\ \ 3 = \{0, 1, 2\}, \ldots$$

i $n' = n \cup \{n\}$. Drugim rečima, svaki prirodan broj je skup prethodnih prirodnih brojeva, dok je $N = \{0, 1, 2, \ldots\}$. Ovako definisanu strukturu $\mathbf{N} = (N, ', 0)$ nazvaćemo Fon Nojmanovim modelom prirodnih brojeva. Zamerka ovoj definiciji prirodnih brojeva leži u činjenici da su prirodni brojevi definisani prebrojivim, dakle beskonačnim nizom definicija (za svaki broj pojedinačno), a to podrazumeva da nam prirodni brojevi već stoje na raspolaganju. Istina, ovakva definicija prirodnih brojeva može se u okviru formalne teorije skupova ZF zameniti (konačnom) definicijom skupa prirodnih brojeva $N$. Ta definicija može se naći u bilo kojoj knjizi u kojoj se izlaže teorija skupova i ona otprilike glasi "da su prirodni brojevi konačni ordinalni, odnosno konačni kardinalni brojevi". Ali sa stanovišta zasnivanja ni ta definicija prirodnih brojeva nije zadovoljavajuća s obzirom da izlaganje teorije ZF takođe podrazumeva već izgrađen deo strukture prirodnih brojeva, pa se i u ovom pristupu krije svojevrsna teškoća.

Ovih nekoliko napomena donekle bliže objašnjavaju smisao pomenute Kronekerove rečenice. Ipak, sa praktičnog stanovišta, u onim delovima matematike gde strogo zasnivanje prirodnih brojeva nije od nekog značaja, Fon Nojmanova definicija je sasvim prihvatljiva, pa ćemo je i mi u ovoj knjizi podrazumevati. Naravno, ostaje da se proveri da tako definisani prirodni brojevi zaista zadovoljavaju Peanove aksiome. U dokazu ove činjenice koristićemo Aksiomu regularnosti teorije skupova, da svaki neprazan skup ima $\in$-minimalan element:

(R) $$\forall x\,(x \neq \emptyset \Rightarrow \exists y \in x\ \ x \cap y = \emptyset)$$

Neposredna posledica ove aksiome je da nema $\in$–regresija, tj. nema beskonačnih nizova skupova $\langle x_n \mid n \in N\rangle$ takvih da je

(R') $$x_0 \ni x_1 \ni x_2 \ni \ldots$$

Zaista, ako neki niz $x_n$ zadovoljava (R$'$), onda $x = \{x_0, x_1, x_2, \ldots\}$ nema $\in$–minimalni element.

**3.1.1 Teorema** *Fon Nojmanov model prirodnih brojeva* **N** *zadovoljava Peanove aksiome.*

**Dokaz** Aksiome P1, P2 i P4 očigledno su zadovoljene u ovako definisanoj strukturi prirodnih brojeva. Proverimo aksiomu P3. Dakle, neka su $m$ i $n$ prirodni brojevi takvi da je $m' = n'$. Tada $m \cup \{m\} = n \cup \{n\}$, pa

(1) $$m \in n \ \text{ ili } \ m = n, \quad \text{i} \quad n \in m \ \text{ ili } n = m.$$

Ako je $m \in n$ i $n \in m$ onda je imamo beskonačnu regresiju $m \ni n \ni m \ni n \ni \ldots$, suprotno Aksiomi regularnosti. Otuda iz (1) sledi $m = n$, pa P3 važi u **N**.

Primetimo da u **N** važi

(2) $$\forall x (x \neq \emptyset \Rightarrow \exists z\, x = z')$$

Dokažimo da Aksioma indukcije važi u **N** za proizvoljno svojstvo $\Phi$. Stoga pretpostavimo da **N** zadovoljava

(3) $$\Phi(0), \quad \forall x (\Phi(x) \Rightarrow \Phi(x'))$$

Dokazujemo da za svaki $n \in N$, $\Phi(n)$ važi u **N**. Pretpostavimo suprotno, tj. neka postoji $n \in N$, takav da $\mathbf{N} \models \neg\Phi(n)$. Onda je prema pretpostavci (3), $n \neq 0$, pa prema (2) postoji $x_0 \in N$ tako da je $n = x_0'$. Otuda je $\mathbf{N} \models \neg\Phi(x_0')$, pa koristeći pretpostavku (3) nalazimo $\mathbf{N} \models \neg\Phi(x_0)$ (jer bi inače $\mathbf{N} \models \Phi(x_0)$ povlačilo $\mathbf{N} \models \Phi(x_0'))$. Na sličan način nalazimo $x_1 \in N$ tako da $\mathbf{N} \models \neg\Phi(x_1)$ i $x_0 = x_1'$, i prema tome $x_0 \ni x_1$. Nastavljajući ovaj postupak *ad infinitum* nalazimo beskonačnu regresiju $x_0 \ni x_1 \ni x_2 \ni \ldots$, suprotno aksiomi regularnosti. Prema tome, uz pretpostavke (3) u **N** zaista važi $\forall x \Phi(x)$, dakle Fon Nojmanov model zadovoljava Peanove aksiome. $\diamondsuit$

Vidimo da se u Fon Nojmanovom modelu relacija nejednakosti između prirodnih brojeva poklapa sa skupovnom relacijom pripadanja, tj. u **N** važi

(4) $$\forall xy \ \ (x < y \Leftrightarrow x \in y).$$

Ako je $S \subseteq N$ neprazan, prema Aksiomi regularnosti $S$ ima $\in$–minimalan element, tj. postoji $m \in S$ takav da je $m \cap S = \emptyset$. To znači da za sve $x \in m$, $x \notin S$, dakle za sve $x < m$, $x \notin S$. Drugim rečima, s obzirom na (4), $S$ ima najmanji element u smislu prirodnog uređenja skupa prirodnih brojeva. Ovu činjenicu možemo formulisati na sledeći način:

**3.1.2** ***Princip najmanjeg elementa za prirodne brojeve*** *Svaki neprazan podskup skupa prirodnih brojeva ima najmanji element.*

Videćemo da je ovo svojstvo zapravo posledica Peanovih aksioma. Linearno uređen skup koji zadovoljava Princip najmanjeg elementa, tj. kod kojeg svaki neprazan podskup ima najmanji element, naziva se *dobro uređenim skupom.* Dakle, prirodno uređenje strukture prirodnih brojeva $(N, \leq)$ je jedan primer dobro uređenog skupa.

Pomoću Aksiome indukcije mogu se definisati i uvoditi novi matematički objekti. Takve definicije u kojima se koristi Aksioma indukcije, nazivaju se *induktivnim* ili *rekurzivnim* definicijama. Sledeća teorema odnosi se upravo na tu vrstu definicija.

**3.1.3** ***Teorema rekurzije*** *Neka su $A$ i $B$ neprazni skupovi, $N$ skup prirodnih brojeva i $f : A \to B$, $g : N \times A \times B \to B$. Tada postoji jedinstvena funkcija $h : N \times A \to B$ tako da je:*

$$\text{(I)} \qquad \begin{aligned} h(0,x) &= f(x), & x \in A, \\ h(n',x) &= g(n,x,h(n,x)), & n \in N,\ x \in A. \end{aligned}$$

**Dokaz** (1) *Jedinstvenost funkcije $h$.* Pretpostavimo da $h$ zadovoljava (I), i neka je $h_1 : N \times A \to B$ tako da je $h_1(0,x) = f(x)$, $h_1(n',x) = g(n,x,h(n,x))$, $n \in N$, $x \in A$. Indukcijom po $n$ dokazujemo da je svaki $x \in N$, $h(n,x) = h_1(n,x)$.

*Slučaj $n = 0$,* $h(0,x) = f(x) = h_1(0,x)$.

Pretpostavimo sada induktivnu hipotezu

$$\text{(IH)} \qquad h(n,x) = h_1(n,x)$$

Prema IH i definicijama funkcija $h$ i $h_1$ sledi:

$$h(n',x) = g(n,x,h(n,x)) = g(n,x,h_1(n,x)) = h_1(n,x).$$

Prema Aksiomi indukcije sledi $h = h_1$.

(2) *Egzistencija funkcije $h$.* Neformalni opis funkcije $h$ je:

$$h = \bigcup_{x \in A} \{(0,x,fx), (1,x,g(0,x,fx)), (2,x,g(1,x,g(0,x,fx))), \ldots\}$$

Navodimo i formalan dokaz egzistencije funkcije $h$. Za $S \subseteq N \times A \times B$ reći ćemo da je $(f,g)$-skup ako su zadovoljeni sledeći uslovi:

1. Za svaki $x \in A$, $(0,x,fx) \in S$.
2. Za sve $n \in N$, $x \in A$, $y \in B$, $(n,x,y) \in S \Rightarrow (n',x,g(n,x,y)) \in S$.

Primetimo da važe sledeće činjenice:

3. $N \times A \times B$ je $(f,g)$-skup.
4. Presek $(f,g)$-skupova je $(f,g)$-skup:

Zaista, neka je $S = \bigcap_i S_i$, gde su $S_i$, $i \in I$, $(f,g)$-skupovi. Tada je za sve $i \in I$, $(0,x,fx) \in S_i$, dakle $(0,x,fx) \in S$. Dalje, za proizvoljan $i \in I$ važi niz implikacija:

$$(n,x,y) \in S \Rightarrow (n,x,y) \in S_i \Rightarrow (n',x,g(n,x,y)) \in S_i$$

prema tome $(n',x,g(n,x,y)) \in S$.

5. Neka je $h = \bigcap\{S \mid S \text{ je } (f,g)\text{-skup}\}$. Tada:
   a. $h$ je $(f,g)$-skup.
   b. $h : N \times A \to B$, tj. h je funkcija iz $N \times A$ u $B$.
   c. $h$ zadovoljava indiktivne uslove (I).

Činjenica a. je neposredna posledica tvrđenja 4.

Što se tiče tvrđenja b., indukcijom po $n$ dokazujemo da je

$$\forall n \in N \;\; \forall x \in A \;\; \exists_1 y \in B \;\; (n, x, y) \in h.$$

Slučaj $n = 0$. Kako $(0, x, fx)$ pripada svakom $(f, g)$-skupu, to $(0, x, fx) \in h$. Pretpostavimo da postoji $y \in B$ takav da $(0, x, y) \in h$ i $y \neq fx$. Neka je $h_1 = h - \{(0, x, y)\}$. Nije teško videti da je $h_1$ takođe $(f, g)$-skup. Otuda prema definiciji skupa (funkcije) $h$ sledi $h \subseteq h_1$, što je kontradikcija s obzirom da je $(0, x, y) \in h - h_1$.

Pretpostavimo sada induktivnu hipotezu za fiksiran $n \in N$:

$$\text{(IH)} \qquad \forall x \exists_1 y \;\; (n, x, y) \in h.$$

Prema (IH) za $x \in A$ postoji $y \in B$ tako da je $(n, x, y) \in h$, pa $(n', x, g(n, x, y)) \in h$, tj. postoji $z \in B$, $z = g(n, x, y)$, tako da je $(n', x, z) \in h$. Element $z$ sa ovom osobinom je jedinstven. U suprotnom, neka je $u \in B$, $(n', x, u) \in h$ i $u \neq g(n, x, y)$. Dalje, neka je $h_2 = h - \{(n', x, u)\}$. Lako je videti da je $h_2$ $(f, g)$-skup, odakle sledi $h \subseteq h_2$, što je kontradikcija uslovu $(n', x, u) \in h - h_2$. Ovim smo dokazali $\forall x \exists_1 y (n', x, y) \in h$, pa prema Aksiomi indukcije $h$ zadovoljava uslov b.

Najzad, razmotrimo tvrđenje c. Primetimo da je $(0, x, fx) \in h$. Kako važi

$$(n, x, y) \in h \Rightarrow (n', x, g(n, x, y)) \in h$$

sledi: $y = h(n, x) \Rightarrow g(n, x, y) = h(n', x)$, tj. $h(n', x) = g(n, x, h(n, x))$.

Prema prethodnom sledi dokaz Teoreme rekurzije. $\diamondsuit$

Za funkciju $h$ induktivno definisanu pomoću formula (I) iz Teoreme rekurzije, često kažemo da je definisana *rekurentnim* formulama (vezama) (I).

Slično prethodnom dokazu izgleda dokaz sledećeg, nešto jednostavnijeg oblika teoreme rekurzije:

**3.1.4 Teorema** *Neka je $B$ neprazan skup, $b \in B$ i $g : N \times B \to B$. Tada postoji jedinstvena funkcija $h : N \to B$ tako da je*

$$\text{(I)} \qquad h(0) = b, \qquad h(n') = g(n, h(n)), \qquad n \in N.$$

Kao prvu primenu Teoreme rekurzije, dokazaćemo da su Peanove aksiome *kategorične*, odnosno da određuju prirodne brojeve do na izomorfizam. Naime, važi sledeća teorema:

**3.1.5 Teorema** *Neka je $\mathbf{N} = (N, ', 0)$ struktura prirodnih brojeva i $\mathbf{M} = (M, \sigma_M, 0_M)$ struktura koje zadovoljava aksiome P.1–P.5, gde su $\sigma_M$ i $0_M$ redom interpretacije simbola $'$ i $0$ u $\mathbf{M}$. Tada $\mathbf{M} \cong \mathbf{N}$.*

**Dokaz** Neka je $h : N \to M$ preslikavanje definisano sa $h0 = 0_M$ i $h(x') = \sigma_M(hx)$ za $x \in N$. Prema teoremi rekurzije ovo preslikavanje je dobro definisano i jedinstveno je sa ovim osobinama. Neka je $S = h[N]$. Tada je $S \subseteq M$. Onda $0_M \in S$ i ako je $x \in S$ tada $x = h(n)$ za neki $n \in N$, pa $\sigma_M x = \sigma_M(hn) = h(x')$, tj. $\sigma_M x \in S$.

Prema aksiomi P.5 onda sledi $S = M$. Dakle $h$ je preslikavanje *na*. Dalje, neka je $g : M \to N$ definisano na sličan način: $g(0_M) = 0$ i $g(\sigma_M x) = (gx)'$ za $x \in M$. Prema Teoremi rekurzije u modelu $\mathbf{M}$, preslikavanje $g$ je dobro definisano i jedino koje zadovoljava ove jednakosti. Dokazujemo da je $g \circ h = i_M$. Najpre primetimo da je $(g \circ h)(0) = g(0_M) = 0$. Dalje, pretpostavimo da je za dato $n \in N$, $(g \circ h)(n) = n$. Tada je

$$(g \circ h)(n') = g(\sigma_M(hn)) = ((g \circ h)(n))' = n'.$$

Prema aksiomi indukcije onda za sve $x \in N$, $(g \circ h)x = x$. Otuda za $x, y \in N$, ako je $hx = hy$, onda $(g \circ h)x = (g \circ h)y$, tj. $x = y$. Prema tome, $h$ je 1–1, dakle $h : \mathbf{N} \cong \mathbf{M}$. $\diamondsuit$

Osnovna primena Teoreme rekurzije odnosi se na definicije aritmetičkih objekata, pre svega osnovnih aritmetičkih funkcija. Inače, pod aritmetičkim funkcijama podrazumevamo preslikavanja kod kojih su vrednosti argumenata prirodni brojevi, kao i vrednosti samih funkcija. Prema teoremi o kategoričnosti Peanove aritmetike, svejedno je da li se te definicije daju u okviru formalnog sistema Peanove aritmetike, ili na primer u strukturi $\mathbf{N}$. Definicije koje slede odnose se na strukturu $\mathbf{N}$. Te definicije kao i neke osobine ovih funkcija date su u sledećim primerima. U svakom od primera navodimo i opis odgovarajućih funkcija $h$, $f$ i $g$ iz Teoreme rekurzije.

**3.1.6 Primer** *Aritmetička funkcija sabiranja* $h(y, x) = x + y$. Induktivna definicija ove funkcije glasi:

$$x + 0 = x, \qquad x + y' = (x + y)'.$$

Ovde je $f(x) = x$, $g(y, x, z) = z'$. S obzirom na definiciju numerala, vidimo da je $x' = x + \underline{1}$, pa ćemo ubuduće često umesto $x'$ pisati jednostavno $x + 1$. Polazeći od definicije operacije $+$ dokažimo da je, na primer,

$$(1) \qquad 2 + 2 = 4$$

Zaista,

$$2 + 2 = 2 + 1' = (2 + 1)' = (2 + 0')' = ((2 + 0)')' = (2')' = 3' = 4.$$

Za operaciju $+$ važe uobičajeni zakoni. Dokažimo, na primer, zakon komutacije

$$(2) \qquad x + y = y + x$$

Pre toga dokažimo indukcijom sledeća dva pomoćna tvrđenja:

$$(3) \qquad 0 + x = x$$

Zaista, ako je $x = 0$, tada $0 + 0 = 0$ prema definicji operacije $+$. Pretpostavimo induktivnu hipotezu (3) za fiksirano $x$. Tada, $0 + x' = (0 + x)' = x'$, pa na osnovu Aksiome indukcije (3) važi za sve prirodne brojeve.

Dokažimo sada indukcijom po $y$:

$$(4) \qquad x + y' = x' + y$$

Kako je $x + 0' = (x+0)' = x' = x' + 0$, (4) važi za $y = 0$. Dalje, pretpostavimo (4) za fiksirano $y$ kao induktivnu hipotezu. Tada, koristeći induktivnu hipotezu i definiciju operacije + imamo

$$x + (y')' = (x + y')' = (x' + y)' = x' + y',$$

pa prema Aksiomi indukcije (4) važi za sve prirodne brojeve.

Najzad, dokažimo (2) indukcijom po $y$. Prema (3) $x + 0 = x = 0 + x$, pa (2) važi za $y = 0$. Dalje, pretpostavimo (2) za fiksirano $y$. Tada koristeći definiciju operacije +, induktivnu hipotezu i (4), nalazimo

$$x + y' = (x + y)' = (y + x)' = y + x' = y' + x,$$

pa na osnovu Aksiome indukcije tvrđenje važi za sve prirodne brojeve.

Na sličan način može se dokazati zakon asocijacije za operaciju +.

**3.1.7 Primer** *Aritmetička funkcija množenja* $h(y, x) = x \cdot y$. Induktivna definicija ove funkcije glasi:

$$x \cdot 0 = 0, \qquad x \cdot y' = x \cdot y + x.$$

U ovom slučaju, $f(x) = 0$ i $g(y, x, z) = z + x$. I u slučaju ove operacije mogu se dokazati uobičajeni algebarski zakoni, kao na primer zakon komutacije, zakon asocijacije kao i zakon distribucije za množenje prema sabiranju.

**3.1.8 Primer** *Aritmetička funkcija stepenovanja* $h(y, x) = x^y$. Induktivna definicija ove funkcije glasi:

$$x^0 = 1, \qquad x^{y+1} = x^y \cdot x.$$

U ovom slučaju, $f(x) = 1$ i $g(y, x, z) = z \cdot x$. I u slučaju operacije stepenovanja mogu se dokazati uobičajeni algebarski zakoni, kao na primer zakoni

$$x^{(y+z)} = x^y \cdot x^z, \qquad x^{y \cdot z} = (x^y)^z.$$

**3.1.9 Primer** Relacija prirodnog uređenja $x \leq y$. Definicija ove relacije glasi

$$x \leq y \Leftrightarrow \exists z \;\; y = x + z.$$

Indukcijom se može dokazati da je ovo relacija linearnog uređenja, kao i da je saglasna sa operacijama + i $\cdot$, tj. u $\mathbf{N}$ važi:

$$x \leq y \Rightarrow x + z \leq y + z, \qquad x \leq y \Rightarrow x \cdot z \leq y \cdot z.$$

Na isti način se u proizvoljnom modelu Peanove aritmetike može uvesti relacija prirodnog uređenja. Podsetimo se da je prema Teoremi 3.1.5 svaki model Peanove aritmetike izomorfan strukturi $\mathbf{N}$. Kako ovaj zadovoljava Princip najmanjeg elementa, to sledi da *svaki* model Peanove aritmetike takođe zadovoljava Princip najmanjeg elementa u odnosu na prirodno uređenje. Drugim rečima, ovaj princip je posledica Peanovih aksioma.

Parcijalna operacija oduzimanja prirodnih brojeva uz pomoć relacije $\leq$ uvodi se u $\mathbf{N}$ na sledeći način

$$\forall x \forall y \leq x (z = x - y \Leftrightarrow x = z + y).$$

Razmotrimo nekoliko drugih primera primene Teoreme rekurzije. Na primer, možemo nastaviti niz aritmetičkih funkcija koje smo upravo definisali uvodeći pojam uopštene stepene funkcije, kao i generalizaciju, tzv. Akermanovu funkciju .

**3.1.10 Primer** *Akermanova funkcija*, $A(z,x,y)$. Najpre uvedimo funkciju uopštenog stepena,

$$h(y,x) = \left.x^{x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}}\right\}y$$

Induktivna definicija ove funkcije glasi:

$$h(0,x) = 1, \qquad h(y+1,x) = x^{h(y,x)}.$$

Dakle, u ovom slučaju je $f(x) = 1$, $g(y,x,z) = x^z$.

Akermanova funkcija $A(z,x,y)$, kao uopštenje stepene funkcije, ima zanimljive i neobične osobine. Ova funkcija je od interesa u formalnoj teoriji izračunljivosti. Najpre ćemo definisati ovu funkciju za $z < 4$:

$$\begin{aligned}
A(0,x,y) &= y + x,\\
A(1,x,y) &= y \cdot x,\\
A(2,x,y) &= y^x,\\
A(3,x,y) &= \left.y^{y^{\cdot^{\cdot^{\cdot^{y}}}}}\right\}x.
\end{aligned}$$

Uzimajući u obzir rekurzivne definicije aritmetičkih funkcija sabiranja, množenja, stepenovanja i uopštenog stepena, nalazimo da $A$ zadovoljava

$$\text{(A)}\qquad \begin{aligned}
A(0,0,y) &= y,\\
A(0,x+1,y) &= A(0,x,y) + 1,\\
A(1,0,y) &= 0,\\
A(z+2,0,y) &= 1, \qquad (z \le 1),\\
A(z+1,x+1,y) &= A(z, A(z+1,x,y),y), \qquad (z \le 2).
\end{aligned}$$

Ukoliko se izostavi gornje ograničenje za $z$, ove jednakosti predstavljaju "rekurzivnu" definiciju Akermanove funkcije. Dokažimo da je Akermanova funkcija dobro definisana odnosno da postoji tačno jedna funkcija koja zadovoljava uslove $(A)$. Neka je niz funkcija $a_n$ definisan pomoću $a_n(x,y) = A(n,x,y)$, $n \in N$. Tada $a_0(x,y) = y + x$, $a_1(x,y) = y \cdot x$. Dalje, neka je $m$ fiksiran prirodan broj $\ge 1$. Vidimo da važi

$$\text{(B)}\qquad a_{m+1}(0,y) = 1, \qquad a_{m+1}(x+1,y) = a_m(a_{m+1}(x,y),y).$$

Prema Teoremi rekurzije uzimajući, prema oznakama u toj teoremi, da je $f(x) = 1$ i $g(x,y,z) = a_m(z,y)$ i pretpostavljajući da je $a_m$ data funkcija, sledi da funkcija $a_{m+1}$ postoji i da je jedinstveno određena. Na osnovu matematičke indukcije sledi da je niz $a_m$ dobro definisan i jedinstven koji zadovoljava (B). Dakle, Akermanova funkcija je dobro definisana i jedinstvena funkcija koja zadovoljava uslove (A).

Spomenimo ovde samo jedno svojstvo ove funkcije, naime Akermanova funkcija je brzo rastuća funkcija. Zaista, ako je $a(x) = A(x,x,x)$, onda

$$a(0) = 0, \quad a(1) = 1, \quad a(2) = 2^2, \quad a(3) = 3^{3^3}, \quad a(4) = \left.4^{4^{\cdot^{\cdot^{\cdot^{4}}}}}\right\} A(4,3,4)$$

gde je $A(4,3,4) = \left.4^{4^{\cdot^{\cdot^{\cdot^{4}}}}}\right\} 4^{4^{4^4}} > \left.4^{4^{\cdot^{\cdot^{\cdot^{4}}}}}\right\} 10^{10^{153}}$. Čitalac može pokušati da zamisli kolika je, na primer, vrednost $a(a(10))$.

Sledećih nekoliko primera odnose se na induktivne definicije funkcija koje nemaju čisto aritmetički karakter.

**3.1.11 Primer** *Operatori* $\prod$ *i* $\sum$. Neka je $(G,\cdot)$ grupoid i neka je $G^N$ skup svih nizova sa vrednostima u domenu $G$. Dakle, ako je $x \in G^N$ onda $x = \langle x_n | n \in N\rangle$. U ovom primeru koristićemo takođe projekcijske funkcije $\pi_n : G^N \to G$. Podsetimo se da je $\pi_n(x) = x_n$ za $x \in G^N$. Funkciju $H : N \times G^N \to G$ definišemo rekurzijom na sledeći način:

$$H(0,x) = x_0, \qquad H(n+1,x) = H(n,x) \cdot x_{n+1}, \ \ n \in N.$$

Dakle, prema oznakama u Teoremi rekurzije, $f = \pi_0$ i $g(n,x,z) = z \cdot \pi_{n+1}(z)$. Operator proizvoda $\Pi$ uvodimo pomoću jednakosti

$$\prod_{i=0}^{n} x_i = H(n,x).$$

Operator proizvoda u slučaju asocijativnog grupoida $(G,\cdot)$ ima sledeća svojstva:

**3.1.12 Teorema** *Neka je grupoid* **G** *asocijativan i neka su $x$, $y$, $z$ nizovi elemenata iz $G$ takvi da je za date prirodne brojeve $m$ i $n$:*

$(z_1, z_2, \ldots, z_{n+m}) = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$. Tada

$$\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m} y_i = \prod_{i=1}^{n+m} z_i.$$

**Dokaz** Dokaz izvodimo indukcijom po $m$.

*Slučaj* $m = 1$.

$$\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{1} y_i = (\prod_{i=1}^{n} x_i) \cdot y_1 = (\prod_{i=1}^{n} x_i) \cdot z_{n+1} = \prod_{i=1}^{n+1} z_i.$$

Pretpostavimo induktivnu hipotezu tj. da tvrđenje važi za fiksiran prirodan broj $m$. Tada

$$\begin{array}{ll}
\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m+1} y_i = & \text{prema definiciji proizvoda} \\
\prod_{i=1}^{n} x_i \cdot ((\prod_{i=1}^{m} y_i) \cdot y_{m+1}) = & \text{prema asocijativnom zakonu} \\
(\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m} y_i) \cdot y_{m+1} = & \text{prema induktivnoj hipotezi} \\
(\prod_{i=1}^{n+m} z_i) \cdot y_{m+1} = & \text{prema definiciji proizvoda} \\
\prod_{i=1}^{n+m+1} z_i. & \diamondsuit
\end{array}$$

**3.1.13 Teorema** *Neka je grupoid* **G** *asocijativan i komutativan i neka je $p$ permutacija skupa $\{1, 2, \dots, n\}$, $n \geq 2$. Tada važi jednakost:*

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{p(i)}.$$

**Dokaz** Dokaz izvodimo indukcijom po $n$. Ako je $n = 2$, tvrđenje je lako proveriti. Stoga neka je $n$ utvrđen prirodan broj, $n \geq 2$, i pretpostavimo induktivnu hipotezu za $n$. Dalje, neka je $p$ permutacija skupa $\{1, 2, \dots, n+1\}$ i neka je $P = \prod_{i=1}^{n} a_{p(i)}$. Razmotrimo sledeće mogućnosti:

*Slučaj* $p(n+1) = n+1$. Restrikcija preslikavanja $p$ na $\{1, 2, \dots, n\}$ je permutacija skupa $\{1, 2, \dots, n\}$, pa je prema induktivnoj hipotezi:

$$P = (\prod_{i=1}^{n} a_{p(i)}) \cdot a_{n+1} = (\prod_{i=1}^{n} a_i) \cdot a_{n+1} = \prod_{i=1}^{n+1} a_i.$$

*Slučaj* $p(n+1) = k_0$ *za neki* $k_0 \leq n$. Neka je niz $b_1, b_2, \dots, b_n$ definisan pomoću $b_i = a_i$ za $i \leq k_0 - 1$, $b_i = a_{i+1}$ inače. Dalje, neka je za $i \leq n$ preslikavanje $q$ određeno pomoću $q(i) = p(i)$ ako je $p(i) < k_0$, i $q(i) = p(i) - 1$ ukoliko je $p(i) > k_0$. Tada je $q$ permutacija skupa $\{1, 2, \dots, n\}$, i pri tome važi $P = (\prod_{i=1}^{n} b_{q(i)}) \cdot a_{k_0}$. Prema induktivnoj hipotezi imamo $\prod_{i=1}^{n} b_{q(i)} = \prod_{i=1}^{n} b_i$. Otuda nalazimo

$$\begin{array}{ll}
P = ((\prod_{i=1}^{n-1} b_i) \cdot b_n) \cdot a_{k_0} = & \text{prema asocijativnom i komutativnom} \\
 & \text{zakonu i zbog } b_n = a_{n+1} \\
((\prod_{i=1}^{n-1} b_i) \cdot a_{k_0}) \cdot a_{n+1} = & r \text{ je permutacija:} \\
(\prod_{i=1}^{n} a_{r(i)}) \cdot a_{n+1} = & \begin{pmatrix} 1 & \dots & k_0 - 1 & k_0 & k_0 + 1 & \dots & n-1 & n \\ 1 & \dots & k_0 - 1 & k_0 + 1 & k_0 + 2 & \dots & n & k_0 \end{pmatrix} \\
(\prod_{i=1}^{n} a_i) \cdot a_{n+1} = \prod_{i=1}^{n+1} a_i & \text{prema induktivnoj hipotezi} \quad \diamondsuit
\end{array}$$

U slučaju komutativnih semigrupa koristi se i aditvina notacija. Naime, ako se za oznaku operacije grupoida uzme $+$ umesto $\cdot$, onda za $\prod_{i=1}^{n} x_i$ takođe pišemo $\sum_{i=1}^{n} x_i$. U tom slučaju je $\sum_{i=1}^{n+1} x_i = \sum_{i=1}^{n} x_i + x_{n+1}$, dok prethodna teorema izgleda ovako:

$$\sum_{i=1}^{n} a_{p(i)} = \sum_{i=1}^{n} a_i$$

Prema Teoremi 3.1.13 u sumi se mogu permutovati sabirci, dakle važe identiteti:

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i, \tag{1}$$

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n}\sum_{i=1}^{m} c_{ij} \tag{2}$$

gde su $a_i$, $b_i$ i $c_{ij}$ nizovi domena $A$.

S obzirom da u komutativnoj semigrupi redosled sabiraka može biti proizvoljan, ako je konačan niz elemenata indeksiran skupom indeksa $S = \{s_1, s_2, \ldots, s_n\}$, onda uobičajena oznaka $\sum_{s\in S} a_s$ zapravo označava sumu $\sum_{i=1}^{n} b_i$, gde je $b_i = a_{s_i}$, $1 \le i \le n$.

U sledećih nekoliko primera razmotrićemo neke kombinatorne funkcije koje se takođe mogu definisati rekurzijom.

**3.1.14 Primer** *Kantorova funkcija nabrajanja,* $h(y, x) = \langle x, y\rangle_K$. Preslikavanje $h$ je aritmetička funkcija i rekurzivna definicija ove funkcije glasi:

$$\langle 0,0\rangle_K = 0, \quad \langle x+1, 0\rangle_K = \langle x, 0\rangle_K + x + 2, \quad \langle x, y+1\rangle_K = \langle x, y\rangle_K + x + y + 1.$$

Prema oznakama u teoremi rekurzije, funkcija $f(x)$ definisana je takođe rekurzivno:

$f(0) = 0$, $f(x+1) = f(x) + x + 2$, dok je $g(y, x, z) = z + x + y + 1$.

Odavde nalazimo $f(x) = \sum_{i=2}^{x+1} i = x(x+3)/2 = \binom{x+1}{2} + x$, i takođe

$$\langle x, y\rangle_K = \langle x, 0\rangle_K + \sum_{i=1}^{y}(x+i) = \binom{x+1}{2} + x + xy + \binom{y+1}{2} = \binom{x+y+1}{2} + x. \tag{1}$$

Funkcija $\langle x, y\rangle_K$ ima osobine uređenog para:

$$\langle x_1, y_1\rangle_K = \langle x_2, y_2\rangle_K \Rightarrow x_1 = x_2 \wedge y_1 = y_2 \tag{2}$$

odnosno važi

**3.1.15 Teorema** *Za Kantorovu funkciju* $h(x, y) = \langle x, y\rangle_K$ *važi* $h : N^2 \xrightarrow[\text{1-1}]{\text{na}} N$.

**Dokaz** Najpre dokažimo da je $h$ $1-1$. Pretpostavimo da je $x_1 + y_1 < x_2 + y_2$. Kako je $\binom{x}{2}$ monotono rastuća funkcija, nalazimo

$$\binom{x_2+y_2+1}{2} \ge \binom{x_1+y_1+1+1}{2} = \binom{x_1+y_1+1}{2} + x_1 + y_1 + 1 > \binom{x_1+y_1+1}{2} + x_1,$$

odakle je $\langle x_1, y_1\rangle_K < \langle x_2, y_2\rangle_K$. Dakle, ako pretpostavimo $\langle x_1, y_1\rangle_K = \langle x_2, y_2\rangle_K$ onda $x_1 + y_1 = x_2 + y_2$, pa koristeći (1) nalazimo $x_1 = x_2$, $y_1 = y_2$.

Dokažimo da je $h$ preslikavanje *na*, tj. da u **N** važi

$$\forall xy \exists z \;\; z = \langle x, y\rangle_K.$$

Neka je $z \in N$ i neka je $n \in N$ najmanji prirodan broj takav da je $z < \binom{n+2}{2}$. Primetimo da je tada $n$ najveći prirodan broj takav da je $\binom{n+1}{2} \le z$. Koristeći jednakost $\binom{n+2}{2} = \binom{n+1}{2} + n + 1$ nalazimo

$$\binom{n+1}{2} \le z < \binom{n+1}{2} + n + 1, \qquad \text{odnosno} \qquad 0 \le z - \binom{n+1}{2} \le n.$$

Dakle $x = z - \binom{n+1}{2}$ i $y = n - x$ su prirodni brojevi, pa

$$z = \binom{n+1}{2} + x = \binom{x+y+1}{2} + x = \langle x, y\rangle_K.$$

tj. $h$ je preslikavanje *na*. $\diamondsuit$

Prema prethodnim osobinama Kantorova funkcija daje jednoznačno nabrajanje parova prirodnih brojeva. Ono izgleda ovako:

$$\langle 0,0\rangle_K,\;\; \langle 0,1\rangle_K,\;\; \langle 1,0\rangle_K,\;\; \langle 0,2\rangle_K,\;\; \langle 1,1\rangle_K,\;\; \langle 2,0\rangle_K,\;\; \langle 0,3\rangle_K,\;\; \langle 1,2\rangle_K,\;\; \ldots$$

S obzirom da je $h$ bijekcija, onda $h^{-1} : N \xrightarrow[\text{1-1}]{\text{na}} N^2$, pa postoje funkcije $L, R : N \to N$ takve da je $h^{-1}(x) = (Lx, Rx)$. Prema definiciji ovih funkcija i inverzne funkcije nalazimo da za sve prirodne brojeve $x, y, z \in N$ važi:

$$L\langle x, y\rangle_K = x, \;\; R\langle x, y\rangle_K = y, \qquad \text{i} \qquad \langle Lz, Rz\rangle_K = z.$$

Ova preslikavanja nazivamo *projekcijskim funkcijama* za Kantorovu funkciju.

Kantorova funkcija širi se dalje induktivno na trojke, četvorke, $n$-torke prirodnih brojeva pomoću

$$\langle x, y, z\rangle_K = \langle\langle x, y\rangle_K, z\rangle_K, \ldots, \langle x_1, x_2, \ldots, x_{n+1}\rangle_K = \langle\langle x_1, x_2, \ldots, x_n\rangle_K, x_{n+1}\rangle_K$$

Polazeći od (2), nije teško proveriti da je onda $h_n(x_1, x_2, \ldots, x_n) = \langle x_1, x_2, \ldots, x_n\rangle_K$ jednoznačno nabrajanje $n$-torki prirodnih brojeva, tj. i za ovu funkciju važi ključno svojstvo $n$-torke:

$$\langle x_1, x_2, \ldots, x_n\rangle_K = \langle y_1, y_2, \ldots, y_n\rangle_K \Rightarrow x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n.$$

S obzirom da $h_n : N^n \xrightarrow[\text{1-1}]{\text{na}} N$, isto tako možemo uvesti projekcijske funkcije $p_i^n : N \to N$, $1 \le i \le n$, tako da je

$$\langle p_1^n x, p_2^n x, \ldots, p_n^n x\rangle_K = x, \qquad p_i^n\langle x_1, x_2, \ldots, x_n\rangle_K = x_i.$$

Pored Kantorove funkcije $\langle x, y\rangle_K$ ima i drugih koje preslikavaju $N^2 \xrightarrow[\text{1-1}]{\text{na}} N$, na primer $\langle y, x\rangle_K$, i $2^x(2y+1) - 1$. Ipak, sledeća hipoteza (nedokazana tvrdnja), Kantorovoj funkciji daje specijalno mesto

**3.1.16** ***Hipoteza*** *Ako je $p(x,y)$ polinom sa realnim koeficijentima koji preslikava $N^2$ $1-1$ i na $N$, onda je $p(x,y)$ jedna od funkcija $\langle x,y\rangle_K$, $\langle y,x\rangle_K$.*

Teorema Feuter-Pólya ovu hipotezu dokazuje za polinome stepena 2.

Kantorova funkcija predstavlja primer jedne *kodirajuće* funkcije parova prirodnih brojeva, odnosno $n$-torki prirodnih brojeva. Naime, pod kodiranjem nekog skupa $A$ podrazumevamo bilo koje $1-1$ preslikavanje $\tau : A \to N$. Ako je $a \in A$ tada se $\tau(a)$ naziva *kôdom* elementa $a$. Primetimo da ukoliko skup $A$ ima kodirajuću funkciju onda neposredno sledi da je $A$ najviše prebrojiv skup. Pomoću kodirajućih funkcija mogu se analizirati aritmetičkim sredstvima svojstva skupa $A$. Takva svojstva skupa $A$ nazivamo onda *aritmetičkim*, a sam proces kodiranja *aritmetizacijom.* Gedel je prvi koristio kodirajuće funkcije u analizi nekih metamatematičkih pojmova. Naime, on je aritmetizovao osnovne logičke pojmove kao što su termi, formule, dokazi, teoreme i pomoću toga dokazao svoje čuvene teoreme nepotpunosti. Danas se kodiranje kao postupak osim u logici široko koristi u teoriji formalne izračunljivosti, računarstvu pa i u algebri. U jednom dosta uobičajenom načinu kodiranja, koji je uveo Gedel, koriste se prosti brojevi. U toj vrsti kodiranja ključnu ulogu ima Osnovna teorema aritmetike, o kojoj će kasnije biti više reči.

**3.1.17** ***Osnovna teorema aritmetike*** *Ako je $n$ prirodan broj veći od 1, onda postoje jedinstveni prosti brojevi $q_1, q_2, \ldots, q_k$ takvi da je $q_1 < q_2 < \ldots < q_k$, i jedinstveni prirodni brojevi $m_1, m_2, \ldots, m_k$ veći od 0 tako da važi $n = q_1^{m_1} q_2^{m_2} \ldots q_k^{m_k}$.*

Ako je $\tau : A \to N$ kodirajuća funkcija, onda se primenom ove teoreme može definisati kôd za sve konačne nizove elemenata iz $A$.

**3.1.18 Definicija** *Ako je $a = \langle a_1, a_2, \ldots, a_n\rangle$ niz elemenata iz $A$, tada je kôd niza $a$*

$$\tau a = p_1^{\tau a_1+1} p_2^{\tau a_2+1} \ldots p_n^{\tau a_n+1}$$

*gde je $p_1, p_2, \ldots, p_n$ početni komad niza prostih brojeva, tj. $p_1 = 2$, $p_2 = 3, \ldots$.*

Ovu kodirajuću funkciju nazvaćemo *Gedelovim kôdom.*

Prema Osnovnoj teoremi aritmetike sledi glavno svojstvo ovako definisanog kôda, da se iz $\tau a$ može rekonstruisati ceo niz $a$. Zaista, za $x \in N$ i razlaganje $x = q_1^{m_1} q_2^{m_2} \ldots q_k^{m_k}$ broja $x$ na proste faktore, neka je $(x)_i = m_i$. U toj novoj notaciji Gedelov kôd niza $a = \langle a_1, a_2, \ldots, a_n\rangle$ je

$$\tau a = p_1^{(\tau a)_1} p_2^{(\tau a)_2} \ldots p_n^{(\tau a)_n}.$$

Prema tome $\tau a_i = (\tau a)_i - 1$, $i = 1, 2, \ldots, n$, gde je $n$ indeks najvećeg prostog broja koji deli $\tau a$.

Pored osnovnog oblika rekurzije opisanog u Teoremi rekurzije, a koji ćemo ubuduće nazivati *običnom rekurzijom*, koriste se i druge vrste rekurzije. Pogledajmo na sledećem primeru kako izgleda *rekurzija tipa Fibonačijevog niza.* U tom istom primeru videćemo kako se ta vrsta rekurzije može svesti na običnu, kao i jednu primenu Kantorove funkcije nabrajanja.

**3.1.19 Primer** *Fibonačijev niz* Fibonačijev niz $f = \langle f_n | n \in N \rangle$ definisan je rekurzivno na sledeći način

$$(1) \qquad f_0 = 0, \quad f_1 = 1, \qquad f_{n+2} = f_n + f_{n+1}, \ n \in N$$

Ovaj čuveni niz uveo je 1202 Leonardo Pisano (Leonardo od Pize), poznatiji pod imenom Leonardo Fibonacci. Naime, u svojoj *Liber Abbaci* Fibonači je postavio ovaj problem "Koliko će parova zečeva nastati od jednog para zečeva za godinu dana?" Da bi rešio ovaj problem, Fibonači je pretpostavio da svaki par zečeva daje par potomaka različitog pola svakog meseca, da zečevi postaju fertilni posle mesec dana, i da zečevi nikad ne umiru (i naravno, niko ih ne jede). Tada će posle mesec dana biti 2 para zečeva, posle dva meseca 3 para; sledećeg meseca prvobitni par, zajedno sa parom rođenim prvog meseca, dobiće dva nova para, što daje ukupno 5 pari zečeva, itd. Prema tome, rekurentne formule (1) daju "matematički model" razmnožavanja zečeva, uzimajući da je $f_{n+2}$ ukupan broj parova zečeva posle $n$ meseci. Spomenimo da se Fibonači smatra najvećim evropskim matematičarem pre Renesanse. Krajem 19. veka E. Lucas nazvao je ovaj niz prema Fibonačiju, i primenio ga u teoriji brojeva, na primer, u dokazu da je $2^{127} - 1$ prost broj.

Kepler je nezavisno otkrio isti niz početkom 17. veka u vezi sa *filotaksijom*, studijama o rasporedu listova i cvetova kod biljaka. Od 1963. godine postoji časopis *Fibonacci Quarterly* u kojem su publikovani brojni radovi u vezi sa Fibonačijevim brojevima.

Kao što vidimo rekurzija tipa Fibonači nije obična rekurzija. Da bismo ovu vrstu rekurzije sveli na običnu, uvedimo funkciju $h_n$ definisanu pomoću $h_0 = \langle 0, 1 \rangle_K$, $h_n = \langle f_n, f_{n+1} \rangle_K$. Tada $h_n$ zadovoljava rekurzivne relacije

$$(2) \quad h_0 = 1, \quad h_{n+1} = \langle f_{n+1}, f_{n+2} \rangle_K = \langle f_{n+1}, f_n + f_{n+1} \rangle_K = \langle R(h_n), L(h_n) + R(h_n) \rangle_K$$

Prema oznakama u Teoremi rekurzije 3.1.4, ovde je $b = 2$ i $g(n, z) = \langle R(z), L(z) + R(z) \rangle_K$ i prema istoj teoremi to je jedina funkcija koja zadovoljava jednakosti (2). S obzirom da je $f_n = L(h_n)$, niz $f_n$ jedinstveno je određen pomoću (1).

Generalni oblik rekurzije tipa Fibonači, opisuje se sledećom teoremom.

**3.1.20 Teorema** *Neka su $A$ i $B$ neprazni skupovi i $f_1, f_2 : A \to B$, i $G : N \times A \times B \times B \to B$. Tada postoji jedinstvena funkcija $H : N \times A \to B$ koja zadovoljava sledeće rekurzivne jednakosti*

$$(1) \qquad \begin{gathered} H(0, x) = f_1(x), \quad H(1, x) = f_2(x), \\ H(y + 2, x) = G(y, x, H(y, x), H(y + 1, x)) \end{gathered}$$

**Dokaz** Pretpostavimo da preslikavanje $H : N \times A \to B$ zadovoljava (1) i neka je $h(y, x) = (H(y, x), H(y + 1, x))$. Tada $h : N \times A \to B \times B$ i $h(y + 1, x) = (H(y + 1, x), G(y, x, H(y, x), H(y + 1, x)))$, pa važe sledeće rekurzivne jednakosti

$$\begin{aligned} h(0, x) &= (f_1(x), f_2(x)), \\ h(y + 1, x) &= (\pi_2(h(y, x)), G(y, x, \pi_1(h(y, x)), \pi_2(h(y, x)))) \end{aligned}$$

U ovim jednakostima $\pi_1, \pi_2 : B^2 \to B$ su projekcijske funkcije. Prema Teoremi rekurzije funkcija $h$ postoji i jedinstveno je određena sa $f(x) = (f_1(x), f_2(x))$ i

$g(y,x,z) = (\pi_2(z), G(y,x,\pi_1(z),\pi_2(z)))$. S obzirom da je $H(y,x) = \pi_1(h(y,x))$, to i funkcija $H$ postoji i jedinstveno je određena. $\diamondsuit$

Na sledećim primerima upoznaćemo potpunu rekurziju, kao i kako se ona može svesti na običnu rekurziju

**3.1.21 Primer** *Binomni koeficijenti.* Binomni koeficijenti su koeficijenti $\binom{n}{k}$ realnog polinoma $(1+x)^n$. Dakle

$$(1) \qquad (1+x)^n = \sum_{i=0}^{n} \binom{n}{k} x^k.$$

Iz (1) nije teško izvesti da važe sledeće jednakosti za sve prirodne brojeve $n$ i $k$.

$$(2) \qquad \binom{n}{0} = 1, \quad \binom{n}{n} = 1, \quad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1},$$

Dokazaćemo da rekurentne veze (2) jednistveno određuju binomne koeficijente. U tom cilju najpre dokažimo da za sve prirodne brojeve $n$ i $k$ iz (2) sledi

$$(3) \qquad \binom{n}{n+k+1} = 0$$

Dokaz izvodimo indukcijom po $k$. Ako je $k = 0$, tada iz $\binom{n+1}{n+1} = \binom{n}{n} + \binom{n}{n+1}$ i (2) sledi $\binom{n}{n+1} = 0$. Pretpostavimo induktivnu hipotezu, tj. jednakost (3) za fiksiran prirodan broj $k$ i *sve* prirodne brojeve $n$. Dalje, $\binom{n+1}{n+k+2} = \binom{n}{n+k+1} + \binom{n}{n+k+2}$, pa prema induktivnoj hipotezi $\binom{n}{n+k+1} = 0$ i takođe uzimajući u induktivnoj hipotezi $n+1$ umesto $n$ nalazimo $\binom{n+1}{n+k+2} = 0$. Otuda je $\binom{n}{n+k+2} = 0$, pa prema indukciji tvrđenje (3) sledi.

**3.1.22 Teorema** *Neka aritmetička funkcija $H(n,k)$ zadovoljava rekurzivne jednakosti*

$$(1) \qquad \begin{gathered} H(n,0) = 1, \quad H(n,n) = 1, \\ H(n+1,k+1) = H(n,k) + H(n,k+1) \quad n,k \in N \end{gathered}$$

*Tada $H(n,k) = \binom{n}{k}$, $n,k \in N$.*

**Dokaz** Najpre primetimo da je kao u slučaju binomnih koeficijenata $H(n,k) = 0$ za $n < k$. U daljem dokazu koristićemo ideju Gedelove kodirajuće funkcije. Neka je $h_n$ kôd niza $H(n,\cdot)$, $i = 0,1,\ldots,n$, tj.

$$h_n = \prod_{i=0}^{n} p_i^{H(n,i)},$$

uz dogovor $p_0 = 1$. Tada, koristeći rekurentnu vezu (1) kao i $H(n,n+1) = 0$, imamo

$$(2) \qquad h_{n+1} = \prod_{i=0}^{n} p_i^{H(n,i)} \cdot \prod_{i=1}^{n+1} p_i^{H(n,i-1)} = h_n \cdot \prod_{i=0}^{n} p_{i+1}^{H(n,i)} = h_n \cdot \prod_{i=0}^{n} p_{i+1}^{(h_n)_i}$$

Dakle, niz $h_n$ definisan je običnom rekurzijom pomoću $h_0 = 1$ i $g(n,z) = z \cdot \prod_{i=0}^{n} p_{i+1}^{(z)_i}$, pa prema Teoremi rekurzije postoji tačno jedan niz koji zadovoljava (2) i $h_0 = 1$. S obzirom da je $H(n,i) = (h_n)_i$, sledi da rekurentne formule (1) takođe određuju tačno jedan niz. Binomni koeficijenti zadovoljavaju istu rekurentnu formulu, prema tome $H(n,i) = \binom{n}{i}$, čime je teorema dokazana. $\diamondsuit$

Razmotrimo nekoliko posledica prethodne teoreme.

**3.1.23 Posledica** Za sve prirodne brojeve $0 \le k \le n$, $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

**Dokaz** Primetimo da niz $H(n,k) = \dfrac{n!}{k!(n-k)!}$ zadovoljava rekurentne formule (1) u prethodnoj teoremi. $\diamondsuit$

**3.1.24 Posledica** Neka skup $A$ ima tačno $n$ elemenata i neka je $C_k^n$ broj $k$–članih podskupova skupa $A$. Tada važi jednakost $C_k^n = \displaystyle\binom{n}{k}$.

**Dokaz** Neka je $A = \{a_1, a_2, \ldots, a_n\}$, gde su $a_i$ različiti elementi, i neka je $S = A \cup \{a\}$ gde $a \notin A$. Tada svaki $k+1$-člani podskup $X$ skupa $S$ pripada jednoj od disjunktnih klasa sa svojstvom:

1. $a \in X$. Takvih podskupova ima koliko i $k$-članih podskupova skupa $A$, dakle $C_k^n$.
2. $a \notin X$. Takvih podskupova ima koliko $k+1$-članih podskupova skupa $A$, dakle $C_{k+1}^n$.

Otuda $C_{k+1}^{n+1} = C_k^n + C_{k+1}^n$. S druge strane očigledno važi $C_0^n = 1$, $C_n^n = 1$, te prema prethodnoj teoremi $C_k^n = \binom{n}{k}$. $\diamondsuit$

Sledeći primeri aritmetičkih funkcija takođe su kombinatornog karaktera. Stirlingovi brojevi, o kojima će biti reči, od značaja su u kombinatorici, teoriji konačnih razlika, algoritmici i asimptotskoj analizi.

**3.1.25 Primer** *Stirlingovi brojevi.* Najpre ćemo razmotriti Stirlingove brojeve druge vrste, $s_k^n$. Rekurentne veze pomoću kojih se definišu brojevi $s_k^n$ za $1 \le n, k$ glase:

$$s_1^n = 1, \quad s_n^n = 1, \qquad s_{k+1}^{n+1} = s_k^n + (k+1)s_{k+1}^n, \quad n, k \in N, n, k \ge 1 \tag{1}$$

Kao i u slučaju binomnih koeficijenata pomoću Teoreme rekurzije dokazuje se da važi teorema:

**3.1.26 Teorema** *Postoji tačno jedan niz $s_k^n$ koji zadovoljava* (1).

Nije teško videti da važi $s_k^n = 0$ za $n < k$. U sledećoj "Stirlingovoj" tablici dajemo nekoliko vrednosti za ove brojeve:

$$\begin{array}{llll} s_1^1 & & & \\ s_1^2 & s_2^2 & & \\ s_1^3 & s_2^3 & s_3^3 & \\ s_1^4 & s_2^4 & s_3^4 & s_4^4 \end{array} \qquad\qquad \begin{array}{llll} 1 & & & \\ 1 & 1 & & \\ 1 & 3 & 1 & \\ 1 & 7 & 6 & 1 \end{array}$$

Stirlingovi brojevi druge vrste imaju interesantne kombinatorne osobine i zadovoljavaju veći broj zanimljivih identiteta. Razmotrimo neke od njih.

**3.1.27 Teorema** *Neka je $A = \{a_1, a_2, \ldots, a_n\}$ skup od $n$ elemenata, $1 \le k \le n$ i neka je $h(n,k)$ broj particija skupa $A$ na tačno $k$ nepraznih skupova. Tada je $h(n,k) = s_k^n$.*

**Dokaz** Neka je $S = A \cup \{a\}$, gde $a \notin A$. Tada $S$ ima $n+1$ element, dok svaka particija $\mathcal{Y} = \{Y_1, Y_2, \ldots, Y_{k+1}\}$ skupa $S$ na $k+1$ klasa pripada jednom od sledećih tipova:

1. Za neki $i \le n$, $Y_i = \{a\}$. Tada preostale klase čine razbijanje skupa $A$ na $k$ klasa, pa ovakvih particija skupa $S$ ima $h(n,k)$.

2. Klasa $Y_i$ koja sadrži $a$ takođe sadrži bar još jedan element. U takvom slučaju particija $\mathcal{Y}$ dobijena je iz neke particije $\mathcal{X} = \{X_1, X_2, \ldots, X_{k+1}\}$ skupa $A$. S obzirom da se iz $\mathcal{X}$ može dobiti $k+1$ particija domena $S$ (dodavanjem elementa $a$ jednom od skupova $X_i$), ovakvih particija skupa $S$ ima $(k+1)h(n, k+1)$.

   Shodno prethodnom razmatranju nalazimo da je

$$h(n+1, k+1) = h(n, k) + (k+1)h(n, k+1),$$

dok je očigledno $h(n, 1) = 1$ i $h(n, n) = 1$. Dakle $h$ zadovoljava rekurentne formule za Stirlingove brojeve druge vrste, pa je prema prethodnoj teoremi $h(n, k) = s_k^n$ za sve pozitivne prirodne brojeve $n$ i $k$. $\diamondsuit$

**3.1.28 Posledica** Broj relacija ekvivalencija na skupu od $n$ elemenata jednak je

$$\sum_{k=1}^{n} s_k^n.$$

Neka su $n, k \in N$ i $f : n \overset{\text{na}}{\to} k$ (podsetimo se da je $n = \{0, 1, \ldots, n-1\}$). Tada je $\mathcal{X} = \{f^{-1}(i) |\ i \in k\}$ jedna particija skupa $n$. S druge strane, ako je $p$ permutacija skupa $k$, onda za $g = p \circ f$ važi $g : n \overset{\text{na}}{\to} k$ i $\mathcal{X} = \{g^{-1}(i) | \, i \in k\}$. Dakle, sledeće tvrđenje je posledica prethodne teoreme.

**3.1.29 Posledica** Neka su $A$ i $B$ konačni skupovi čiji su kardinalni brojevi redom $n$ i $k$, gde je $k \leq n$. Tada je $|\{f| \ f : A \overset{\text{na}}{\to} B\}| = k! s_k^n$.

Neka su $n$ i $m$ proizvoljni prirodni brojevi. Ako je $f : n \to m$ onda postoji $k \in N$ i $X \subseteq m$, $|X| = k$, tako da $f : n \overset{\text{na}}{\to} X$. Prema tome, skup $\mathcal{F} = \{f | \, f : n \to m\}$ jednak je disjunktnoj uniji skupova $\mathcal{F}_X$, $X \subseteq m$, gde je $\mathcal{F}_X = \{f | \, f : n \overset{\text{na}}{\to} X\}$. Dakle,

$$|\mathcal{F}| = \sum_{k=1}^{n} \sum_{X \subseteq m, |X| = k} |\mathcal{F}_X|.$$

S obzirom da $k$–članih podskupova skupa $m$ ima $\binom{m}{k}$, važi $m^n = \displaystyle\sum_{k=1}^{n} k! \binom{m}{k} s_k^n$

**3.1.30 Posledica** $m^n = \displaystyle\sum_{k=1}^{n} m(m-1)\ldots(m-k+1) s_k^n.$

Neka $x^{(k)}$ označava realan polinom $x(x-1)\ldots(x-k+1)$, za $k > 0$, i $x^{(0)} = 1$. Podsetimo se na sledeću činjenicu iz teorije polinoma: *Ako polinomi $f(x)$ i $g(x)$ stepena $\leq k$ imaju iste vrednosti za $k+1$ različitih vrednosti argumenata, onda su $f(x)$ i $g(x)$ identični polinomi.* Koristeći ovu činjenicu, s obzirom da prethodni identitet važi za beskonačno mnogo vrednosti - za sve prirodne brojeve $m$, sledi:

**3.1.31 Posledica** $\forall n \in N \forall x \in R \ x^n = \displaystyle\sum_{k=1}^{n} s_k^n x^{(k)}$

*Stirlingovi brojevi prve vrste* $S_i^n$ definišu se kao koeficijenti polinoma $x^{(n)}$, tj. definicioni identitet za ove brojeve je

$$x^{(n)} = \sum_{k=1}^{n} S_k^n x^k.$$

Dakle, $S_k^n$ su celi brojevi, i neki od njih su negativni. Malom modifikacijom, uvodeći niz $\sigma_k^n = (-1)^{n+k} S_k^n$ dobijamo

$$x^{(n)} = \sum_{k=1}^{n} (-1)^{n-k} \sigma_k^n x^k. \tag{3.1.32}$$

Za brojeve $\sigma_k^n$ će se ispostaviti da su prirodni brojevi. Polazeći od prethodnog identiteta, nalazimo

$$\begin{aligned}\sum_{k=1}^{n+1} (-1)^{n-k+1} \sigma_k^{n+1} x^k = x^{(n+1)} &= x^{(n)}(x-n) \\ &= \sum_{k=1}^{n} (-1)^{n-k} \sigma_k^n x^{k+1} - \sum_{k=1}^{n} (-1)^{n-k} n \sigma_k^n x^k \\ &= \sum_{k=1}^{n} (-1)^{n-k+1} (\sigma_{k-1}^n + n\sigma_k^n) x^k + \sigma_n^n x^{n+1}\end{aligned}$$

odakle nalazimo

$$\sigma_0^n = 0, \quad \sigma_n^n = 1, \qquad \sigma_k^{n+1} = \sigma_{k-1}^n + n\sigma_k^n, \quad k = 1, 2, \ldots, n. \tag{3.1.33}$$

Prema Teoremi rekurzije ove rekurentne jednakosti određuju niz $\sigma_k^n$ jednoznačno.

U vezi sa Stirlingovim brojevima postoje mnogobrojne sumacione formule. Koristeći brojeve $s_k^n$ odredićemo zbir $k$–tih potencija prvih $n$ prirodnih brojeva. U tom cilju uvedimo operator konačne razlike $\Delta_x$. Neka je $f : R \to R$ realna funkcija.

**3.1.34 Definicija** $\Delta_x f(x) = f(x+1) - f(x)$.

Iz definicije operatora $\Delta_x$ neposredno se proveravaju sledeća svojstva ovog operatora:

1. $\Delta_x$ je linearan operator na vektorskom prostoru svih realnih funkcija nad poljem $\mathbf{R}$.
2. $\sum_{i=0}^{n} \Delta_i f(i) = f(n+1) - f(0)$.

Za polinom $x^{(n)}$ takođe nije teško proveriti sledeće jednakosti:

$$\Delta_x x^{(n)} = n x^{(n-1)}, \qquad (x+1)^{(n)} = (x+1) \cdot x^{(n-1)} \tag{3.1.35}$$

Otuda nalazimo

$$\begin{aligned}
\sum_{i=0}^{n} i^k &= \sum_{i=0}^{n}\sum_{j=1}^{k} i^{(j)} s_j^k = \sum_{j=1}^{k}\sum_{i=0}^{n} i^{(j)} s_j^k \\
&= \sum_{j=1}^{k} s_j^k \sum_{i=0}^{n} i^{(j)} = \sum_{j=1}^{k} s_j^k \sum_{i=0}^{n} \frac{1}{j+1}\Delta_i i^{(j+1)} \\
&= \sum_{j=1}^{k} \frac{1}{j+1} s_j^k \sum_{i=0}^{n} \Delta_i i^{(j+1)} = \sum_{j=1}^{k} \frac{1}{j+1} s_j^k (n+1)^{(j+1)} \\
&= (n+1)\sum_{j=1}^{k} \frac{s_j^k}{j+1} n^{(j)}.
\end{aligned}$$

Dakle važi

**3.1.36 Tvrđenje** $1^k + 2^k + \ldots + n^k = (n+1)\sum_{j=1}^{k} \frac{s_j^k}{j+1} n^{(j)}$.

Na primer,

$$\begin{aligned}
1^3 + 2^3 + \ldots + n^3 &= (n+1)\left(\frac{s_1^3}{2} n^{(1)} + \frac{s_2^3}{3} n^{(2)} + \frac{s_3^3}{4} n^{(3)}\right) \\
&= n(n+1)\left(\frac{1}{2} + \frac{3}{3}(n-1) + \frac{1}{4}(n-1)(n-2)\right) = \frac{1}{4}\cdot n^2(n+1)^2.
\end{aligned}$$

Iz aksiome indukcije mogu se izvesti takođe druge vrste indukcije, kao metode dokazivanja teorema o prirodnim brojevima. Razmotrimo dva takva primera.

**3.1.37** *Princip indukcije sa dve hipoteze.* *Neka je $\Psi(n)$ bilo koje svojstvo prirodnih brojeva. Tada je*

$$\text{(I2)} \qquad \Psi(0) \wedge \Psi(1) \wedge \forall n((\Psi(n) \wedge \Psi(n+1)) \Rightarrow \Psi(n+2)) \Rightarrow \forall n\, \Psi(n)$$

*posledica Peanovih aksioma.*

**Dokaz** Neka je $\Phi(n)$ formula $(\Psi(n) \wedge \Psi(n+1))$ u običnoj indukciji. Kako je formula $(\Psi(n) \wedge \Psi(n+1)) \Rightarrow (\Psi(n+1) \wedge \Psi(n+2))$ logički ekvivalentna formuli $(\Psi(n) \wedge \Psi(n+1)) \Rightarrow \Psi(n+2)$, tvrđenje sledi. $\diamondsuit$

Primetimo da (I2) daje sledeći metod dokazivanja svojstava prirodnih brojeva: Neka je $\Psi(n)$ bilo koji iskaz koji se odnosi na prirodne brojeve, i pretpostavimo da u $\mathbf{N}$ važi

1. $\Psi(0)$ i $\Psi(1)$.
2. Za svaki $n \in N$, iz $\Psi(n)$ i $\Psi(n+1)$ sledi $\Psi(n+2)$.

Tada $\mathbf{N} \models \forall n \Psi(n)$.

**3.1.38 Primer** Neka je $\mathcal{R}^N = (\mathbf{R}^N, \mathbf{R}, \cdot)$ vektorski prostor realnih nizova i neka je $L : R^N \to R^N$ linearan operator definisan pomoću $L(f)_n = f_{n+2} - f_n - f_{n+1}$. Jezgro operatora $L$, $W = \{f \in R^N \,|\, L(f) = \mathbf{0}\}$, je skup rešenja diferencne jednačine $f_{n+2} - f_n - f_{n+1} = 0$ (primetimo da je Fibonačijev niz rešenje ove jednačine). Neka su $\lambda_1, \lambda_2$ rešenja karakteristične jednačine $x^2 - 1 - x = 0$ ove diferencne jednačine. Tada $\lambda_i^{n+2} - \lambda_i^n - \lambda_i^{n+1} \equiv \lambda_i^n(\lambda_i^2 - 1 - \lambda_i) \equiv 0$, pa nizovi $g = \langle \lambda_1^n | n \in N \rangle$ i $h = \langle \lambda_2^n | n \in N \rangle$ pripadaju prostoru $W$, tj. linearni pokrivač $\mathcal{L}(g, h)$ je podskup od $W$. S druge strane, za proizvoljan $f \in W$ sistem linearniih jednačina

$$\begin{aligned} xg_0 + yh_0 &= f_0 \\ xg_1 + yh_1 &= f_1 \end{aligned} \qquad \text{tj.} \qquad \begin{aligned} x + y &= f_0 \\ x\lambda_1 + y\lambda_2 &= f_1 \end{aligned}$$

ima jedinstveno rešenje, neka je to $(\alpha, \beta)$. Dalje, uvedimo niz $F = \alpha g + \beta h$. Tada $F_0 = f_0$ i $F_1 = f_1$. Ako pretpostavimo $F_n = f_n$ i $F_{n+1} = f_{n+1}$, tada

$$\begin{aligned} F_{n+2} =& \alpha g_{n+2} + \beta h_{n+2} = \alpha(g_{n+1} + g_n) + \beta(h_{n+1} + h_n) = \\ & (\alpha g_{n+1} + \beta h_{n+1}) + (\alpha g_n + \beta h_n) = F_n + F_{n+1} = f_n + f_{n+1} = f_{n+2}, \end{aligned}$$

pa prema (I2) $F = f$. Dakle, $W = \mathcal{L}(g, h)$. Odavde za Fibonačijev niz važi

(3.1.39)
$$f_n = \frac{1}{\sqrt{5}}\Big(\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big)$$

*Potpuna indukcija* pored obične indukcije daje važan metod za izvođenje dokaza teorema o prirodnim brojevima. Posebnu zanimljivost predstavlja činjenica da je ova vrsta indukcije zapravo logički ekvivalent Principa najmanjeg elementa za standardno uređenje prirodnih brojeva. Za razliku od obične indukcije, kod potpune indukcije induktivna hipoteza sastoji se od svih iskaza $\Psi(0)$, $\Psi(1)$, …, $\Psi(n-1)$, gde je $\Psi$ formula koja se dokazuje potpunom indukcijom. Evo precizne formulacije.

**3.1.40** ***Princip potpune indukcije*** *Neka je $\Psi(n)$ bilo koje svojstvo prirodnih brojeva. Tada je*

$$\forall n((\forall k < n)\Psi(k) \Rightarrow \Psi(n)) \Rightarrow \forall n \Psi(n)$$

*posledica Peanovih aksioma.*

**Dokaz** Pretpostavimo

(1)
$$\forall n((\forall k < n)\Psi(k) \Rightarrow \Psi(n))$$

Neka je $S = \{k \in N \,|\, \mathbf{N} \models \Psi(k)\}$. Pretpostavimo da $\Psi(n)$ ne važi za sve prirodne brojeve $n$, tj. neka je $S^c \neq \emptyset$. Prema Principu najmanjeg elementa postoji najmanji prirodan broj $m \in S^c$. Tada $\Psi(k)$ važi u $\mathbf{N}$ za sve $k < m$, pa prema (1) onda i $\Psi(m)$ važi u $\mathbf{N}$, suprotno izboru broja $m$. Dakle, $\Psi(n)$ važi za sve prirodne brojeve $n$, što je i trebalo dokazati.

Princip potpune indukcije može se i direktno dokazati polazeći od Aksiome indukcije. Zaista, u Aksiomi indukcije

(2)
$$\Phi(0) \land \forall n(\Phi(n) \Rightarrow \Phi(n+1)) \Rightarrow \forall n \Phi(n)$$

izaberimo za $\Phi(n)$ formulu $(\forall k < n)\Psi(k)$. Kako je formula

$$\Psi(0) \wedge \Psi(1) \wedge \ldots \wedge \Psi(n-1) \Rightarrow \Psi(0) \wedge \Psi(1) \wedge \ldots \wedge \Psi(n-1) \wedge \Psi(n)$$

logički ekvivalentna formuli

$$\Psi(0) \wedge \Psi(1) \wedge \ldots \wedge \Psi(n-1) \Rightarrow \Psi(n)$$

iz (2) sledi

$$(\Psi(0) \wedge \forall n(\Psi(0) \wedge \Psi(1) \wedge \ldots \wedge \Psi(n-1) \Rightarrow \Psi(n))) \Rightarrow \forall n \Psi(n). \tag{3}$$

S obzirom da je $(\forall k < 0)\Psi(0)$ logički tačna formula, za $n = 0$ formula $(\forall k < n)\Psi(k) \Rightarrow \Psi(n)$ svodi se na $\Psi(0)$. Dakle u (3), u hipotezi se $\Psi(0)$ može izostaviti, a time se dobija Princip potpune indukcije. $\diamondsuit$

U prethodnom dokazu videli smo da je Princip potpune indukcije posledica Principa najmanjeg elementa. Da važi i obrnuto možemo se uveriti na osnovu sledećeg izvođenja. Neka je $\Phi(n)$ proizvoljan iskaz o prirodnim brojevima. Stavljajući $\neg\Phi(n)$ umesto $\Psi(n)$ u formuli pomoću koje je iskazan Princip potpune indukcije, nalazimo

$$\forall n((\forall k < n)\neg\Phi(k) \Rightarrow \neg\Phi(n)) \Rightarrow \forall n \neg\Phi(n)$$

Odavde, koristeći jednostavne tautologije i valjane formule, kao što su

$$\neg\neg P \Leftrightarrow P, \;\; (P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P), \;\; \neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q), \;\; \neg\forall x\Theta \Leftrightarrow \exists x \neg\Theta,$$

dobijamo ekvivalentne formule

$$\neg\forall n \neg\Phi(n) \Rightarrow \neg\forall n((\forall k < n)\neg\Phi(k) \Rightarrow \neg\Phi(n)),$$
$$\exists n \Phi(n) \Rightarrow \exists n((\forall k < n)\neg\Phi(k) \wedge \Phi(n)),$$

od kojih je poslednja Princip najmanjeg elementa za prirodne brojeve. Skupovnu formu ovog principa možemo dobiti uzimajući $n \in S$ za $\Phi(n)$.

U vezi sa Principom potpune indukcije je definisanje nizova pomoću potpune rekurzije; jedan primer te vrste videli smo kod binomnih koeficijenata. Za niz $H = \langle H_n | \, n \in N \rangle$ elemenata domena $A$ kažemo da je definisan potpunom rekurzijom ako se svaki član $H_n$ ovog niza izračunava koristeći prethodne članove niza $H_0$, $H_1$, $\ldots$, $H_{n-1}$. Drugim rečima za neku funkciju $G$, važi $H_n = G(n, H|n)$, gde je $H|n$ restrikcija funkcije $H$ na $n = \{0, 1, \ldots, n-1\}$ (primetimo da je $H|0 = \emptyset$, tj. $H|0$ je tzv. *prazna funkcija*). O egzistenciji ovako definisanog niza govori sledeća teorema.

**3.1.41** ***Teorema potpune rekurzije*** *Neka je $A$ neprazan skup, $\mathcal{F}$ skup svih konačnih nizova domena $A$ i neka je $G : N \times \mathcal{F} \to A$. Tada postoji tačno jedan niz $H : N \to A$ tako da važi*

$$H(n) = G(n, H|n), \quad n \in N \tag{PI}$$

**Dokaz** *Najpre primetimo sledeću činjenicu.*

*(1) Ako je* $s \in \mathcal{F}$ *i* $n \notin \mathrm{dom}(s)$, *onda* $s \cup \{(n, G(n,s))\} \in \mathcal{F}$.

Dalje, neka je $\mathcal{S}$ skup svih konačnih podskupova skupa $N \times A$ i neka je $\overline{G} : N \times \mathcal{S} \to A$ bilo koje preslikavanje takvo da je $G \subseteq \overline{G}$. Prema Teoremi rekurzije 3.1.4 za $b = \emptyset$ i $g : N \times \mathcal{S} \to \mathcal{S}$, $g : (n, z) \mapsto z \cup \{(n, \overline{G}(n, z))\}$ rekurentnim formulama

$$h_0 = \emptyset \qquad h_{n+1} = h_n \cup \{(n, \overline{G}(n, h_n))\}$$

odgovara jedinstven niz $h : N \to \mathcal{S}$. S obzirom na (1), indukcijom po $n$ nije teško dokazati da je $h_n$ zapravo konačan niz elemenata iz $A$, tj. $h_n \in \mathcal{F}$ za sve $n \in N$. Otuda, $\overline{G}(n, h_n) = G(n, h_n)$, pa

$$h_{n+1} = h_n \cup \{(n, G(n, h_n))\} \tag{2}$$

S obzirom da je $h_0 \subseteq h_1 \subseteq h_2 \subseteq \ldots$, to je $H = \bigcup_{n \in N} h_n$ preslikavanje iz $N$ u $A$ i važi $H|n = h_n$. S obzirom na (2), preslikavanje $H$ zadovoljava (PI), čime je dokazana egzistencija funkcije $H$.

Jedinost funkcije $H$ sledi na osnovu potpune indukcije: pretpostavimo da funkcija $H' : N \to A$ zadovoljava $H'(n) = G(n, H'|n) = G(n, H|n) = H(n)$, pa prema Principu potpune indukcije tvrđenje sledi. $\diamondsuit$

**3.1.42 Primer** *Bernulijevi brojevi*, $b_n$ (prema J. Bernoulli). Uzećemo da je u $\mathbf{N}$ za $n < k$, $\sum_{i=k}^{n} x_i = 0$. Tada se niz Bernulijevih brojeva definiše rekurzijom

$$b_n = \frac{1}{n+1}\left(n + 1 - \sum_{k=0}^{n-1} \binom{n+1}{k} b_k\right), \quad n \in N. \tag{1}$$

Ovaj niz brojeva uveo je Jakob Bernuli (Jakob Bernoulli) 1713 g. u vezi sa sumom $P_k(n) = \sum_{i=1}^{n} i^k$. Podsetimo se da je prema Tvrđenju 3.1.36, $P_n(x)$ polinom stepena $n+1$. J. Bernuli otkrio je identitet

$$P_n(x) = \frac{1}{n+1}\left(\binom{n+1}{0} B_0 x^{n+1} + \binom{n+1}{1} B_1 x^{n-1} + \ldots + \binom{n+1}{n} B_n x\right). \tag{2}$$

Uzimajući u (2) $x = 1$, nalazimo $n = \sum_{k=1}^{n} \binom{n+1}{k} B_k$, odakle neposredno sledi da niz $B_k$ zadovoljava (1) (za $b_n = B_n$). Prema Teoremi potpune rekurzije sledi da je $B_n$ niz Bernulijevih brojeva.

S obzirom da se u dokazu identiteta (2) koristi delom teorija polinoma, taj dokaz razmotrićemo kasnije. Primetimo da je zapravo dovoljno dokazati da u (2) koeficijent $B_i$ ne zavisi od $n$. Ovde samo nalazimo vezu između Bernulijevih brojeva i Stirlingovih brojeva 2. vrste.

Prema identitetima 3.1.35 i 3.1.36 nalazimo

$$P_n(x) = (x+1)x \sum_{k=1}^{n} \frac{s_k^n}{k+1}(x-1)^{(k-1)} = \frac{x}{n+1} \sum_{i=0}^{n} \binom{n+1}{i} b_i x^{n-i} \tag{3.1.43}$$

Deleći sa $x$, zatim stavljajući $x = 0$ i koristeći $(-1)^{(k-1)} = (-1)^{k-1}(k-1)!$, nalazimo

$$b_n = \sum_{k=1}^{n} \frac{(-1)^{k-1}(k-1)!}{k+1} s_k^n$$

Koristeći ovaj identitet, ili rekurentnu formulu (1), nalazimo prvih nekoliko Bernulijevih brojeva: $b_0 = 1$, $b_1 = 1/2$, $b_2 = 1/6$, $b_3 = 0$.

U leto 1900. godine, održan je u Parizu Drugi međunarodni kongres matematičara. Ovaj kongres zapamćen je po predavanju Davida Hilberta u kojem je Hilbert izložio pravce kojima treba da se kreće matematika 20. veka. To svoje predavanje izložio je u vidu 23 problema. Drugi problem glasi:

*Dokazati da aksiome aritmetike nisu protivrečne, tj. da se polazeći od njih u konačnom broju logičkih koraka ne može doći do rezultata koji protivreče jedan drugom*

Glavni motiv koji je ležao u osnovi Hilbertovog predavanja je pitanje neprotivrečnosti matematike. S obzirom da je aritmetika osnovna matematička teorija, Hilbert je očekivao direktan dokaz neprotivrečnosti ove teorije. U tu svrhu bilo je neophodno izvršiti formalizaciju aritmetike, odnosno da se aritmetika postavi kao formalan sistem. Potpunu formalizaciju aritmetike Hilbert će uraditi tek dvadesetih godina ovog veka, i taj sistem danas je poznat kao *Peanova aritmetika prvog reda*, odnosno *formalna Peanova aritmetika*, ili jednostavno *Formalna aritmetika*. Danas se ova teorija smatra zadovoljavajućim aksiomatskim sistemom prirodnih brojeva i osim u metamatematici izučava se i primenjuje u drugim oblastima matematike, kao što je kombinatorna teorija brojeva, teorija algoritama i nestandardna analiza. Aksiome ove teorije, koju ćemo kraće obeležiti sa FPA, date su u predikatskom računu prvog reda i glase:

| | | | |
|---|---|---|---|
| 1. | $x' \neq 0,$ | 2. | $x' = y' \Rightarrow x = y,$ |
| 3. | $x + 0 = x,$ | 4. | $x + y' = (x + y)'$ |
| 5. | $x \cdot 0 = 0$ | 6. | $x \cdot y' = x \cdot y + x$ |

i shema aksioma indukcije

7. $(\varphi(0) \wedge \forall x(\varphi(x) \Rightarrow \varphi(x'))) \Rightarrow \forall x \varphi(x)$

Kao što vidimo, Formalna aritmetika je teorija prvog reda jezika $\{', +, \cdot, 0\}$. Polazeći od ovih aksioma mogu se dokazati uobičajeni algebarski zakoni za $+$ i $\cdot$. Takođe se može uvesti relacijski simbol $<$ koji zadovoljava aksiome linearnog uređenja saglasne sa $+$ i $\cdot$, kao i simbol eksponencijalne funkcije sa očekivanim osobinama. Spomenimo da uvođenje ove funkcije u formalnu aritmetiku nije trivijalan zadatak. U formalnoj aritmetici mogu se definisati i razne druge funkcije, odnosno u njoj se mogu izgraditi sve elementarne funkcije pa i dokazati njihove osobine koje se inače izvode u Peanovoj aritmetici. Dakle, moglo bi se očekivati da je formalna aritmetika dovoljna za zasnivanje prirodnih brojeva. Ali, Gedelovi rezultati, tzv. *teoreme nepotpunosti*, iz tridesetih godina ovog veka pokazali su da to nije slučaj, niti da je to moguće uraditi na način kako je izgrađena formalna aritmetika (tj. da ne postoji rekurzivan sistem aksioma čije su teoreme tačno rečenice koje važe u strukturi prirodnih brojeva). Istina, tek 1978. godine pronađen je primer, o kojem će kasnije biti reči, iz kombinatorne teorije brojeva koji je istinit u $\mathbf{N}$ ali ne i dokaziv u formalnoj aritmetici. Reč je o jednoj varijanti Remzijeve teoreme, dok su raniji primeri nedokazivih u FPA ali istinitih tvrdnji bili metamatematičkog karaktera.

Primetimo da je FPA mnogo slabija teorija od Peanove aritmetike, ali s druge strane FPA je teorija prvog reda dok Peanova aritmetika to nije. Naime, u Peanovoj aritmetici Aksioma indukcije odnosi se na bilo kakve iskaze, pa i one koji se ne mogu zapisati pomoću predikatskog računa prvog reda. Otuda mnoge teoreme Peanove aritmetike važe sa ograničenjem u FPA. Na primer, Princip najmanjeg elementa važi u FPA samo za *definabilne* skupove, tj. one podskupove prirodnih brojeva koji se mogu opisati pomoću neke formule teorije FPA. Mada to može izgledati kao manjkavost Formalne aritmetike, ipak FPA predstavlja osnovno sredstvo za izučavanje i precizno definisanje fundamentalnih metamatematičkih pojmova, kao što su broj, dokaz, neprotivurečnost i algoritamska odlučivost.

Formalna aritmetika daje i jedan "gratis". Naime, s obzirom da struktura prirodnih brojeva zadovoljava aksiome FPA, prema Teoremi kompaktnosti, preciznije prema Teoremi 2.3.5, postoje modeli ove teorije proizvoljno velike kardinalnosti. Dakle, postoje strukture koje zadovoljavaju aksiome Formalne aritmetike, a nisu izomorfne strukturi prirodnih brojeva. Takve strukture nazivamo *nestandardnim modelima* prirodnih brojeva. Tu činjenicu prvi je uočio Thorn Skolem tridesetih godina ovog veka. Kako neobično izgledaju nestandarni modeli prirodnih brojeva pokazuje sledeći primer.

**3.1.44 Teorema** *Neka je* $\mathbf{M} = (M, +, \cdot, <, 0)$ *nestandardni model prirodnih brojeva. Tada se u* $(M, <)$ *može utopiti uređenje racionalnih brojeva* $(Q, <)$.

**Dokaz** Neka je relacija $\sim$ u $M$ definisana pomoću

$$x \sim y \Leftrightarrow \exists n \in N(x + n = y \vee y + n = x), \qquad x, y \in M.$$

Za $x, y \in N$ reći ćemo da su na konačnom rastojanju ako $x \sim y$; inače su na beskonačnom rastojanju. Onda je $\sim$ relacija ekvivalencije domena $M$ i $M/\sim$ je tada linearno uređen pomoću

$$x/\sim \prec y/\sim \ \Leftrightarrow x < y \wedge \ x \text{ i } y \text{ "su na beskonačnom rastojanju"}$$

Ako su $\mathbf{a}, \mathbf{b} \in M/\sim$, $\mathbf{a} = x/\sim$, $\mathbf{b} = y/\sim$, i ako je $\mathbf{a} \prec \mathbf{b}$, tada za $z = (x + y)/2$ ako je $x + y$ paran, odnosno $z = (x + y + 1)/2$ ako je $x + y$ neparan, i za $c = z/\sim$ važi $\mathbf{a} \prec \mathbf{c} \prec \mathbf{b}$. Drugim rečima, dokazali smo da u $\mathbf{M}/\sim$ važi

$$\forall xy(x \prec y \Rightarrow \exists z(x \prec z \prec y))$$

tj. $(M/\sim, \prec)$ je gusto linerno uređen skup. Otuda sledi da $(M/\sim, \prec)$ sadrži uređenu kopiju racionalnih brojeva, v. Primer 3.3.11; neka je to $S = \{a_q/\sim \mid q \in Q\}$. Tada je $\{a_q | \, q \in Q\}$ uređena kopija racionalnih brojeva sadržana u $M$. $\diamondsuit$

Prethodno tvrđenje pokazuje da nestandardni modeli prirodnih brojeva nisu dobro uređeni, dakle, nijedan nestandardan model FPA ne zadovoljava Princip najmanjeg elementa za proizvoljne podskupove. Ovom napomenom istovremeno završavamo izučavanje zasnivanja prirodnih brojeva.

## 3.2 Celi brojevi

Izgradnja uređenog prstena celih brojeva zasniva se na strukturi prirodnih brojeva. Uverićemo se da je taj cilj, zasnivanje celih brojeva, daleko jednostavniji u odnosu na prirodne brojeve. Osnovna ideja prisutna u izgradnji celih brojeva je da se uvede još jedna operacija – oduzimanje. Otuda će celi brojevi u osnovi biti predstavljeni kao razlike prirodnih brojeva. Samo, umesto $x - y$ pisaćemo $(x, y)$ s tim da ćemo "izjednačavati" parove čije koordinate imaju iste razlike. Prateći ovu ideju, neka je $D = N^2$, i $\mathbf{D} = (D, +, \cdot, (0,0), (1,0))$, gde je za parove $(x_1, y_1), (x_2, y_2) \in N^2$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 + y_1 y_2, x_1 y_2 + x_2 y_1)$$

**3.2.1 Lema** *Struktura* $\mathbf{D}$ *ima sledeća svojstva:*

1. $(D, +, (0,0))$ *je komutativna semigrupa sa neutralnim elementom.*
2. $(D, \cdot, (1,0))$ *je komutativna semigrupa sa neutralnim elementom.*
3. *U* $\mathbf{D}$ *važe zakoni leve i desne distribucije operacije* $\cdot$ *prema* $+$.

**Dokaz** 1. Primetimo da je $(D, +, (0,0))$ kvadrat strukture $(N, +, 0)$, pa s obzirom da je $(N, +, 0)$ komutativna semigrupa sa neutralnim elementom, prema Posledici 1.8.9, tvrđenje sledi.
2. Dokažimo, na primer, asocijativni zakon. Za parove $(x_i, y_i) \in D$, $i = 1, 2, 3$ koristeći odgovarajuće algebarske zakone za $\cdot$ i $+$ u $\mathbf{N}$, imamo

$$\begin{aligned}
&((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = (x_1 x_2 + y_1 y_2, x_1 y_2 + x_2 y_1)(x_3, y_3) = \\
&((x_1 x_2 + y_1 y_2) x_3 + (x_1 y_2 + x_2 y_1) y_3, (x_1 x_2 + y_1 y_2) y_3 + x_3 (x_1 y_2 + x_2 y_1)) = \\
&(x_1 (x_2 x_3 + y_2 y_3) + y_1 (y_2 x_3 + x_2 y_3), x_1 (x_2 y_3 + x_3 y_2) + (y_2 y_3 + x_2 x_3) y_1) = \\
&(x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)).
\end{aligned}$$

Slično se dokazuju i ostali zakoni u 2. i 3. $\diamondsuit$

**3.2.2 Lema** *Neka je* $\sim$ *binarna relacija domena* $D$ *definisana pomoću*

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

*Tada je* $\sim$ *kongruencija algebre* $\mathbf{D}$.

**Dokaz** S obzirom da su operacije $+, \cdot$ komutativne, prema Lemi 1.10.8 dovoljno je dokazati

$$x \sim y \Rightarrow a + x \sim a + y, \quad a \cdot x \sim a \cdot y, \qquad a, x, y \in D$$

Dokažimo, na primer, da je $\sim$ sleva saglasna sa operacijom $\cdot$. Neka su $a$, $b$, $x_1$, $y_1$, $x_2$, $y_2$ prirodni brojevi i pretpostavimo $(x_1, y_1) \sim (x_2, y_2)$. Tada

$$x_1 + y_2 = x_2 + y_1$$
$$(a, b) \cdot (x_1, y_1) = (ax_1 + by_1, ay_1 + bx_1), \quad (a, b) \cdot (x_2, y_2) = (ax_2 + by_2, ay_2 + bx_2)$$

odakle nalazimo

$$(ax_1 + by_1) + (ay_2 + bx_2) = (ax_2 + by_2) + (ay_1 + bx_1). \qquad \diamondsuit$$

Dakle, možemo formirati količničku algebru

$$\mathbf{D}/\!\sim\; = (D, +/\!\sim, \cdot/\!\sim, (0,0)/\!\sim, (1,0)/\!\sim)$$

koju ćemo označiti sa $\mathbf{Z} = (Z, +, \cdot, \mathbf{0}, \mathbf{1})$. Za $n \in N$, neka $\mathbf{n}$ označava element $(n, 0)/\!\sim$. Najzad, neka je $\nu : N \to Z$ preslikavanje definisano pomoću $\nu : n \mapsto \mathbf{n}$, $n \in N$. Za algebru $\mathbf{Z}$ i ovako uvedene konstante i funkciju $\nu$ važi sledeće tvrđenje.

**3.2.3 Lema** 1. *$\mathbf{Z}$ je komutativan prsten sa jedinicom.*
2. *Za svako $x \in Z$ postoji $n \in N$ tako da je $x = \mathbf{n}$ ili $x = -\mathbf{n}$.*
3. *Preslikavanje $\nu$ je utapanje strukture $(N, +, \cdot, 0, 1)$ u $\mathbf{Z}$.*

**Dokaz** 1. $\mathbf{Z}$ je homomorfna slika algebre $\mathbf{D}$, pa prema Lemi 3.2.1, Lemi 1.6.2 i Teoremi 1.10.14, imamo
a) $(Z, +, \mathbf{0})$ je komutativan monoid.
b) $(Z, \cdot, \mathbf{1})$ je komutativan monoid.
c) U $\mathbf{Z}$ važi distribitivan zakon operacije $+$ prema $\cdot$.
d) $(x, y)/\!\sim + (y, x)/\!\sim\; = \mathbf{0}$.

2. Neka je $x \in Z$, na primer $x = (a, b)/\!\sim$. Tada:
a) Ako je $a \geq b$, onda $a = b + n$ za neki $n \in N$, odakle $x = (b + n, b)/\!\sim$. S obzirom da je $(b + n, b) \sim (n, 0)$, sledi $x = (n, 0)/\!\sim$, tj. $x = \mathbf{n}$.
b) Ako je $a \leq b$, onda $b = a + n$ za neki $n \in N$, prema tome $x = (a, a + n)/\!\sim = (0, n)/\!\sim$. S obzirom da je $\mathbf{n} + (0, n)/\!\sim = \mathbf{0}$, sledi $(0, n)/\!\sim = -\mathbf{n}$, tj. $x = -\mathbf{n}$.

3. Neka su $m$ i $n$ prirodni brojevi. Tada

$$\begin{aligned}
\nu(n + m) &= (n + m, 0)/\!\sim\; = ((n, 0) + (m, 0))/\!\sim \\
&= (n, 0)/\!\sim + (m, 0)/\!\sim\; = \mathbf{n} + \mathbf{m} = \nu(m) + \nu(n), \\
\nu(n \cdot m) &= (nm, 0)/\!\sim\; = ((n, 0) \cdot (m, 0))/\!\sim \\
&= (n, 0)/\!\sim \cdot (m, 0)/\!\sim\; = \mathbf{n} \cdot \mathbf{m} = \nu(n) \cdot \nu(m), \\
\nu(0) &= (0, 0)/\!\sim\; = \mathbf{0} \quad \nu(1) = (1, 0)/\!\sim\; = \mathbf{1}, \\
\nu(n) = \nu(m) &\Rightarrow (n, 0)/\!\sim\; = (m, 0)/\!\sim \Rightarrow (n, 0) \sim (m, 0) \\
& n + 0 = m + 0 \Rightarrow n = m, \quad \text{tj. } \nu \text{ je 1–1 preslikavanje.}
\end{aligned}$$

Dakle, $\nu$ je utapanje strukture $(N, +, \cdot, 0, 1)$ u $\mathbf{Z}$. $\diamondsuit$

Algebru $\mathbf{Z}$ nazvaćemo *strukturom – prstenom celih brojeva*, a prirodne brojeve možemo identifikovati sa $\{\mathbf{n} | n \in N\}$, videti Teoremu 2.2.5. Prema prethodnom tvrđenju, onda se skup $Z$ može razbiti na dva skupa; skup $N$ nenegativnih celih brojeva i skup negativnih celih brojeva $\{-\mathbf{n} | n \in N, n \neq 0\}$. U $\mathbf{Z}$ se uvode uobičajene operacije, pre svega operacija oduzimanja: $x - y = x + (-y)$, dok se apsolutna vrednost za $x \in Z$ definiše pomoću $|x| = n$ ako je $x = \mathbf{n}$, odnosno $|x| = n$ ako je $x = -\mathbf{n}$, $n \in N$. Prsten $\mathbf{Z}$ je bez delitelja nule, tj. nije teško proveriti da u $\mathbf{Z}$ važi

$$x \cdot y = 0 \Rightarrow x = 0 \vee y = 0, \quad x, y \in Z \tag{3.2.4}$$

U dokazu ove činjenice može se poći od toga da tu istu osobinu ima struktura prirodnih brojeva.

Sledeće svojstvo celih brojeva određuje mesto strukture $\mathbf{Z}$ u algebarskom varijetetu svih prstena sa jedinicom.

**3.2.5 Teorema** $\mathbf{Z}$ *je najmanji prsten koji sadrži izomorfnu kopiju prirodnih brojeva u sledećem smislu: Neka je* $\mathbf{N} = (N, +, \cdot, 0, 1)$ *i neka je* $\mathbf{P}$ *bilo koji prsten sa jedinicom. Ako je* $\rho : \mathbf{N} \to \mathbf{P}$ *utapanje, tada postoji utapanje* $\theta : \mathbf{Z} \to \mathbf{P}$ *tako da dijagram (D) komutira.*

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\theta} & \mathbf{P} \\ & {\scriptstyle \nu} & \uparrow{\scriptstyle \rho} \\ & & \mathbf{N} \end{array} \qquad \rho = \theta \circ \nu \tag{D}$$

**Dokaz** Preslikavanje $\theta$ definišemo na sledeći način:

$$\theta(x) = \begin{cases} \rho(n), & \text{ako je } x = \mathbf{n} \text{ za neki } n \in N, \\ -\rho(n), & \text{ako je } x = -\mathbf{n} \text{ za neki } n \in N. \end{cases}$$

Prema prethodnoj lemi, preslikavanje $\theta$ je dobro definisano, i važi $\rho = \theta \circ \nu$. Dalje, neka su $a, b \in Z$. Tada postoje $n, m \in N$ tako da je $a = \mathbf{n}$, $b = \mathbf{m}$, ili $a = \mathbf{n}$, $b = -\mathbf{m}$, ili $a = -\mathbf{n}$, $b = \mathbf{m}$, ili $a = -\mathbf{n}$, $b = -\mathbf{m}$.

Pretpostavimo, na primer, drugi slučaj: $a = \mathbf{n}$, $b = -\mathbf{m}$. Tada imamo dve mogućnosti: $n = m + k$, ili $m = n + k$ za neki $k \in N$. Recimo da je $n = m + k$. Tada $\rho(n) = \rho(m + k) = \rho(m) + \rho(k)$, dakle, prema definiciji preslikavanja $\theta$,

$$\rho(k) = \rho(n) - \rho(m) = \rho(n) + (-\rho(m)) = \theta(a) + \theta(b). \tag{1}$$

S druge strane,

$$\begin{aligned} \theta(a + b) = &\theta(\nu(n) + (-\nu(m))) = \theta((n, 0)/\sim + (0, m)/\sim) = \\ &\theta((n, m)/\sim) = \theta((k, 0)/\sim) = \theta(\nu(k)) = \rho(k), \end{aligned}$$

odakle, prema (1) sledi, $\theta(a + b) = \theta(a) + \theta(b)$. Na isti način razmatramo i drugu mogućnost $m = n + k$, kao i ostala tri slučaja za $a$ i $b$.

Na sličan način dokazuje se da je $\theta(ab) = \theta(a) \cdot \theta(b), a, b \in Z$, kao i da je $\theta$ $1-1$ preslikavanje. Otuda sledi da je $\theta$ utapanje prstena $\mathbf{Z}$ u prsten $\mathbf{P}$, kao i da je $\theta \circ \nu = \rho$. $\diamondsuit$

Relacija standardnog uređenja može se proširiti i na domen Z, kao što pokazuje sledeća teorema. U iskazu i dokazu teoreme, $\underline{N}$ označava skup $\{\mathbf{n} | \, n \in N\}$. Primetimo da je $\underline{N}$ podalgebra prstena $\mathbf{Z}$.

**3.2.6 Teorema** *Neka je relacija $\leq$ domena $Z$ definisana pomoću $x \leq y$ akko $y - x \in \underline{N}$. Tada:*
1. *$\leq$ je relacija linearnog uređenja domena $Z$,*
2. *$\leq$ je saglasna sa operacijama prstena $\mathbf{Z}$, tj. u $\mathbf{Z}$ važi:*
   $x \leq y \Rightarrow x + z \leq y + z, \ x \leq y \wedge 0 \leq z \Rightarrow xz \leq yz.$
3. *Za sve $m, n \in N$, $m \leq n$ akko $\mathbf{m} \leq \mathbf{n}$.*

**Dokaz** Neka su $x$, $y$, $z$ celi brojevi. 1. Dokažimo tranzitivnost relacije $\leq$. Pretpostavimo $x \leq y$ i $y \leq z$. Tada $y - x \in \underline{N}$, $z - y \in \underline{N}$, odakle $(y - x) + (z - y) \in \underline{N}$, tj. $z - x \in \underline{N}$, pa $x \leq z$.

Slično se dokazuju antisimetričnost i refleksivnost relacije $\leq$. Najzad, dokažimo da je $\leq$ linearna relacija. Za neki $n \in N$ važi $x - y = \mathbf{n}$, ili $x - y = -\mathbf{n}$, dakle $x - y \in \underline{N}$ ili $y - x \in \underline{N}$, pa $x \leq y$ ili $y \leq x$.

Dokazi za 2. i 3. su slični prethodnim dokazu, pa ih izostavljamo. $\diamondsuit$

Ubuduće strukturu prirodnih brojeva identifikovaćemo sa podalgebrom $\underline{N}$ prstena celih brojeva $\mathbf{Z}$.

Za strukturu celih brojeva važi sledeći oblik principa najmanjeg elementa.

**3.2.7 *Princip najmanjeg elementa za cele brojeve*** *Svaki neprazan i ograničen odozdo podskup skupa celih brojeva ima najmanji element.*

**Dokaz** Neka je $S \subseteq Z$ neprazan. Ako je $S \subseteq N$ tvrđenje sledi prema Principu najmanjeg elementa za prirodne brojeve. Pretpostavimo da postoji $a \in S$, $a < 0$, i neka je $m$ donja granica skupa $S$. Neka je $S' = \{-x | \, x \in S, x < 0\}$. Tada je $S' \neq \emptyset$ i $S' \subseteq \{0, 1, \ldots, m\}$; dakle, $S'$ je konačan i prema tome postoji $n = \max S'$. Tada je $-n = \min S$. $\diamondsuit$

## 3.3 Racionalni brojevi

Izgradnja polja racionalnih brojeva izvodi se slično zasnivanju celih brojeva. Jedino što se u ovom slučaju polazi od već izgrađenog prstena celih brojeva, a operacija koju želimo da uvedemo – proširimo jeste operacija deljenja. Otuda se racionalni brojevi predstavljaju kao količnici – razlomci celih brojeva. Uređen par $(x, y)$ predstavljaće razlomak $x/y$, s tim da ćemo "ujednačavati" one parove koji daju iste razlomke. Dakle, neka je

$$S = \{(x, y) | \, x, y \in Z, y \neq 0\} = Z \times (Z - \{0\}).$$

Na skupu $S$ definišemo sledeće operacije:

$$(3.3.1) \qquad \begin{aligned} (x_1, y_1) + (x_2, y_2) &= (x_1 y_2 + x_2 y_1, y_1 y_2), \\ (x_1, y_1) \cdot (x_2, y_2) &= (x_1 x_2, y_1 y_2), \quad (x_1, y_1), (x_2, y_2) \in S. \end{aligned}$$

Primetimo da je operacija $\cdot$ dobro definisana s obzirom da prsten $\mathbf{Z}$ nema delitelja nule. Neka je $\mathbf{S} = (S, +, \cdot, (0,1), (1,1))$. Nije teško proveriti da $\mathbf{S}$ zadovoljava algebarske zakone navedene u sledećoj lemi:

**3.3.2 Lema** *Algebra* $\mathbf{S}$ *zadovoljava sledeće zakone:*

1. *Asocijativne zakone za* $+$ *i* $\cdot$.
2. *Komutativne zakone za* $+$ *i* $\cdot$.
3. $(0,1)$ *je neutralni element za operaciju* $+$, *dok je* $(1,1)$ *neutralni element za operaciju* $\cdot$. ♢

Relaciju $\sim$ domena $S$ definišemo na sledeći način:

$$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 y_2 = x_2 y_1, \quad (x_1, y_1), (x_2, y_2) \in S \tag{3.3.3}$$

**3.3.4 Lema** *Relacija* $\sim$ *je kongruencija algebre* $\mathbf{S}$.

Dokaz ove leme sličan je dokazu analogne Leme 3.2.2 za cele brojeve, pa zato taj dokaz ispuštamo. Dakle, možemo formirati količničku algebru $\mathbf{S}/\sim$, a sledećom teoremom pokazuje se da je to zapravo polje racionalnih brojeva. Klasu ekvivalencije $(x,y)/\sim$, $(x,y) \in S$, obeležavaćemo pomoću razlomka $\frac{x}{y}$, ili $x/y$. Otuda operacije u polju $\mathbf{Q}$ izgledaju ovako:

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2}, \quad \frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 x_2}{y_1 y_2}.$$

**3.3.5 Teorema** *Neka je* $\mathbf{Q} = S/\sim$ *količnička algebra. Tada važi:*

1. $\mathbf{Q}$ je polje.
2. Prsten celih brojeva utapa se u $\mathbf{Q}$.

**Dokaz** 1. Neka je $k : \mathbf{S} \to \mathbf{Q}$ kanonski homomorfizam. Tada je $\mathbf{Q}$ homomorfna slika algebre $\mathbf{S}$, dakle u $\mathbf{Q}$ važe svi algebarski zakoni navedeni u Lemi 3.3.2, s tim da je $\mathbf{0} = (0,1)/\sim$, $\mathbf{1} = (1,1)/\sim$, tj. $\mathbf{0} = \frac{0}{1}$, $\mathbf{1} = \frac{1}{1}$. Osim toga nije teško proveriti da u $\mathbf{Q}$ važi i distributivni zakon za $\cdot$ prema $+$. Neka je $x/y \in Q$. S obzirom da je $(0, y^2) \sim (0,1)$, imamo

$$\frac{x}{y} + \frac{-x}{y} = \frac{0}{y^2} = \frac{0}{1} = \mathbf{0},$$

prema tome $(Q, +, \mathbf{0})$ je Abelova grupa. Dalje, neka je $x/y \in Q - \{\mathbf{0}\}$. Dakle, $x, y \neq 0$ i kako je $\mathbf{Z}$ prsten bez delitelja nule, važi $xy \neq 0$, pa

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{yx} = \frac{1}{1} = \mathbf{1},$$

prema tome $(Q - \{0\}, \cdot, \mathbf{1})$ je Abelova grupa. S obzirom da važi zakon distribucije operacije $\cdot$ prema $+$, $\mathbf{Q}$ je polje.

2. Neka je $\theta : Z \to Q$ definisano pomoću $\theta : x \mapsto x/1$. Tada je $\theta : \mathbf{Z} \xrightarrow[1\text{-}1]{} \mathbf{Q}$. Zaista, za $x, y \in Z$ važi:

$$\begin{aligned}
\theta(x+y) &= (x+y)/1 = (x+y,1)/\!\sim\ = ((x,1)+(y,1))/\!\sim \\
&= (x,1)/\!\sim + (y,1)/\!\sim\ = x/1 + y/1 = \theta(x) + \theta(y), \\
\theta(x \cdot y) &= (x \cdot y)/1 = (x \cdot y, 1)/\!\sim\ = ((x,1)\cdot(y,1))/\!\sim \\
&= (x,1)/\!\sim \cdot (y,1)/\!\sim\ = x/1 \cdot y/1 = \theta(x) \cdot \theta(y), \\
\theta(0) &= 0/1 = \mathbf{0}, \quad \theta(1) = 1/1 = \mathbf{1}, \\
\theta(x) &= \theta(y) \Rightarrow x/1 = y/1 \Rightarrow x \cdot 1 = y \cdot 1 \Rightarrow x = y,
\end{aligned}$$

čime je dokazano i drugo tvrđenje. $\diamondsuit$

Primetimo da je polje $\mathbf{Q}$ *karakteristike* 0, tj. u $\mathbf{Q}$ važi $\sum_{i=1}^{n} 1 \neq 0$, odnosno $n \cdot 1 \neq 0$ za svaki prirodan broj $n > 0$. S obzirom na utapanje $\theta$, $\mathbf{Z}$ je izomorfno podalgebri $\theta(\mathbf{Z})$ polja $\mathbf{Q}$. Tako dobijamo ovaj osnovni niz algebri - brojevnih struktura:

(3.3.6) $$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q}$$

Ako je $\mathbf{F}$ bilo koje polje karakteristike 0, nije teško dokazati da je preslikavanje $\psi : Z \to F$, definisano pomoću $\psi : x \mapsto x \cdot 1_{\mathbf{F}}$ utapanje prstena $\mathbf{Z}$ u polje $\mathbf{F}$. S tim u vezi je sledeće tvrđenje.

**3.3.7 Teorema** *Polje* $\mathbf{Q}$ *je najmanje polje koje sadrži prsten celih brojeva, tj. ako je* $\mathbf{F}$ *polje i* $\alpha : \mathbf{Z} \to \mathbf{F}$ *je utapanje, tada postoji utapanje* $\beta : \mathbf{Q} \to \mathbf{F}$ *tako da sledeći dijagram komutira:*

(D)
$$\begin{tikzcd}
\mathbf{Q} \arrow[r, "\beta"] & \mathbf{F} \\
 & \mathbf{Z} \arrow[u, "\alpha"'] \arrow[ul, "\theta"]
\end{tikzcd} \qquad \alpha = \beta \circ \theta$$

**Dokaz** Definišimo preslikavanje $\beta$ pomoću $\beta(x/y) = \alpha(x) \cdot \alpha(y)^{-1}$. Preslikavanje $\beta$ je dobro definisano. Zista, neka su $x_1/y_1, x_2/y_2 \in Q$. Tada $y_1, y_2 \neq 0$, odakle $\alpha(y_1), \alpha(y_2) \neq 0$. Dalje,

$$\begin{aligned}
x_1/y_1 = x_2/y_2 &\Rightarrow x_1 y_2 = x_2 y_1 \Rightarrow \alpha(x_1 y_2) = \alpha(x_2 y_1) \\
&\Rightarrow \alpha(x_1)\alpha(y_2) = \alpha(x_2)\alpha(y_1) \Rightarrow \alpha(x_1)\alpha(y_1)^{-1} = \alpha(x_2)\alpha(y_2)^{-1}.
\end{aligned}$$

Proverimo da je $\beta$ homomorfizam.

$$\begin{aligned}
\beta(x_1/y_1 + x_2/y_2) &= \beta((x_1 y_2 + x_2 y_1)/y_1 y_2) = \alpha(x_1 y_2 + x_2 y_1)\alpha(y_1 y_2)^{-1} \\
&= (\alpha(x_1 y_2) + \alpha(x_2 y_1))\alpha(y_1^{-1})\alpha(y_2^{-1}) = \beta(x_1/y_1) + \beta(x_2/y_2).
\end{aligned}$$

Na sličan način dokazuje se da je $\beta(x_1/y_1 \cdot x_2/y_2) = \beta(x_1/y_1) \cdot \beta(x_2/y_2)$, kao i da je $\beta$ $1-1$ preslikavanje, dakle $\beta$ je utapanje. Najzad za $x \in Z$, $(\beta \circ \theta)(x) = \beta(x/1) = \alpha(x) \cdot \alpha(1)^{-1}$, dakle $\beta \circ \theta = \alpha$. $\diamondsuit$

U dokazu Teoreme 3.3.5 koristili smo osim činjenice da je $\mathbf{Z}$ prsten sa jedinicom i to da je $\mathbf{Z}$ domen, odnosno prsten bez delitelja nule. Istom konstrukcijom i istim dokazom može se dokazati sledeće uopštenje Teoreme 3.3.7.

**3.3.8 Teorema** *Ako je* **P** *komutativan prsten sa jedinicom bez delitelja nule, tada postoji najmanje polje, u smislu prethodne teoreme, koje sadrži* **P**. $\diamondsuit$

Skup racionalnih brojeva može se urediti tako da je sa jedne strane dobijena struktura uređeno polje, a sa druge da to uređenje produžuje uređenje celih brojeva. S tim u vezi uvedimo skup – segment nenegativnih racionalnih brojeva

$$Q^+ = \{x/y |\, x, y \in Z, x, y > 0\}, \quad Q_0^+ = Q^+ \cup \{0\}$$

i za racionalne brojeve $p, q$ uzećemo da je

$$p \leq q \Leftrightarrow q - p \in Q_0^+.$$

**3.3.9 Teorema** *Struktura* $\mathbf{Q} = (Q, +, \cdot, \leq, 0, 1)$ *je uređeno polje.*

**Dokaz** Najpre primetimo da za $Q^+$ i $Q_0^+$ važi:

$$\text{(1)} \qquad \begin{array}{l} 0 \in Q_0^+, \quad x, y \in Q_0^+ \Rightarrow x + y \in Q_0^+ \quad x, -x \in Q_0^+ \Rightarrow x = 0 \\ p \in Q^+ \Rightarrow -p \notin Q^+, \quad \forall x \in Q(x \in Q^+ \vee -x \in Q^+ \vee x = 0). \end{array}$$

Neka su $p, q, r \in Q$. Tada je očigledno $p \leq p$, dakle $\leq$ je refleksivna relacija. Dalje, ako je $p \leq q$ i $q \leq p$, onda $p - q, q - p \in Q_0^+$. S obzirom da je $q - p = -(p - q)$, sledi $p - q = 0$. Otuda $p = q$, odnosno relacija $\leq$ je antisimetrična. Pretpostavimo $p \leq q$ i $q \leq r$. Tada $q - p, r - q \in Q_0^+$, pa prema (1) sledi $(q - p) + (r - q) \in Q_0^+$, tj. $p \leq r$, čime smo dokazali tranzitivnost relacije $\leq$. Najzad, s obzirom na (1), važi $p - q \in Q_0^+$ ili $q - p \in Q_0^+$, tj. $q \leq p$ ili $p \leq q$. Dakle, $\leq$ je relacija linearnog uređenja domena $Q$.

Kako je $q - p = (q + r) - (p + r)$, iz $p \leq q$ sledi $p + r \leq q + r$. Neka je $0 \leq r$ i $p \leq q$; tada $r(q - p) \in Q_0^+$, odakle je $rp \leq rq$. Prema tome, relacija uređenja $\leq$ saglasna je sa operacijama polja **Q**, čime smo pokazali da je **Q** uređeno polje. $\diamondsuit$

Nije teško videti da je utapanje $\theta : \mathbf{Z} \to \mathbf{Q}$ iz Teoreme 3.3.5 monotono; prema tome $\theta : (Z, +, \cdot, \leq, 0, 1) \to (Q, +, \cdot, \leq, 0, 1)$. Dakle, uz izabranu identifikaciju prstena **Z** sa odgovarajućom podalgebrom polja $Q$, ovako uvedeno uređenje racionalnih brojeva je raširenje uređenja celih brojeva. $\diamondsuit$

Uređenje racionalnih brojeva je *gusto*, odnosno ima ovo svojstvo:

$$\text{(3.3.10)} \qquad x < y \Rightarrow \exists z(x < z \wedge z < y).$$

Zaista, ako su $p, q \in Q$, $p < q$, tada se $r = (p + q)/2$ nalazi između $p$ i $q$. Osim toga, očigledno u $Q$ nema najmanjeg, niti najvećeg elementa. Zanimljivo je da prethodna svojstva prvog reda u potpunosti opisuju uređenje racionalnih brojeva. Naime, važi sledeće tvrđenje koje je dokazao Kantor.

**3.3.11 Primer** Neka je $(A, \leq_A)$ prebrojiv, gusto linearno uređen skup, bez najvećeg i najmanjeg elementa. Tada je $(Q, \leq) \cong (A, \leq_A)$.

**Dokaz** S obzirom da su $Q$ i $A$ prebrojivi skupovi, možemo elemente tih skupova poređati u nizove: $Q = \{q_0, q_1, q_2, \dots\}$ i $A = \{a_0, a_1, a_2, \dots\}$. Induktivno definišemo nabrajanja

$$q'_0, q'_1, q'_2, \dots \quad a'_0, a'_1, a'_2, \dots$$

redom skupova $Q$ i $A$ na sledeći način.

Neka je $q'_0 = q_0$ i $a'_0 = a_0$. Induktivne definicije ovih nizova dajemo odvojeno po parnim i neparnim koracima.

*Neparan korak*, $n = 2m + 1$. Neka su nizovi $q'_0, q'_1, \dots, q'_{n-1}$, $a'_0, a'_1, \dots, a'_{n-1}$ definisani. Neka je $k$ najmanji prirodan broj $i$ takav da je $q_i \in Q - \{q'_0, q'_1, \dots, q'_{n-1}\}$. Tada biramo $q'_n = q_k$. Za element $a'_n$ uzećemo prvi neiskorišćen element iz skupa A koji ima isti raspored prema $\{a'_0, a'_1, \dots, a'_{n-1}\}$ kao $q'_n$ prema $q'_0, q'_1, \dots, q'_{n-1}$. Precizniji opis konstrukcije izgleda ovako. Za element $q'_n$ postoje sledeće mogućnosti.

1) $q'_n < q'_0, q'_1, \dots, q'_{n-1}$.
2) $q'_0, q'_1, \dots, q'_{n-1} < q'_n$.
3) Ako elemente $q'_0, q'_1, \dots, q'_{n-1}$ uredimo u rastući niz $\{b_0, b_1, \dots, b_{n-1}\}$, onda za neki $0 < j < n$, $b_0 < b_1 < \dots < b_{j-1} < q'_n < b_j < \dots < b_{n-1}$.

Neka je $t$ najmanji prirodan broj $i$ takav da je $a_i \in A - \{a'_0, a'_1, \dots, a'_{n-1}\}$, i u zavisnosti od toga koji od gornjih slučajeva važi za $q'_n$, $a_t$ zadovoljava jedan od korespondentnih uslova

1') $a_t <_A a'_0, a'_1, \dots, a'_{n-1}$.
2') $a'_0, a'_1, \dots, a'_{n-1} <_A a_t$.
3') Ako elemente $a'_0, a'_1, \dots, a'_{n-1}$ uredimo u rastući niz $\{c_0, c_1, \dots, c_{n-1}\}$, onda: $c_0 <_A c_1 <_A \dots <_A c_{j-1} <_A a_t <_A c_j <_A \dots <_A c_{n-1}$.

Element $a_t$ s ovakvim osobinama postoji s obzirom da je **A** gusto uređen skup bez najvećeg i najmanjeg elementa. Neka je $a'_n = a_t$.

*Paran korak*, $n = 2m + 2$. Ponavljamo prethodnu konstrukciju, ali sada sa uzajamno promenjenim ulogama za nizove $a'_0, a'_1, \dots, a'_n$ i $q'_0, q'_1, \dots, q'_n$.

Neka je preslikavanje $f : Q \to A$ definisano pomoću $f : q'_n \mapsto a'_n$, $n \in N$. Tada nije teško proveriti da je $f : (Q, \leq) \cong (A, \leq_A)$. $\diamondsuit$

Neka je $(A, \leq)$ linearno uređen skup. Podskup $X \subseteq A$ je *kofinalan* u $A$ akko $\forall a \in A \ \exists x \in X \ a \leq x$, dok je podskup $Y \subseteq A$ je *koinicijalan* u $A$ ako i samo ako $\forall a \in A \ \exists y \in Y \ y \leq a$. Uređenje racionalnih brojeva ima sledeće svojstvo.

**3.3.12** ***Arhimedovsko svojstvo uređenja racionalnih brojeva*** *Skup prirodnih brojeva je kofinalan u skupu racionalnih brojeva.*

**Dokaz** Neka je $m/n \in Q$. Tada postoji $m'/n' \in Q$ tako da je $m/n = m'/n'$ i $n' \in N$. Tada $m/n \leq |m'|$. $\diamondsuit$

Arhimedovsko svojstvo racionalnih brojeva omogućava da se uvede funkcija *ceo deo od* $x$, koju obeležavamo sa $[x]$:

$$[x] = \text{ najmanji } k \in N \text{ takav da je } x - 1 < k.$$

Umesto $[x]$ takođe koristimo oznaku $\lfloor x \rfloor$. U vezi sa ovom funkcijom je i

$$\lceil x \rceil = \text{ najmanji } k \in N \text{ takav da je } x \leq k.$$

## 3.4 Brojevne baze

U ovom odeljku razmotrićemo problem predstavljanja brojeva u pozicionoj notaciji u datoj brojevnoj bazi. Takođe ćemo videti kako se vrši konverzija – pretvaranje brojeva predstavljenih u jednoj brojevnoj bazi u neku drugu brojevnu bazu. Danas su ti postupci – algoritmi od posebnog značaja za rad binarnih računara kod kojih se ulazni i izlazni podaci po pravilu daju u dekadnom brojevnom zapisu, dok računar aritmetičke operacije interno izvodi u binarnom sistemu. Spomenimo da se potreba za predstavljanjem brojeva u različitim brojevnim sistemima javila još u antičkim vremenima u vezi sa korišćenjem različitih sistema mera (težine, dužine, promena novca itd.), gde su se pored dekadnog sistema koristili i takvi egzotični sistemi kao što je seksagesimalan, sistem sa brojnom osnovom 60. Ostatak tog sistema i danas je prisutan u merenju vremena.

Egzistenciju i jedinstvenost reprezentacije prirodnog broja u datoj brojevnoj bazi obezbeđuju sledeće leme.

**3.4.1** ***Lema o ostatku*** *Neka su $a, b \in N$, $b > 0$. Tada postoje jedinstveni $q, r \in N$ takvi da je $a = qb + r$ i $0 \leq r < b$.*

**Dokaz** Neka je $S = \{x \in N \mid a \leq xb\}$. S obzirom da je $a \in S$, $S$ je neprazan skup, pa prema Principu najmanjeg elementa postoji najmanji element skupa $S$, neka je to $m$. Onda $a \leq mb$, i postoje ove mogućnosti:

1. $a = mb$. Tada biramo $q = m$ i r=0.
2. $a < mb$. Tada je očito $m \neq 0$, pa postoji $q \in N$ tako da je $m = q + 1$. Tada, s obzirom na izbor broja $m$, $qb < a < qb + b$, odakle $a = qb + r$ i $0 < r < b$, gde je $r = qb - a$.

Ovim smo dokazali egzistenciju navedenog razlaganja, pa sada dokažimo jedinost takvog razlaganja. Pretpostavimo $a = q_1b+r_1$, $0 \leq r_1 < b$, i $a = q_2b+r_2$, $0 \leq r_2 < b$. Tada

$$(1) \qquad |q_1 - q_2|b = |r_1 - r_2|.$$

Ako je $q_1 \neq q_2$, onda $|q_1 - q_2|b \geq b$, dok je s druge strane $|r_1 - r_2| < b$, što je kontradikcija jednakosti (1). Dakle $q_1 = q_2$ i $r_1 = r_2$. ♢

Broj $q$ naziva se količnikom brojeva $a$ i $b$, dok je $r$ ostatak dobijen deljenjem broja $a$ brojem $b$. Primetimo da je $q = [a/b]$, dok je $r = a - [a/b]b$. Prema Primeru 1.1.11, $r = \mathrm{rest}(a, b)$. Odgovarajuće tvrđenje važi i za cele brojeve.

**3.4.2** **Posledica** Neka su $a$ i $b$ celi brojevi, $b \neq 0$. Tada postoji jedinstven ceo broj $q$ i prirodan broj $r$ tako da je

$$a = qb + r, \qquad 0 \leq r < |b|.$$

**Dokaz** Imamo sledeće mogućnosti:

1. $a, b \in N$. Tada se tvrđenje svodi na prethodnu lemu.
2. $a < 0$, $b > 0$. Tada prema prethodnoj lemi postoje $q', r' \in N$ tako da je $-a = q'b + r'$, $0 \leq r' < b$. Ako je $r' = 0$, onda biramo $q = -q'$ i $r = 0$. Pretpostavimo $r' > 0$. Tada $a = qb + r$, gde je $q = -q' - 1$ i $r = b - r'$.

Slučajevi $a > 0$, $b < 0$ i $a < 0$, $b < 0$ dokazuju se na sličan način kao pod 2. ♢

**3.4.3** ***Lema o brojevnoj bazi*** *Neka su $a$, $b$ prirodni brojevi, $a > 0$, $b \geq 2$. Tada postoje jedinstveni prirodni brojevi $q$, $r$, $n$ takvi da je*

$$a = qb^n + r, \quad 1 \leq q < b, \quad 0 \leq r < b^n. \tag{1}$$

**Dokaz** Neka je $S = \{k \in N \mid a \leq b^k\}$. Kako je $b \geq 2$ to je $a \in S$, tj. $S$ je neprazan, pa prema Principu najmanjeg elementa postoji najmanji element skupa $S$, neka je to $m$. Tada imamo sledeće mogućnosti.

1. $a = b^m$. Tada biramo $n = m$, $q = 1$ i $r = 0$.
2. $a < b^m$. Kako je $a > 0$, to je $m > 0$, i prema izboru broja $m$ važi

$$b^{m-1} < a < b \cdot b^{m-1}. \tag{2}$$

Neka je $n = m-1$. Prema Lemi o ostatku postoje $q, r \in N$ takvi da je $a = qb^n + r$, $0 \leq r < b^n$, odakle je prema (2), $1 \leq q < b$. Dokažimo jedinost razlaganja (1). Pretpostavimo

$$\begin{aligned} a &= q_1 b^{n_1} + r_1, \quad 1 \leq q_1 < b, \quad 0 \leq r_1 < b^{n_1} \\ a &= q_2 b^{n_2} + r_2, \quad 1 \leq q_2 < b, \quad 0 \leq r_2 < b^{n_2} \end{aligned} \tag{3}$$

Ako je $n_1 \neq n_2$, recimo $n_1 < n_2$, onda

$$q_1 b^{n_1} + r_1 < q_1 b^{n_1} + b^{n_1} \leq b^{n_1+1} \leq b^{n_2} + r_2.$$

tj. $q_1 b^{n_1} + r_1 < q_2 b^{n_2} + r_2$, što je kontradikcija prema (3). Dakle $n_1 = n_2$. Dalje dokaz teče kao u dokazu Leme o ostatku. $\diamondsuit$

Neka su $a \geq 1$ i $b \geq 2$ prirodni brojevi. Prema poslednjoj lemi možemo konstruisati nizove $q_i$, $n_i$ i $r_i$ tako da je

$$\begin{aligned} r_0 &= a, \\ r_0 &= q_1 b^{n_1} + r_1 \qquad 1 \leq q_i < b, \\ r_1 &= q_2 b^{n_2} + r_2 \qquad n_1 > n_2 > \dots \\ r_2 &= q_3 b^{n_3} + r_3 \qquad r_1 > r_2 > \dots, \quad 0 \leq r_i < b^{n_i} \\ &\dots \end{aligned}$$

Prema Principu najmanjeg elementa za prirodne brojeve, skup $\{r_1, r_2, \dots\}$ mora biti konačan (inače ne bi imao najmanji element), dakle za neki $k \in N$ važi $r_1 > r_2 > \dots > r_{k-1} > r_k = 0$. Otuda nalazimo:

$$a = \sum_{i=1}^{k} q_i b^{n_i}, \qquad 1 \leq q_i < b, \quad n_1 > n_2 > \dots > n_k. \tag{3.4.4}$$

Primetimo da su nizovi $q_i$, $n_i$ jedinstveno određeni. Zaista, ako je $r = \sum_{i=2}^{k} q_i b^{n_i}$, tada $a = q_1 b^{n_1} + r$, $1 \leq q_1 < b$, $0 \leq r < b^{n_1}$, pa su prema poslednjoj lemi $q_1$, $n_1$ i $r$

jedinstveno određeni. Nastavljajući postupak za $2, 3, \ldots, k$, nalazimo da isto važi i za $q_2, n_2, \ldots, q_k, n_k$. Dakle, reprezentacijom (3.4.4) prirodan broj $a$ je predstavljen na jedinstven način. Neka je $n = n_1$ i $c_0, c_1, \ldots, c_n$ niz prirodnih brojeva definisan pomoću $c_{n_i} = q_i$, $i = 1, \ldots, k$, i $c_j = 0$ za $j \neq n_1, \ldots, n_k$, $0 \leq j \leq n$. Tada imamo sledeće jedinstveno predstavljanje broja $a$:

$$a = \sum_{i=0}^{n} c_i b^i = c_0 + c_1 b + \ldots + c_n b^n. \tag{3.4.5}$$

Neka su prirodni brojevi $0, 1, \ldots, b-1$ označeni posebnim znacima, koje ćemo nazvati *ciframa* u brojevnoj bazi $b$. Neka su $d_i$ cifre koje odgovaraju brojevima $c_i$ u predstavljanju 3.4.5. Tada je reč $d_n d_{n-1} \ldots d_0$ reprezentacija broja $a$ u bazi $b$, i tu činjenicu zapisujemo pomoću

$$a = (d_n d_{n-1} \ldots d_0)_b$$

U daljem izlaganju, kad god je to jasno, radi jednostavnije notacije umesto $a = (d_n d_{n-1} \ldots d_0)_b$ pisaćemo najčešće $a = (c_n c_{n-1} \ldots c_0)_b$, tj. identifikovaćemo cifre baze $b$ sa odgovarajućim prirodnim brojevima cifarskog intervala $\{0, 1, \ldots, b-1\}$.

**3.4.6 Primer** *Dekadni brojevni sistem.* Cifre ovog sistema, u kojem inače zapisujemo prirodne brojeve, su $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, dok je baza broj deset.

**3.4.7 Primer** *Binarni brojevni sistem.* Baza binarnog sistema je broj 2, dok su cifre 0 i 1. Ovaj brojevni sistem postao je od izuzetnog značaja sa pojavom savremenih digitalnih elektronskih računara, s obzirom da se prirodni brojevi u ovim računarima predstavljaju kao nizovi nula i jedinica, dakle u binarnom sistemu. U ovoj oblasti koristi se i termin *bit* za cifre binarnog sistema. Na primer, ako je $a = 101101_2$, onda $a = 2^0 + 2^2 + 2^3 + 2^5 = 45$. U vezi sa binarnom notacijom su sledeća dva brojevna sistema.
*Oktalni sistem* za bazu ima $b = 8$, dok su cifre ovog sistema $0, 1, 2, 3, 4, 5, 6, 7$.
*Heksadecimalni sistem* za bazu ima $b = 16$, a cifre ovog sistema su $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, A,B,C,D,E,F. Dakle, ovde simboli A,B,C,D,E,F stoje redom za 10,11,12,13,14,15. Na primer, $\mathrm{F08A}_{16} = 10 \cdot 16^0 + 8 \cdot 16^1 + 15 \cdot 16^3 = 61578_{10}$

Razmotrimo problem određivanja predstavljanja prirodnih brojeva u datoj bazi $b \geq 2$. Ako je $a = (c_n c_{n-1} \ldots c_0)_b$, onda $a = \sum_{i=0}^{n} c_i b^i$. Uvodeći niz $a_i$, odavde nalazimo

$$\begin{aligned} a_0 &= a, & c_0 &= \mathrm{rest}(a_0, b) \\ a_{i+1} &= (a_i - c_i)/b & c_{i+1} &= \mathrm{rest}(a_{i+1}, b) \end{aligned} \tag{3.4.8}$$

Dužina $n$ nizova $a_i$, $c_i$ određuje se iz uslova $a_{n+1} = 0$, $a_n \neq 0$.

**3.4.9 Primer** Formule 3.4.8 daju postupak – algoritam za predstavljanje brojeva u datoj brojevnoj bazi. Recimo neka je $a = 973$ i $b = 7$. Tada

$$\begin{array}{ll} a_0 = 973, & c_0 = \mathrm{rest}(973, 7) = 0 \\ a_1 = 973/7 = 139, & c_1 = \mathrm{rest}(139, 7) = 6 \\ a_2 = (139 - 6)/7 = 19, & c_2 = \mathrm{rest}(19, 7) = 5 \\ a_3 = (19 - 5)/7 = 2, & c_3 = \mathrm{rest}(2, 7) = 2 \\ a_4 = (2 - 2)/7 = 0, & \text{dakle, } a = 2560_7. \end{array}$$

**3.4.10 Primer** Ako su $b, B$ brojevne baze takve da je $B = b^k$ za neki prirodan broj $k \geq 2$, tada je lako naći reprezentaciju prirodnog broja $a$ u bazi $B$ ako je data njegova brojevna reprezentacija u bazi $b$ i obrnuto. Naime, pretpostavimo da je $a = (c_n c_{n-1} \dots c_0)_b$, tj. $a = \sum_{i=0}^{n} c_i b^i$, i neka je $n + 1 = km + r$, $m, r \in N$, $0 \leq r < k$. Tada za $r > 0$

$$
\begin{aligned}
a =&(c_0 + c_1 b + \dots + c_{k-1} b^{k-1}) + (c_k + c_{k+1} b + \dots + c_{2k-1} b^{k-1})B + \dots \\
&(c_{mk-k} + c_{mk-k+1} b + \dots + c_{mk-1} b^{k-1})B^{m-1} + \\
&(c_{mk} + c_{mk+1} b + \dots + c_{mk+r-1} b^{r-1})B^m
\end{aligned} \tag{1}
$$

dok je za $r = 0$,

$$
\begin{aligned}
a =&(c_0 + c_1 b + \dots + c_{k-1} b^{k-1}) + (c_k + c_{k+1} b + \dots + c_{2k-1} b^{k-1})B + \dots \\
&(c_{mk-k} + c_{mk-k+1} b + \dots + c_{mk-1} b^{k-1})B^{m-1}
\end{aligned} \tag{2}
$$

Pretpostavimo, recimo, prvi slučaj. Tada su $c_{jk} + c_{jk+1} b + \dots + c_{jk+k-1} b^{k-1}$, $0 \leq j < m$, odnosno $c_{mk} + c_{mk+1} b + \dots + c_{mk+r-1} b^{r-1}$ predstavljeni redom nekim ciframa $d_j$, $0 \leq j \leq m$ u bazi $B$, pa $a = \sum_{j=0}^{m} d_j B^j = (d_m d_{m-1} \dots d_0)_B$. Za drugi slučaj biće $a = (d_{m-1} \dots d_0)_B$. Prema tome, možemo smatrati da su cifre baze $B$ kodirane nizovima dužine $k$ sastavljenih od cifara baze $b$ na opisan način. Naime, ako grupišemo cifre broja $a$ u bazi $b$ u nizove dužine $k$ i odredimo koje cifre u bazi $B$ one predstavljaju, onda smo odredili i predstavljanje za $a$ u bazi $B$. S druge strane, ukoliko pođemo od reprezentacije broja $a$ u bazi $B$, tj, $a = (d_{m-1} \dots d_0)_B$, onda za odgovarajuća, prethodno opisana razlaganja brojeva $d_j$ u bazi $b$, odnosno zamenom cifara $d_j$ njihovim kodovima u bazi $b$, dolazimo do jedne od jednakosti (1) ili (2), a time i do brojevne reprezentacije broja $a$ u bazi $b$.

Ovakav prelaz u brojevnoj notaciji iz baze $b$ u bazu $B$, odnosno iz baze $B$ u bazu $b$, naziva se u žargonu računarskih nauka *ravnomernim kôdom*, i specijalno je važan za brz prelaz iz binarne baze u heksadecimalnu, i obrnuto.

Recimo neka je $b = 2$, $B = 16 = 2^4$, i neka je $a = \mathrm{A70F}_{16}$. Tada

$$a = \underbrace{1010}_{\mathrm{A}}\ \underbrace{0111}_{7}\ \underbrace{0000}_{0}\ \underbrace{1111}_{\mathrm{F}} = 1010011100001111_2.$$

Ako je, na primer $a = 10101010001100_2$, onda $a = 0010\ 1010\ 1000\ 1100 = \mathrm{2A8C}_{16}$.

Racionalni brojevi takođe se mogu predstavljati u različitim brojevnim bazama. Uzmimo da je $q \in Q^+$, $0 < q < 1$, i neka je $b \in N$, $b \geq 2$. Tada za neki niz cifara $c_n$, $n > 0$, brojevne baze $b$ važi

$$q = \frac{c_1}{b} + \frac{c_2}{b^2} + \frac{c_3}{b^3} + \dots . \tag{3.4.11}$$

i tada pišemo $q = (0.c_1 c_2 c_3 \dots)_b$, a taj zapis nazivamo reprezentacijom racionalnog broja $q$ u brojevnom sistemu (bazi) $b$. Niz $c_n$, definisan pomoću sledećeg niza jednakosti:

$$
\begin{aligned}
c_1 &= [qb] \\
c_2 &= [R(qb)b] \\
c_3 &= [R(R(qb)b)b] \\
&\dots
\end{aligned} \tag{3.4.12}
$$

gde je $R(x) = x - [x]$, $x \in Q$, zadovoljava 3.4.11. Primetimo da je

$$c_n = [u_n], \quad n \in N, \qquad \text{gde je } u_1 = qb \text{ i } u_{n+1} = R(u_n)b, \ n = 2, 3, \ldots \tag{3.4.13}$$

Prema teoremi rekurzije ovakav niz $u_n$ postoji, odakle sledi i egzistencija reprezentacije 3.4.11. Primetimo da predstavljanje racionalnih brojeva u datoj bazi ne mora biti konačno. Za proizvoljni pozitivan racionalni broj $q$, razvoj u bazi $b$ određuje se kao spoj razvoja za $[q]$ i $R(q)$.

**3.4.14 Primer** 1. Odredimo prema prethodnim formulama prvih nekoliko cifara u razvoju za 0.1 u bazi 7.

$$c_1 = [0.1 \cdot 7] = 0, \ c_2 = [R(0.1 \cdot 7)7] = 4,$$
$$c_3 = [R(R(0.1 \cdot 7)7)7] = 6, \ c_4 = [R(R(R(0.1)7)7)7] = 2, \ldots$$

pa $0.1 = (0.0462\ldots)_7$.

2. Broj $(0.1)_{10}$ ima u bazi 2 beskonačan razvoj $0.0001100110011\ldots$.

3. $0.1000\ldots = 0.0999\ldots$ ima dvostruki razvoj, prema tome reprezentacija racionalnih brojeva u datoj bazi ne mora biti jedinstvena.

Jedna od posledica Leme o ostatku je Euklidov algoritam – postupak za određivanje najvećeg zajedničkog delioca za dva data cela broja. Ovaj algoritam se nalazi opisan u Euklidovim *Elementima* (300 g. pre n.e.), i smatra se da je to najstariji netrivijalan algoritam koji je ostao nepromenjen do današnjih dana. Spomenimo da neki istoričari matematike smatraju da je Euklid ovaj postupak preuzeo od Eudoksa. Euklidov algoritam daje efikasan način za izračunavanje najvećeg zajedničkog delioca dva cela broja, pa otuda se i danas objavljuju radovi čija je tema izučavanja ovaj algoritma. Jedna od najdetaljnijih studija Euklidovog algoritma nalazi se na nekoliko desetina stranica Druge knjige *Umetnost programiranja* D. Knutha. Ovde ćemo ukratko prikazati ovaj algoritam, kao i neke jednostavne posledice.

Neka su $a \neq 0$ i $b \neq 0$ celi brojevi, i neka je $S = \{x \in N \mid x > 0, x|a, x|b\}$. Tada je $S$ neprazan (jer $1 \in S$) i konačan (jer $x \in S \Rightarrow x \leq \max(a, b)$). Dakle, u $S$ postoji najveći element, neka je to $m$. Ovaj broj je najveći zajednički delilac brojeva $a$ i $b$ i označavamo ga sa $\mathrm{NZD}(a, b)$. Iz definicije funkcije NZD, odmah nalazimo za $a \neq 0$:

$$\begin{aligned} &\mathrm{NZD}(b, a) = \mathrm{NZD}(a, b) = \mathrm{NZD}(-a, b) = \mathrm{NZD}(a, -b) \\ &\mathrm{NZD}(a, 0) = a, \mathrm{NZD}(a, a) = a, \quad \text{dok } \mathrm{NZD}(0, 0) \text{ nije definisan} \end{aligned} \tag{3.4.15}$$

Zanimljivo je da ukoliko se u definiciji NZD "najveći element" odnosi na relaciju deljivosti | (koja je takođe relacija poretka), onda je $\mathrm{NZD}(0, 0) = 0$. S obzirom na svojstva 3.4.15, ograničićemo se na izučavanje $\mathrm{NZD}(a, b)$ za pozitivne prirodne brojeve $a$ i $b$.

**3.4.16** ***Euklidov algoritam*** *Neka su $a$ i $b$ prirodni brojevi, $a > b > 0$. Prema Lemi o ostatku možemo konstruisati nizove $q_i$ i $r_i$ tako da je*

$$\begin{aligned} r_0 &= a, \quad r_1 = b \\ r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \qquad 0 \leq r_{i+1} < r_i \\ r_2 &= q_3 r_3 + r_3 \\ \ldots \end{aligned}$$

Prema Principu najmanjeg elementa za prirodne brojeve, skup $\{r_0, r_1, r_2, \ldots\}$ mora biti konačan (inače ne bi imao najmanji element). Dakle za neki $k \in N$ važi

$$\begin{aligned} r_0 &= a, \quad r_1 = b \\ r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \qquad 0 < r_i < r_{i+1}, \quad 0 \leq i \leq k+1 \\ &\ldots \\ r_{k-1} &= q_k r_k + r_{k+1} \\ r_k &= q_{k+1} r_{k+1} \end{aligned} \tag{3.4.17}$$

**3.4.18 Tvrđenje** $r_{k+1} = \mathrm{NZD}(a, b)$.

**Dokaz** Polazeći u 3.4.17 od poslednje jednakosti i idući prema prvoj nalazimo $r_{k+1}|r_k, r_{k+1}|r_{k-1}, \ldots, r_{k+1}|r_1,\ r_{k+1}|r_0$, tj. $r_{k+1}|a$ i $r_{k+1}|b$. S druge strane, pretpostavimo da $m \in N$ deli $a$ i $b$. Polazeći sada u 3.4.17 od prve jednakosti i idući prema poslednjoj, nalazimo $m|r_0, m|r_1, m|r_2, \ldots, m|r_k, m|r_{k+1}$, pa $m \leq r_{k+1}$. Dakle $r_{k+1}$ je najveći zajednički delilac brojeva $a$ i $b$. $\diamondsuit$

**3.4.19 Primer** Na osnovu prethodnog dokaza i 3.4.17 odmah imamo: $\mathrm{NZD}(a, b) = \mathrm{NZD}(r_1, r_2) = \ldots = \mathrm{NZD}(r_k, r_{k+1})$. Tako

$$\begin{aligned} \mathrm{NZD}(3456, 2348) &= \mathrm{NZD}(2348, 1108) = \mathrm{NZD}(1108, 132) \\ &= \mathrm{NZD}(132, 52) = \mathrm{NZD}(52, 28) = \mathrm{NZD}(28, 24) = 4 \end{aligned}$$

Direktna posledica Euklidovog algoritma je uslov egzistencije rešenja linearne Diofantovske jednačine.

**3.4.20** ***Bezuova teorema*** *(prema E. Bézout). Neka su $a, b, c$ celi brojeva. Tada jednačina $ax + by = c$ ima celobrojna rešenja akko $\mathrm{NZD}(a, b)|c$, tj.*

$$\exists x\; ax + by = c \Leftrightarrow \mathrm{NZD}(a, b)|c$$

**Dokaz** Neka je $d = \mathrm{NZD}(a, b)$. Prema Euklidovom algoritmu – jednakostima 3.4.17, $d = r_{k+1}$. Dalje, $r_2$ je celobrojna linearna kombinacija od $a$ i $b$, tj. za $\alpha_2 = 1$, $\beta_2 = -q_1$, imamo $r_2 = \alpha_2 a + \beta_2 b$. Kako su celobrojne linearne kombinacije zatvorene za supstituciju, zamenjujući redom $r_i$ iz $i$-te jednakosti u 3.4.17 u sledećoj jednakosti iz tog niza, nalazimo da je i $r_{k+1}$, dakle i $d$, celobrojna linearna kombinacija brojeva $a$ i $b$. Dakle za neke $\alpha, \beta \in Z$, $d = \alpha a + \beta b$. Otuda, ako $d|c$, tj. $c = md$ za neki $m \in Z$, onda jednačina $ax + by = c$ ima celobrojno rešenje $X = m\alpha$, $Y = m\beta$. S druge strane, ako je za neke cele brojeve $X, Y$, $aX + bY = c$, s obzirom da $\mathrm{NZD}(a, b)|a, b$, odmah sledi $\mathrm{NZD}(a, b)|c$. $\diamondsuit$

Navodimo nekoliko posledica Bezuove teoreme iz elementarne teorije brojeva. Podsećamo čitaoca da su celi brojevi $a, b$ uzajamno prosti akko $\mathrm{NZD}(a, b) = 1$.

**3.4.21 Primer** U elementarnoj teoriji brojeva $(a, b)$ označava $\mathrm{NZD}(a, b)$ celih brojeva $a, b$. U ovom primeru koristićemo tu notaciju. Ako su $a, b, c$ celi brojevi, tada važi:

1. $(a, b) = 1 \Leftrightarrow \exists x, y \in Z\; ax + by = 1$. Ovo tvrđenje je posledica Bezuove teoreme uzimajući $c = 1$.
2. $(a, b) = 1 \wedge (b, c) = 1 \Rightarrow (ab, c) = 1$. Dokaz: pretpostavimo $(a, c) = 1, (b, c) = 1$. Prema 1. postoje $x_1, y_1, x_2, y_2 \in Z$ takvi da je $ax_1 + cy_1 = 1$, $bx_2 + cy_2 = 1$, odakle je $abx_1x_2 = (1 - cy_1)(1 - cy_2)$. Dakle za neke cele brojeve $X, Y$ imamo $abX + cY = 1$, te prema Bezuovoj teoremi sledi $(ab, c) = 1$.
3. $(a, b) = 1 \Rightarrow (a^m, b^n) = 1$. Zaista, prema 2. imamo ovaj niz implikacija: $(a, b) = 1 \Rightarrow (a^2, b) = 1 \Rightarrow \ldots \Rightarrow (a^m, b) = 1 \Rightarrow (a^m, b^2) = 1 \Rightarrow \ldots \Rightarrow (a^m, b^n) = 1$
4. $a|c \wedge b|c \wedge (a, b) = 1 \Rightarrow ab|c$. Dokaz: pretpostavimo $a|c, b|c, (a, b) = 1$. Tada za neke cele brojeve $X, Y$ važi $aX + bY = 1$, pa $acX + bcY = c$. S obzirom da $ab|ac$ i $ab|bc$, sledi $ab|c$.
5. $c|ab \wedge (c, a) = 1 \Rightarrow c|b$. Dokaz: pretpostavimo $c|ab, (c, a) = 1$. Tada za neke cele brojeve $X, Y$ imamo $aX + cY = 1$, pa $abX + bcY = b$. Kako $c|ab$ i $c|bc$, na osnovu prethodne jednakosti sledi $c|b$.
6. Neka je $p$ prost broj. Tada $p|ab \Rightarrow p|a \vee p|b$. Dokaz: navedena implikacija ekvivalentna je sa $p \not| a \wedge p \not| b \Rightarrow p \not| ab$. S obzirom da je $p$ prost broj, ova implikacija ekvivalentna je, opet, sa $(p, a) = 1 \wedge (p, b) = 1 \Rightarrow (p, ab) = 1$, što je tačno prema 2.

Jedna od posledica Bezuove teoreme je dokaz Osnovne teoreme aritmetike.

**3.4.22 *Dokaz Osnovne teoreme aritmetike*** (3.1.17)

Pretpostavimo oznake kao u iskazu Teoreme 3.1.17. Najpre dokažimo potpunom indukcijom

(1) Svaki prirodan broj $n > 1$ je prost ili je proizvod prostih brojeva.

Zaista, neka je $a > 1$ fiksiran prirodan broj, i pretpostavimo induktivnu hipotezu, da tvrđenje važi za sve prirodne brojeve $< a$. Ako je $a$ prost, tvrđenje sledi. Pretpostavmo da je $a$ složen, tj. neka je $a = bc$, gde su $b, c$ prirodni brojevi $> 1$. Prema induktivnoj hipotezi svaki od brojeva $b$ i $c$ je prost ili je proizvod prostih brojeva, dakle $a$ je proizvod prostih brojeva. Prema Principu potpune indukcije onda (1) važi.

Neka je $n > 1$ proizvoljan prirodan broj. Prema (1) postoji konačan niz prostih brojeva $q_1, q_2, \ldots, q_m$ tako da je $n = q_1 q_2 \ldots q_m$. Tada postoji konačan niz prostih brojeva $p_1 < p_2 < \ldots < p_k$ tako da je $\{q_1, q_2, \ldots, q_m\} = \{p_1, p_2, \ldots, p_k\}$. Neka je $S_i = \{q_j \mid q_j = p_i, 1 \leq j \leq m\}$, gde $1 \leq i \leq k$. Prema Teoremi 3.1.13, onda:

$$n = \prod_{j=1}^{m} q_j = \prod_{i=1}^{k} \prod_{q \in S_i} q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

gde $\alpha_i = |S_i|$ za $1 \leq i \leq k$. Ovim je dokazana egzistencija razlaganja u Teoremi 3.1.17. Dokažimo jedinost ove reprezentacije. Pretpostavimo

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \quad p_1 < p_2 < \dots < p_s, \quad \alpha_1, \alpha_2, \dots, \alpha_s > 0,$$
$$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k}, \quad q_1 < q_2 < \dots < q_k, \quad \beta_1, \beta_2, \dots, \beta_k > 0.$$

S obzirom da $p_i | p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, $1 \leq i \leq s$, onda $p_i | q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k}$. Prema Primeru 3.4.20.6 onda $p_i | q_1 \vee p_i | q_2 \vee \dots \vee p_i | q_k$, pa $p_i = q_1 \vee p_i = q_2 \vee \dots \vee p_i = q_k$. Dakle, $\{p_1, p_2, \dots, p_s\} \subseteq \{q_1, q_2, \dots, q_k\}$, i simetrično, $\{q_1, q_2, \dots, q_k\} \subseteq \{p_1, p_2, \dots, p_s\}$. Prema tome, $k = s$, i s obzirom da su nizovi $p_1, p_2, \dots, p_s$ i $q_1, q_2, \dots, q_k$ rastući, sledi $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$. Pretpostavimo $\alpha_1 \neq \beta_1$, na primer $\alpha_1 = \beta_1 + \delta$, $\delta > 0$. Tada $p_1^{\delta} p_2^{\alpha_2} \dots p_s^{\alpha_s} = p_2^{\beta_2} \dots p_s^{\beta_s}$, pa $p_1$ deli levu stranu i ne deli desnu stranu ove jednakosti, što je kontradikcija, pa $\alpha_1 = \beta_1$, i slično $\alpha_2 = \beta_2, \dots, \alpha_s = \beta_s$. $\diamondsuit$

## 3.5 Kombinatorni univerzum

Drugi naziv ovog odeljka mogao bi biti: Još jedan pogled na prirodne brojeve. Naime, nerazdvojno povezane sa strukturom prirodnih brojeva su kombinatorne funkcije, kao i drugi kombinatorni objekti. Neke od kombinatornih pojmova već smo upoznali u Odeljku 3.1. Otuda možemo postaviti pitanje da li je moguće uvesti na prirodan način domen u kojem se mogu izgraditi *svi* konačni kombinatorni pojmovi, pa i neki beskonačni. Možemo takođe postaviti pitanje o vezi između strukture prirodnih brojeva i konačne kombinatorike. Ovo pitanje je od interesa za algebru, s obzirom da su konačne algebre važan primer konačnih kombinatornih objekata.

Kada govorimo o konačnoj kombinatorici, pod tim podrazumevamo da je reč o konačnim skupovima i finitarnim operacijama nad njima. Dakle, u takvom pristupu u izučavanju kombinatornih osobina nekog konačnog skupa $x$, možemo uzeti da je skup $x$ *striktno konačan*, tj. da je svaki skup u svakom lancu $x_0 \in x_1 \in \dots \in x_n \in x$ konačan. Na taj način dolazimo do niza skupova $V_n$, $n \in \omega$ definisanog u Primeru 1.1.10. Podsetimo se te definicije: $V_0 = \emptyset$, i $V_{n+1} = \mathbf{P}(V_n)$, $n \in N$. Skup $V = \bigcup_{n \in N} V_n$ nazvaćemo *domenom konačne kombinatorike*. U ZF – teoriji skupova može se dokazati da je $V$ tačno skup svih striktno konačnih skupova, kao i da model $(V, \in)$ zadovoljava sve aksiome teorije ZF osim aksiome beskonačnosti; umesto nje zadovoljava negaciju te aksiome. Otuda, teoriju ZF bez aksiome beskonačnosti, zajedno sa njenom negacijom, nazivamo *teorijom striktno konačnih skupova* i kraće je označamo pomoću $\mathrm{ZF}_f$. Nije teško dokazati da u $(V, \in)$ važi aksioma izbora: Ako je $x \in V$ kolekcija nepraznih skupova, tada $x$ ima izbornu funkciju, tj. postoji funkcija $f$ sa domenom $x$ tako da za svaki $y \in x$, $f(y) \in y$. Ta se činjenica jednostavno dokazuje, na primer, indukcijom po $n$ za elemente skupa $V_n$.

Sledeća svojstva domena $V$ daju nam dovoljno razloga da $V$ zaista smatramo kombinatornim univerzumom. U iskazu ove teoreme koristićemo pojam *tranzitivnog* skupa; skup $x$ je tranzitivan ako za svaki $y \in x$ važi $y \subseteq x$.

**3.5.1 Teorema** 1. Univerzum $V$ je *tranzitivan*, odnosno ako $x \in V$ i $y \in x$, onda $y \in V$.
2. $x_1, x_2, \dots, x_n \in V \Rightarrow \{x_1, x_2, \dots, x_n\} \in V$.
3. $x, y \in V \Rightarrow (x, y) \in V$, gde je $(x, y) = \{\{x\}, \{x, y\}\}$.

4. $x \in V \Rightarrow \bigcup x \in V$.
5. $x, y \in V \Rightarrow x \times y \in V$.
6. Ako su $x, y \in V$ i $f : x \to y$, onda $f \in V$.
7. Ako su $x, y \in V$, onda $x^y \in V$, gde je $x^y = \{f |\, f : y \to x\}$.
8. $x \in V \Rightarrow \mathbf{P}(x) \in V$, gde je $\mathbf{P}(x)$ partitivan skup skupa $x$.
9. Ako je $\mathbf{A}$ algebra konačne signature i $A \in V$, onda $\mathbf{A} \in V$.

**Dokaz** Dokazaćemo jedino tvrđenja 1. i 2., ostala se dokazuju na sličan način.
1. Indukcijom po $n$ dokazujemo da je $V_n$ tranzitivan skup. Prazan skup očigledno jeste tranzitivan, dakle tvrđenje važi za $n = 0$. Pretpostavimo induktivnu hipotezu za fiksiran prirodan broj $n$, tj. neka je $V_n$ tranzitivan. Dokazujemo da je i $V_{n+1}$ tranzitivan. Neka je $x \in V_{n+1}$, i $y \in x$. Tada je $x \subseteq V_n$, odakle sledi $y \in V_n$. S obzirom na induktivnu hipotezu, onda je $y \subseteq V_n$, odakle sledi $y \in V_{n+1}$. Prema tome i $V_{n+1}$ je tranzitivan. Primetimo da odavde odmah sledi

$$V_0 \subseteq V_1 \subseteq V_2 \subseteq \dots \tag{1}$$

2. Pretpostavimo $x_1, x_2, \dots, x_n \in V$. Tada postoje $k_1, k_2, \dots, k_n$ takvi da je $x_i \in V_{k_i}$. Neka je $k \in N$ takav da je $k > \max\{k_1, k_2, \dots, k_n\}$. Tada prema (1) važi $x_1, x_2, \dots, x_n \in V_k$, dakle $x_1, x_2, \dots, x_n \in V$. $\diamondsuit$

S obzirom na Fon Nojmanovu definiciju prirodnih brojeva, odmah nalazimo $N \subseteq V$. Skup prirodnih brojeva se može definisati u univerzumu $V$ na sledeći način:

$$N = \{x \in V |\, \forall y, z \in x(y \in z \vee z \in y \vee y = z) \wedge \forall y \in x \forall z \in y(z \in x)\}. \tag{3.5.2}$$

Formula kojom se opisuju prirodni brojevi u prethodnom identitetu, zapravo definiše prirodne brojeve u $\mathrm{ZF}_f$. Primetimo da ta formula opisuje skup prirodnih brojeva kao skup svih tranzitivnih skupova za koje važi uslov linearnosti u odnosu na $\in$, odnosno koji su linearno uređeni pomoću $\in$.

Na sličan način mogu se definisati i drugi kombinatorni, odnosno skupovni objekti u okviru ove teorije. Na primer, predikat $\mathcal{F}$ definiše pojam funkcije na sledeći način:

$$\mathcal{F}(x) \Leftrightarrow \forall y, z, u((u, y) \in x \wedge (u, z) \in x \Rightarrow y = z) \wedge \forall y \in x\ \exists u, v(y = (u, v)).$$

Tada za $f \in V$, $V \models \mathcal{F}[f]$ ako i samo ako je $f$ funkcija. Domen funkcije $f$ uvodimo pomoću $\mathrm{dom}(f) = \{x |\, \exists y(x, y) \in f\}$, dok kodomen funkcije $f$ definišemo pomoću $\mathrm{codom}(f) = \{y |\, \exists x \in \mathrm{dom}(f)(x, y) \in f\}$. Ako je $f \in V$, nije teško videti da je onda i $\mathrm{dom}(f), \mathrm{codom}(f) \in V$. Dalje, možemo definisati predikat $z : x \to y$ pomoću $\mathcal{F}(z) \wedge x = \mathrm{dom}(z) \wedge \mathrm{codom}(z) \subseteq y$, što čitamo "$z$ je preslikavanje iz skupa $x$ u skup $y$". Izgradnja drugih skupovnih i kombinatornih pojmova u $\mathrm{ZF}_f$, odnosno $V$ izvodi se na sličan način. Razmotrimo sada detaljnije vezu između kombinatornog univerzuma i strukture prirodnih brojeva.

Uvedimo binarnu relaciju $\epsilon$ u skup prirodnih brojeva na sledeći način:

$$x \epsilon y \Leftrightarrow \text{"}x \text{ se pojavljuje u binarnom razvoju za } y\text{"}. \tag{3.5.3}$$

Dakle, ako je $y = \sum_{i=1}^{n} 2^{z_i}$ binarni razvoj za $y$, onda $x \epsilon y$ ako i samo ako $x \in \{z_1, z_2, \ldots, z_n\}$. Na primer, $4 \epsilon 14$ jer $14 = 2^1 + 2^2 + 2^4$. Neka je $\tau : N \to V$ preslikavanje definisano na sledeći način. Ako je $x \in N$, $x > 0$, i $x = \sum_{i=1}^{n} 2^{x_i}$ binarni razvoj za $x$, neka je $\tau(x) = \{\tau x_1, \tau x_2, \ldots, \tau x_n\}$, i neka je $\tau(0) = \emptyset$. Prema napomeni 3.4.4, $n \in N$ jedinstveno je određen, kao i niz $x_1, x_2, \ldots, x_n$. Otuda, prema Teoremi rekurzije preslikavanje $\tau$ je dobro definisano.

**3.5.4 Teorema** $\tau : (N, \epsilon) \cong (V, \in)$.

**Dokaz** 1. Da je $\tau$ 1–1 preslikavanje, dokazaćemo indukcijom po $k$: $\tau u, \tau v \in V_k$ i $\tau u = \tau v$ povlači $u = v$. Tvrđenje trivijalno važi za $k = 0$, pa pretpostavimo induktivnu hipotezu za $k$, i neka su $x, y > 0$ takvi da $\tau x, \tau y \in V_{k+1}$ i $\tau x = \tau y$. Dalje, neka su $x = \sum_{i=1}^{m} 2^{x_i}$ i $y = \sum_{i=1}^{n} 2^{y_i}$ binarni razvoji redom za $x$ i $y$. Prema napomeni 3.4.4, $m$ i $n$ su jedinstveno određeni, kao i nizovi $x_1, x_2, \ldots, x_m$, i $y_1, y_2, \ldots, y_n$. S druge strane, zbog tranzitivnosti skupa $V_{k+1}$, imamo $\tau x, \tau y \subseteq V_k$, odakle sledi $\tau x_i, \tau y_j \in V_k$, pa prema induktivnoj hipotezi ako je $\tau x_i = \tau z$, onda $x_i = z$, i slično za $y_i$. Otuda skup $\{\tau x_1, \tau x_2, \ldots, \tau x_m\}$ ima tačno $m$ elemenata, dok skup $\{\tau y_1, \tau y_2, \ldots, \tau y_n\}$ ima tačno $n$ elemenata. S obzirom da je $\tau x = \tau y$ sledi $m = n$, kao i da je za neku permutaciju $\alpha$ skupa $\{1, 2, \ldots, n\}$, $x_i = y_{\alpha i}$, prema tome:
$x = \sum_{i=1}^{n} 2^{x_i} = \sum_{i=1}^{n} 2^{y_{\alpha i}}$, tj. $x = y$.

2. Neka su $x, y \in N$. Prema definiciji preslikavanja $\tau$, $x \epsilon y$ povlači $\tau x \in \tau y$. S druge strane, pretpostavimo $\tau x \in \tau y$ i neka je $y = \sum_{i=1}^{n} 2^{y_i}$ binarni razvoj za $y$. Tada $\tau x = \tau y_i$ za neki $1 \leq i \leq n$, pa kako je $\tau$ 1–1 preslikavanje, $x = y_i$, dakle $x \epsilon y$. Ovim smo dokazali da je $x \epsilon y$ ako i samo ako $\tau x \in \tau y$.

3. Dokažimo da je $\tau$ preslikavanje *na*. Indukcijom po $n$ dokazujemo da za svaki $x \in V_n$ postoji $a \in N$ tako da je $x = \tau a$. Za $n = 0$ tvrđenje očigledno važi, pa pretpostavimo induktivnu hipotezu za fiksiran prirodan broj $n$. Neka je $x \in V_{n+1}$. Tada za neke $x_1, x_2, \ldots, x_m$, imamo $x = \{x_1, x_2, \ldots, x_m\}$, pa s obzirom na definiciju skupa $V_{n+1}$ sledi $x \subseteq V_n$. Dakle $x_1, x_2, \ldots, x_m \in V_n$, te prema induktivnoj hipotezi postoje $a_i \in N$ tako da je $x_i = \tau a_i$. Otuda nalazimo da za $a = \sum_{i=1}^{m} 2^{a_i}$ važi $\tau a = x$.

$\diamondsuit$

Nije teško videti da je preslikavanje $\sigma : V \to N$ definisano pomoću

$$\sigma(\{x_1, x_2, \ldots, x_n\}) = \sum_{i=1}^{n} 2^{\sigma x_i}, \qquad \sigma(\emptyset) = 0,$$

dobro definisano "$\in$–rekurzijom u $V$", kao i da je $\sigma = \tau^{-1}$. Prema prethodnoj teoremi, svaka konstrukcija, definicija, teorema, ... u, ili o strukturi $(V, \in)$, ima svoju analognu konstrukciju, definiciju, teoremu, ... u strukturi prirodnih brojeva. Drugim rečima možemo uzeti da se teorija $ZF_f$ takođe odnosi na prirodne brojeve – samo na drugi način.

U knjizi smo do sada slobodno koristili pojam konačnog i beskonačnog skupa. Isto tako pretpostavljali smo neka intuitivna svojstva ovih pojmova, na primer da je unija dva konačna skupa takođe konačan skup. Razmotrimo sada kako se uz pomoć prirodnih brojeva, odnosno striktno konačnih skupova, može precizno formulisati pojam konačnog, odnosno beskonačnog skupa, a zatim kako se izvode svojstva tako definisanih konačnih skupova. Naravno, u tim dokazima više ne možemo koristiti, niti pretpostavljati intuitivna svojstva konačnih i beskonačnih skupova. Osnova za naše izvođenje biće teorija o prirodnim brojevima, dakle Peanova aritmetika, odnosno u slučaju beskonačnih skupova ZFC sistem. U izlaganju koje sledi koristićemo činjenicu da je za $n \in N$, $n = \{0, 1, \dots, n-1\}$ ili $n = \emptyset$.

**3.5.5 Definicija** 1. *Skup $X$ je konačan ako postoji $n \in N$ i $f : n \xrightarrow[1\text{-}1]{\text{na}} X$.*
2. *Skup $X$ je beskonačan ako $X$ nije konačan.*

Ako je $n \in N$ i $f : n \xrightarrow[1\text{-}1]{\text{na}} X$, kažemo da skup $X$ ima tačno $n$ elemenata i tu činjenicu zapisujemo pomoću $|X| = n$.

**3.5.6 Lema** *Za svaki skup $S$, ako $S \subseteq n$, $n \in N$, onda je $S$ konačan.*

**Dokaz** Dokaz izvodimo indukcijom po $n$. Za $n = 0$ tvrđenje je očigledno tačno. Pretpostavimo induktivnu hipotezu, da tvrđenje važi za fiksiran prirodan broj $n$, i neka je $S \subseteq n' = n \cup \{n\}$. Tada imamo ove dve mogućnosti:
1. $S \subseteq n$, pa je $S$ konačan po induktivnoj hipotezi.
2. $S = S' \cup \{n\}$, gde je $S' \subseteq n$. Po induktivnoj hipotezi postoji $g' : m \xrightarrow[1\text{-}1]{\text{na}} S'$, pa za $g = g' \cup \{(m, n)\}$ važi $g : m' \xrightarrow[1\text{-}1]{\text{na}} S$, dakle $S$ je konačan. $\diamondsuit$

**3.5.7 Lema** *Za svaki prirodan broj $n$, $V_n$ je konačan.*

**Dokaz** Neka je $\tau : N \to V$ preslikavanje iz Teoreme 3.5.4. Kako $\tau : N \xrightarrow[1\text{-}1]{\text{na}} V$ i $V_n \in V$, postoji $k \in N$ tako da je $V_n = \tau(k)$. Tada

$$x \epsilon k \Rightarrow \tau x \in \tau k \Rightarrow \tau x \in V_n,$$

dakle

$$\{\tau x |\, x \epsilon k\} \subseteq V_n. \tag{1}$$

S druge strane ako je $v \in V_n$, onda s obzirom da je $\tau$ preslikavanje *na*, postoji $m \in N$ tako da je $v = \tau(m)$. Tada $\tau(m) \in \tau(k)$, prema tome $m \epsilon k$, tj. $V_n \subseteq \{\tau x |\, x \epsilon k\}$, što zajedno sa (1) daje $V_n = \{\tau x |\, x \epsilon k\}$. Neka je $S = \{x |\, x \epsilon k\}$. Kako $x \epsilon k \Rightarrow x < k$, to je $S \subseteq k$, pa je prema Lemi 3.5.6 $S$ konačan, odnosno postoji $m \in N$ i $g : m \xrightarrow[1\text{-}1]{\text{na}} S$. Tada $\tau \circ g : m \xrightarrow[1\text{-}1]{\text{na}} V_n$. $\diamondsuit$

**3.5.8 Lema** *Svaki $v \in V$ je konačan.*

Neka je $v \in V$. Tada za neki $n \in N$, $v \in V_n$, pa sa obzirom na tranzitivnost skupa $V_n$, $v \subseteq V_n$. Neka je $V_n = \tau k$ i $S = \tau^{-1}[v]$. Prema dokazu prethodne leme $V_n = \{\tau x |\, x \epsilon k\}$, pa onda $S \subseteq k$. Otuda, prema Lemi 3.5.6, postoji $m \in N$ i $g : m \xrightarrow[1\text{-}1]{\text{na}} S$, dakle $\tau \circ g : m \xrightarrow[1\text{-}1]{\text{na}} v$, tj. $v$ je konačan. $\diamondsuit$

Prema sledećem tvrđenju uslov da je skup $x$ konačan možemo zameniti uslovom da je $x$ ekvipotentan nekom striktno konačnom skupu. Naime važi:

**3.5.9 Teorema** *Skup $X$ je konačan ako i samo ako postoji $S \in V$ i $f : S \xrightarrow[1\text{-}1]{\text{na}} X$.*

**Dokaz** Pretpostavimo da je $X$ konačan. Dakle postoji $n \in N$ i $f : n \xrightarrow[1\text{-}1]{\text{na}} X$, pa možemo uzeti $S = n$. Pretpostavimo obrnuto, da je $f : S \xrightarrow[1\text{-}1]{\text{na}} X$, gde je $S \in V$. Prema prethodnoj lemi $S$ je konačan, dakle postoji $n \in N$ i $g : n \xrightarrow[1\text{-}1]{\text{na}} S$. Tada $f \circ g : n \xrightarrow[1\text{-}1]{\text{na}} X$, prema tome $X$ je konačan. ♢

U sledećem tvrđenju navedena su neka važnija svojstva konačnih skupova. U dokazu tih svojstava koristićemo uslov konačnosti skupova opisan prethodnom teoremom bez eksplicitnog pozivanja na tu teoremu.

**3.5.10 Teorema** 1. *Podskup konačnog skupa je konačan skup.*
2. *Ako je $X$ konačan skup i $f$ funkcija sa domenom $X$, onda je $f[X] = \{f(x) | x \in X\}$ konačan skup.*
3. *Konačna unija konačnih skupova je konačna.*
4. *Dekartov proizvod konačne familije konačnih skupova je konačan.*
5. *Ako je $X$ konačan, onda je i partitivan skup $\mathbf{P}(X)$ konačan.*
6. *(Dirišleov princip). Ako je $X$ konačan skup tada $f : X \xrightarrow{\text{na}} X$ ako i samo ako $f : X \xrightarrow[1\text{-}1]{} X$.*
7. *Ako su $X$ i $Y$ konačni skupovi onda $|X \cup Y| + |X \cap Y| = |X| + |Y|$.*
8. *Ako je $X \subseteq N$ konačan i neprazan, onda $X$ ima najveći element.*

**Dokaz** Dokazujemo samo tvrđenja 1. i 2., ostala se dokazuju na sličan način.
1. Neka je $X$ konačan i $Y \subseteq X$. Tada postoji $S \in V$ i $f : S \xrightarrow[1\text{-}1]{\text{na}} X$. Onda za $S' = f^{-1}[Y]$ važi $S' \in V$ i $f' : S' \xrightarrow[1\text{-}1]{\text{na}} Y$, gde je $f' = f|S'$, pa tvrđenje sledi prema Teoremi 3.5.9.
2. Neka je $X$ konačan i $f : X \xrightarrow{\text{na}} Y$. Tada postoji $S \in V$ i $g : S \xrightarrow[1\text{-}1]{\text{na}} X$. Za $h = f \circ g$ važi $h : S \xrightarrow{\text{na}} Y$, dok je $\{h^{-1}[y] : y \in Y\}$ particija skupa $S$, gde je $h^{-1}[y] = \{s \in S | h(s) = y\}$. Prema Aksiomi izbora (koja važi u V), postoji transverzala $T$ ove particije, tj. skup $T \subseteq S$ tako da za svaki $y \in Y$, skup $T \cap h^{-1}[y]$ ima tačno jedan element. Tada $T \in V$ jer $T \subseteq S$, i za $h' = h|T$ važi $h' : T \xrightarrow[1\text{-}1]{\text{na}} Y$, što znači da je $Y$ konačan. ♢

Pogledajmo jedan primer iz beskonačne kombinatorike, tzv. Remzijevu teoremu. Videćemo nekoliko interesantnih primera primene ove teoreme u algebri.

Za skup $X$ i pozitivan prirodan broj $k$, neka je $[X]^k$ skup svih $k$–članih podskupova skupa $X$, tj. $[X]^k = \{y \subseteq X | |y| = k\}$. Tako, $[X]^2$ biće skup svih dvočlanih podskupova skupa $X$. Dalje, ovom prilikom pod particijom skupa $X$ podrazumevaćemo bilo koje preslikavanje $\pi : X \xrightarrow{\text{na}} n$ za neki pozitivan prirodan broj $n$. Primetimo da je $\{\pi^{-1}(i) | i \in n\}$ particija skupa $X$ u ranije definisanom smislu. Nekad je zgodno smatrati da su vrednosti preslikavanja $\pi$ boje. Naime, pretpostavimo da je dato $n$ boja koje su označene brojevima $0, 1, \ldots, n-1$. Ako je $\pi(a) = i$, $i \in n$, smatraćemo onda da je element $a$ obojen bojom $i$. Pod ovim pretpostavkama su svi članovi jedne klase particije $\pi$ obojeni jednom bojom. Dakle, možemo koristiti još jedan naziv za particiju $\pi$ skupa $X$ – bojenje skupa $X$. Pretpostavimo da je $\pi : [X]^k \xrightarrow{\text{na}} n$ particija skupa $[X]^k$. Reći ćemo da je $Y \subseteq X$ *homogen* za particiju $\pi$ ako je restrikcija preslikavanja $\pi$ na $[Y]^k$ konstantna funkcija. Drugim rečima, ako je $\pi$ bojenje skupa $[X]^k$, onda su svi članovi iz $[Y]^k$ obojeni istom bojom.

**3.5.11** ***Remzijeva teorema*** *Neka su $k$ i $r$ pozitivni prirodni brojevi, i neka je $\pi : [N]^k \xrightarrow{\text{na}} r$. Tada postoji beskonačan $T \subseteq N$ homogen za $\pi$, tj. $\pi$ je konstantna funkcija na $[T]^k$.*

**Dokaz** Dokaz ove teoreme izvešćemo indukcijom po $k$. Najpre primetimo da je tvrđenje trivijalno tačno za $r = 1$, pa pretpostavimo da je $r \geq 2$.

Za $k = 1$ tvrđenje očigledno važi jer je konačna unija konačnih skupova takođe konačan skup.

Neka je $k > 1$ fiksiran prirodan broj i pretpostavimo induktivnu hipotezu – da je Remzijeva teorema tačna za $k - 1$. Konstruišemo niz nepraznih skupova $X_i \subseteq N$ i funkcija $\pi_i$, $i \in N$, na sledeći način.

Neka je $X_0 = N$. Pretpostavimo da smo konstruisali skupove $X_0, X_1, \ldots X_n$, i neka je $x_{n+1}$ najmanji element skupa $X_n$. Preslikavanje $\pi_{n+1} : [X_n - \{x_{n+1}\}]^{k-1} \to r$ definišemo pomoću

$$\begin{aligned} &\pi_{n+1}(\{y_1, y_2, \ldots, y_{k-1}\}) = \pi(\{x_{n+1}, y_1, y_2, \ldots, y_{k-1}\}), \\ &y_1 < y_2 < \ldots y_{k-1}, \qquad y_1, y_2, \ldots, y_{k-1} \in X_n - \{x_{n+1}\}. \end{aligned}$$

Prema induktivnoj hipotezi, postoji beskonačan $X_{n+1} \subseteq X_n - \{x_{n+1}\}$ homogen za $\pi_{n+1}$, tj. za neki $r_{n+1} < r$ restrikcija $\pi_{n+1}|[X_{n+1}]^{k-1}$ uzima vrednost $r_{n+1}$. Na ovaj način definisali smo niz skupova $X_n$, preslikavanja $\pi_n$ i prirodnih brojeva $r_n < r$. S obzirom da ima konačno mnogo vrednosti u nizu $r_n$, postoji rastući niz $n_i \in N$ i $s < r$ tako da je za sve $i \in N$, $r_{n_i} = s$. Neka je $X = \{x_{n_0}, x_{n_1}, x_{n_2}, \ldots\}$. Tada za sve $Y \in [X]^k$ važi $\pi(Y) = s$, tj. $X$ je homogen za $\pi$. $\diamondsuit$

U iskazu Remzijeve teoreme umesto skupa prirodnih brojeva $N$ možemo uzeti bilo koji beskonačan skup $A$. Naime, u tom slučaju biramo neki prebrojiv $S \subseteq A$, i zatim se dokaz izvodi na isti način za skup $S$ umesto za $N$. Pogledajmo nekoliko primera primene Remzijeve teoreme.

**3.5.12 Primer** Neka je $(X, \leq)$ linearno uređen skup i neka je $x = \langle x_n | n \in N \rangle$ niz elemenata skupa X. Tada postoji podniz niza $x$ koji je ili monoton ili konstantan.

**Dokaz** Neka je $\pi : [N]^2 \to 3$ particija definisana na sledeći način:

$$\pi(m, n) = \begin{cases} 0, & \text{ako } a_m < a_n \\ 1, & \text{ako } a_m > a_n \\ 2, & \text{ako } a_m = a_n \end{cases} \qquad \{m, n\} \in [N]^2, \quad m < n.$$

Neka je $T = \{n_0, n_1, n_2, \ldots\}$ homogen za $\pi$. Tada je niz $\langle x_{n_i} | i \in N \rangle$ monoton ili konstantan.

**3.5.13 Primer** Graf je svaki par $\mathbf{G} = (G, \mathcal{E})$, gde je $G$ neprazan skup, a $\mathcal{E} \subseteq [G]^2$. Elemente domena $G$ nazivamo *čvorovima* grafa $G$, a par $\{a, b\} \in \mathcal{E}$ *granom* koja povezuje čvorove $a$ i $b$. Graf $(G, [G]^2)$ naziva se *potpunim* grafom; u tom grafu svi su čvorovi međusobno povezani. Remzijeva teorema primenjena na potpune grafove glasi: Pretpostavimo da su grane beskonačnog kompletnog grafa obojene u $r$ boja. Tada postoji beskonačan kompletan podgraf grafa $G$ čije su sve grane obojene jednom bojom. Zaista, neka je $\pi : [G]^2 \to r$ particija definisana pomoću $\pi(\{a, b\}) = i$ ako je grana $\{a, b\}$ obojena bojom $i$. Neka je $T \subseteq G$ beskonačan i homogen za $\pi$; tada je $T$ domen beskonačnog, kompletnog podgrafa grafa $G$ čije su sve grane obojene jednom bojom.

Osim ove beskonačne verzije Remzijeve teoreme, postoji i konačna verzija. Ona glasi:

**3.5.14 Teorema** *Neka su $k, t, r$ pozitivni prirodni brojevi. Tada postoji prirodan broj $m$ tako da za sve $n \in N$, $n > m$, i sve particije $\pi : [n]^k \xrightarrow{\text{na}} r$, postoji skup $e \subseteq n$ kardinalnosti $t$, koji je homogen za $\pi$.*

Ovde nećemo dokazivati ovu teoremu. Ipak, spomenimo da postoji relativno jednostavan, istina nekonstruktivan dokaz, primenjujući, na primer, Teoremu kompaktnosti, ili neke druge infinitarne principe, kao što je Königova lema za beskonačna drveta, na beskonačnu verziju Remzijeve teoreme. Zanimljiva je i sledeća finitarna verzija Ramzejeve teoreme. Najpre kažimo da je konačan podskup $S \subseteq N$ relativno veliki ako je $|S| \geq \min S$. Tada konačna verzija Remzijeve teoreme za relativno velike skupove glasi kao i Teorema 3.5.14, sa dodatkom da podskup $e$ koji se pominje u toj teoremi mora biti relativno veliki. Označimo tu verziju Remzijeve teoreme sa $\mathrm{RT}_v$. Značaj ove teoreme je sledeći. Iako je to iskaz konačne kombinatorike, J. Paris i L. Harrington dokazali su 1978 g. da niti $\mathrm{RT}_v$, niti negacija od $\mathrm{RT}_v$ nisu dokazive u teoriji striktno konačnih skupova $\mathrm{ZF}_f$, dakle ni u formalnoj Peanovoj aritmetici, dok s druge strane $\mathrm{RT}_v$ važi u kombinatornom univerzumu. Naravno, provera istinitosti iskaza $\mathrm{RT}_v$ u $(V, \in)$ zasniva se na jačim principima nego što ima teorija striktno konačnih skupova; to je ZFC teorija skupova. $\mathrm{RT}_v$ bio je prvi primer neodlučivog iskaza formalne aritmetike (videti kraj Odeljka 3.1) koji se odnosi na neko određeno kombinatorno svojstvo prirodnih brojeva.

Zaključimo ovaj odeljak jednom primenom konačne verzije Remzijeve teoreme na konačne semigrupe.

**3.5.15 Primer** Svaka konačna semigrupa $(S, \cdot)$ ima idempotentan element.

**Dokaz** Neka je $x = \langle x_0, x_1, \ldots, x_t \rangle$ proizvoljan konačan niz elemenata iz $S$ i neka je $s = |S|$. Definišimo bojenje $\pi$ kompletnog $\mathbf{G}_t$ grafa sa domenom $t = \{0, 1, \ldots, t-1\}$ u $s$ boja pomoću $\pi(i, j) = x_{i+1} \cdot x_{i+2} \cdot \ldots x_j$, $i < j$. Prema Teoremi 3.5.14 možemo izabrati $m$ i $t > m$ tako da $\mathbf{G}_t$ sadrži "trougao" u jednoj boji, tj. da je za neke $i < j < k$, $\pi(\{i, j\}) = \pi(\{i, k\}) = \pi(\{j, k\}) = a$, $a \in S$. Tada $a^2 = a$, jer

$$\prod_{i<u\leq j} x_u = \prod_{j<v\leq k} x_v = \prod_{i<w\leq k} x_w = \prod_{i<u\leq j} x_u \cdot \prod_{j<v\leq k} x_v = a. \qquad \diamondsuit$$

## 3.6 Realni brojevi

Pored prirodnih brojeva, pojam realnih brojeva je drugo osnovno mesto u razmatranjima o brojevima. Predstava o pravoj kao uređenom kontinuumu tačaka daje intuitivnu osnovu za uvođenje realnih brojeva. Poznato je više pristupa u izgradnji polja realnih brojeva. Svakako najpoznatiji način zasnivanja realnih brojeva su Kantorova, odnosno Dedekindova teorija iz druge polovine prošlog veka (i Kantor i Dedekind objavili su svoje konstrukcije 1872. godine). Pojavom ovih teorija na egzaktan način se završava zasnivanje realnog kontinuuma. Istaknimo da je problem zasnivanja realnih brojeva veoma star. Naime, veću šestom veku pre nove ere, matematičari pitagorejske škole otkrili su prilikom rešavanja jednostavnih geometrijskih zadataka da ima "nesamerljivih" veličina. Tako je nastala takozvana pitagorejska ravan kao proširenje racionalne ravni, o čemu će kasnije biti više reči, a koja se sastoji iz tačaka koje se mogu konstruisati koristeći lenjir i šestar. Zatim su se javili i drugi problemi kao što je rešavanje algebarskih jednačina, zatim razni problemi iz analize i analitičke geometrije koji su ukazivali na potrebu upotpunjavanja, odnosno proširenja brojevnog domena. I tako se Dedekind–Kantorova teorija pojavljuje kao kruna duhovnog napora koji vodi poreklo iz daleke prošlosti. Dedekindov pristup zasniva se na Dedekindovim presecima, dok se Kantorova teorija oslanja na teoriju tzv. Košijevih nizova. Ovde ćemo ukratko razmotriti ovaj drugi način izgradnje realnih brojeva.

Izgradnja uređenog polja realnih brojeva zasniva se na uređenom polju racionalnih brojeva. Stoga uvodimo sledeće strukture i pojmove. Neka je $\mathbf{Q}$ uređeno polje racionalnih brojeva i $\mathbf{Q}^N$ stepen strukture $\mathbf{Q}$. Dakle domen je $Q^N$, skup svih racionalnih nizova, dok su operacije u $\mathbf{Q}^N$ po koordinatama, v. Primer 1.8.7. Prema Posledici 1.8.10, važi:

**3.6.1 Teorema** $\mathbf{Q}^N$ *je komutativan prsten.*

Ako je $q \in Q$, onda $\mathbf{q}$ označava konstantan niz $\langle q, q, q, \ldots\rangle$. Primetimo da je preslikavanje $q \mapsto \mathbf{q}$, $q \in Q$ utapanje polja $\mathbf{Q}$ u prsten $\mathbf{Q}^N$. Ako se racionalni nizovi $x, y$ razlikuju u konačno mnogo indeksa, tj. postoji $m \in N$ tako da je za sve prirodne brojeve $n \geq m$, $x_n = y_n$, reći ćemo da su $x$ i $y$ *skoro jednaki*, i tu činjenicu zapisaćemo sa $x =_s y$. Očigledno, relacija $=_s$ je relacija ekvivalencije domena $Q^N$. Najzad, niz $x$ je *skoro konstantan* ako je skoro jednak nekom $\mathbf{q}$, gde $q \in Q$.

Kao što je napomenuto, u Kantorovoj teoriji ključnu ulogu imaju Košijevi nizovi. Sledećom definicijom uvodimo pojam Košijevog niza i nula niza racionalnih brojeva.

**3.6.2 Definicija** 1. *Niz racionalnih brojeva* $x = \langle x_n \,|\, n \in N\rangle$ *je nula niz ako:* $\forall\varepsilon \in Q^+ \exists m \in N\, \forall n > m \ |x_n| < \varepsilon$.

2. *Racionalni nizovi* $x, y$ *su ekvivalentni, ako je* $x - y$ *nula niz. Činjenicu da su racionalni nizovi* $x$ *i* $y$ *ekvivalentni obeležavamo pomoću* $x \sim y$.
3. *Racionalan niz* $x = \langle x_n \,|\, n \in N\rangle$ *je Košijev, ako:* $\forall\varepsilon \in Q^+ \exists m \in N\, \forall n > m \ |x_n - x_m| < \varepsilon$.

Simbolom $\mathcal{C}$ obeležićemo skup svih racionalnih Košijevih nizova. Sledeća tvrđenja opisuju neke elementarne osobine Košijevih nizova.

**3.6.3 Lema** *Neka su $x, y$ racionalni nizovi. Tada važi:*
1. *Svaki Košijev niz je ograničen.*
2. *Ako $x =_s y$, onda je $x \sim y$.*
3. *Ako $x$ je Košijev niz i $y$ je nula niz, tada je $x + y$ Košijev niz i $x + y \sim x$.*
4. *Ako $x =_s y$ i $x$ je Košijev, tada je $y$ Košijev niz i $x \sim y$.*
5. *Svaki skoro konstantan racionalan niz je Košijev.*
6. *Podniz $y$ Košijevog niza $x$ je Košijev i $y \sim x$.*

**Dokaz** 1. Izaberimo u definiciji Košijevog niza $\varepsilon = 1$. Tada za neki prirodan broj $m$ važi: za sve prirodne brojeve $n > m$, $|x_n - x_m| < 1$. Otuda za proizvoljan $n \in N$,

$$|x_n| = |(x_n - x_m) + x_m| \leq |x_n - x_m| + |x_m|, \qquad n > m$$

tj. $|x_n| \leq M$, gde je $M = 1 + |x_m|$.
2. Pretpostavimo $x =_s y$. Tada za neki $m \in N$, za sve prirodne brojeve $n \geq m$, $x_n = y_n$, dakle $|x_n - y_n| < \varepsilon$ za proizvoljno $\varepsilon \in Q^+$.
3. Neka je $x$ Košijev i $y$ nula niz. Dalje, neka je $\varepsilon \in Q^+$. S obzirom da je $x$ Košijev, postoji $m_1 \in N$ tako da za sve $n \in N$, $n \geq m_1$, važi $|x_n - x_{m_1}| < \varepsilon/2$. S obzirom da je $y$ nula niz, postoji $m_2 \in N$ tako da za sve $n \in N$, $n \geq m_2$, važi $|y_n| < \varepsilon/2$. izaberimo $m \geq m_1, m_2$. Tada za $n > m$,

$$|(x_m + y_n) - x_n| \leq |x_m - x_n| + |y_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

tj. $x + y$ je Košijev niz i $x + y \sim x$.
4. Pretpostavimo da je $x$ Košijev niz i neka je $x =_s y$. Prema 2., tada je $y - x$ nula niz, a prema 3., $y = x + (y - x)$ je Košijev.
5. Očigledno je svaki $\mathbf{q}$ Košijev niz, gde $q \in Q$. Tada je prema 4. i svaki $x =_s \mathbf{q}$ Košijev niz.
6. Neka je $x$ Košijev niz i $y = \langle x_{n_k} | k \in N \rangle$ podniz niza $x$, gde je $n_k$ strogo monotono rastući niz prirodnih brojeva. Neka je $\varepsilon \in Q^+$ i $m \in N$ tako da je za sve $n \in N$, $|x_m - x_n| < \varepsilon/2$. Neka je $p$ najmanji prirodan broj takav da je $n_p > m$. Tada za $k > p$ imamo

$$|x_{n_p} - x_{n_k}| \leq |x_m - x_{n_p}| + |x_m - x_{n_k}| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Dakle, $y$ je Košijev niz. Dalje, za gore izabrano $\varepsilon$ i $m$ i za $k > m$, s obzirom da je $n_k \geq k$, imamo

$$|x_k - x_{n_k}| \leq |x_m - x_k| + |x_m - x_{n_k}| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

tj. $x \sim y$. $\diamondsuit$

**3.6.4 Teorema** *$\mathcal{C}$ je podalgebra prstena $\mathbf{Q}^N$.*

**Dokaz** S obzirom da su prema prethodnoj lemi $\mathbf{0}, \mathbf{1} \in \mathcal{C}$, dovoljno je dokazati da je domen $\mathcal{C}$ zatvoren za operacije $+$ i $\cdot$ algebre $\mathbf{Q}^N$.

1. Neka su su $x, y \in \mathcal{C}$, $\varepsilon \in Q^+$ i neka je $z = x + y$. S obzirom da su $x$ i $y$ Košijevi nizovi, postoje $m_1, m_2 \in N$ tako da je za $n > m_1$, $|y_{m_1} - y_n| < \varepsilon/2$, i za $n > m_2$, $|x_{m_2} - x_n| < \varepsilon/2$. Izaberimo $m > m_1, m_2$. Tada za $n > m$

$$|z_m - z_n| \leq |x_m - x_n| + |y_m - y_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon,$$

tj. $x + y \in \mathcal{C}$.
2. Neka su su $x, y \in \mathcal{C}$, $\varepsilon \in Q^+$ i neka je $z = x \cdot y$. S obzirom da su $x$ i $y$ Košijevi nizovi, prema Lemi 3.6.3.1, $x$ i $y$ su ograničeni, tj. za neke $M_1, M_2 \in Q^+$, za sve $n \in N$ važi $|x_n| \leq M_1$ i $|y_n| \leq M_2$. Izaberimo $M \geq M_1, M_2$. Tada postoje $m_1, m_2 \in N$ tako da za sve $n > m_1$, $|x_{m_1} - x_n| < \varepsilon/(2M)$, i za sve $n > m_2$, $|y_{m_2} - y_n| < \varepsilon/(2M)$. Neka je $m \geq m_1, m_2$. Tada za $n \geq m$ važi

$$\begin{aligned} |z_m - z_n| \leq & |x_m y_m - x_m y_n| + |x_m y_n - x_n y_n| = \\ & |x_m||y_m - y_n| + |y_n||x_m - x_n| < M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \varepsilon, \end{aligned}$$

tj. $x \cdot y \in \mathcal{C}$. ♢

**3.6.5 Posledica** Algebra $(\mathcal{C}, +, \cdot, \mathbf{0}, \mathbf{1})$ je komutativan prsten sa jedinicom.

Neka je $\mathcal{C}_0$ skup svih racionalnih nula nizova. Tada nije teško videti da je $\mathcal{C}_0 \subseteq \mathcal{C}$.

**3.6.6 Lema** *$\mathcal{C}_0$ je ideal prstena $\mathcal{C}$, tj. važi*
1. $\mathbf{0} \in \mathcal{C}_0$.
2. *$(\mathcal{C}_0, +, 0)$ je podgrupa grupe $(\mathcal{C}, +, 0)$.*
3. *Ako $x \in \mathcal{C}$ i $y \in \mathcal{C}_0$, tada $xy \in \mathcal{C}_0$.*

**Dokaz** Tvrđenje 1. očigledno važi, pa dokazujemo 2. Dovoljno je dokazati zatvorenost domena $\mathcal{C}_0$ u odnosu na operaciju $+$. Zaista, neka su $x, y \in \mathcal{C}_0$, i neka je $\varepsilon \in Q^+$. Tada za neke prirodne brojeve $m_1, m_2$ važi: ako je $n > m_1$ onda $|x_n| < \varepsilon/2$, odnosno ako je $n > m_2$, onda $|y_n| < \varepsilon/2$. Izaberimo $m > m_1, m_2$. Tada za $n > m$

$$|x_n + y_n| \leq |x_n| + |y_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

tj. $x + y$ je nula niz.
3. Neka su $x \in \mathcal{C}$, $y \in \mathcal{C}_0$ i $\varepsilon \in Q^+$. Kako je niz $x$ ograničen, postoji $M \in Q^+$ tako da je za sve $n \in N$, $|x_n| \leq M$. S obzirom da je $y$ nula niz, postoji $m \in N$ tako da je za sve $n > m$, $|y_n| < \varepsilon/M$. Tada za sve $n > m$

$$|x_n y_n| = |x_n||y_n| < M \cdot \frac{\varepsilon}{M} = \varepsilon,$$

tj. $xy$ je nula niz. ♢

**3.6.7 Lema** *Relacija $\sim$ je relacija kongruencije prstena $(\mathcal{C}, +, \cdot, \mathbf{0}, \mathbf{1})$.*

**Dokaz** Lako je proveriti da je relacija $\sim$ refleksivna i simetrična. Dokažimo da je $\sim$ tranzitivna. Neka su $x, y, z \in \mathcal{C}$, i pretpostavimo da je $x \sim y$, $y \sim z$. No tada $x-y, y-z \in \mathcal{C}_0$, pa obzirom na prethodnu lemu, takođe imamo $(x-y)+(y-z) \in \mathcal{C}_0$, tj. $x \sim z$.

U dokazu saglasnosti relacije $\sim$ koristićemo Lemu 1.10.18. Neka su $x, y, z \in \mathcal{C}$ i pretpostavimo $x \sim y$. Tada je $(x+z)-(y+z)$ nula niz, dakle $x+z \sim y+z$, tj. relacija $\sim$ saglasna je sa operacijom $+$. Dalje, $xz - yz = (x-y)z$, pa kako je $x-y$ nula niz, prema prethodnoj lemi $(x-y)z \in \mathcal{C}_0$, tj. $xz \sim yz$; prema tome relacija $\sim$ saglasna je i sa operacijom $\cdot$ algebre $(\mathcal{C}, +, \cdot, \mathbf{0}, \mathbf{1})$. $\diamondsuit$

Dakle, postoji količnička algebra $\mathbf{R} = (\mathcal{C}, +, \cdot, \mathbf{0}, \mathbf{1})/\!\sim$. Prema tome, domen ove algebre je $R = \mathcal{C}/\!\sim$, dok je prema Teoremi 1.10.14 i Posledici 3.6.5, $\mathbf{R}$ komutativan prsten sa jedinicom. Primetimo da je nula ovog prstena klasa kongruencije $\mathbf{0}/\!\sim$. Elemente skupa $R$ nazivamo *realnim brojevima*. Pre određivanja daljih osobina strukture realnih brojeva dokažimo dve leme.

**3.6.8** ***Lema separacije*** *Neka su $a$, $b$ racionalni Košijevi nizovi takvi da $a \not\sim b$. Tada postoji $m \in N$ i $q, q' \in Q$ takvi da je $q < q'$ i:*

$$\forall n \geq m \;\; a_n < q < q' < b_n, \qquad \text{ili}$$
$$\forall n \geq m \;\; b_n < q < q' < a_n.$$

**Dokaz** S obzirom da $a-b$ nije nula niz, postoji $d \in Q^+$ i $n_0 \in N$ tako da je za svaki $n \geq n_0$, $|a_n - b_n| \geq d$.

S obzirom da je $a_n$ Košijev niz, postoji $n_1 \in N$ takav da je za sve $n \geq n_1$, $|a_{n_1} - a_n| < d/8$.

S obzirom da je $b_n$ Košijev niz, postoji $n_2 \in N$ takav da je za sve $n \geq n_2$, $|b_{n_2} - b_n| < d/8$.

Izaberimo prirodan broj $m > n_0, n_1, n_2$. Tada za svaki $n \geq m$

$$|a_m - a_n| \leq |a_{n_1} - a_m| + |a_{n_1} - a_n| < \frac{d}{8} + \frac{d}{8} = \frac{d}{4}.$$

Slična nejednakost važi i za niz $b$, dakle za svaki $n \geq m$ važe nejednakosti

$$|a_n - b_n| \geq d, \quad |a_m - a_n| < \frac{d}{4}, \quad |b_m - b_n| < \frac{d}{4}.$$

Tada $a_m < b_m$ ili $b_m < a_m$. Pretpostavimo, recimo, $a_m < b_m$. Tada za svaki $n \geq m$ važi

$$b_n - a_n \geq d, \quad a_m - \frac{d}{4} \leq a_n \leq a_m + \frac{d}{4}, \quad b_m - \frac{d}{4} \leq b_n \leq b_m + \frac{d}{4},$$

S obzirom da je skup racionalnih brojeva gusto uređen, i kako je $a_m + d/4 < b_m - d/4$, postoje racionalni brojevi $q, q' \in Q$ takvi da je

$$a_m + \frac{d}{4} < q < q' < b_m - \frac{d}{4},$$

tj. za svaki $n \geq m$ važi $a_n < q \leq q' < b_n$. Primetimo da se odavde odmah izvodi na izgled jače svojstvo: za sve $n, n' \geq m$, $a_n \leq q \leq q' \leq b_{n'}$ .

Slučaj $b_m < a_m$ razmatra se na sličan način. $\diamondsuit$

Uz oznake u prethodnoj lemi, za racionalne brojeve $q$ i $q'$ reći ćemo da razdvajaju nizove $a$ i $b$ počev od $m$.

**3.6.9 Lema** *Neka je $x$ Košijev niz. Tada postoji strogo monotono rastući Košijev niz $u$ i strogo monotono opadajući niz $v$ tako da je $u \sim x$ i $v \sim x$.*

**Dokaz** Pretpostavimo najpre da postoji racionalan broj $q$ tako da je $x \sim \mathbf{q}$. Tada možemo uzeti

$$u = \langle q - \frac{1}{n+1} | \, n \in N\rangle, \qquad v = \langle q + \frac{1}{n+1} | \, n \in N\rangle.$$

Pretpostavimo drugi slučaj, da nema racionalnog broja $q$ tako da je $x \sim \mathbf{q}$. Primenom Remzijeve teoreme, videti Primer 3.5.12, postoji podniz $y$ niza $x$ koji je monoton ili konstantan. Ako je $y$ konstantan, onda je za neki racionalan broj $q$, $y = \mathbf{q}$, pa bi s obzirom na Lemu 3.6.3.6 bilo $x \sim \mathbf{q}$, suprotno pretpostavci. Dakle, $y$ je strogo monoton, recimo monotono opadajući. Tada prema Lemi 3.6.6.3 možemo uzeti $v = y$. Niz $u$ konstruisaćemo na sledeći način. Najpre dokažimo:

(1) Neka je $m$ pozitivan prirodan broj i $p \in Q$ takav da za svaki $n \in N$ važi $p < v_n$. Tada postoji $r \in Q$ i $k \in N$ tako da za svaki prirodan broj $n$ važi $p < r < v_n$ i $v_k - r < 1/m$

Zaista, ako $p$ zadovoljava uslov iz (1), kako $v \not\sim p$, prema Lemi separacije, uzimajući u lemi $b = \langle p, p, p, \dots \rangle$, postoji $n' \in N$ i racionalni brojevi $q, q'$ takvi da je za sve $n > n'$, $p < q < q' < v_n$. S obzirom da je $v_n$ monotono opadajući niz, prethodna nejednakost zapravo važi za svaki $n \in N$. Izaberimo racionalan $\delta < q' - q, 1/m$. Tada $q + \delta < v_n$ za sve $n \in N$, dok sa druge strane, prema arhimedovskom svojstvu uređenog polja racionalnih, brojeva (v. Teoremu 3.3.12,) za neki $s \in N$ postoji $k \in N$ tako da je $q + s\delta \geq v_k$. Dakle, prema Principu najmanjeg prirodnog broja, postoji najmanji prirodan broj $s$ sa tim svojstvom. S obzirom da je $v$ monotono opadajući niz, prema istom principu možemo izabrati najmanji $k \in N$ tako da je onda $q + s\delta \geq v_k$. Tada

$$\forall n \in N \quad q + (s-1)\delta < v_n, \qquad v_k \leq q + s\delta.$$

Dakle $r = q + (s-1)\delta$ i $k$ zadovoljavaju tražene uslove u (1), čime je tvrđenje (1) dokazano.

Izaberimo proizvoljan $u_0$ takav da je $\forall n \in N \ u_0 < v_n$. Primetimo da takav $u_0$ postoji s obzirom da $Q$ nije ograničen odozdo i da je $v$ Košijev, dakle ograničen. Pretpostavimo da smo konstruisali članove niza $u_0 < u_1 < \ldots < u_m$, kao i podniz $v_{n_0}, v_{n_1} \dots, v_{n_m}$ za koje važi:

$$(2) \qquad u_i < v_{n_i} < u_i + \frac{1}{i}, \qquad i = 1, 2, \ldots, m; \qquad \forall n \in N \, u_m < v_n$$

Prema (1) postoji $r \in Q$ i $k \in N$ tako da je

$$(3) \qquad \forall n \in N\, u_m < r < v_n, \qquad v_k < r + \frac{1}{m+1}.$$

Tada biramo $u_{m+1} = r$, dok je $n_{m+1}$ najmanji prirodan broj $k > n_m$ tako da važi (3). Ovim smo konstruisali strogo monotono rastući niz $u$. Neka je $v' = \langle v_{n_m} \,|\, m \in N \rangle$. Tada je $v'$ je podniz niza $v$, dakle $v' \sim v$ i $v'$ je Košijev. Dalje, $v' - u$ je nula niz, dakle $u \sim v'$ i $u$ je Košijev niz. Kako je $v' \sim v$, onda i $u \sim v$. ♢

**3.6.10 Teorema** 1. $\mathbf{R}$ *je polje.*
2. *Preslikavanje* $\sigma : q \mapsto \mathbf{q}/\sim$, $q \in Q$ *je utapanje polja* $\mathbf{Q}$ *u* $\mathbf{R}$.

**Dokaz** 1. Već smo primetili da je $\mathbf{R}$ komutativan prsten, pa dokazujemo da svaki realan broj različit od nule ima inverzan u odnosu na operaciju množenja. Neka je $r \in R - \{\mathbf{0}/\sim\}$, $r = x/\sim$, gde je $x$ Košijev niz. Tada $x \not\sim \mathbf{0}$, pa postoji $m \in N$ i $\varepsilon \in Q^+$ tako da je $|x_n| \geq \varepsilon$ za sve $n > m$. Neka je niz $y$ definisan pomoću

$$y_n = \begin{cases} 1, & n \leq m \\ 1/x_n, & n > m \end{cases}$$

Nije teško videti da je $y/\sim = r^{-1}$.
2. Preslikavanje $\sigma$ je homomorfizam u odnosu na operacije $+$ i $\cdot$ s obzirom na definiciju količničke algebre. Dokažimo da je $\sigma$ 1–1 preslikavanje. Neka su $p, q \in Q$, $p \neq q$ i pretpostavimo da je $\sigma p = \sigma q$. S obzirom da je $\sigma$ homomorfizam, sledi $\sigma(p - q) = \mathbf{0}/\sim$. Dakle, za $r = p - q$, $\mathbf{r}$ je nula niz, što očigledno nije moguće jer je $r$ racionalan broj različit od nule. ♢

Kao što smo uradili u slučaju prirodnih i celih, odnosno celih i racionalnih brojeva, i ovde ćemo identifikovati polje racionalnih brojeva sa njegovom izomorfnom slikom $\sigma Q$. Tako na primer, konstantu 0 identifikujemo sa $\mathbf{0}/\sim$, a 1 sa $\mathbf{1}/\sim$. Otuda, ako je iz konteksta jasno, za racionalan broj $q$ umesto $\mathbf{q}/\sim$ pisaćemo jednostavno $q$.

Razmotrimo pitanje uređenja polja realnih brojeva. Naime, uređenje polja racionalnih brojeva može se proširiti na ceo domen $R$.

**3.6.11 Definicija** *Neka su* $r = a/\sim$ *i* $s = b/\sim$ *različiti realni brojevi, gde su* $a$ *i* $b$ *racionalni Košijevi nizovi. Dalje, neka su prema Lemi separacije* $q$ *i* $q'$ *racionalni brojevi koji razdvajaju nizove* $a$ *i* $b$ *počev od nekog* $m$.
- *Ako za* $\forall n > m\ a_n < q < q' < b_n$, *onda* $r < s$.
- *Ako za* $\forall n > m\ b_n < q < q' < a_n$, *onda* $s < r$.

*Za proizvoljne* $r, s \in R$, *uzećemo* $r \leq s \overset{\text{def}}{\Longleftrightarrow} r < s \vee r = s$

U prethodnoj definiciji $r \leq s$ definisali smo pomoću predstavnika (nizova $x$, $y$) iz odgovarajućih klasa. Ovako definisana relacija ne zavisi od izbora predstavnika, tj. relacija $\leq$ je dobro definisana na $R$. Zaista, neka su $x, y, u, v$ Košijevi nizovi i uzmimo da je $r = x/\sim = u/\sim$, $s = y/\sim = v/\sim$. Pretpostavimo da su ispunjeni uslovi definicije, recimo neka postoje $q, q' \in Q$ koji razdvajaju nizove $x$ i $y$ počev od nekog $m$, tj.

$$\forall n > m\ x_n < q < q' < y_n$$

Dokazujemo da su onda i nizovi $u$ i $v$ razdvojeni nekim parom racionalnih brojeva počev od nekog prirodnog broja. Neka je $\varepsilon = (q' - q)/4$ i neka su $p, p' \in Q$ takvi da je $q + \varepsilon < p < p' < q' - \varepsilon$. S obzirom da $u \sim x$ i $v \sim y$, postoje $m_0, m_1 \in N$ tako da je

$$\forall n > m_0 \ |x_n - u_n| < \varepsilon, \qquad \forall n > m_1 \ |y_n - v_n| < \varepsilon.$$

Izaberimo prirodan broj $m' > m, m_0, m_1$. Tada za $n > m'$ važi

$$u_n < x_n + \varepsilon < q + \varepsilon < p < p' < q' - \varepsilon < y_n - \varepsilon < v_n$$

dakle $p, p'$ razdvajaju (tim redom) nizove $u$ i $v$ počev od $m'$.

**3.6.12 Teorema** *Struktura* $\mathbf{R} = (R, +, \cdot, \leq, 0, 1)$ *je uređeno polje.*

**Dokaz** Najpre dokažimo da je $\leq$ linearno uređenje skupa realnih brojeva. Za to je dovoljno videti da je relacija $<$ relacija striktnog linearnog uređenja, odnosno da $<$ zadovoljava ove uslove za proizvoljne realne brojeve $a, b, c$.

(1) $a < b \Rightarrow \neg b < a$.
(2) $a < b \wedge b < c \Rightarrow a < c$, *svojstvo tranzitivnosti relacije* $<$.
(3) $a < b \vee a = b \vee b < a$, *svojstvo linearnosti relacije* $<$.

Neka je $a < b$ i neka je $x$ strogo monotono rastući Košijev niz racionalnih brojeva tako da je $a = x/\!\sim$, i neka je $y$ strogo monotono opadajući niz racionalnih brojeva tako da je $b = y/\!\sim$ (takvi nizovi postoje prema Lemi 3.6.9). S obzirom da je $a < b$, postoje $q, q' \in Q$ tako da je za neki $m$, za sve $n > m$, $x_n < q < q' < y_n$. S obzirom na monotonost ovih nizova, ove nejednakosti važe za proizvoljan $n \in N$. Tada očigledno nema para racionalnih brojeva koji bi razdvajali ove nizove u obrnutom redosledu, dakle $\neg b < a$, odnosno (1) važi.

Pretpostavimo da je $a < b$ i $b < c$, i neka su $a = x/\!\sim$, $b = y/\!\sim$, $c = z/\!\sim$ gde su $x, y, z$ racionalni Košijevi nizovi. Tada neki par racionalnih brojeva $q, q'$ razdvaja $x$ i $y$ tim redom počev od nekog $m_0$, i slično, neki par racionalnih brojeva $p, p'$ razdvaja $y$ i $z$ tim redom počev od nekog $m_1$. Izaberimo $m > m_0, m_1$. Tada na primer par $q, q'$ razdvaja $x$ i $z$ tim redom počev od $m$, dakle važi i (2).

Neka su $a = x/\!\sim$ i $b = y/\!\sim$ različiti realni brojevi. Tada $x \not\sim y$, pa prema Lemi separcije postoje racionalni brojevi koji razdvajaju nizove $x$ i $y$ počev od nekog $m \in N$, odnosno ili $a < b$ ili $b < a$, dakle važi i (3).

Dokažimo sledeće tvrđenje za realne brojeve $a, b$:

(4) $a \leq b \Leftrightarrow$ postoje Košijevi nizovi $x, y$ tako da $a = x/\!\sim$, $b = y/\!\sim$ i $\forall n \ x_n \leq y_n$

Zaista, pretpostavimo najpre $a \leq b$. Neka je $x$ monotono rastući racionalan niz tako da je $a = x/\!\sim$ i neka je $y$ monotono opadajući racionalan niz tako da je $b = y/\!\sim$. Ako je $a = b$, onda očigledno važi $\forall n \ x_n < y_n$. Ako je $a < b$ onda postoje racionalni brojevi $q, q'$ koji razdvajaju nizove $x$ i $y$ počev od nekog m, pa s obzirom na monotonost nizova $x$, $y$ opet važi $\forall n \ x_n \leq y_n$. Ovim je dokazana u (4) implikacija ($\Rightarrow$). Pretpostavimo sada obrnuto, da je za neke racionalne Košijeve nizove $x$, $y$ takve da je $a = x/\!\sim$ i $b = y/\!\sim$ ispunjeno $\forall n \ x_n \leq y_n$. Tada za nizove

$x$ i $y$ razlikujemo dva slučaja. Prvi slučaj je $x \sim y$, tj. $a = b$, dakle i $a \leq b$. Drugi slučaj je $x \not\sim y$. Prema Lemi separacije onda postoje racionalni brojevi $q, q'$ koji razdvajaju nizove $x$ i $y$ počev od nekog $m \in N$. S obzirom na pretpostavljeni uslov $\forall n\ \ x_n \leq y_n$, ne može biti $\forall n > m\, y_n < q < q' < x_n$. Dakle mora biti $\forall n > m\ \ x_n < q < q' < y_n$, što znači da je $a \leq b$. Ovim je dokazan i deo ($\Leftarrow$) tvrđenja (4).

Dokažimo saglasnost uređenja $\leq$ sa operacijama $+$ i $\cdot$ polja realnih brojeva. Najpre ćemo dokazati

$$a \leq b \Rightarrow a + c \leq b + c, \quad a, b, c \in R. \tag{5}$$

Pretpostavimo da je $a \leq b$. Tada prema (4) postoje racionalni Košijevi nizovi $x, y$ tako da je $a = x/\sim$, $b = y/\sim$ i $\forall n\, x_n \leq y_n$. Tada $\forall n\, x_n + z_n \leq y_n + z_n$, te prema (4), $a + c \leq b + c$, pa je ovim tvrđenje (5) dokazano. Dokažimo sada

$$a \leq b \wedge 0 \leq c \Rightarrow ac \leq bc, \quad a, b, c \in R. \tag{6}$$

Pretpostavimo $a \leq b$. Kao u prethodnom slučaju nalazimo racionalne nizove $x, y, z$ tako da je $a = x/\sim$, $b = y/\sim$, $c = z/\sim$ i $\forall n \in N\, (x_n \leq y_n \wedge 0 \leq z_n)$. Tada za bilo koji $n \in N$, $x_n z_n \leq y_n z_n$, pa prema (4) sledi $ac \leq bc$, dakle (5) važi.

Ovim smo proverili sve aksiome uređenog polja u strukturi $\mathbf{R}$. $\Diamond$

Ako je $a \in R$ i $r > 0$, onda kažemo da je $a$ pozitivan broj, inače kažemo da je negativan. Skup svih pozitivnih realnih brojeva obeležavamo sa $R^+$. Apsolutnu vrednost realnog broja $a$ definišemo na sličan način kao kod racionalnih brojeva: $|a| = a$ ako je $a$ pozitivan ili 0, inače $|a| = -a$. Dualna relacija za "$<$" je "$>$", gde $a > b$ ako i samo ako $a < b$. Slično definišemo relaciju $\geq$. Neposredna posledica ovakve definicije uređenja je da je uređeno polje $\mathbf{R}$ arhimedovsko. Naime, važi sledeće tvrđenje.

**3.6.13 Teorema** 1. *Skup racionalnih brojeva je gust u* $\mathbf{R}$.
2. *Uređeno polje* $\mathbf{R}$ *je arhimedovsko, tj.* $\forall x \in R\ \exists n \in N\ \ x < n$.
3. *Ako je* $a \in R^+$ *onda postoji* $n \in N$ *tako da je* $1/n < a$.

**Dokaz** 1. Neka su $a, b \in R$ i $a < b$. Za $a = x/\sim$, $b = y/\sim$ prema Lemi separacije, odnosno (4) u prethodnoj teoremi, postoje racionalni brojevi $q, q'$ tako da je za sve $n \in N$, $x_n < q < q' < y_n$. Neka je $r$ racionalan broj takav da je $q < r < q'$. Tada prema definiciji uređenja $<$ sledi $a < r < b$.
2. Neka je $a \in R$. Prema prethodnom postoji racionalan broj $q$ takav da je $a < q < a + 1$. Ako je $n \in N$ tako da je $q \leq n$, onda $a < n$.
3. Neka je $a \in R^+$ i $1/a < n$. Tada $1/n < a$. $\Diamond$

Arhimedovsko svojstvo realnih brojeva omogućava nam da uvedemo ceo deo od $x$, tj. funkciju $y = [x]$, na isti način kao kod racionalnih brojeva. Dakle, $[x]$ biće najveći ceo broj $\leq x$. Kao i kod racionalnih brojeva, v. Odeljak 3.4, neka je $R(x) = x - [x]$

Ako je $(X, \leq)$ uređen skup i $S \subseteq X$ je neprazan, tada je *supremum* skupa $S$ najmanja gornja granica skupa $S$. Infimum skupa $S$ biće najveća donja granica skupa $S$. Supremum skupa $S$ obeležavamo pomoću $\sup S$, dok infimum obeležavamo pomoću $\inf S$. Primetimo da nema svaki skup supremum (niti infimum). Na primer, ne postoji supremum prirodnih brojeva u $(R, \leq)$, niti supremum skupa $\{q \in Q^+ | \, q^2 < 2\}$ u $(Q, \leq)$. Fundamentalno svojstvo realnih brojeva je da je R uređen kontinuum. Naime, **R** ima sledeće svojstvo neprekidnosti.

**3.6.14** ***Teorema supremuma za* R** *Svaki neprazan odozgo ograničen skup $S \subseteq R$ ima supremum.*

**Dokaz** Neka je $S \subseteq R$ neprazan i neka je $M \in Q$ jedna njegova gornja granica. Neka je $X$ skup svih vrednosti (strogo) monotono rastućih nizova čije klase kongruencije pripadaju $S$, tj.

$$X = \{x_n | \, x/\!\sim\, \in S, x \text{ je monotono rastući}, n \in N\}.$$

S obzirom da je $M$ gornja granica za $S$, prema Lemi separacije za $x/\!\sim\,\in S$ postoji $m \in N$ tako da za $n > m$, $x_n \leq M$. Ako je $x$ monotono rastući onda je za sve $n \in N$, $x_n < M$. Dakle,

(1) $M$ je gornja granica skupa $X$.

Skup $X$ nema najveći element, jer ako je $x_n \in X$ za neki rastući $x$, neki $n \in N$, onda $x_n < x_{n+1}$ i $x_{n+1} \in X$. Primetimo da je $X \subseteq Q$, dakle $X$ je *prebrojiv* skup, pa sve članove skupa $X$ možemo poređati u niz, tj. možemo uzeti da je $X = \{q_0, q_1, q_2, \dots\}$. Induktivno konstruišemo niz $w_n$ kofinalan u $X$: Neka je $w_0 = q_0$, i pretpostavimo da su članovi $w_0, w_1, \dots, w_{n-1}$, $n > 0$ konstruisani. S obzirom da $X$ nema najvećeg elementa, postoji $a \in X$ takav da je $a > w_0, w_1, \dots, w_{n-1}$, i $a > q_n$. Neka je $w_n = a$. Prema konstrukciji za niz $w = \langle w_n | \, n \in N\rangle$ važi:

(2) Niz $w$ je kofinalan u $X$ jer $\forall n \in N \, q_n < w_n$.
(3) Niz $w$ je monotono rastući.
(4) $\forall n \in N \, w_n \leq M$.

Takođe

(5) Niz $w$ je Košijev.

Pretpostavimo suprotno. Tada postoji $d \in Q^+$ tako da za svaki $m \in N$ postoji $n > m$ tako da je $|x_n - x_m| \geq d$, odnosno s obzirom na monotonost niza $w$, $x_n - x_m \geq d$. Dakle, postoji podniz $v_i = w_{n_i}$ tako da je $v_{i+1} - v_i \geq d$, odakle sledi $v_k \geq v_0 + kd$, pa s obzirom na arhimedovsko svojstvo uređenja realnih brojeva, za neki $m$ važi $v_m > M$, dakle $w_{n_m} > M$, suprotno (4). Dakle (5) važi. Dalje,

(6) $b = w/\!\sim$ je supremum skupa $S$.

Neka je $s \in S$ bilo koji element. Prema Lemi 3.6.9 postoji monotono rastući niz $x$ tako da je $s = x/\!\sim$. Tada prema definiciji skupa $X$, za svaki $n \in N$, $x_n \in X$. Dakle $\{x_n | \, n \in N\} \subseteq X$, pa s obzirom da je $w$ kofinalan u $X$, to je $w$ kofinalan i u $\{x_n | \, n \in N\}$. Prema tome za svaki $m$ postoji $n \geq m$ tako da je $x_m \leq w_n$, pa postoji podniz $u_i = w_{n_i}$ niza $w$ tako da je za sve $i$, $x_i \leq u_i$. Kao podniz Košijevog niza, $u$ je Košijev i $u \sim w$, pa $s \leq u/\!\sim\; = w/\!\sim\; = b$, tj. $b$ je gornja granica skupa $S$.

Dalje, pretpostavimo da je $c \in R$ bilo koja gornja granica skupa $S$. Prema Lemi 3.6.9 postoji monotono opadajući niz $y$ tako da je $c = y/\!\sim$. Tada za sve $q \in X$ važi $q \leq y_n$ za sve $n$, prema tome za sve $n$, $w_n \leq y_n$, pa (v. Teoremu 3.6.12(4)), sledi $w/\!\sim\; \leq y/\!\sim$, tj. $b \leq c$, što znači da je $b$ najmanja gornja granica skupa $S$. Ovim je dokazano svojstvo (6), a time i teorema. $\diamondsuit$

Prema dokazu prethodne teoreme, imamo sledeće tvrđenje.

**3.6.15 Posledica** Neka je $S$ odozgo ograničen podskup realnih brojeva i neka je $x$ kofinalan niz racionalnih brojeva u $S$. Tada $x/\!\sim\; = \sup S$.

**3.6.16 Primer** 1. Neka je $x_n$ ograničen i monotono rastući niz racionalnih brojeva. Tada je skup $S = \{x_n | \, n \in N\}$ ograničen, dok je niz $x$ kofinalan u njemu, dakle $x/\!\sim\; = \sup S$. Za $\sup S$ koristimo i oznaku $\sup_n x_n$.

**3.6.17 Posledica** Svaki neprazan odozdo ograničen skup $S$ ima infimum.

**Dokaz** $\inf S = -\sup\{-x | \, x \in S\}$. $\diamondsuit$

**3.6.18 Lema** *Neka je $a$ realan broj i neka je $S_a = \{q \in Q | \, q < a\}$. Tada $a = \sup S_a$.*

**Dokaz** Broj $a$ je gornja granica skupa $S_a$, pa prema Teoremi supremuma $S_a$ ima supremum, neka je to $s$. Kako za svaki $q \in S_a$ važi $q < a$, to je $s \leq a$. Pretpostavimo da je $s < a$. S obzirom da je $Q$ gust u $R$, postoji $q \in Q$ tako da je $s < q < a$, dakle $q \in S_a$. Prema definiciji supremuma onda mora biti $q \leq s$, suprotno pretpostavci $s < q$. Otuda $a = s$. $\diamondsuit$

Možemo postaviti pitanje da li ima realnih brojeva koji nisu racionalni. Odgovor nam daje teorema o kardinalnom broju skupa realnih brojeva. U dokazu te teoreme koristićemo Kantor-Bernštajnovu teoremu iz elementarne teorije skupova.

**3.6.19 Teorema** *Neka su $X$ i $Y$ proizvoljni skupovi, i neka su $f : X \underset{1\text{-}1}{\longrightarrow} Y$ i $g : Y \underset{1\text{-}1}{\longrightarrow} X$. Tada su skupovi $X$ i $Y$ iste kardinalnosti, tj. postoji $h : X \xrightarrow[1\text{-}1]{\text{na}} Y$.*

Osim ove teoreme koristićemo i druge činjenice iz elementarne teorije skupova. Na primer da je $|N| < |\mathbf{P}(N)|$, tj. da se ne mogu poređati u niz svi podskupovi skupa prirodnih brojeva, (ako $h : N \to \mathbf{P}(N)$, onda za $X = \{n \in N | \, n \notin h(n)\}$ ne postoji $m \in N$ tako da je $X = h(m)$, tj. $h$ ne može biti *na*), ili $|2^N| = |\mathbf{P}(N)|$ (bijekcija između skupova $2^N$ i $\mathbf{P}(N)$ je, na primer, preslikavanje koje svakom podskupu skupa $N$ pridružuje njegovu karakterističnu funkciju).

**3.6.20 Teorema** *Realnih brojeva ima neprebrojivo mnogo, tačnije, $|R| = 2^{\aleph_0}$.*

**Dokaz** Neka je $2^N$ skup svih binarnih nizova. Preslikavanje $h : 2^N \to R$ definišemo na sledeći način. Primetimo najpre da je za $\alpha \in 2^N$, $\alpha = \langle \alpha_i \, | \, i \in N \rangle$,

$$\text{(1)} \qquad \sum_{i=0}^{n} \frac{\alpha_i}{3^{i+1}} \leq \frac{1}{3} \cdot \frac{1 - 1/3^{n+1}}{1 - 1/3} < \frac{1}{2}$$

Dakle, skup $X_\alpha = \{\sum_{i=0}^{n} \alpha_i/3^{i+1} | \, n \in N\}$ ima gornju granicu $1/2$, pa prema Teoremi supremuma ovaj skup ima supremum. Definišemo $h(\alpha) = \sup X_\alpha$. Dokažimo da je $h$ 1–1 preslikavanje. Neka su $\alpha, \beta \in 2^N$ i pretpostavimo da je $\alpha \neq \beta$. Tada za neki $m \in N$ važi $\alpha_m \neq \beta_m$, recimo $\alpha_m > \beta_m$, tj. $\alpha_m = 1$ i $\beta_m = 0$, i za $i < m$, $\alpha_i = \beta_i$. Otuda za proizvoljan $k \in N^+$ i $n = m + k$, nalazimo kao u (1)

$$\sum_{i=0}^{n} \frac{\alpha_i - \beta_i}{3^{i+1}} \geq \frac{1}{3^m} - (\frac{1}{3^{m+1}} + \frac{1}{3^{m+2}} + \ldots + \frac{1}{3^n}) =$$

$$\frac{1}{3^m} - \frac{1}{3^m}(\frac{1}{3} + \frac{1}{3^2} + \ldots + \frac{1}{3^k}) \geq \frac{1}{3^m} - \frac{1}{3^m} \cdot \frac{1}{2} = \frac{1}{2} \cdot \frac{1}{3^m}$$

Odavde sledi $\sum_{i=0}^{n} \alpha_i/3^{i+1} \geq \dfrac{1}{2} \cdot \dfrac{1}{3^m} + \sum\limits_{i=0}^{n} \beta_i/3^{i+1}$, odakle je $h(\alpha) \geq \dfrac{1}{2} \cdot \dfrac{1}{3^m} + h(\beta)$. Prema tome, $h\alpha > h\beta$, tj. $h\alpha \neq h\beta$, čime je dokazano da je $h$ 1-1 preslikavanje. S obzirom da je $|2^N| = 2^{\aleph_0}$, sledi

$$|R| \geq 2^{\aleph_0}. \tag{2}$$

S druge strane, ako je $a \in R$, neka je $S_a = \{q \in Q | \, q < a\}$. Ovim je definisano preslikavanje $g : R \to \mathbf{P}(Q)$, gde je $\mathbf{P}(Q)$ skup svih podskupova skupa $Q$. Prema Lemi 3.6.18, preslikavanje $g$ je 1–1, jer ako $S_a = S_b$, $a, b \in R$, onda $a = \sup S_a = \sup S_b = b$. S obzirom da je $Q$ prebrojiv skup, sledi $|\mathbf{P}(Q)| = 2^{\aleph_0}$; prema tome $|R| \leq 2^{\aleph_0}$. Odavde i prema Kantor–Bernštajnovoj teoremi sledi $|R| = 2^{\aleph_0}$ ♢

Imajući u vidu prethodnu teoremu, za skupove koji imaju kardinalni broj $2^{\aleph_0}$ kažemo takođe da imaju moć kontinuuma. Zanimljivo je da je dugo ostala otvorena hipoteza da ne postoji beskonačan podskup $S$ realnih brojeva takav da je $\aleph_0 < |S| < 2^{\aleph_0}$. Drugim rečima, da je svaki podskup realnih brojeva ili konačan ili prebrojiv ili moći kontinuuma. Ta hipoteza poznata je kao Kontinuum hipoteza. Ovu hipotezu postavio je G. Kantor, dok je D. Hilbert pitanje istinitosti ove hipoteze uvrstio kao prvi na listi problema na pomenutom svetskom kongresu matematičara u Parizu 1900. godine. Delimičan odgovor dao je tek K. Gedel krajem tridesetih godina tako što je dokazao da ta hipoteza ne protivreči aksiomama teorije ZFC. Potpun odgovor dao je P. Koen (Paul Cohen) 1963. godine dokazavši da niti negacija Kontinuum hipoteze ne protivreči teoriji ZFC, što znači da Kontinuum hipoteza ne zavisi od aksioma teorije ZFC. Drugim rečima, njen status u okviru ove teorije analogan je statusu petog Euklidovog postulata u odnosu na ostale aksiome Euklidske geometrije, ili statusu aksiome izbora u okviru teorije ZF. Važnost ove hipoteze leži u činjenici da se istinitost nekih značajnih tvrđenja iz matematike, pre svega iz analize, topologije i algebre, svodi na pitanje istinitosti Kontinuum hipoteze.

S obzirom da je $R$ neprebrojiv i $Q$ prebrojiv, to je skup $R - Q$ neprazan. Unija dva prebrojiva skupa je prebrojiv skup, pa kako je $R = Q \cup (R - Q)$, sledi da je skup $R - Q$ takođe neprebrojiv. Elemente skupa $R - Q$ nazivamo *iracionalnim brojevima* i shodno prethodnom, iracionalnih brojeva ima više nego racionalnih (neprebrojivo mnogo, a nije teško videti da ih zapravo ima kontinuum mnogo).

**3.6.21 Primer** Ovde ćemo razmotriti funkciju korenovanja realnih brojeva. Naime, dokazaćemo da za svaki pozitivan realan broj $a$ i svaki prirodan broj $m \geq 2$ postoji jedinstven pozitivan realan broj $b$ tako da je $b^m = a$. Tu jedinstvenu vrednost $b$ označićemo sa $a^{\frac{1}{m}}$ ili $\sqrt[m]{a}$.

Neka je $0 < a < 1$ i $u$ racionalan monotono rastući niz tako da je $a = u/\!\sim$ i $0 < u_0$. S obzirom na Lemu 3.6.9, nije teško videti da takav niz $u$ postoji. Niz racionalnih brojeva $x = \langle x_n | \, n \in N \rangle$ definišemo pomoću rekurentne formule

$$x_{n+1} = 1 - (1 - u_n)\frac{1 - x_n}{1 - x_n^m}, \qquad x_0 = 0 \tag{1}$$

Tada

$$\text{Za svaki } n \in N^+ \text{ važi} \qquad 0 < x_n < 1. \tag{2}$$

Dokaz tvrđenja (1) izvodimo indukcijom. Za $n = 0$ tvrđenje očigledno važi, pa prelazimo na dokaz induktivnog koraka. Po induktivnoj hipotezi $0 < x_n < 1$, dakle $0 < x_n^m < 1$. S obzirom da je $1 - x_{n+1} = (1 - u_n)(1 - x_n)/(1 - x_n^m)$, sledi $0 < x_{n+1} < 1$, čime je svojstvo (2) dokazano.

Dokažimo indukcijom da je niz $x_n$ monotono rastući. Očigledno $x_0 < x_1$, pa pretpostavimo $n > 0$ i induktivnu hipotezu $x_{n-1} < x_n$. Tada

$$x_{n+1} - x_n = \frac{1 - u_{n-1}}{1 + x_n + \ldots + x_{n-1}^m} - \frac{1 - u_n}{1 + x_n + \ldots + x_n^m}, \tag{3}$$

odakle, s obzirom na induktivnu hipotezu i $u_{n-1} < u_n$, odmah nalazimo $x_{n+1} - x_n > 0$, tj. $x_{n+1} > x_n$, čime smo dokazali da je niz monotono rastući. S obzirom da je niz $x$ ograničen i monotono rastući niz racionalnih brojeva, on je Košijev i postoji $\sup_n x_n$. Označimo taj supremum sa $b$; tada $b = x/\!\sim$, v. Primer 3.6.16. Dalje, neka je $y = \langle x_{n+1} | \, n \in N \rangle$. Tada je $y$ podniz niza $x$, dakle $y \sim x$ i $b = y/\!\sim$. Iz jednakosti (1) onda nalazimo

$$y_n(1 + x_n + \ldots + x_n^{m-1}) = u_n + x_n + x_n^2 + \ldots + x_n^{m-1},$$

odakle je

$$y_n/\!\sim (1 + x_n/\!\sim + \ldots + x_n^{m-1}/\!\sim) = u_n/\!\sim + x_n/\!\sim + x_n^2/\!\sim + \ldots + x_n^{m-1}/\!\sim,$$

odnosno

$$b(1 + b + \ldots + b^{m-1}) = a + b + b^2 + \ldots + b^{m-1}.$$

Odave neposredno sledi $b^m = a$. Primetimo da je $0 < b$ s obzirom da je za sve $n \in N$, $x_n > 0$. Pretpostavimo da je $c^m = a$ i $c > 0$. Tada $b^m = c^m$, odakle sledi $(b/c)^m = 1$. S obzirom na identitet $1 - t^m = (1 - t)(1 + t + t^2 + \ldots t^{m-1})$ i $1 + t + t^2 + \ldots t^{m-1} > 0$ za $t = b/c$, sledi $b/c = 1$. Dakle, postoji tačno jedan realan broj $b$ takav da je $b^m = a$, i prema tome preslikavanje $x \mapsto \sqrt[m]{x}$, $x \in [0, 1]_R$ je dobro definisano. Ako je $a > 1$, tada definišemo $\sqrt[m]{a} = 1/\sqrt[m]{1/a}$, i na taj način smo definisali $x \mapsto \sqrt[m]{x}$, $x \in R^+$. Nije teško proveriti da ovo preslikavanje zadovoljava uobičajena svojstva korenske fukcije, kao na primer

$$\sqrt[m]{xy} = \sqrt[m]{x}\,\sqrt[m]{y}, \qquad \sqrt[mn]{x} = \sqrt[n]{\sqrt[m]{x}}, \qquad m, n \in N^+, \quad x, y \in R^+. \tag{4}$$

Primetimo da rekurentna formula (1) daje efikasan algoritam za određivanje $\sqrt[m]{a}$ za $a > 0$. Najzad, ako je $a \in Q$, možemo uzeti $x_{n+1} = 1 - (1-a)(1-x_n)/(1-x_n^m)$ u (1).

Evo najzad i "konkretnog" primera iracionalnog broja, koji je bio poznat još starogrčkim matematičarima. Dokazaćemo da je $a = \sqrt{2}$ iracionalan broj. Pretpostavimo suprotno. Neka su $m, n \in N$ uzajamno prosti takvi da je $a = m/n$. Tada $n^2 = 2m^2$, odakle sledi da je $n$ paran, pa neka je $n = 2k$. Otuda $2k^2 = m^2$, što znači da je i $m$ paran, dakle $m$ i $n$ nisu uzajamno prosti, suprotno pretpostavci. Prema tome $a$ nije racionalan broj.

**3.6.22 Primer** Neka je $c$ iracionalan broj. Tada je $Z + cZ = \{x + yc \mid x, y \in Z\}$ gust u $R$.

**Dokaz** Možemo uzeti da je $c > 0$. Neka je $f : N \to [0,1)$ preslikavanje definisano pomoću $f(x) = R(cx) = cx - [cx]$, $x \in N$. Preslikavanje $f$ je $1-1$. Zaista, ako je $f(m) = f(n)$, $m, n \in N$, onda $(m-n)c = [cn] - [cm]$. Ako je $m \neq n$ onda $c = (m-n)/([cn]-[cm])$, što bi značilo da je $c$ racionalan broj, suprotno pretpostavci. Dakle $m = n$, odnosno $f$ jeste $1-1$.

Dalje, neka je $n \in N^+$ i neka je preslikavanje $g : N \to \{0, 1, 2, \ldots, n\}$ definisano na sledeći način: $g(x) =$ najmanji $i \in N$ tako da je $f(x) \in [i/(n+1), (i+1)/(n+1)]$. S obzirom da je $g$ preslikavanje beskonačnog skupa u konačan, postoje različiti $x, y \in N$ tako da je $g(x) = g(y)$, odakle sledi $|f(x) - f(y)| \leq 1/(n+1) < 1/n$. Neka je $d = u + vc$, gde $u = [yc] - [xc]$ i $v = x - y$. Možemo pretpostaviti da je $d > 0$, inače biramo $d = -u - vc$. Prema tome važi

1. Za svaki $n \in N^+$ postoji $d \in Z + cZ$ tako da je $0 < d < 1/n$.

Neka su $x, y \in R$, $0 < x < y$. S obzirom da je $\mathbf{R}$ arhimedovski uređeno polje, postoji $n \in N$ tako da je $0 < 1/n < y - x$. Prema 1. postoji $d \in Z + cZ$ tako da je $0 < d < 1/n$. Neka je $m$ najveći prirodan broj takav da je $md < x$. Tada $x < md + d < x + 1/n < y$. Onda za $a = md + d$ važi $x < a < y$ i $a \in Z + cZ$. Na sličan način se raspravljaju slučajevi $x < 0 < y$ i $x < y < 0$, čime je tvrđenje dokazano.

Jedna posledica prethodnog tvrđenja je da za preslikavanje $f : Z \to [0,1)$, gde $f(x) = R(cx), x \in Z$, važi: $f(Z)$ je gust u $[0,1]$. Zaista, pretpostavimo $0 < x < y < 1$. Prema prethodnom postoje $m, n \in Z$ tako da je $x < m + nc < y$, tj. $0 < x < m + [nc] + f(n) < y < 1$. Kako je $m + [nc]$ ceo broj i $0 \leq f(x) < 1$, na osnovu ove nejednakosti sledi $m + [nc] = 0$, dakle $x < f(n) < y$.

U poglavlju iz teorije polja koristićemo sledeća svojstva realnih polinoma. Podsećamo čitaoca da su realni polinomi zapravo termi jezika $\{+, \cdot\} \cup \{\underline{a} \mid a \in R\}$ oblika $\underline{a}_0 + \underline{a}_1 x + \ldots + \underline{a}_n x^n$, $n \in N$. Neka je $p(x)$ realan polinom. Polinomna funkcija pridružena polinomu $p(x)$ je preslikavanje $p_R : R \to R$ koje svakom realnom broju $r$ dodeljuje vrednost polinoma $p$ u $\mathbf{R}$ za vrednost promenljive $x = r$. Drugim rečima, $p_R(r) = p^{\mathbf{R}}[r]$, u smislu kako smo definisali vrednost terma u prvom poglavlju. Često ćemo koristiti istu oznaku za polinom i pridruženu polinomnu funkciju. Takav dogovor u notaciji opravdava sledeće tvrđenje. Naime, za realne polinome važi:

**3.6.23 Teorema** 1. *Realne polinomne funkcije su neprekidne funkcije svojih argumenata.*
2. *Svaki realan polinom neparnog stepena ima bar jedan realan koren.*

3. *Ako su $p(x)$ i $q(x)$ realni polinomi koji imaju jednake pridružene polinomne funkcije, onda su oni identični polinomi.*

**Dokaz** Tvrđenja (1) i (2) obično se dokazuju u okviru predmeta matematičke analize, pa te dokaze izostavljamo. Što se tiče tvrđenja (3), dovoljno je dokazati: ako je $p_R$ nula funkcija, onda je $p(x)$ nula polinom. Zaista, pretpostavimo da je $p(x) = \sum_{i=0}^{n} \underline{a}_i x^i$ i neka je $p_R(r) = 0$ za svaki $r \in R$. Razmotrimo sledeći sistem homogenih linearnih jednačina po nepoznatim $a_0, a_1, \ldots, a_n$:

$$\text{(S)} \qquad \begin{aligned} a_0 + a_1 + a_2 + \ldots + a_n &= 0 \\ a_0 + a_1 \cdot 2 + 2^2 + \ldots + a_n \cdot 2^n &= 0 \\ &\ldots \\ a_0 + a_1 \cdot (n+1) + (n+1)^2 + \ldots + a_n \cdot (n+1)^n &= 0 \end{aligned}$$

Determinanta sistema $S$ je Vandermondova determinanta

$$W(1, 2, \ldots, n+1) = \prod_{i<j\leq n+1} (j-i).$$

Dakle, determinanta sistema $S$ je različita od nule; prema tome sistem $S$ ima jedino trivijalno rešenje, što znači da je $p(x)$ nula polinom. $\diamondsuit$

Primetimo da uz malu adapatciju prethodnog dokaza dobijamo jače tvrđenje: ako su $p(x)$ i $q(x)$ realni polinomi stepena najviše $n$, i ako ti polinomi imaju $n+1$ istu vrednost (za odgovarajuće argumente), onda su oni identični. Drugim rečima, svaki realan polinom stepena $n$ u potpunosti je određen sa nekih svojih $n+1$ vrednosti.

Svojstvo neprekidnosti, odnosno Teorema supremuma jedinstveno određuje polje realnih brojeva. Naime, svako uređeno polje koje zadovoljava Teoremu supremuma (koju onda u tom kontekstu nazivamo Aksiomom supremuma) izomorfno je uređenom polju realnih brojeva. Neka je $\mathbf{F} = (F, +, \cdot, \leq, 0_F, 1_F)$ uređeno polje. Primetimo da $\mathbf{F}$ sadrži izomorfnu kopiju uređenog polja racionalnih brojeva. S obzirom da je $0_F < 1_F$, sledi da za svaki $n \in N$ važi $0_F < n \cdot 1_F$, dakle $\mathbf{F}$ je polje karakteristike 0; u $\mathbf{F}$ se utapa prsten celih brojeva, i prema Teoremi 3.3.7 onda se i $\mathbf{Q}$ utapa u $\mathbf{F}$. Stoga ćemo u izlaganju što sledi podrazumevati da svako uređeno polje sadrži kao potpolje polje racionalnih brojeva.

**3.6.24 Teorema** *Neka je $\mathbf{F} = (F, +, \cdot, \leq, 0, 1)$ uređeno polje koje zadovoljava Aksiomu supremuma: Svaki neprazan odozgo ograničen podskup u $F$ ima supremum. Tada $\mathbf{R} \cong \mathbf{F}$.*

**Dokaz** Najpre dokažimo

(1) $\mathbf{F}$ je arhimedovsko polje.

Pretpostavimo da je $N$ nije kofinalan u $\mathbf{F}$. Tada je $N$ ograničen odozgo skup u $\mathbf{F}$, te prema Aksiomi supremuma postoji $\sup N$; neka je to $m$. Tada postoji $n \in N$ tako da je $m - 1 < n$. Dakle $m < n + 1$, što je kontradikcija prema izboru za $m$, čime je tvrđenje (1) dokazano.

Posledica tvrđenja (1) je

(2) Skup racionalnih brojeva je gust u **F**.

Zaista, neka je $r \in F$, $r > 0$. Tada postoji $n \in N$ tako da je $1/r < n$, odakle sledi $1/n < r$. Neka su $x, y \in F$ bilo koji tako da je $0 < x < y$. Prema prethodnom postoji prirodan broj $n$ tako da je $0 < 1/n < y - x$. S obzirom da je za neki $k \in N$ $x < k \cdot 1/n$, postoji najmanji $m \in N$ tako da je $x < m/n$. Tada takođe i $m/n < y$. Slično se pokazuje i za slučajeve $x < 0 < y$, $x < y < 0$ da postoji racionalan broj između $x$ i $y$, i time je dokazano i tvrđenje (2).

Neka je za $a \in F$, $S_a = \{q \in Q | \, q < a\}$. Isto kao u Lemi 3.6.18 dokazuje se da u **F** važi:

(3) $a = \sup^F S_a$.

Da bismo razlikovali operacije polja $F$ od operacija nad realnim brojevima, označimo operacije sabiranja i množenja u **F** redom sa $+_F$ i $\cdot_F$, nejednakost u **F** sa $\leq_F$, i supremum nekog skupa $X$ u $F$ sa $\sup^F X$. Uz ove oznake i pretpostavku $Q \subseteq R$, primetimo da je za $a, b \in Q$, $a \leq_F b$ ako i samo ako $a \leq b$. Preslikavanje $h : R \to F$ definišemo na sledeći način: ako je $r \in R$, neka je $x$ monotono rastući racionalan niz tako da je $r = x/\sim$. Tada $h(r) = \sup^F_n x_n$. Primetimo odmah da je za $q \in Q$, $h(q) = q$. Pokažimo najpre da je $h$ dobro definisano preslikavanje. Neka je $y$ bilo koji drugi monotono rastući niz takav da $r = y/\sim$. S obzirom da

$$\forall m \exists n > m \;\; x_m < y_n, \qquad \text{i} \qquad \forall m \exists n > m \;\; y_m < x_n,$$

sledi $\sup^F_n x_n = \sup^F_n y_n$, tj. $h$ je dobro definisano.

Dokažimo da je $h$ $1-1$ preslikavanje. Neka su $a, b \in R$ različiti realni brojevi, recimo $a < b$. Neka su prema Lemi separacije $q, q' \in Q$ takvi da je $a < q < q' < b$. Neka su $x, y$ monotono opadajući racionalni nizovi takvi da je $a = x/\sim$ i $b = y/\sim$. S obzirom da je za neki $m$ za sve $n > m$, $q' < y_n$, sledi $\sup^F_n x_n \leq_F q <_F q' \leq_F \sup^F_n y_n$, tj. $h(a) < h(b)$, dakle $h(a) \neq h(b)$. Ovaj dokaz istovremeno pokazuje da je $h$ monotono preslikavanje.

Dokažimo da je $h$ preslikavanje *na*. Neka je $b \in F$ i neka je $r = \sup S_b$. Ako je $x$ monotono racionalan ratući niz tako da je $r = x/\sim$, onda je $x$ kofinalan u $S_b$; dakle, prema (3), $b = \sup^F S_b = \sup^F_n x_n = h(r)$.

Dokažimo, najzad, da je $h$ homomorfizam, odnosno da je saglasno sa operacijama polja. Neka su $a, b \in R$ i $c = a + b$. Neka su $x, y$ monotono rastući racionalni nizovi takvi da je $a = x/\sim$, $b = y/\sim$. S obzirom da je $c = a + b = x/\sim + y/\sim = (x + y)/\sim$, to je $h(a + b) = h(c) = \sup^F_n(x_n + y_n)$. S obzirom da je $x_n = h(x_n) \leq_F h(a)$, sledi $x_n \leq_F h(a)$ i slično $y_n \leq_F h(b)$, prema tome $x_n +_F y_n \leq_F h(a) +_F h(b)$, odnosno $h(c) \leq_F h(a) +_F h(b)$. Neka je $\varepsilon \in Q^+$. Tada postoje $m_0, m_1 \in N$ tako da je za $n > m_0$, $a - \varepsilon/2 < x_n$ i za $n > m_1$, $b - \varepsilon/2 < y_n$. Izaberimo $m > m_0, m_1$. Tada, s obzirom da su $x_n + \varepsilon/2$ i $y_n + \varepsilon/2$ racionalni brojevi, za $n > m$ važi $h(a) < x_n +_F \varepsilon/2$ i $h(b) < y_n +_F \varepsilon/2$, tj. $h(a) +_F h(b) <_F x_n +_F y_n +_F \varepsilon <_F c +_F \varepsilon$. Dakle, za svaki $\varepsilon \in Q^+$, imamo $h(a) +_F h(b) <_F h(c) +_F \varepsilon$. S obzirom da je $Q$ gust u **F** sledi $h(a) +_F h(b) \leq_F c$, što zajedno sa prethodno dokazanom nejednakošću $h(c) = \leq_F h(a) +_F h(b)$ daje $h(c) = h(a) +_F h(b)$, odnosno preslikavanje $h$ je saglasno sa operacijama sabiranja polja **R** i **F**. Na sličan način se dokazuje da je $h$ saglasno i sa operacijama množenja ovih polja. Dakle $h : \mathbf{R} \to \mathbf{F}$ je homomorfizam. $\diamondsuit$

Ovom teoremom završavamo zasnivanje realnih brojeva prema Kantorovoj teoriji. Naravno, mnoga pitanja u vezi izgradnje strukture realnih brojeva ovde nismo raspravljali, kao na primer teoriju decimalnog razvoja realnog broja, topološke osobine realnog kontinuuma, ili izgradnju elementarnih funkcija. Tradicionalno se te oblasti izučavaju u okviru predmeta realna analiza, pa zainteresovanog čitaoca upućujemo na bogatu literaturu iz te oblasti.

## 3.7 Kompleksni brojevi

Izgradnja polja kompleksnih brojeva dosta je jednostavnija nego što je to slučaj sa realnim brojevima. Razlog za to leži u činjenici da se polje kompleksnih brojeva izgrađuje konačnom konstrukcijom polazeći od realnih brojeva, za razliku od konstrukcije polja realnih brojeva zasnovanoj na racionalnim brojevima. Najzad, konstrukcijom polja kompleksnih brojeva završava se izgradnja fundamentalnih brojevnih domena zatvorenih za osnovne aritmetičke i algebarske operacije: sabiranje, množenje, određivanje inverznog elementa i korenovanje. U ovom odeljku **R** označava polje realnih brojeva.

**3.7.1 Definicija** *Struktura kompleksnih brojeva je algebra*

$$\mathbf{C} = (C, +_C, \cdot_C, \mathbf{0}, \mathbf{1}), \qquad \mathbf{0} = (0,0), \; \mathbf{1} = (1,0),$$

*gde je domen $C = R^2$, dok su operacije $+_C$ i $\cdot_C$ definisane na sledeći način:*

$$(x_1, y_1) +_C (x_2, y_2) = (x_1 + y_1, x_2 + y_2), \qquad x_1, y_1, x_2, x_2, y_2 \in R$$
$$(x_1, y_1) \cdot_C (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

*Elemente skupa $C$ nazivamo kompleksnim brojevima.*

Sledeća teorema opisuje fundamentalna svojstva algebre kompleksnih brojeva.

**3.7.2 Teorema** 1. *Algebra* **C** *je polje.*
2. *Preslikavanje $\sigma : R \to C$ definisano pomoću $\sigma : r \mapsto (r, 0)$, $r \in R$, je utapanje polja* **R** *u polje* **C**.

**Dokaz** Do sada smo imali nekoliko sličnih dokaza, na primer kod izgradnje prstena celih brojeva, pa izostavljamo dokaz ove teoreme. Ipak spomenimo, ako je $z \in C$, $z = (x, y)$, i $z \neq (0,0)$, onda $z^{-1_C} = (x/(x^2+y^2), -y/(x^2+y^2))$. $\diamondsuit$

Prema prethodnoj teoremi $R' = \{(x,0) \mid x \in R\}$ je potpolje polja **C**, izomorfno polju realnih brojeva. Otuda možemo identifikovati realne brojeve sa $R'$, odnosno možemo pisati $x$ umesto $(x, 0)$. Uvedimo *imaginarnu jedinicu* $\imath = (0,1)$. Primetimo da je $(y,0)(0,1) = (0,y)$, pa s obzirom na jednakost $(x,y) = (x,0) +_C (0,y)$, uz ovu identifikaciju realnih brojeva, nalazimo da je $(x,y) = x +_C \imath \cdot_C y$. Uobičajeno se ispušta donji indeks $_C$ u oznakama algebarskih operacija polja $C$, tako da dolazimo do standardne reprezentacije kompleksnih brojeva: $C = \{x + \imath y \mid x, y \in R\}$.

ispušta donji indeks $_C$ u oznakama algebarskih operacija polja $C$, tako da dolazimo do standardne reprezentacije kompleksnih brojeva: $C = \{x + \imath y |\, x, y \in R\}$.

Kako je $\imath^2 = (0,1)\cdot(0,1) = (-1,0) = -1$, imamo osnovni identitet $\imath^2 = -1$. Drugim rečima, algebarska jednačina $x^2 = -1$ ima rešenje u polju kompleksnih brojeva. Uz tako uvedene oznake, operacije sa kompleksnim brojevima izgledaju ovako:

$$(x_1 + \imath y_1) + (x_2 + \imath y_2) = (x_1 + x_2) + \imath(y_1 + y_2)$$
$$(x_1 + \imath y_1)\cdot(x_2 + \imath y_2) = (x_1x_2 - y_1y_2) + \imath(x_1y_2 + x_2y_1)$$
$$\frac{1}{x+\imath y} = \frac{x}{x^2+y^2} + \imath\cdot\frac{-y}{x^2+y^2}, \qquad \text{ako } x^2 + y^2 \neq 0$$

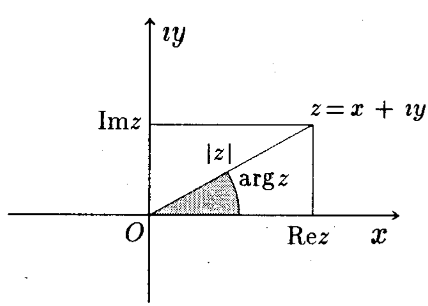
Neka je $z = x + \imath y$ kompleksan broj. Tada se $x$ naziva *realnim delom* i obeležava se pomoću $\mathrm{Re}(z)$, dok se $y$ naziva *imaginarnim delom* kompleksnog broja $z$ i obeležava se sa $\mathrm{Im}(z)$. Dakle, $z = \mathrm{Re}z + \imath \mathrm{Im}z$. Konjugacija je preslikavanje skupa $C$ u $C$ definisano pomoću $\bar{z} = x - \imath y$. Apsolutna vrednost kompleksnog broja uvodi se pomoću $|z| = \sqrt{x^2+y^2}$. Primetimo da je apsolutna vrednost kompleksnog broja realan broj. Sledeća teorema opisuje osnovna svojstva uvedenih pojmova.

**3.7.3 Teorema** *Neka su $u$, $v$ i $z$ kompleksni brojevi. Tada*

1. $\mathrm{Re}(u+v) = \mathrm{Re}(u) + \mathrm{Re}(v)$, $\mathrm{Im}(u+v) = \mathrm{Im}(u) + \mathrm{Im}(v)$.
2. $\overline{u+v} = \bar{u} + \bar{v}$, $\overline{u\cdot v} = \bar{u}\cdot\bar{v}$, $\bar{\bar{z}} = z$.
3. *Konjugacija $z \mapsto \bar{z}$, $z \in C$ je automorfizam polja* $\mathbf{C}$.
4. $|z| = 0 \Leftrightarrow z = 0$, $z\cdot\bar{z} = |z|^2$, $|u+v| \leq |u| + |v|$.

S obzirom da je dokaz Teoreme elementaran, izostavljamo ga. Spomenimo samo da je svojstvo 3. posledica svojstava opisanih pod 2.

Kompleksni brojevi imaju takođe geometrijsku interpretaciju. Naime, neka je u euklidskoj ravni $\mathcal{E}$ dat pravougli koordinantni sistem $Oxy$.




Neka je $\tau : C \longrightarrow \mathcal{E}$ preslikavanje koje svakom kompleksnom broju $z = x + \imath y$ pridružuje tačku $M$ ravni $\mathcal{E}$ sa koordinatama $(x,y)$. Drugim rečima, $\tau : x + \imath y \mapsto M(x,y)$, $x + \imath y \in C$. Trojka $(\tau, \mathbf{C}, \mathcal{E})$ naziva se *Gausovom ravni.* Za Gausovu ravan takođe se koristi i termin *kompleksna ravan.* Struktura $\mathcal{C} = ((C,+,0),\mathbf{R},\cdot$

kompleksni brojevi, dok je operacija množenja skalara i vektora: $r(x+\imath y) = rx+\imath ry$, $r \in R$, $x + \imath y \in C$. Očigledno, baza ovog prostora je $\langle 1, \imath\rangle$, dakle dimenzija ovog prostora je 2. Uz ovako uvedene oznake, preslikavanje $\tau$ je izomorfizam prostora $\mathcal{C}$ i vektorskog prostora $\mathcal{E}^2$ orijentisanih duži u ravni $\mathcal{E}$ (čiji je početak fiksirana tačka - koordinantni početak), tj. važi $\tau(u + v) = \tau u + \tau v$, $\tau(r \cdot u) = r\tau(u)$, $u, v \in C$, $r \in R$. Dakle, možemo identifikovati kompleksne brojeve $z$ sa svojim slikama $\tau z$, s obzirom da je $\tau$ izomorfizam, tj. da je bijekcija i da održava algebarsku strukturu. Na opisan način dobijamo reprezentaciju kompleksnih brojeva kao vektora – orijentisanih duži u euklidskoj ravni. Otuda, na primer, imamo i dobro poznat način sabiranja kompleksnih brojeva kao vektora – orijentisanih duži u euklidskoj ravni.

U ovoj geometrijskoj interpretaciji kompleksnih brojeva, vidimo da, na primer, apsolutnoj vrednosti $|z|$ kompleksnog broja $z$ odgovara dužina – intenzitet ili norma vektora određenog sa $z$ (radijus vektor tačke $M$). U daljem izlaganju nećemo razlikovati kompleksni broj $z$ i vektor njime određen. Otuda se ugao koji $z$ čini sa $x > 0$ polupravom naziva *argumentom* kompleksnog broja $z$, dok se $|z|$ naziva i *normom* kompleksnog broja $z$. Argument kompleksnog broja $z$ obeležavamo pomoću $\arg z$. Ako je $\varphi = \arg z$ i $\rho = |z|$, na osnovu pravouglog trougla $\triangle OMM'$ nalazimo

$$\begin{aligned} &x = \rho\cos\varphi, \quad y = \rho\sin\varphi, &&0 \le \rho,\ 0 \le \varphi < 2\pi \\ &\rho = \sqrt{x^2 + y^2}, \quad \operatorname{tg}\varphi = \frac{y}{x} &&x, y \in R \end{aligned} \tag{3.7.4}$$

Par $(\rho, \varphi)$ iz 3.7.4, naziva se *polarnim koordinatama* kompleksnog broja $z$. Vidimo da jednakosti 3.7.4 daju prelazak sa Dekartovih na polarne koordinate kompleksnog broja $z$ i obrnuto. Iz 3.7.4 takođe dobijamo tzv. trigonometrijski oblik komleksnog broja

$$z = \rho(\cos\varphi + \imath\sin\varphi), \qquad 0 \le \rho,\ 0 \le \varphi < 2\pi. \tag{3.7.5}$$

Za trigonometrijski oblik kompleksnog broja lako se proverava matematičkom indukcijom (najpre ako je $n$ prirodan broj) tzv. Moavrov obrazac

$$(\cos\varphi + \imath\sin\varphi)^n = \cos n\varphi + \imath\sin n\varphi, \qquad n \in Z. \tag{3.7.6}$$

Otuda iz 3.7.5 imamo, na primer,

$$z^{-1} = \rho^{-1}(\cos\varphi - \imath\sin\varphi),$$

$$u \cdot v = |u| \cdot |v|(\cos(\arg u + \arg v) + \imath\sin(\arg u + \arg v)).$$

Uz pomoć kompleksne eksponencijalne funkcije $e^z$, 3.7.5 postaje

$$z = \rho e^{\imath\varphi}, \qquad \rho \in [0, +\infty)_R,\ \varphi \in [0, 2\pi)_R. \tag{3.7.7}$$

Neka je $k$ pozitivan prirodan broj, i neka je za $0 \le k < n$, $\varepsilon_k = \cos(2\pi k/n) + \imath\sin(2\pi k/n)$. Prema 3.7.6 vidimo da je $\varepsilon_k = \varepsilon^k$, gde je $\varepsilon = \cos(2\pi/n) + \imath\sin(2\pi/n)$, kao i da $\varepsilon_k$, $k = 0, 1, \dots, n-1$, leže na jediničnom krugu u kompleksnoj ravni određujući temena pravilnog $n$-tougla, čije je jedno teme kompleksan broj 1. Sa algebarskog stanovišta zanimljiva je činjenica da važi $\varepsilon_k^n = 1$, dakle $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$ su $n$ različitih korena algebarske jednačine $z^n = 1$ u polju kompleksnih brojeva. Otuda odmah imamo razlaganje polinoma $z^n - 1$ na linearne faktore

$$z^n - 1 = \prod_{k=0}^{n-1} (z - \varepsilon^k). \tag{3.7.8}$$

Nije teško proveriti da je $\mathbf{C}_n = (\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}, \cdot, 1)$ ciklična grupa reda $n$, dakle, $\mathbf{C}_n$ je izomorfna sa grupom $(Z_n, +_n, 0)$, gde $Z_n = \{0, 1, \dots, n-1\}$. Jedan izomorfizam ovih grupa je preslikavanje $h : k \mapsto \varepsilon^k$, $k \in Z_n$. Generatori grupe $\mathbf{C}_n$ nazivaju se *primitivnim korenima* polinoma $z^n - 1$, dakle kompleksni broj $\varepsilon$ je jedan primitivan koren ovog polinoma.

Već smo se sasvim približili glavnoj teoremi ovog odeljka – Osnovnoj teoremi algebre, prema kojoj svaki polinom sa koeficijentima u polju $\mathbf{C}$ i stepena $\geq 1$ ima koren u $\mathbf{C}$. Najpre dokažimo sledeće leme.

**3.7.9 Lema** *Neka je $a \in C - \{0\}$ i $n \in N$, $n \geq 1$. Tada jednačina $x^n = a$ ima tačno $n$ rešenja u polju $\mathbf{C}$.*

**Dokaz** Neka je $\rho = |a|$, $\varphi = \arg a$. Prema 3.7.8, skup $S$ svih rešenja jednačine $x^n = a$ izgleda ovako:

$$S = \{ \sqrt[n]{\rho}(\cos \frac{2\pi k}{n} + \imath \sin \frac{2\pi k}{n}) |\ k = 0, 1, \dots, n-1\}$$

$\diamondsuit$

**3.7.10 Lema** *Neka je $p(x)$ polinom sa realnim koeficijentima. Ako je $p(0) < 0$, onda postoji $t \in R$, $0 < t < 1$ tako da je $p(t) < 0$.*

**Dokaz** Ovo svojstvo realnih polinoma je neposredna posledica neprekidnosti realnih polinomnih funkcija, s obzirom da lema važi za proizvoljne neprekidne realne funkcije. Ipak, zanimljivo je pogledati neposredan dokaz, jer se taj dokaz ne zasniva na pojmu neprekidnosti. Kao posledicu dobićemo da ova lema važi u bilo kojem uređenom polju $\mathbf{F}$ (tj. ako se u lemi $\mathbf{R}$ zameni sa $\mathbf{F}$). Neka je $p(x) = a_0 + a_1 x + \dots + a_n x^n$, stepena $\geq 1$ (razmatramo netrivijalan slučaj). Tada je prema pretpostavci $p(0) = a_0 < 0$. Neka je $t = |a_0|/(1 + |a_0| + |a_1| + \dots + |a_n|)$. Očigledno $0 < t < 1$ i

$$\begin{aligned} t|a_1 + a_2 t + \dots + a_n t^{n-1}| &\leq t(|a_1| + |a_2| \cdot |t| + \dots + |a_n| \cdot |t|^{n-1}) < \\ &\frac{|a_0|}{1 + |a_0| + |a_1| + \dots + |a_n|} \cdot (|a_1| + |a_2| + \dots + |a_n|) < |a_0|, \end{aligned}$$

dakle $p(t) < 0$. $\diamondsuit$

**3.7.11 Lema** *Neka je $p(z)$ polinom nad poljem* $\mathbf{C}$ *stepena* $\geq 1$. *Ako je* $p(u) \neq 0$, *gde* $u \in C$, *onda postoji* $v \in C$ *tako da je* $|p(v)| < |p(u)|$.

**Dokaz** Neka je $z = u + h$. Tada za neke koeficijente $a_i \in C$ važi

$$p(z) = a_0 + a_1(z-u) + \ldots + a_n(z-u)^n, \quad \text{tj.} \quad p(u+h) = p(u) + a_1 h + \ldots + a_n h^n.$$

Neka je $a_k$ prvi u nizu $a_1, \ldots, a_n$ različit od nule. Dalje, neka je $\varepsilon$ rešenje jednačine $x^k = -p(u)/a_k$, koje postoji prema Lemi 3.7.9. Neka je $h = t\varepsilon$, gde $0 \leq t \leq 1$, i uvedimo $b_j = a_j \varepsilon^j$, $j = k+1, \ldots, n$. Tada za $v = u + h$ važi

$$\begin{aligned}
|p(v)| &= |p(u) - t^k p(u) + t^{k+1} b_{k+1} + \ldots + t^n b_n| \\
&\leq |(1-t^k)p(u)| + t^{k+1}|b_{k+1}| + \ldots + t^n|b_n| \\
&= (1-t^k)|p(u)| + t^{k+1}|b_{k+1}| + \ldots + t^n|b_n| \\
&= |p(u)| + t^k(-|p(u)| + t|b_{k+1}| + \ldots + t^{n-k}|b_n|) \\
&= |p(u)| + t^k q(t), \qquad \text{gde je } q(t) = -|p(u)| + t|b_{k+1}| + \ldots + t^{n-k}|b_n|.
\end{aligned}$$

Prema tome $|p(v)| \leq |p(u)| + t^k q(t)$. Primetimo da je $q(t)$ realan polinom. S obzirom da je $q(0) = -|p(u)| < 0$, prema Lemi 3.7.10 postoji $0 < \bar{t} < 1$, tako da je $q(\bar{t}) < 0$. Tada za $h = \bar{t}\varepsilon$ važi

$$|p(u+h)| \leq |p(u)| + \bar{t}^k q(\bar{t}) < |p(u)|,$$

Dakle, možemo uzeti $v = u + h = u + \bar{t}\varepsilon$. $\diamondsuit$

Podskup $S \subseteq C$ je *neograničen* ako za svaki $z \in C$ postoji $s \in S$ tako da je $|s| \geq |z|$. Na primer, skup $C$ je neograničen skup. Preslikavanje $f : C \to C$ je neograničeno na $S$ ako je $f(S)$ neograničen skup.

**3.7.12 Lema** *Neka je* $S \subseteq C$ *neograničen. Tada je svaki polinom stepena* $\geq 1$ *sa koeficijentima u* $\mathbf{C}$ *neograničen na* $S$.

**Dokaz** Tvrđenje ćemo dokazati za normiran polinom $p(z) = a_0 + a_1 z + \ldots + a_{n-1}z^{n-1} + z^n$, $n \geq 1$. Izaberimo proizvoljan $w \in C$ i neka je $M = |w|$. Dalje, neka je za $i = 0, 1, \ldots, n-1$, $z_i \in C$ tako da je $|a_i|/|z_i| < 1/2n$. S obzirom da je $S$ neograničen skup, postoji $s \in S$ tako da je $|s| > 1, 2M, |z_0|, |z_1|, \ldots, |z_{n-1}|$. Tada

$$\begin{aligned}
|p(s)| &= |s^n(1 + \frac{a_{n-1}}{s} + \ldots + \frac{a_0}{s^n})| \\
&\geq (2M)^n(1 - (|\frac{a_{n-1}}{s}| + \ldots + |\frac{a_0}{s^n}|)) \\
&\geq 2^n M^n (1 - n \cdot \frac{1}{2n}) = 2^{n-1}M^n > M.
\end{aligned}$$

$\diamondsuit$

Ovaj stari naziv sledeće teoreme donekle je anahron, ali u svakom slučaju pokazuje kakav se značaj pridavao toj teoremi u matematici.

**3.7.13** ***Osnovna teorema algebre*** *Svaki polinom $p(z)$ sa kompleksnim koeficijentima stepena $\geq 1$, ima bar jedan koren u polju kompleksnih brojeva.*

**Dokaz** Neka je $S = \{|p(z)| \,|\, z \in C\}$. S obzirom da je 0 donja granica skupa $S$, prema Teoremi supremuma postoji $\inf S$. Neka je $s = \inf S$. Primetimo da je $s \in R$ i da je $s \geq 0$. Dokažimo da je $\inf S$ dostignut, tj. da je za neki $w \in C$, $|p(w)| = s$.

Prema definiciji infimuma, postoji niz kompleksnih brojeva $\langle z_n \,|\, n \in N\rangle$ tako da je

$$s \leq |p(z_n)| \leq s + 1/(n+1), \qquad n \in N. \tag{1}$$

Kako je skup $\{|p(z_n)| \,|\, n \in N\}$ ograničen, prema Lemi 3.7.12 i skup $\{z_n \,|\, n \in N\}$ je ograničen, tj. postoji $M \in R^+$ tako da je za sve $n \in N$, $|z_n| \leq M$. Neka su $x = \langle x_n \,|\, n \in N\rangle$ i $y = \langle y_n \,|\, n \in N\rangle$ realni nizovi takvi da je $z_n = x_n + \imath y_n$. Kako su $|x_n|, |y_n| \leq |z_n|$, nizovi $x$ i $y$ su takođe ograničeni. Neka su $x'$ i $y'$ monotoni podnizovi nizova $x$ i $y$; podsetimo se da takvi postoje prema Remzijevoj teoremi. Tada su nizovi $x'$ i $y'$ monotoni i ograničeni, dakle Košijevi, te uz notaciju iz Odeljka 3.6, postoje realni brojevi $a, b \in R$ takvi da je $a = x'/\!\sim$ i $b = y'/\!\sim$. Neka je $w = a + \imath b$. S obzirom da je preslikavanje $x \mapsto x/\!\sim$, $x$ je Košijev niz, homomorfizam, koristeći nejednakosti (1), imamo

$$s \leq |p(x/\!\sim + \imath y/\!\sim)| \leq s + \langle 1/(n+1) \,|\, n \in N\rangle/\!\sim .$$

odnosno $|p(a + \imath b)| = s$, ili $|p(w)| = s$. Pretpostavimo da je $|p(w)| > 0$. Onda prema Lemi 3.7.11 postoji $v \in C$ tako da je $|p(v)| < |p(w)| = s$, suprotno definiciji konstante $s$. Prema tome $|p(w)| = 0$, odnosno $p(w) = 0$, što znači da je $w$ koren polinoma $p(z)$. ♢

Prethodni dokaz mogao se učiniti nešto jednostavnijim da smo koristili aparat matematičke analize (svojstva konvergentnih realnih i kompleksnih nizova). Čitaocu predlažemo da izvede i taj dokaz.

Evo nekih posledica Osnovne teoreme algebre.

**3.7.14 Posledica** Ako je $p(z)$ polinom sa kompleksnim koeficijentima, onda se $p(z)$ razlaže na proizvod linearnih faktora nad poljem $\mathbf{C}$, tj. ako je $p(z) = \sum_{i=0}^{n} a_j z^j$, tada postoje $z_1, z_2, \ldots, z_n \in C$ tako da identitet $p(z) = a_n \prod_{j=0}^{n} (z - z_j)$ važi u $\mathbf{C}$.

Zaista, ako je $w$ koren polinoma $p(z)$, onda $p(z) = (z - w)q(z)$ za neki polinom $q(z)$ stepena $n - 1$, pa višestrukom primenom Osnovne teoreme algebre dolazimo do traženog identiteta.

Neka je $p(x)$ polinom sa realnim koeficijentima stepena $\geq 1$. Prema Osnovnoj teoremi algebre, $p(x)$ ima koren $a \in C$. Pretpostavimo da $a$ nije realan. S obzirom da je konjugacija homomorfizam polja $\mathbf{C}$, iz $p(a) = 0$ sledi takođe $p(\bar{a}) = 0$, prema tome i $\bar{a}$ je koren polinoma $p(x)$. Kako je $(x - a)(x - \bar{a}) = x^2 - (a + \bar{a})x + a\bar{a}$ realan polinom, prema prethodnoj posledici odmah imamo:

**3.7.15 Posledica** Svaki realan polinom stepena $\geq 1$ razlaže se nad poljem realnih brojeva na proizvod linearnih i kvadratnih polinoma.

Ovim napomenama završavamo zasnivanje polja kompleksnih brojeva.

## Zadaci

**3.1** Neka je $M$ skup svih numerala i neka je operacija $'_M$ skupa $M$ definisana na sledeći način: $\underline{m} = \underline{n}'_M \Leftrightarrow m = n + 1,\ m, n \in N$. Dokazati da struktura $(M, '_M, \underline{0})$ zadovoljava Peanove aksiome.

**3.2** Na osnovu Peanovih aksioma dokazati: zakon komutacije za množenje, zakone asocijacije za sabiranje i množenje i zakon distribucije za operaciju množenja u odnosu na sabiranje prirodnih brojeva.

**3.3** U Peanovoj aritmetici dokazati:
**a.** $x + y = x + z \Rightarrow y = z$. **b.** $(x + 1)y = (x + 1)z \Rightarrow y = z$.

**3.4** U Peanovoj aritmetici dokazati da prirodno uređenje prirodnih brojeva, v. Primer 3.1.9, zadovoljava aksiome linearnog uređenja.

**3.5** Dokazati osnovne aritmetičke zakone u formalnoj artimetici.

**3.6** Neka je **M** bilo koji model formalne aritmetike. Dokazati da je struktura prirodnih brojeva **N** izomorfna nekom početnom komadu (u odnosu na prirodno uređenje) od **M**.

**3.7*** Dokazati **a.** da postoji prebrojiv model formalne aritmetike, i **b.** da ima kontinuum mnogo neizomorfnih prebrojivih modela formalne aritmetike.

**3.8** Neka su $L$ i $R$ projekcijske funkcije za Kantorovu funkciju i neka je za $x \in R$, $\lceil x \rceil$ najmanji ceo broj $\geq x$. Dokazati: ako je $a \in N$ i $n = \lceil(-3 + \sqrt{9 + 8a})/2\rceil$, onda $L(a) = a - \langle 0, n \rangle_K$ i $R(a) = \langle n, 0 \rangle_K - a$.

**3.9** Dokazati: ako skup $A$ ima kodirajuću funkciju, onda je $A$ prebrojiv. Odrediti jednu kodirajuću funkciju $\tau$ jezika teorije uređenih polja u okviru predikatskog računa prvog reda i izračunati $\tau\varphi$, gde je $\varphi = \forall x(\neg x = 0 \Rightarrow \exists y(x \cdot y = 1))$.

**3.10** (*Dvojna ili simultana rekurzija*) Neka su $A$, $B$ i $C$ neprazni skupovi i neka su $f_1 : A \to B$, $f_2 : A \to C$, $g_1 : N \times A \times B \times C \to B$ $g_2 : N \times A \times B \times C \to C$. Dokazati da postoje jedinstvene funkcije $h_1 : N \times A \to B$ i $h_2 : N \times A \to C$ takve da je

$$\begin{aligned} h_1(0, x) &= f_1(x), \qquad & h_1(y + 1, x) &= g_1(y, x, h_1(y, x), h_2(y, x)), \\ h_2(0, x) &= f_2(x), \qquad & h_2(y + 1, x) &= g_2(y, x, h_1(y, x), h_2(y, x)). \end{aligned}$$

**3.11** (*Regresivna indukcija*) Neka je $\varphi(n)$ aritmetički iskaz. Dokazati: Ako $\varphi(n)$ važi za beskonačno mnogo prirodnih brojeva $n$ i ako za svaki pozitivan $k \in N$, iz $\varphi(k)$ sledi $\varphi(k - 1)$, onda $\varphi(n)$ važi za sve prirodne brojeve $n$.

**3.12** (*Jensenova nejednakost*) Neka su $a, b \in R$, $a < b$. Za funkciju $f : [a,b]_R \to R$ kažemo da je *konveksna* ako za sve $x, y \in [a,b]_R$ važi $f\left(\dfrac{x+y}{2}\right) \leq \dfrac{f(x)+f(y)}{2}$. Dokazati da je onda za sve $x_1, x_2, \ldots, x_n \in [a,b]_R$:

$$f((x_1 + x_2 + \ldots + x_n)/n) \leq (f(x_1) + f(x_2) + \ldots + f(x_n))/n.$$

Dokazati da za pozitivne realne brojeve $x_1, x_2, \ldots, x_n$ važi:

$$(x_1 + x_2 + \ldots + x_n)/n \geq \sqrt[n]{x_1 x_2 \ldots x_n}.$$

**3.13** Dokazati da za svaka dva prirodna broja $a$ i $b$ važi $\mathrm{NZD}(a,b) \cdot \mathrm{NZS}(a,b) = ab$.

**3.14** Dokazati da za Fibonačijeve brojeve važi:
**a.** $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ (J.D.Cassini 1680g.).
**b.** $f_{n+k} f_{n-k} - f_n f_m = (-1)^n f_{m-n-k} f_k$, uzimajući da je $f_n$ definisan za sve $n \in Z$, prema definicionoj rekurentnoj formuli za Fibonačijeve brojeve.

**3.15** Dokazati da za Fibonačijeve brojeve važi
**a.** $2^n f_n = 2 \sum_{k \in 2N+1} \binom{n}{k} 5^{(k-1)/2}$.
**b.** Ako je $p$ neparan prost broj, onda $f_p =_p 5^{(p-1)/2}$.

**3.16** (*Fibonačijev brojevni sistem*) Neka $k \gg m$ znači $k \geq m + 2$. Pokazati da svaki pozitivan prirodan broj $n$ ima jedinstvenu reprezentaciju:

$$n = f_{k_1} + f_{k_2} + \ldots + f_{k_r}, \quad \text{gde } k_1 \gg k_2 \gg \ldots \gg k_r \gg 0.$$

**3.17** Dokazati sledeće identitete za binomne koeficijente:
**a.** $\binom{n}{k} = \binom{n}{n-k}$. **b.** $k\binom{n}{k} = n\binom{n-1}{k-1}$. **c.** $\sum_k \binom{r}{k}\binom{s}{n+k} = \binom{r+s}{r+n}$.
**d.** $\sum_{k \geq 0} \frac{(-1)^k}{k+1} \binom{n+k}{2k}\binom{2k}{k} = 0$ za $n > 0$.
**e.** $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots = 2^n$. **f.** $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = 2^{n-1}$
**g.** $\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \ldots = (2^n + 2\cos((n-2)\pi/3))/3$

**3.18** Neka su $m, n \in N$. Dokazati:

$$(\sum_{k=1}^{m} x_i)^n = \sum_{k_1 + \cdots + k_m = n} \frac{n!}{k_1! k_2! \ldots k_m!} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m}$$

**3.19** Neka su $S_k^n$ i $s_k^n$ redom Stirlingovi brojevi prve i druge vrste. Dokazati da su matrice $A = \|s_k^n\|$ i $B = \|S_k^n\|$ uzajamno inverzne.

**3.20** Dokazati sledeće identitete za Stirlingove brojeve:
**a.** $s_k^n = \dfrac{1}{k!}\Delta^k 0^n$, gde $\Delta^k 0^n = q(0)$, $q(x) = \Delta^k x^n$.
**b.** $s_k^n = \dfrac{(-1)^k}{k!} \sum_i (-1)^i \binom{k}{i} i^n$. **c.** $s_{k+1}^{n+1} = \sum_j \binom{n}{j} s_k^j$.

**3.21** Neka su $m$ i $n$ prirodni brojevi $\geq 2$. Napisati algoritam (program) koji iz zapisa $(a)_m$ broja $a$ u bazi $m$ nalazi zapis $(a)_n$ broja $a$ u bazi $n$.

**3.22** Neka je $c_n$ zapis broja $5^n$ u bazi 2. Dokazati da $c_n$ zadovoljava sledeću rekurentnu formulu (u bazi 2): $c_n = 1 + 100(1 + c_1 + c_2 + \ldots + c_{n-1})$.

**3.23** Dokazati da za svaki prirodan broj $n > 0$ postoji prirodan broj $g(n)$ koji zapisan u dekadnom sistemu ima samo cifre 0 i 1, a deljiv je sa $n$. Odrediti algoritam za određivanje broja $g(n)$ za dato $n$.

**3.24** Neka su $A$ i $X$ proizvoljni skupovi.
**a.** Ako je $A$ konačan i $f : A \xrightarrow{\text{na}} X$, dokazati da je $X$ konačan.
**b.** Ako je $A$ beskonačan i $f : A \xrightarrow[\text{1-1}]{} X$, dokazati da je $X$ beskonačan.

**3.25** Neka su $A$ i $B$ konačni ekvipotentni skupovi i neka je $f : A \to B$. Dokazati da je $f$ $1-1$ akko je $f$ *na*. Dokazati da ovo tvrđenje ne važi za beskonačne skupove.

**3.26** Neka je $A = \{a_1 < a_2 < \ldots\} = \{4^i + 4^j \,|\, 0 \leq i < j\}$. Dokazati:
**a.** Svaki $n \in N$ ima najviše tri reprezentacije oblika $a_i + a_j$, $i < j$.
**b.** Za bilo koju particiju skupa $A$ na konačno mnogo skupova, recimo $A = A_1 \cup A_2 \cup \ldots \cup A_r$, za neki $A_i = \{a_1' < a_2' < \ldots\}$, beskonačno mnogo $n \in N$ može se napisati u obliku $a_i' + a_j'$, $i < j$ na najmanje tri načina.

**3.27*** (*Špernerova teorema*) Neka je $n \in N$ i neka je $\mathcal{A} = \langle A_1, A_2, \ldots, A_k\rangle$ niz podskupova od $n$. Niz $\mathcal{A}$ je *Špernerov* ako nijedan član niza nije podskup nekog drugog člana niza $\mathcal{A}$. Dokazati da za Špernerov niz $\mathcal{A}$ važi $k \leq \binom{n}{[n/2]}$.

**3.28** (*Formula uključivanja–isključivanja*) Dokazati da za proizvoljne skupove $A_1, A_2, \ldots, A_n$ važi:

$$|A_1 \cup \ldots \cup A_n| = \sum_{1 \leq i_1 \leq n} |A_{i_1}| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \ldots + (-1)^{n-1} \cdot \sum_{1 \leq i_1 < \ldots < i_n \leq n} |A_{i_1} \cap \ldots \cap A_{i_n}|.$$

Odrediti broj $D_n$ svih permutacija $p$ skupa $n$ koje imaju neku fiksnu tačku, tj. postoji $i \in n$ tako da je $p(i) = i$.

**3.29** Neka su $m$ i $n$ pozitivni prirodni brojevi, gde $n < m$. Dokazati da

$\dfrac{1}{n} + \dfrac{1}{n+1} + \ldots + \dfrac{1}{m}$ nije ceo broj.

**3.30** Neka su $a, b, c, d \in Q$, $c \neq 0$, i neka je $\alpha$ iracionalan broj. Dokazati:

$\dfrac{a\alpha + b}{c\alpha + d} \in Q \Leftrightarrow ad = bc.$

**3.31** Dokazati:
**a.** $[nx] = \sum_{j=0}^{n-1} [x + j/n]$, $x \in R$, $n \in N^+$.
**b.** $[\sqrt[k]{x}]^k \leq [x] \leq \sum_{j=0}^{k-1} \binom{k}{j} [\sqrt[k]{x}]^{k-j}$, $x \in R^+$, $k \in N^+$.

**3.32** Dokazati da se uređenje realnih brojeva možde definisati pomoću operacija sabiranja i množenja.

**3.33** Dokazati da se svaki prebrojiv linearno uređen skup može utopiti u uređenje racionalnih brojeva.

**3.34*** (Đ. Kurepa) Neka je $(X, \leq)$ linearno uređen skup sa osobinom da se u njega može utopiti svaki prebrojiv dobro uređen skup. Dokazati da se u $(X, \leq)$ može utopiti uređenje racionalnih brojeva.

**3.35** Dokazati da iracionalnih brojeva ima kontinuum mnogo.

**3.36*** (*Hamelova baza*) Za podskup $H \subseteq R$ kažemo da je *Hamelova baza* akko je $H$ baza vektorskog prostora $((R, +, 0), \mathbf{Q}, \cdot)$. Dokazati:
**a.** Postoji Hamelova baza. **b.** Svaka Hamelova baza je moći kontinuuma.
**c.** Postoji $2^{2^{\aleph_0}}$ mnogo Hamelovih baza.
**d.** Postoji Hamelova baza Lebegove mere 0. Ako je $H$ Hamelova baza i $H$ je merljiv skup u smislu Lebegove mere, onda je $m(H) = 0$ .

**3.37*** (*Košijeva funkcionalna jednačina*). Za funkciju $f : R \to R$ kažemo da ima *Košijevu osobinu* ako za sve $x, y \in R$ važi $f(x + y) = f(x) + f(y)$. Ako realna funkcija $f$ ima Košijevo svojstvo dokazati da su sledeći iskazi ekvivalentni:
**a.** Postoji $c \in R$ tako da je $f(x) = cx$, $x \in R$. **b.** $f$ je neprekidna funkcija.
**c.** $f$ je monotona funkcija na nekom intervalu.
**d.** $f$ je ograničena funkcija na nekom intervalu.
**e.** Grafik funkcije $f$ nije svuda gust u $R^2$.

**3.38** Uređeno polje $\mathbf{F}$ je arhimedovsko ako je skup $\{n \cdot 1_F \mid n \in N\}$ kofinalan u $\mathbf{F}$. Dokazati da se svako arhimedovsko polje može izomorfno utopiti u uređeno polje realnih brojeva.

**3.39** Neka je $Z$ skup celih brojeva i neka je $S = \{a \in R^Z \mid \exists k \in Z \ \forall n < k \ \ a_n = 0\}$. Neka su binarne operacije $+$ i $\cdot$ definisane na sledeći način:

$$(a + b)_n = a_n + b_n, \quad (a \cdot b)_n = \sum_{i+j=n} a_i b_j, \qquad a, b \in R^Z,\ n \in Z.$$

Konstante $\mathbf{0}$, $\mathbf{1}$ i $\varepsilon$ uvodimo na sledeći način: $\mathbf{0} = \langle 0 \mid n \in Z \rangle$; $\mathbf{1}_n = 1$ ako $n = 0$, inače $\mathbf{1}_n = 0$; $\varepsilon_n = 1$ ako $n = 1$, inače $\varepsilon_n = 0$, $n \in N$.
**a.** Dokazati da je $\mathbf{S} = (S, +, \cdot, \mathbf{0}, \mathbf{1})$ polje.
**b.** Dokazati da postoji utapanje $h : \mathbf{R} \to \mathbf{S}$.
**c.** Za $a \in S - \{0\}$ kažemo da je *pozitivan* ako za najmanji $k$ takav da je $a_k \neq 0$, važi $a_k > 0$. Binarnu relaciju $\leq$ na $S$ definišemo pomoću:
$a \leq b$ akko $b - a$ je pozitivan ili $a = b$.
Dokazati da je $(\mathbf{S}, \leq)$ uređeno polje. Dokazati da uz identifikaciju određenu sa **b.** polja $\mathbf{R}$ sa podpoljem polja $\mathbf{S}$, $\leq$ produžuje uređenje realnih brojeva, kao i da u $\mathbf{S}$ onda važi: $\forall r \in R^+ \ \ 0 < \varepsilon < r$.

**3.40*** Za uređeno polje $\mathbf{F}$ kažemo da je *Scott kompletno* (prema Dana Scott), ako za svako uređeno polje $\mathbf{G}$ važi: $\mathbf{F} \subseteq \mathbf{G}$ i $F$ je gusto u $\mathbf{G} \Rightarrow F = G$. Dokazati:
**a.** $\mathbf{F}$ je Scott–kompletno akko svaki početni komad $X$ od $\mathbf{F}$ koji zadovoljava:

(*) $\forall \varepsilon > 0 \ \exists a \in X \ \ a + \varepsilon \notin X$, ima supremum.

**b.** Dokazati da za svako uređeno polje $\mathbf{F}$ postoji Scott–kompletno polje $\mathbf{G}$ takvo da je $\mathbf{F} \subseteq \mathbf{G}$ i $F$ je gusto u $\mathbf{G}$.
**c.** Dokazati jedinstvenost polja pod **b.**

**3.41** Dokazati da je $\mathrm{Aut}(R, +, \cdot, 0, 1) = \{i_R\}$.

**3.42*** **a.** Navesti primer nearhimedovskog polja.
**b.** Dokazati da se svako uređeno polje može potopiti u neko nearhimedovsko polje.

**3.43** Izračunati $\sqrt[3]{2}$ sa greškom $< 10^{-5}$.

**3.44** Dokazati: **a.** U svakom uređenom polju važi $x^2 \geq 0$.
**b.** Polje kompleksnih brojeva ne može se proširiti do uređenog polja.

**3.45** Dokazati da za polinom $x^n - 1$ važe sledeće faktorizacije u polju $\mathbf{R}$:
**a.** $x^n - 1 = (x-1)\prod_{k=1}^{m}(x^2 - 2x\cos(\frac{2\pi k}{n}) + 1)$, ako $n = 2m+1$.
**b.** $x^n - 1 = (x^2-1)\prod_{k=1}^{m-1}(x^2 - 2x\cos(\frac{2\pi k}{n}) + 1)$, ako $n = 2m$.

**3.46** Ako je $\mathbf{S}$ konačna podgrupa multiplikativne grupe polja kompleksnih brojeva, dokazati da je $\mathbf{S} = \langle \varepsilon \rangle$, gde je $\varepsilon$ $n$–ti koren jedinice na neki $n \in N$.

**3.47** Neka je $S$ skup svih primitivnih korena polinoma $x^n - 1$. Dokazati da je $\Phi_n(x) = \prod_{\tau \in S}(x - \tau)$ polinom sa celobrojnim koeficijentima.

**3.48** Rešiti jednačinu $(z + \imath)^n + (z - \imath)^n = 0$ u polju $\mathbf{C}$.

**3.49** Neka je $f(x)$ realan polinom takav da je za sve $x \in R$, $f(x) \geq 0$. Dokazati da postoje realni polinomi $g(x)$ i $h(x)$ takvi da je $f = g^2 + h^2$.

**3.50*** Neka je $A$ skup svih kompleksnih brojeva koji su koreni nekog polinoma sa racionalnim koeficijentima. Dokazati da je $A$ podpolje polja $\mathbf{C}$.

# Rešenja zadataka

## 1. ALGEBRE

**1.1** Pretpostavimo da je $(x,y)=(x',y')$, dakle $\{\{x\},\{x,y\}\}=\{\{x'\},\{x',y'\}\}$. Pošto su dva skupa jednaka akko su im svi elementi jednaki, imamo dve mogućnosti:
**i.** $\{x\}=\{x'\}$ i $\{x,y\}=\{x',y'\}$; iz ovoga sledi tvrđenje zadatka. **ii.** $\{x\}=\{x',y'\}$ i $\{x,y\}=\{x'\}$. Na osnovu prve jednakosti, skup $\{x',y'\}$ ima samo jedan element, dakle $x'=y'$. Tada (ponovo na osnovu prve jednakosti) $x=x'$. Na sličan način se iz druge jednakosti dobija $x=y$, čime je dokaz završen. $\diamondsuit$

**1.3** **a.** Dokazaćemo samo asocijativnost. Ako sa $p\underline{\vee}q$ označimo formulu $(p\wedge\neg q)\vee(\neg p\wedge q)$ (*ekskluzivna disjunkcija*) imamo $x\in U\Delta V$ akko $x\in U\underline{\vee}x\in V$. Korišćenjem tautologije $((p\underline{\vee}q)\underline{\vee}v)\leftrightarrow(p\underline{\vee}(q\underline{\vee}v))$ dobijamo ($S$, $U$ i $V$ su bilo koji skupovi):

$$\begin{aligned}(x\in(S\Delta U)\Delta V)&\Leftrightarrow(x\in(S\Delta U)\underline{\vee}x\in V)\\ \Leftrightarrow((x\in S\underline{\vee}x\in U)\underline{\vee}x\in V)&\Leftrightarrow(x\in S\underline{\vee}(x\in U\underline{\vee}x\in V))\\ &\Leftrightarrow(x\in S\Delta(U\Delta V)).\quad\Box\end{aligned}$$

**b.** Dokažimo prvo sledeće tvrđenje ($a,b,c\in\mathbf{Q}$):

$a+b\sqrt[3]{2}+c\sqrt[3]{2}^2\Leftrightarrow a^2+b^2+c^2\neq0.$

**Dokaz** (Samo netrivijalan smer). Pošto je polinom $x^3-2$ nesvodljiv nad poljem $Q$, nijedan polinom drugog stepena nad $Q$ nema $\sqrt[3]{2}$ za koren.

Broj $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$ ima inverzni element akko jednačina $(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)(x+y\sqrt[3]{2}+z\sqrt[3]{2}^2)=1$ ima racionalno rešenje. Ova jednačina se svodi na

$$(ax+2cy+2bz-1)+(bx+ay+2cz)\sqrt[3]{2}+(cx+by+az)\sqrt[3]{2}^2=0,$$

što je, na osnovu tvrđenja, ekvivalentno sistemu

$$ax+2cy+2bz=1,\qquad bx+ay+2cz=0,\qquad cx+by+az=0.$$

Ovaj sistem linearnih jednačina ima netrivijalno racionalno rešenje akko je determinanta sistema $D$ različita od 0; ali $D=\begin{vmatrix}a&2c&2b\\b&a&2c\\c&b&a\end{vmatrix}=a^3+2b^3+4c^3-6abc$. Pretpostavimo da je $D=0$. Svođenjem na zajednički imenilac dobijamo da jednačina $a^3+2b^3+4c^3-6abc$ ima celobrojno rešenje, i to takvo da $a,b$ i $c$ nemaju zajednički delilac. Ali ako su $a,b$ i $c$ celi, onda je $a=2a_1$; dobijamo jednačinu $4a_1^3+b^3+2c^3-6a_1bc=0$, dakle $b=2b_1$. Sada imamo $2a_1^3+4b_1^3+c^3-6a_1b_1c=0$, kontradikcija. Dakle $D\neq0$ i postoji racionalno rešenje sistema. $\diamondsuit$

**1.4** **a.** Na osnovu Posledice 1.7.5 i činjenice da je $1 \in P$, dovoljno je dokazati da je skup $P$ zatvoren za operacije $+, -, \cdot$ i $^{-1}$. Kompleksne brojeve poistovećujemo sa vektorima čiji je početak u tački $(0, 0)$. **i. Sabiranje i oduzimanje.** Zbir dva vektora je moguće konstruisati pomoću lenjira i šestara, kao i vektor suprotan datom vektoru. **ii. Recipročna vrednost.** Konstrukcija ugla jednakog $\arg z$, ali suprotne orijentacije je jednostavna. Dužine $|w| = 1/|z|$ se konstruiše primenom Talesove teoreme na proporciju $|w|/1 = 1/|z|$ (jedinična duž je data). **iii. Množenje.** Konstrukciju vektora koji odgovara proizvodu $z_1 z_2$ izvodimo u dva dela. U prvom konstruišemo zbir uglova koje dati vektori zaklapaju sa $x$-osom. U drugom treba naći dužinu $|z|$ takvu da je $|z| = |z_1||z_2|$, dakle $|z|/|z_1| = |z_2|/1$ – ovo se ponovo svodi na primenu Talesove teoreme. $\diamondsuit$

**1.5** **c.** Na osnovu **b.**, $(\mathbf{P}X, \cup, \cap, ^c, \emptyset, X)$ je Bulova algebra. Pošto su skupovi $\emptyset$ i $X$ otvoreno-zatvoreni, na osnovu Posledice 1.7.5 dovoljno je dokazati da je mnoštvo $S$ zatvoreno za operacije $\cup$, $\cap$ i $^c$, a ovo sledi iz činjenice da su mnoštva otvorenih i zatvorenih podskupova prostora $X$ zatvorene za konačne unije i preseke i iz činjenice da je komplement otvorenog skupa zatvoren i obratno. $\diamondsuit$

**1.7** **a.** U dokazu ćemo iskoristiti Zornovu lemu. Neka je $K$ mnoštvo svih komutativnih podgrupoida grupoida $\mathbf{G}$. Struktura $(K, \subset)$ je parcijalno uređen skup, dokažimo da je on zatvoren za unije lanaca, naime:

*Ako je $\mathbf{A}_i, i \in I$ lanac komutativnih podgrupoida grupoida $\mathbf{G}$ tada je i $\bigcup_{i \in I} A_i$ komutativan podgrupoid grupoida $\mathbf{G}$.*

**Dokaz** Primetimo da je $\bigcup_{i \in I} A_i$ grupoid. Neka je $x, y \in \bigcup_{i \in I} A_i$. Tada je $x \in A_m$ i $y \in A_n$ za neke $m, n \in I$, dakle $x, y \in A_{\max(m,n)}$. Pošto je grupoid $A_{\max(m,n)}$ komutativan važi $x \cdot y = y \cdot x$.

Po upravo dokazanom tvrđenju, parcijalno uređen skup $(K, \subset)$ je zatvoren za unije lanaca i neprazan (jer mu pripada trivijalni grupoid), i prema Zornovoj lemi ima maksimalni element, a to je upravo traženi podgrupoid. $\diamondsuit$

**1.8** Neka je $\mathbf{A}$ algebra jezika $L$ sa tačno $k$ elemenata. Izaberimo funkcijski simbol $F \in \mathrm{Fun}_L$; radi jednostavnosti uvedimo novi unarni funkcijski simbol $G(x) = F^{\mathbf{A}}(\underbrace{x, x, \ldots, x}_{\mathrm{ar}(F)\ \mathrm{puta}})$. Jasno je da svaki algebarski zakon jezika $L \cup \{G\}$ može da se "prevede" na jezik $L$ jednostavnom eliminacijom simbola $G$. Neka je $g$ operacija $G^{\mathbf{A}}$. Posmatrajmo niz operacija $g, g^2, g^3, \ldots, g^i, \ldots$ Pošto na skupu $A$ ima tačno $k^k$ unarnih operacija (Tvrđenje 1.1.5), postoje različiti $i, j \in N$ takvi da se operacije $g^i$ i $g^j$ poklapaju, dakle u $\mathbf{A}$ važi zakon $G^i(x) = G^j(x)$. $\diamondsuit$

**Napomena** *Primer beskonačne algebre u kojoj ne važi ni jedan netrivijalan algebarski zakon je term algebra iz Zadatka 1.6.*

**1.9** **a.** Relacija $\leq$ je: refleksivna, pošto je $x = x \wedge x$; antisimetrična, pošto iz $x = x \wedge y$ i $y = y \wedge x$ sledi $x = y$; i tranzitivna, pošto iz $x = x \wedge y$ i $y = y \wedge z$ sledi $x = (x \wedge y) \wedge z = x \wedge z$. $\square$ **b.** Ako $x \leq y$ onda $x = x \wedge y$, pa $x \vee y = (x \wedge y) \vee y = y$. Ako $y = x \vee y$ onda $x \wedge y = x \wedge (x \vee y) = x$. $\square$ **c.** Na osnovu **b.** je $x \vee y \geq x, y$. Pretpostavimo da je $z \geq x, y$; tada je $z = x \vee z$ i $z = y \vee z$ i $z \wedge (x \vee y) = (z \vee (x \vee y)) \wedge (x \vee y) = x \vee y$, pa je $z \geq x \vee y$; dakle $x \vee y = \sup\{x, y\}$. $\square$ Tvrđenje $x \wedge y = \inf\{x, y\}$ se dokazuje na sličan način. $\square$ **d.** Pošto je $((x \vee y) \wedge z) \wedge (x \wedge z) = ((x \vee y) \wedge x) \wedge z = x \wedge z$, imamo $(x \vee y) \wedge z \geq x \wedge z$ (na osnovu **c.**). Izmenom mesta $x$ i $y$ u ovoj formuli dobijamo $(x \vee y) \wedge z \geq y \wedge z$, dakle $(x \vee y) \wedge z \geq (x \wedge z) \vee (y \wedge z)$. $\diamondsuit$

**1.11** **a.** $\Leftrightarrow$ **b.** Za sve $a, b, c$ važi sledeće:

$$
\begin{aligned}
& a \wedge b \leq c, \quad a \leq b \vee c \quad \text{implicira} \quad a \leq c \\
& \quad \text{akko} \quad \exists x((a \wedge b) \vee x = c \wedge a \leq b \vee (a \wedge b) \vee x) \quad \text{implicira} \quad a \leq c \\
& \quad \text{akko} \quad \forall x((a \wedge b) \vee x = c, \quad a \leq b \vee x) \quad \text{implicira} \quad a \leq c) \\
& \quad \text{akko} \quad a \leq b \vee x \quad \text{implicira} \quad a \leq (a \wedge b) \vee x \\
& \quad \text{akko} \quad \exists z \ \ a = (b \vee x) \wedge z \quad \text{implicira} \quad a \leq (a \wedge b) \vee x \\
& \quad \text{akko} \quad \forall z (a = (b \vee x) \wedge z \quad \text{implicira} \quad a \leq (a \wedge b) \vee x) \\
& \quad \text{akko} \quad (b \vee x) \wedge z \leq (b \wedge z) \vee x \\
& \quad \text{akko} \quad (y \vee x) \wedge z \leq (y \wedge z) \vee x \qquad (y = b) \quad \square
\end{aligned}
$$

**b.** $\Longrightarrow$ **c.** Dokazujemo da u **c.** važi relacija $\leq$.

$$
\begin{aligned}
& (x \vee y) \wedge z \leq (x \wedge z) \vee y \\
\Leftrightarrow\ & (x \vee y) \wedge z \leq ((x \wedge z) \vee y) \wedge z \qquad (\text{pošto je } a \wedge b \leq c \Leftrightarrow a \wedge b \leq c \wedge b) \\
& \qquad \leq (x \wedge z) \vee (y \wedge z) \qquad (\text{iz } \mathbf{b.} \text{ zamenom } x \text{ sa } (x \wedge z)) \quad \square
\end{aligned}
$$

**c.** $\Longrightarrow$ **b.** Imamo $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \leq (x \wedge z) \vee y$. $\diamondsuit$

**1.12** Asocijativnost sabiranja: $((f+g)+h)(x) = (f+g)(x)+h(x) = f(x)+g(x)+h(x) = f(x) + (g+h)(x) = (f + (g+h))(x)$. Ostale aksiome prstena se proveravaju na sličan način. Jedinični element je identičko preslikavanje, $i_A$. $\diamondsuit$

**1.15** Ako su $f, g$ automorfizmi iz (respektivno) $\mathrm{Aut}(\mathbf{A})$ i $\mathrm{Aut}(\mathbf{B})$, definišimo funkciju $\phi(f,g)\colon A \times B \to A \times B$ sa $\phi(f,g)(x,y) = \langle f(x), g(y) \rangle$. Ovim je definisano preslikavanje $\phi\colon \mathrm{Aut}(\mathbf{A}) \times \mathrm{Aut}(\mathbf{B}) \to \mathrm{Aut}(\mathbf{A} \times \mathbf{B})$ za koje se lako proveri da je $1-1$ i homomorfizam. $\diamondsuit$

**Napomena** *Preslikavanje $\phi$ može, ali ne mora da bude izomorfizam. Uzmimo da je $\mathbf{A} = (Z_2, +_2, 0)$ i $\mathbf{B} = (Z_3, +_3, 0)$ kao primer kada $\phi$ jeste izomorfizam i bilo koje $\mathbf{A} = \mathbf{B}$ kao primer kada $\phi$ nije izomorfizam (pogledati rešenje zadatka 1.18.)*

**1.17** Trivijalan primer je prebrojiva algebra praznog jezika. Interesantniji primer nam daje vektorski prostor $\mathbf{V}$ nad poljem $\mathbf{Q}$ dimenzije $\aleph_0$. Neka je baza prostora $\mathbf{V}$ skup $\{e_i \,|\, i \in N\}$; tada se lako proveri da je baza prostora $\mathbf{V}^n$ skup svih $n$-torki vektora iz $\{e_i \,|\, i \in N\}$, dakle jeste dimenzije $\aleph_0$. Svaka dva vektorska prostora iste dimenzije nad istim poljem su izomorfna, pa je $V^n \cong V$. Da bi dobili **algebru** sa traženom osobinom, uzmimo aditivnu grupu $\mathbf{A} = (V, +, \mathbf{0})$ ovog vektorskog prostora; prema prethodnom važi $\mathbf{A}^n \cong \mathbf{A}$ za sve $n \in N$. $\diamondsuit$

**Napomena** *Primetimo da i bilo koja algebra oblika $\mathbf{A}^N$ zadovoljava uslove zadatka ($\mathbf{A}$ je neka netrivijalna algebra.) Ovakva algebra je uvek neprebrojiva (tačnije, bar kardinalnosti kontinuuma), dok je u rešenju dat primer prebrojive algebre sa traženom osobinom.*

**1.18** Izomorfizam je funkcija $f\colon \mathbf{A} \to \mathbf{A}$ definisana sa $f(\langle x, y \rangle) = \langle y, x \rangle$. $\diamondsuit$

**1.19** Iskoristite rešenje prethodnog zadatka da bi pokazali da svakoj bijekciji $f\colon N \to N$ može da se pridruži $h_f \in \mathrm{Aut}\mathbf{A}^N$, tako da je pridruživanje $f \to h_f$ bijekcija. $\diamondsuit$

**Napomena** *Prema prethodnom zadatku, prsten realnih nizova* $\mathbf{R}^N$ *ima bar* $2^{\aleph_0}$ *automorfizama. Dokažimo da automorfizama ima upravo* $2^{\aleph_0}$*. Neka je* $V$ *vektorski prostor dimenzije* $\aleph_0$ *nad poljem* $\mathbf{R}$*; imamo* $\left|\mathrm{Aut}\mathbf{R}^N\right| = |\mathrm{Aut}V| = |\{E = \langle e_i \,|\, e_i \in V, i \in N\rangle \mid$ *skup* $E$ *čini bazu za* $V\}|$ *(jer za datu bazu* $B$ *vektorskog prostora* $V$ *i* $f \in \mathrm{Aut}V$ *skup* $f(B)$ *je baza od* $V$*, a ovako se može dobiti svaka baza od* $V$*). Odredimo broj baza od* $V$*. Vektor* $e_i$ *(*$i \in N$*) biramo iz skupa* $\mathbf{R}^N$*; dakle postoji* $2^{\aleph_0}$ *mogućnosti. Prema tome, različitih nizova* $\langle e_i \,|\, e_i \in V, i \in N\rangle$ *vektora ima* $\prod_{i<\aleph_0} 2^{\aleph_0} = 2^{\aleph_0}$*, pa i baza ima najviše toliko. Da bi konstruisali tačno* $2^{\aleph_0}$ *baza, primetimo da su za fiksiranu bazu* $E = \langle e_i \,|\, i \in N\rangle$ *se baze* $E_r = \langle re_i \,|\, i \in N\rangle$ *(za* $r \in R$*) različite. Ovim je dokaz završen.*

**1.20** **a.** Neka je $\mathbf{A} = \{a_i \,|\, i = 1, 2, \ldots, n\}$, definišimo operaciju $\circ$ tako da važi

$$a_i^2 = \begin{cases} a_{i+1}, & i = 1, 2, \ldots, n-1 \\ a_1, & i = n. \end{cases}$$

Jasno je da svaka podalgebra koja sadrži $a_i$ sadrži i $a_{i+1}$, $a_{i+2}$, kao i sve ostale elemente skupa $A$. **b.** Neka je $\mathbf{A} = \{a_i \,|\, i \in N\}$, operaciju $\circ$ definišemo sa $a_i \circ a_j = a_{i+\mathrm{sgn}(1+i-j)}$ za sve $i, j \in N$. **c.** Neka je $\mathbf{A}$ algebra prebrojivog jezika $L$. Naći ćemo podalgebru algebre $\mathbf{A}$ koja je najviše prebrojiva. Izaberimo element $a \in A$. Na osnovu Teoreme 1.9.8 imamo $|\langle\{a\}\rangle_{\mathbf{A}}| \leq \aleph_0$, dakle $\langle\{a\}\rangle_{\mathbf{A}}$ je prava podalgebra algebre $\mathbf{A}$, čime je dokaz završen. $\diamondsuit$

**Napomena** *Ambicioznijem čitaocu savetujemo da izvede direktan dokaz tvrđenja pod* **c.** *direktnom konstrukcijom podalgebre* $\langle\{a\}\rangle_{\mathbf{A}}$ *kao unije prebrojivog rastućeg niza prebrojivih skupova. Ovakve konstrukcije se često sreću u Teoriji modela i Teoriji skupova.*

**Napomena** *Postavlja se i sledeće pitanje: da li svaka bekonačna algebra ima pravu podalgebru iste kardinalnosti? Negativan odgovor na ovo pitanje je 1975. godine dao izraelski matematičar S. Shelah koji je konstruisao grupu kardinalnosti* $\aleph_1$ *bez prave neprebrojive podgrupe. Ovakve grupe (algebre) nazivamo Jóhnsonovim.*

**1.21** Neka je $\mathbf{G} = (G, +, -, 0)$ generisana elementom $e$. Definišimo preslikavanje $f\colon Z \to G$ sa $f(1) = e$. Ako definišmo $f(n)$ za ostale $n \in Z$ kao u Primeru 1.9.2-1, dobijeno preslikavanje će biti homomorfizam. Pošto je grupa $\mathbf{G}$ generisana elementom $e$, preslikavanje $f$ je na. Dokažimo još i da je $f$ $1-1$; ukoliko ovo nije tačno, postoje $m, n \in Z$ takvi da je $f(m) = f(n)$. Bez gubitka opštosti pretpostavimo da je $m > n$, dakle $f(m-n) = 0$, tj. $\underbrace{e + e + \cdots + e}_{m-n \text{ puta}} = 0^{\mathbf{G}}$. Iz ovoga sledi da grupa $\mathbf{G}$ ima konačno mnogo (najviše $m - n$) elemenata, što je kontradikcija. Ovim je dokaz završen. $\diamondsuit$

**1.22** Dokažimo prvo sledeću varijantu Primera 1.9.2-2:

*Svaka konačno generisana podgrupa aditivne grupe celih brojeva je generisana jednim elementom, i prema tome izomorfna aditivnoj grupi celih brojeva ili trivijalnoj grupi.*

**Dokaz** Dovoljno je dokazati da tvrđenje važi za podgrupe generisane sa dva elementa, recimo $m$ i $n$. Pretpostavimo bez gubitka opštosti da bar jedan od brojeva $m$ i $n$ nije 0. Na osnovu Bézoutove teoreme,

$$\mathrm{NZD}(m, n) = \min(\{xm + yn \,|\, x, y \in Z\} \cap N^+) = \min(\langle m, n\rangle_{\mathbf{Z}} \cap N^+).$$

Dakle, $\langle m, n\rangle_{\mathbf{Z}} = \langle \mathrm{NZD}(m, n)\rangle_{\mathbf{Z}}$. Ova grupa je beskonačna pošto je $\mathrm{NZD}(m, n) \neq 0$, i po prethodnom zadatku je izomorfna grupi $\mathbf{Z}$.

Vratimo se na tvrđenje zadatka. Primetimo da za sve $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in Q$ važi

$$\begin{aligned}\left\langle \frac{m_1}{n_1}, \frac{m_2}{n_2} \right\rangle_{\mathbf{Q}} &= \left\{ \frac{xm_1n_2 + ym_2n_1}{n_1n_2} \,\middle|\, x, y, \in Z \right\} = \left\{ \frac{z}{n_1n_2} \,\middle|\, z \in \langle m_1n_2, m_2n_1 \rangle_{\mathbf{Z}} \right\} \\ &= \left\{ \frac{z}{n_1n_2} \,\middle|\, z \in \langle \mathrm{NZD}(m_1n_2, m_2n_1) \rangle_{\mathbf{Z}} \right\} = \left\{ t\frac{\mathrm{NZD}(m_1n_2, m_2n_1)}{n_1n_2} \,\middle|\, t \in Z \right\} \\ &= \left\langle \frac{\mathrm{NZD}(m_1n_2, m_2n_1)}{n_1n_2} \right\rangle_{\mathbf{Q}}.\end{aligned}$$

Dakle, svaka konačno generisana podgrupa grupe **Q** je generisana jednim elementom, i prema tome je izomorfna grupi **Z** ili je trivijalna.

*Grupa* **Q** *nije izomorfna grupi* **Z**.

**Dokaz** Jednačina $2x = 1$ ima rešenje u $Z$, ali nema rešenje u $Q$.

Pošto je svaka netrivijalna konačno generisana podgrupa grupe **Q** izomorfna sa **Z**, a grupa **Q** nije izomorfna sa **Z**, dokaz je završen. $\diamondsuit$

**1.23** Neka je $X$ konačan skup takav da je $\mathbf{A} = \langle X \rangle_{\mathbf{A}}$. Dokažimo prvo da je algebra **A** prebrojiva. Po Teoremi 1.9.9 imamo$|A| = |\langle X \rangle_{\mathbf{A}}| = \max\{\aleph_0, |L|, |X|\}$. Po Teoremi 1.9.1 svaki endomorfizam $f \in \mathrm{End}\mathbf{A}$ je jednoznačno određen restrikcijom $f \restriction X$. Ali različitih funkcija $g: X \to A$ ima tačno koliko i nizova dužine $|X|$ koji se sastoje od elemenata skupa $A$; pošto je $X$ konačan, takvih nizova ima $\aleph_0$, dakle $|\mathrm{End}\mathbf{A}| \leq \aleph_0$, s obzirom na činjenicu da ne mora svaka $f: X \to A$ da bude proširiva do endomorfizma. $\diamondsuit$

**Napomena** *Primer algebre* $\mathbf{A} = \langle X \rangle_{\mathbf{A}}$ *takve da je skup generatora* $X$ *minimalan, ali postoji preslikavanje* $f: X \to A$ *koje nije proširivo do endomorfizma je, recimo,* $\mathbf{A} = \langle Z, + \rangle$ *i* $X = \{1, -1\}$*; preslikavanje* $f$ *je definisano sa* $f(1) = f(-1) = 1$.

**1.24** Neka je $X = \{x_1, x_2, \ldots, x_n\}$ konačan skup takav da je $\mathbf{A} = \langle X \rangle_{\mathbf{A}}$, i neka je $P$ skup svih pravih podalgebri algebre **A** koje sadrže **B** uređen inkluzijom. Primetimo da je $P \neq \emptyset$ jer $\mathbf{B} \in P$. Dokažimo da je ovaj parcijalno uređen skup zatvoren za unije lanaca. Neka je $\langle \mathbf{B}_i, i \in I \rangle$ rastuća familija elemenata skupa $P$. Pretpostavimo da je $\mathbf{B}' = \bigcup_{i \in I} \mathbf{B}_i = \mathbf{A}$. Dakle $X \subset \mathbf{B}'$; neka je $m_i$ minimalan $i \in I$ takav da je $x_i \in B_{m_i}$. Označimo broj $\max\{m_i \mid i \leq n\}$ sa $m$, tada je $X \subset B_m$, dakle i $\mathbf{A} \subset B_m$, što je u kontradikciji sa pretpostavkom da je $B_m$ prava podalgebra. $\square$ Primenom Zornove leme dobijamo traženu maksimalnu pravu podalgebru. $\diamondsuit$

**1.25** U rešenju zadatka koristićemo sledeće činjenice koje se odnose na podskupove skupa realnih brojeva $R$:

1. *Za Borelove podskupove realne prave važi Kontinuum hipoteza (M. Suslin), naime ako je* $X \subseteq R$ *Borelov, onda je* $X$ *najviše prebrojiv, ili je* $X$ *moći kontinuuma. Specijalno, ukoliko je* $X$ *zatvoren, ili otvoren, ili je prebrojiva unija zatvorenih poskupova (tj.* $X$ *je* $F_\sigma$*), ili je prebrojiv presek otvorenih podskupova (tj.* $X$ *je* $G_\delta$ *skup) od* $R$*, onda važi* $|X| \leq \aleph_0$*, ili* $|X| = 2^{\aleph_0}$. $\square$

2. *Kantorov trijadski skup* $K$ *je zatvoren podskup od* $R$ *moći kontinuuma. (Podsećamo čitaoca da je* $K$ *skup svih realnih brojeva* $x \in [0,1]_R$*, koji zapisani u brojevnom sistemu sa osnovom 3, dakle pomoću cifara 0, 1, 2, imaju u zapisu jedino cifre 0 i 2).* $\square$

3. *Neka je na $X$ prebrojiv skup. Tada je $2^X \approx K$ (tj. $2^X$ je homeomorfan prostoru $K$); ovde je uzeta diskretna topologija na 2 ($2 = \{0,1\}$, v. 3. Poglavlje), $K$ je Kantorov trijadski skup, dok je na $2^X$ uzeta proizvodna (Tihonovljeva) topologija.* □

Radi jednostavnije notacije, pretpostavićemo da je $\mathbf{A} = (A, \cdot)$ grupoid; dokaz za proizvoljne prebrojive algebre teče na sličan način. Neka je $\mathcal{F}$ skup svih preslikavanja (karakterističnih funkcija) $k : A^2 \to 2$, koja zadovoljavaju sledeće uslove:

(1) $\forall a, a', b, b' \in A \ (k(a,a') = 1 \wedge k(b,b') = 1 \Rightarrow k(a \cdot b, a' \cdot b') = 1)$,

(2) $\forall a, a', b \in A \ (k(a,a') = 1 \wedge b \neq a \Rightarrow k(b,a') = 0)$,

(3) $\forall b \in A\, \exists a \in A \ k(a,b) = 1$.

Ako je $f \in \mathrm{Aut}\mathbf{A}$, neka je $k_f : A^2 \to 2$ definisana pomoću $k_f(a,b) = 1$ akko $b = f(a)$, $a, b \in A$. Tada nije teško proveriti da $k_f$ zadovoljava uslove (1), (2), (3), kao i da različitim automorfizmima $f$ i $f'$ odgovaraju različite funkcije $k_f$ i $k_{f'}$ (ako, na primer, $f(a) = b \neq f'(a)$, onda $k_f(a,b) = 1$, dok $k_{f'}(a,b) = 0$). S druge strane, ako $k \in \mathcal{F}$ i $f : A \to A$ je definisana pomoću $b = f(a)$ akko $k(a,b) = 1$, $a, b \in A$, onda $f \in \mathrm{Aut}\mathbf{A}$. Dakle, za $\phi : f \to k_f$, $f \in \mathrm{Aut}\mathbf{A}$, važi $\phi : \mathrm{Aut}\mathbf{A} \xrightarrow[\text{1-1}]{\text{na}} \mathcal{F}$, pa (4) $|\mathrm{Aut}\mathbf{A}| = |\mathcal{F}|$. □ Neka su $\mathcal{F}_1$, $\mathcal{F}_2$ i $\mathcal{F}_3$ skupovi funkcija $k : A^2 \to 2$ koje redom zadovoljavaju uslove (1), (2) i (3). Tada:

$$\begin{aligned}\mathcal{F}_1 &= \textstyle\bigcap_{a,a',b,b' \in A}(\{k \in 2^{A^2} \mid k(a,a') = 0\} \\ &\qquad \cup \{k \in 2^{A^2} \mid k(b,b') = 0\} \cup \{k \in 2^{A^2} \mid k(a \cdot b, a \cdot b') = 1\}) \\ \mathcal{F}_2 &= \textstyle\bigcap_{a,a' \in A}(\{k \in 2^{A^2} \mid k(a,a') = 0\} \cup \bigcap_{\substack{b \in A \\ b \neq a}}\{k \in 2^{A^2} \mid k(b,a') = 0\}) \\ \mathcal{F}_3 &= \textstyle\bigcap_{b \in A} \bigcup_{a \in A}\{k \in 2^{A^2} \mid k(a,b) = 1\}\end{aligned}$$

Neka je na $2^{A^2}$ definisana Tihonovljeva topologija, gde je na 2 uzeta diskretna topologija. Tada je skup $\{k \in 2^{A^2} \mid k(a,b) = \alpha\}$, $a, b \in A$, $\alpha \in 2$, otvoren i zatvoren, s obzirom na definiciju proizvodne topologije, i da su $\{0\}$ i $\{1\}$ otvoreno-zatvoreni podskupovi u 2. Dakle, $\mathcal{F}_1$ i $\mathcal{F}_2$ su zatvoreni, dok je $\mathcal{F}_3$ prebrojiv presek otvorenih skupova, pa kako je $\mathcal{F} = \mathcal{F}_1 \cap \mathcal{F}_2 \cap \mathcal{F}_3$, onda je $\mathcal{F}$ neki $G_\delta$ podskup u $2^X$. Prema tvrđenjima 2. i 3. možemo uzeti da je onda $\mathcal{F}$ prebrojiv presek otvorenih podskupova realne prave; dakle, prema tvrđenju 1. važi $|\mathcal{F}| \leq \aleph_0$ ili $|\mathcal{F}| = 2^{\aleph_0}$. Prema (4) onda sledi tvrđenje zadatka. ♢

**1.27** (Uporediti sa Posledicom 3.1.28.) Tvrđenje dokazujemo matematičkom indukcijom. Za $n = 1$ imamo $p_1 = \binom{0}{0}p_0 = 1$, što je tačno. Pretpostavimo da tvrđenje važi za $n = k$, i da je $A$ skup sa tačno $k+1$ elemenata. Fiksirajmo element $a$ iz $A$. Neka je $\sim$ relacija ekvivalencije skupa $A$, definišimo $A' = A \setminus [a] = \{x \in A \mid x \not\sim a\}$. Relacija $\sim$ je jednoznačno određena skupom $A'$ i restrikcijom $\sim'$ relacije $\sim$ na $A'$, koja je takođe relacija ekvivalencije, takođe svakom takvom paru $\langle A', \sim_1 \rangle$ odgovara jedinstvena relacija ekvivalencije $\sim$ skupa $A$. Dakle, relacija ekvivalencije skupa $A$ ima koliko i ovakvih parova; skup $A' \subset A$ sa tačno $i \leq k$ elemenata možemo izabrati na tačno $\binom{k}{i}$ načina, i na svakom takvom skupu ima tačno $p_i$ relacija ekvivalencije. Iz ovoga sledi $p_{k+1} = \sum_{i=0}^{k} \binom{k}{i} p_i$, čime je tvrđenje dokazano. □ Prema Posledici 3.1.28 važi $p_{100} = \sum_{i=1}^{100} s_i^{100}$, gde su $s_i^k$ Stirlingovi brojevi 2. vrste. U programskom jeziku *Mathematica* ova činjenica zapisuje se ovako: `Sum[StirlingS2[100,i],{i,100}]`, što daje rezultat:

```
47585391276764833658790768841387207826363669686825611466616334637559114497892442622672724044217756306953557882560751
```
♢

**1.28** Neka je $\sim$ kongruencija prstena celih brojeva, i neka je $n = \min\{k \in N \mid k \sim 0\}$. Dokazaćemo da je $x =_n y$ akko $x \sim y$. □ Neka je $x =_n y$. Tada za neki ceo broj $k$ važi $x = y + k \cdot n$, pa je $x \sim y$. Neka su $x \sim y$ takvi da nije $x =_n y$; neka je

$z = \min\{k > y \mid k =_n x\}$ (ovaj skup je po Arhimedovoj aksiomi neprazan). Tada je $0 < z - y < n$ i važi niz implikacija $z =_n x \Rightarrow z \sim x \Rightarrow z \sim y \Rightarrow z - y \sim 0$, što je u kontradikciji sa definicijom broja $n$. $\diamondsuit$

**1.31** Imamo $p \circ q \neq q \circ p \Leftrightarrow \exists x, y(\exists z(x\,p\,z \wedge z\,q\,y) \wedge \forall z \neg(x\,q\,z \wedge z\,p\,y) \Leftrightarrow x(p \circ q)y \wedge \neg(y(p \circ q)x \Leftrightarrow$ relacija $p \circ q$ nije simetrična. $\square$ Lako se proveri da ostale osobine relacije kongruencije važe i bez uslova $p \circ q = q \circ p$. $\diamondsuit$

**1.32** **a.** Dokazujemo netrivijalan deo ekvivalencije. $\square$ Pretpostavimo $y \leq z$, gde $y, z \in A$. Prema Zadatku 1.9.**d**, u proizvoljnoj mreži važi $(x \vee y) \wedge z \geq (x \wedge z) \vee (y \wedge z)$, što uz uslov $y \leq z$ daje $(x \vee y) \wedge z \geq (x \wedge z) \vee y$. Odatle, uz pretpostavku zadatka, sledi $(x \vee y) \wedge z = (x \wedge z) \vee y$. **b.** Za date kongruencije $p$, $q$, $r$ algebre $\mathbf{A}$ proveravamo modularan zakon: $q \subseteq r \Rightarrow (p \circ q) \cap r \subseteq (p \cap r) \circ q$. Neka su $a, b \in A$ takvi da je $(a, b) \in (p \circ q) \cap r$. Tada za neki $c \in A$ važi $a\,p\,c$ i $c\,q\,b$, kao i $a\,r\,b$. S obzirom na $q \subseteq r$, onda $c\,r\,b$, odnosno $b\,r\,c$. Iz $a\,r\,b$ i $b\,r\,c$ sledi $a\,r\,c$; prema tome $a(p \cap r)c$, tj. $(a, b) \in (p \cap r) \circ q$. $\diamondsuit$

**1.33** Dokazujemo samo **d.**, iz čega slede preostala tri tvrđenja (proveriti!). $\square$ Refleksivnost sledi iz (i), a simetričnost iz simetričnosti same definicije. Ako je $f \sim g$ i $g \sim h$, onda je $\{i \in N \mid f(i) = h(i)\} \supset \{i \in N \mid f(i) = g(i)\} \cup \{i \in N \mid g(i) = h(i)\}$, pa $f \sim h$ sledi iz (iii) i (ii). $\square$ Primetimo da se (iii) indukcijom lako dokazuje da je skup $\mathcal{S}$ zatvoren za konačne preseke. Neka je $F$ $n$-arni funkcijski simbol, i neka je $f_i \sim g_i$ $(i = 1, \ldots, n)$. Neka su skupovi $D_i \subset N$ definisani sa $D_i = \{k \in N \mid f_i(k) = g_i(k)\}$. Tada imamo $\{k \in N \mid F(f_1(k), \ldots, f_n(k)) = F(g_1(k), \ldots, g_n(k))\} \supset \bigcap_{i \leq n} D_i \in \mathcal{S}$, i na osnovu (ii) dokaz je završen. $\diamondsuit$

## 2. ALGEBRE SA RELACIJAMA

**2.1** Formule jezika $L$ su konačni nizovi simbola iz skupa $L_1 = L \cup \mathrm{Var} \cup \{(, ), ,\} \cup \{=, \neg, \vee, \wedge, \rightarrow, \leftrightarrow, \exists, \forall\}$, dakle $\|L\| \leq \max\{|L_1|, \aleph_0\} = \max\{|L|, \aleph_0\}$. $\diamondsuit$

**2.3** Neka su $x, y, z \in X$. Tada $x < y \wedge y < x \rightarrow x \leq y \wedge x \geq y \wedge x \neq y \rightarrow x = y \wedge x \neq y$, što je kontradikcija; dakle imamo $\neg(x < y \wedge y < x)$, što je logički ekvivalentno sa $x < y \rightarrow \neg y < x$. $\square$ Ako je $x < y \wedge y < z$, onda je $x \leq y \wedge y \leq z$ i $x \leq z$; ako važi $x = z$ imamo $x < y \wedge y < x$ što je u kontradikciji sa prethodnim, dakle $x < z$. $\square$ $x \leq' y \Leftrightarrow x < y \vee x = y \Leftrightarrow (x \leq y \wedge x \neq y) \vee x = y \Leftrightarrow (x \leq y \vee x = y) \wedge (x \neq y \vee x = y) \Leftrightarrow x \leq y$. $\diamondsuit$

**2.4** Dokazaćemo samo aksiomu regularnosti. Za $x \in V$ definišimo *rang* elementa $x$ sa $\mathrm{rang}(x) = \min\{n \in N \mid x \in V_n\}$. Skup sa desne strane jednakosti je neprazan, i po principu najmanjeg elementa $\mathrm{rang}(x)$ je dobro definisan. Ako je $x \in V_{n+1}$ onda su svi njegovi elementi u $V_n$; dakle $y \in x \rightarrow \mathrm{rang}(y) < \mathrm{rang}(x)$. $\square$ Ako je skup $x \in V$ neprazan, tada je i skup $\{\mathrm{rang}(y) \mid y \in x\}$ neprazan i ima najmanji element $m$. Neka je $y \in x$ ranga $m$, tada $z \in y \Rightarrow \mathrm{rang}(z) < m \Rightarrow \neg z \in x$, čime je dokaz završen. $\diamondsuit$

**2.5** Dokaz izvodimo indukcijom po složenosti formule $\varphi$. Ukoliko je formula $\varphi$ oblika $t_1 = t_2$ za neke terme $t_1$ i $t_2$, tvrđenje se svodi na činjenicu da homomorfizmi čuvaju algebarske zakone, a ukoliko je $\varphi$ oblika $R(t_1, \ldots, t_n)$ za neki $n$-arni relacijski simbol $R$, tvrđenje se svodi na definiciju homomorfizma. $\square$ Ako je $\varphi \equiv \psi \vee \theta$, onda ako $\mathbf{A} \models \varphi$ onda $\mathbf{A} \models \psi \vee \theta$, pa $\mathbf{A} \models \psi$ ili $\mathbf{A} \models \theta$; dakle $\mathbf{B} \models \psi$ ili $\mathbf{B} \models \theta$, i konačno $\mathbf{B} \models \psi \vee \theta$, drugim rečima, $\mathbf{B} \models \varphi$. $\square$ Ako je $\varphi \equiv \exists x \psi$, onda $\mathbf{A} \models \varphi$, pa $\mathbf{A} \models \exists x \psi(x)$, i postoji $a \in A$ takav da $(\mathbf{A}, \mathbf{a}) \models \psi(\mathbf{a})$; tada $(\mathbf{B}, h(\mathbf{a})) \models \psi(h(\mathbf{a}))$, pa $\mathbf{B} \models \exists x \psi(x)$ i $\mathbf{B} \models \varphi$. Ostali slučajevi se dokazuju na sličan način. $\diamondsuit$

**Napomena** *Važi i obrat ovog tvrđenja; dokaz se izvodi metodom korišćenim u Teoremi 2.3.15.*

**2.6** Teorija ove klase je $\mathrm{Ab} \cup \{\forall y \exists x\, n \cdot x = y \mid n \in N^+\}$. $\diamondsuit$

**2.8** Neka je $(A, \preceq)$ parcijalno uređen skup koji nije linearno uređen. Po Teoremi 2.3.6 postoji linearno uređenje $\preceq'$ domena $A$ koje proširuje $\preceq$. Tada za $h$ uzmimo identičko preslikavanje modela $\mathbf{A} = (A, \preceq)$ na $\mathbf{B} = (A, \preceq')$. $\diamondsuit$

**Napomena** *Moguće je naći modele* $\mathbf{A}$ *i* $\mathbf{B}$ *koji ispunjavaju uslove prethodnog zadatka i izomorfni su. Uzmimo* $\mathbf{A} = (N \times N, \prec)$, *gde je* $\prec$ *definisano sa* $(m_0, n_0) \prec (m_1, n_1)$ *akko* $m = m_0$ *i* $n_0 < n_1$. *Definišimo* $f\colon A \to A$ *sa* $f(2m, n) = (m, 2n)$ *i* $f(2m{+}1, n) = (m, 2n{+}1)$. *Tada je* $f\colon A \to A$ *bijekcija i homomorfizam, ali nije izomorfizam.*

**2.10** **a.** Pošto su svaka dva prebrojiva gusto uređena skupa bez krajeva izomorfna, dovoljno je da nađemo broj automorfizama strukture $(Q \times Q, \prec)$, gde je $(p_1, q_1) \prec (p_2, q_2)$ akko je $p_1 < p_2$ ili $p_1 = p_2$ i $q_1 < q_2$ (takozvano *leksikografsko uređenje*). Svakoj funkciji $f\colon Q \to \{0,1\}$ pridružimo $f^*\colon Q \times Q \to Q \times Q$ definisanu sa $f^*(p,q) = (p, q + f(p))$. Lako se proveri da je $f \mapsto f^*$ injekcija skupa ${}^Q\{0,1\}$ u skup $\mathrm{Aut}(Q \times Q, <)$, čime je dokaz završen. $\square$ **b.** Neka je $f \in \mathrm{Aut}(Q(\sqrt{2}), +, \leq, 0)$ i $m/n \in Q$; tada je $n \cdot m/n = m \cdot 1 \Rightarrow nf(m/n) = mf(1) \Rightarrow f(m/n) = m/nf(1)$ (Primetimo da je $f(1) > 0$, pošto je $f$ rastuće preslikavanje). Slično se dobija i $f(p + q\sqrt{2}) = pf(1) + qf(\sqrt{2})$. Preostaje samo da se dokaže da je $f(\sqrt{2}) = \sqrt{2}f(1)$. Pretpostavimo da je $\sqrt{2}f(1) < f(\sqrt{2})$ (drugi slučaj se dokazuje analogno); tada postoje $r, s \in Q$ takvi da je $\sqrt{2}f(1) < s = f(r) < f(\sqrt{2})$. Na osnovu leve nejednakosti imamo $\sqrt{2}f(1) < rf(1) \Rightarrow \sqrt{2} < r$, a na osnovu desne $r < \sqrt{2}$, što je kontradikcija. $\square$ **c.** sledi direktno iz **b.** $\diamondsuit$

**2.11** Neka je $f \in \mathrm{Aut}(R, +, \cdot, 0, 1)$; imamo $f(p) = p$ za sve $p \in Q$ (videti rešenje zadatka 2.10 **b.**). Dokaz da je $f(a) = af(1) = a$ za $a \in R \setminus Q$ je identičan sa dokazom da je $f(\sqrt{2}) = \sqrt{2}f(1)$ u 2.10 **b.** Dakle, jedini automorfizam je identičko preslikavanje $i_R$. $\diamondsuit$

**Napomena** *Tvrđenje prethodnog zadatka važi i ako posmatramo neuređeno polje realnih brojeva* $(R, +, \cdot, 0, 1)$, *jer se uređenje može definisati sa* $x < y \Leftrightarrow \exists z\, x + z^2 = y$.

**2.12** Neka je $T$ teorija klase $\mathfrak{M}$, $\kappa$ beskonačan kardinal, $C = \{c_i \mid i \in \kappa\}$ skup novih konstantnih simbola (tj. simbola koji se ne pojavljuju u jeziku teorije $T$), $T_C = \{c_i \neq c_j \mid i, j \in \kappa, i \neq j\}$ i $T' = T \cup T_C$. Dokažimo da teorija $T'$ ima model. Bilo koji konačan podskup $S$ teorije $T'$ je oblika $S_T \cup S_C$, gde je $S_T \subset T$ i $S_C \subset T_C$. Ali u skupu $S_C$ se pojavljuje samo konačno mnogo konstanata iz $C$, a u svakom beskonačnom modelu možemo naći $n$ različitih elemenata; dakle, bilo koji beskonačan $\mathbf{A} \in \mathfrak{M}$ je model za $S$. Po Stavu kompaktnosti (2.3.4) teorija $T'$ ima model i ovaj model je kardinalnosti $\geq \kappa$. $\square$ Pošto postoji beskonačno polje (recimo $\mathbf{Q}$), tvrđenje direktno sledi. $\diamondsuit$

**Napomena** *Pretpostavka prethodnog zadatka se može i oslabiti na: "*$\mathfrak{M}$ *je aksiomatska klasa koja ima modele proizvoljno velike konačne kardinalnosti". S druge strane, može se izvući i jači zaključak: "klasa* $\mathfrak{M}$ *ima model svake beskonačne kardinalnosti* $\geq |T|$*" (uporediti sa Napomenom posle rešenja zadatka 1.20.)*

**2.13** **a.** Pretpostavimo da je $T$ skup aksioma za teoriju cikličnih grupa. Na osnovu prethodnog zadataka postoji neprebrojiva ciklična grupa; ali svaka ciklična grupa može da ima najviše prebrojivo mnogo elemenata – kontradikcija. $\square$ **c.** Pretpostavimo da je $T$ teorija dorog uređenja. Neka je $C = \{c_i \mid i \in N\}$ skup novih konstantnih simbola, i

$T' = T \cup \{c_i < c_j \mid i > j \in N\}$. Ako je $S$ konačan podskup teorije $T$, onda važi $(\omega, <) \models S$ jer u $(\omega, <)$ postoji opadajući niz proizvoljne konačne dužine. Dakle postoji model teorije $T'$; ovaj model je dobro uređen i ima beskonačan opadajući niz, što je kontradikcija. $\diamondsuit$

**2.14** Dokažimo prvo sledeće tvrđenje:

*Ako je $T_1 \subset T_2 \subset \dots$ $(i \in N)$ niz teorija prvog reda takav da za svako $i \in N$ postoji model $\mathbf{A}_i$ takav da $\mathbf{A}_i \models T_i$ i $\mathbf{A}_i \not\models T_{i+1}$, onda teorija $T = \bigcup_{i\in N} T_i$ nije konačno aksiomatska.*

**Dokaz** Pretpostavimo da teorija $T$ ima konačan skup aksioma $S$. Neka je $\phi$ teorema teorije $T$; tada (prema definiciji dokaza u predikatskom računu prvog reda) postoji konačan skup formula $F_\phi$ iz $T$ takav da je $\phi$ dokaziva iz $F_\phi$; ovaj konačan skup je sadržan u nekom $T_i$ – označimo najmanji takav $i$ sa $i(\varphi)$. Neka je $i(S) = \max\{i(\varphi) \mid \varphi \in S\}$; tada je $S \subset T_{i(S)}$, i $\mathbf{A}_i \models S$. Ali $\mathbf{A}_i$ nije model teorije $T_{i(S)+1}$, što je kontradikcija. $\square$ **c.** Iskoristićemo rečenicu $\tau_n \equiv \exists x_1, \dots, x_n \bigwedge_{\substack{i,j\le n\\ i\neq j}} x_n \neq x_j$ koja je zadovoljena tačno u modelima koji imaju bar $n$ elemenata. Uzmimo za $T_n$ teoriju $\mathrm{Gp} \cup \{\tau_i \mid i \le n\}$, za $\mathbf{A}_n$ cikličku grupu reda $n$ i primenimo tvrđenje. $\diamondsuit$

**2.15** Iskoristiti pomoćno tvrđenje iz rešenja zadatka 1.14 i činjenicu da $T_1 \subset T_2 \Rightarrow \mathfrak{M}(T_1) \supset \mathfrak{M}(T_2)$. $\square$ Neka je $T(\mathfrak{M}) = \{\varphi \mid \mathbf{A} \models \varphi$ za svaki model $\mathbf{A} \in \mathfrak{M}\}$. Tada je traženi skup aksioma $T = \bigcup_{i\in N} T(\mathfrak{M}_i)$. Svaki konačan podskup od $T$ ima model, pa prema Stavu kompaktnosti $T$ ima model, dakle klasa $\mathfrak{M}$ je neprazna. $\diamondsuit$

**2.16** Koristeći rečenice $\tau_n$ iz rešenja zadatka 2.14 imamo $|A| = n \Rightarrow \mathbf{A} \models \tau_n \wedge \neg\tau_{n+1}$ povlači $\mathbf{B} \models \tau_n \wedge \neg\tau_{n+1} \Rightarrow |B| = n$, dakle $\mathbf{A}$ i $\mathbf{B}$ imaju isti broj elemenata. Važi i sledeće:

*Za svaki $a \in A$ postoji $b \in B$ takav da su modeli $(\mathbf{A}, \mathbf{a})$ i $(\mathbf{B}, \mathbf{b})$ elementarno ekvivalentni.*

**Dokaz** Pretpostavimo da ovo nije tačno. Tada za svaki $b \in B$ postoji formula $\varphi_b(x)$ takva da $(\mathbf{A}, \mathbf{a}) \models \varphi_b(\mathbf{a})$ i $(\mathbf{B}, \mathbf{b}) \models \neg\varphi_b(\mathbf{b})$. Neka je $\varphi(x)$ rečenica $\exists x \bigwedge_{b\in B} \varphi_b(x)$. Tada $\mathbf{A} \models \varphi$ i $\mathbf{B} \models \neg\varphi$, što je kontradikcija.

Neka je $A = \{a_1, \dots, a_n\}$. Primenjujući tvrđenje redom na modelima $\mathbf{A}$ i $\mathbf{B}$, $(\mathbf{A}, \mathbf{a}_1)$ i $(\mathbf{B}, \mathbf{b}_1)$, $(\mathbf{A}, \mathbf{a}_1, \mathbf{a}_2)$ i $(\mathbf{B}, \mathbf{b}_1, \mathbf{b}_2)$ ... dobijamo niz $\langle b_1, \dots, b_n\rangle$ takav da su modeli $(\mathbf{A}, \mathbf{a}_i)_{i=1,\dots,n}$ i $(\mathbf{B}, \mathbf{b}_i)_{i=1,\dots,n}$ elementarno ekvivalentni. Preslikavanje $f\colon A \to B$ definisano sa $f(a_i) = b_i$ $(i = 1, \dots, n)$ je izomorfizam; proveru prepuštamo čitaocu. $\diamondsuit$

**2.17** Pretpostavimo da se od nejednakosti u sistemu $S$ javlja samo $\ge$. Dodavanjem novih nepoznatih, $S$ je ekvikonzistentan sistemu $S'$ nad poljem $\mathbf{Q}$ – konjunkciji nekog sistema linearnih jednačina $S_1$, i nekog sistema linearnih nejednačina $S_2$ vida $x_i \ge 0$. $\square$ Skup rešenja $\mathcal{R}$ sistema $S'$ je *konveksan*: ako $\mathbf{a}, \mathbf{b} \in \mathcal{R}$ onda za $\alpha, \beta \in R$, $\alpha + \beta = 1$, važi $\alpha\mathbf{a} + \alpha\mathbf{b} \in \mathcal{R}$. $\square$ Najzad, iskoristiti činjenicu da je $Q^n$ gust u $R^n$ za $n \in N^+$. $\diamondsuit$

**2.18** Neka je $\mathbf{M} = (M, \oplus, \otimes)$ algebra kvadratnih matrica reda $n$ nad poljem $\mathbf{F} = (F, +, \cdot, 0, 1)$ (simboli $\oplus$ i $\otimes$ označavaju respektivno sabiranje i množenje matrica). Uzmimo jezik $L_F = \{\bullet, f_{ij} \mid i, j = 1, \dots, n\}$, gde je $\bullet$ binarni, a $f_{ij}$ unarni operacijski simboli, takvi da $\bullet\colon F \times M \to M$ (odgovara množenju matrice skalarom), a $f_{ij}\colon M \to F$ (ovde je $f_{ij}(M)$ element $i$-te vrsti i $j$-te koloni matrice $M$) za sve $i, j$. Aksiome su aksiome polja za $\mathbf{F}$ i (za sve $i, j \le n$):

**i.** $f_{ij}(a \bullet M) = a \cdot f_{ij}(M)$,
**ii.** $f_{ij}(M \oplus N) = f_{ij}(M) + f_{ij}(N)$, i
**iii.** $f_{ij}(M \otimes N) = \sum_{k=1}^{n} f_{ik}(M) \cdot f_{kj}(N)$.

Ovo su, u stvari, definicione sheme za matrične operacije, i $(\mathbf{M}, \mathbf{F}, \bullet, f_{ij})_{i,j\le n}$ je tražena dvodomenska algebra. $\diamondsuit$

## 3. BROJEVI

**3.3** **a.** Dokažimo tvrđenje indukcijom po $x$. Ukoliko je $x = 0$ imamo $y = 0 + y = 0 + z = z$ (videti Primer 3.1.6.) Ako tvrđenje važi za fiksirano $x$, onda $x' + y = x' + z \Leftrightarrow x + y' = x + z' \Leftrightarrow x = y$ (tvrđenje $x + y' = x' + y$ je dokazano u Primeru 3.1.6.) $\diamondsuit$

**3.4** Dokazaćemo samo antisimetričnost. Primetimo da na osnovu zadatka 3.3 **a.** i komutativnosti sabiranja imamo $x + z = x$ akko je $z = 0$. Imamo $x \le y \wedge y \le x \Rightarrow \exists z, t\ x + z = y \wedge y + t = x \Rightarrow \exists z, t\ x = (x + z) + t = x + (z + t) \Rightarrow z = t = 0 \Rightarrow x = y$. $\diamondsuit$

**3.6** Neka je $M \models$FPA. Definišemo $f\colon N \to M$ sa $f(0) = 0$ i $f(n') = f(n)'$. $\diamondsuit$

**Napomena** *Kažemo da je element nestandardnog modela Formalne aritmetike standardan akko je sadržan u početnom komadu modela izomorfnom sa $N$, dok su nestandardni elementi svi ostali (beskonačni) elementi.*

**3.7** **a.** Neka je $c$ novi simboli konstanti, i neka je $P$ skup prostih brojeva. Teorija $T$ je data sa $T = \mathrm{FPA} \cup \{\underline{x}|c : x \in P\}$ (ovde $x|c$ označava formulu $\exists y\, xy = c$). Na osnovu Stava kompaktnosti ova teorija ima model, a ovaj model možemo izabrati tako da bude prebrojiv (videti napomenu posle rešenja zadatka 2.12.) $\square$ **b.** Zadržimo oznake iz **a.** Neka je $X \subset P$ i neka je $T_X = \mathrm{FPA} \cup \{\underline{x}|c : x \in X\} \cup \{\neg \underline{x}|c : x \notin X\}$. Teorija $T_X$ ima prebrojiv model $\mathbf{A}$. Skup svih standardnih (videti resenje zadatka 3.6 i Napomenu) prostih brojeva koji dele $c^{\mathbf{A}}$ je upravo $X$. *(Primetimo da je $X$ pravi podskup skupa $\{x \in A \mid \mathbf{A} \models \underline{x}|c\}$; takođe $c$ nije jedinstven broj čiji je skup standardnih činilaca upravo $X$ – recimo i $c^2$ ima tu osobinu.)* Neka je $a$ nestandardni element modela aritmetike $\mathbf{A}$; označimo sa $X_a^{\mathbf{A}}$ skup $\{p \in P \mid \mathbf{A} \models \underline{p}|\underline{a}\}$. Pretpostavimo da ima $\kappa < 2^{\aleph_0}$ neizomorfnih prebrojivih modela aritmetike; tada različitih skupova $X \subset P$ takvih da je $X = X_a^{\mathbf{A}}$ za neke $a$ i $\mathbf{A}$ ima najviše $\aleph_0 \cdot \kappa = \kappa < 2^{\aleph_0}$, dakle postoji skup $X$ koji nije oblika $X_a^{\mathbf{A}}$ ni za jedan par $a, \mathbf{A}$. Ovo je kontradikcija, čime je dokaz završen. $\diamondsuit$

**3.8** Neka je $a = \langle x, y\rangle_K$ i $n = x + y$. Tada je $a = \binom{n+1}{2} + x$, pa je (pošto je $0 \le x \le n$) $n^2 + n - 2a \le 0$ i $n^2 + 3n - 2a \ge 0$, i imamo $(-3 + \sqrt{9 + 8a})/2 \le n \le (-1 + \sqrt{1 + 8a})/2$. S druge strane, označimo $f(a) = (-1 + \sqrt{1 + 8a})/2 - (-3 + \sqrt{9 + 8a})/2 = (2 + \sqrt{1 + 8a} - \sqrt{9 + 8a})/2$; funkcija $f(a)$ je rastuća, $f(0) = 0$ i $\lim_{a\to\infty} f(a) = 1$, dakle $f(a) < 1$ za sve $a \ge 0$. Prema tome, $x + y = n = \lceil(-3 + \sqrt{9 + 8a})/2\rceil = [(-1 + \sqrt{1 + 8a})/2]$, i $x = a - \binom{n+1}{2} = a - \langle 0, n\rangle_K$, $y = n - x = n - a + \binom{n+1}{2} = \langle n, 0\rangle_K - a$. $\diamondsuit$

**3.10** Neka je $f\colon A \to B \times C$ definisana sa $f(x) = (f_1(x), f_2(x))$, neka je $g\colon N \times A \times B \times C \to B \times C$ definisana sa $g(n, x, y, z) = (g_1(n, x, y, z), g_2(n, x, y, z))$. Tada na osnovu Teoreme rekurzije postoji jedinstvena funkcija $h\colon N \times A \to B \times C$ koja zadovoljava uslove $h(0, x) = (h_1(0, x), h_2(0, x))$ i (uz neformalniju notaciju koja olakšava čitljivost) $h(y + 1, x) = (g_1(y, x, h(y, x)), g_2(y, x, h(y, x)))$. Iz ovoga sledi jedinstevnost i egzistencija funkcija $h_1$ i $h_2$. $\diamondsuit$

**3.11** Pretpostavimo da je $\phi(x)$ aritmetički iskaz koji daje kontraprimer za tvrđenje zadatka. Tada postoji $n \in N$ takav da $\neg\phi(n)$. Neka je $m = \min_k\{k > n \mid \phi(k)\}$ (pošto je skup $\{k \mid \phi(k)\}$ beskonačan, $m$ je dobro definisan). Tada (na osnovu pretpostavke zadatka) važi $\phi(m - 1)$, dok prema definiciji boja $m$ važi $\neg\phi(m - 1)$ – kontradikcija. $\diamondsuit$

**3.12** Dokažimo tvrđenje primenom regresivne indukcije (zadatak 3.11). Neka $S(k)$ označava tvrđenje "Jensenova nejednakost je tačna za $n = k$" Ako važi $S(n)$, onda za sve $x_1, \ldots, x_{2n} \in R$ imamo

$$\begin{aligned} f\left(\tfrac{1}{2n}\sum_{i=1}^{2n} x_i\right) &= f\left(\frac{\frac{1}{n}\sum_{i=1}^{n} x_i + \frac{1}{n}\sum_{i=n+1}^{2n} x_i}{2}\right) \\ &\leq \frac{1}{2}\left(f\left(\tfrac{1}{n}\sum_{i=1}^{n} x_i\right) + f\left(\tfrac{1}{n}\sum_{i=n+1}^{2n} x_i\right)\right) \\ &\leq \frac{1}{2}\left(\tfrac{1}{n}\sum_{i=1}^{n} f(x_i) + \tfrac{1}{n}\sum_{i=n+1}^{2n} f(x_i)\right) = \frac{\sum_{i=1}^{2n} f(x_i)}{2n}, \end{aligned}$$

dakle važi i $S(2n)$. Pošto je $S(1)$ tačno, imamo da $S(k)$ važi za beskonačnačno mnogo prirodnih brojeva. □ Pretpostavimo da važi $S(n+1)$; tada je

$$\begin{aligned} f\left(\tfrac{1}{n}\sum_{i=1}^{n} x_i\right) &= f\left(\tfrac{1}{n+1}\left(\sum_{i=1}^{n} x_i + \tfrac{1}{n}\sum_{i=1}^{n} x_i\right)\right) \\ &\leq \frac{1}{n+1}\left(\sum_{i=1}^{n} f(x_i) + \tfrac{1}{n}\sum_{i=1}^{n} f(x_i)\right) = \frac{1}{n}\sum_{i=1}^{n} f(x_i). \end{aligned}$$

Na osnovu regresivne indukcije $S(n)$ važi za sve $n \in N$. □ Iskoristiti Jensenovu jednakost sa $f(x) = \ln(x)$. ◊

**3.13** Označimo sa $P$ skup svih prostih brojeva. Neka je $n$ prirodan broj, definišimo funkciju $f\colon P \times N \to N$ sa $f(p,n) = \max\{k : p^k | n\}$. Sada iskoristimo Osnovnu teoremu aritmetike; imamo

$$f(p, \mathrm{NZD}(a,b)) = \min(f(p,a), f(p,b)) \text{ i } f(p, \mathrm{NZS}(a,b)) = \max(f(p,a), f(p,b))$$

za sve $p \in P$. Prema tome, $f(p, \mathrm{NZS}(a,b)\mathrm{NZD}(a,b)) = f(p, ab)$ za sve $p \in P$; ponovnim korišćenjem Osnovne teoreme algebre završavamo dokaz. ◊

**3.14** **a.** Ako je matrica $A = \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix}$ imamo $A^n = \begin{Vmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{Vmatrix}$, i $f_{n+1}f_{n-1} - f_n^2 = \det A^n = (\det A)^n = (-1)^n$. ◊

**3.15** **a.** Na osnovu formule 3.1.39 imamo

$$\begin{aligned} 2^n f_n &= \frac{1}{\sqrt{5}}\left(\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n\right) \\ &= \frac{1}{\sqrt{5}}\left(\sum_{k=o}^{n}\binom{n}{k}\left(\sqrt{5}^k - (-1)^k\sqrt{5}^k\right)\right) = 2\sum_{k\in 2N+1}\binom{n}{k}5^{(k-1)/2}. \end{aligned}$$

**b.** Sledi iz **a.** i činjenice da $p|\binom{p}{k}$ za svaki prost broj $p$ (pošto je $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$, a u imeniocu $p$ ne figuriše kao činilac), i, prema Maloj Fermaovoj teoremi, $2^{p-1} = 1 \bmod p$, gde je $p > 2$ prost broj. ◊

**3.17** **g.** Rešenje ovog zadatka daje opšti metod za nalaženje sličnih suma. Neka je $\epsilon = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, dakle $\epsilon^3 = 1$. Definišimo cele brojeve $A_n$, $B_n$ i $C_n$ sa $(1+\epsilon)^n = A_n + B_n\epsilon + C_n\epsilon^2$, dakle $A_n = \binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \ldots$, $B_n = \binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \ldots$, i $C_n = \binom{n}{2} + \binom{n}{5} + \binom{n}{8} + \ldots$. Takođe je $(1+\epsilon)^{n+1} = (1+\epsilon)(A_n + B_n\epsilon + C_n\epsilon^2) = (A_n + C_n) + (B_n + A_n)\epsilon + (C_n + B_n)\epsilon^2$, u matričnom zapisu

$$\begin{Vmatrix} A_{n+1} \\ B_{n+1} \\ C_{n+1} \end{Vmatrix} = M \begin{Vmatrix} A_n \\ B_n \\ C_n \end{Vmatrix} = M^{n+1} \begin{Vmatrix} 1 \\ 0 \\ 0 \end{Vmatrix}, \qquad \text{gde je } M = \begin{Vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{Vmatrix}.$$

Metodima linearne algebre nalazimo da je $M^n$ jednako

$$\frac{1}{3}\begin{Vmatrix} 2^n + 2\cos\frac{n\pi}{3} & 2^n - \cos\frac{n\pi}{3} - \sqrt{3}\sin\frac{n\pi}{3} & 2^n - \cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3} \\ 2^n - \cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3} & 2^n + 2\cos\frac{n\pi}{3} & 2^n - \cos\frac{n\pi}{3} - \sqrt{3}\sin\frac{n\pi}{3} \\ 2^n - \cos\frac{n\pi}{3} - \sqrt{3}\sin\frac{n\pi}{3} & 2^n - \cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3} & 2^n + 2\cos\frac{n\pi}{3} \end{Vmatrix}.$$

Iz ovoga se dobija

$$\begin{Vmatrix} A_n \\ B_n \\ C_n \end{Vmatrix} = \begin{Vmatrix} \frac{1}{3}\left(2^n + 2\cos\frac{n\pi}{3}\right) \\ \frac{1}{3}\left(2^n - \cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3}\right) \\ \frac{1}{3}\left(2^n - \cos\frac{n\pi}{3} - \sqrt{3}\sin\frac{n\pi}{3}\right) \end{Vmatrix}, \qquad \text{i konačno}$$

$$\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \cdots = \frac{1}{3}\left(2^n - \cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3}\right) = \frac{1}{3}\left(2^n + 2\cos\frac{(n-2)\pi}{3}\right). \ \Diamond$$

**3.18** Dokaz izvodimo indukcijom po $m$. Za $m = 1$ formula se svodi na $x_1^n = x_1^n$. Pretpostavimo da je formula tačna za $m$; imamo

$$\begin{aligned}
\left(\sum_{k=1}^{m+1} x_k\right)^n &= \left(\sum_{k=1}^{m-1} x_k + (x_m + x_{m+1})\right)^n \\
&= \sum_{k_1+\cdots+k_m=n} \frac{n!}{k_1!\ldots k_m!} x_1^{k_1}\ldots x_{m-1}^{k_{m-1}}(x_m + x_{m+1})^{k_m} \\
&= \sum_{k_1+\cdots+k_m=n} \frac{n!}{k_1!\ldots k_m!} x_1^{k_1}\ldots x_{m-1}^{k_{m-1}} \sum_{i=1}^{k_m} \frac{k_m!}{i!(k_m-i)!} x_m^i x_{m+1}^{k_m-i} \\
&= \sum_{k_1+\cdots+k_m=n} \sum_{i=1}^{k_m} \frac{n!}{k_1!\ldots k_m!} \frac{k_m!}{i!(k_m-i)!} x_1^{k_1}\ldots x_{m-1}^{k_{m-1}} x_m^i x_{m+1}^{k_m-i} \\
&= \sum_{k_1+\cdots+k_{m+1}=n} \frac{n!}{k_1!\ldots k_{m+1}!} x_1^{k_1}\ldots x_{m+1}^{k_{m+1}}
\end{aligned} \qquad \Diamond$$

**3.19** Skup svih polinoma stepena $\leq n$ nad poljem $\mathbf{R}$ deljivih sa $x$ čini vektorski prostor. Jednu bazu ovog prostora čini skup $E_1 = \langle x, \ldots, x^n \rangle$, a drugu $E_2 = \langle x, x(x-1), \ldots, x^{(n)} \rangle$. Na osnovu Posledice 3.1.31, matrica $A$ je matrica prelaska sa $E_2$ na $E_1$, dok je na osnovu definicije Stirlingovih brojeva prve vrste $B$ matrica prelaska sa baze $E_1$ na bazu $E_2$; dakle $A \cdot B$ je matrica identičkog preslikavanja. $\diamondsuit$

**3.20** **a.** Na osnovu Posledice 3.1.31 imamo $x^n = \sum_{i=0}^n s_i^n x^{(i)}$. Primenom linearnog operatora $\Delta^k$ (Definicija 3.1.34) na ovu jednakost dobijamo $\Delta^k x^n = \sum_{i=0}^n s_i^n \Delta^k x^{(i)} = \sum_{i=k}^n s_i^n k(k-1)\ldots(k-i+1)x^{(k-i)}$. Zamenom $x = 0$ dobijamo $\Delta^k 0^n = s_k^n k!$, i $s_k^n = \dfrac{1}{k!}\Delta^k 0^n$. $\square$
**b.** Primetimo da je $(1+x)^n = \sum_{i=0}^n \binom{n}{i} x^n$ i $x^n = ((1+x)-1)^n = \sum_{i=0}^n (-1)^{n-i}\binom{n}{i}(1+x)^i$. Za vektorske prostore $\mathcal{L}(x, \ldots, x^n)$ i $\mathcal{L}(x+1, \ldots, (x+1)^n)$ matrice $A = \left\| \binom{n}{i} \right\|_{1 \leq i,n \leq m}$ i $B = \left\| (-1)^{n-i}\binom{n}{i} \right\|_{1 \leq i,n \leq m}$ definišu linearne operatore čija je kompozicija identičko preslikavanje, i imamo da su $A$ i $B$ uzajamno inverzne. $\square$ Neka je $k_k^n = |\{f \mid f\colon n \xrightarrow{na} k\}|$; imamo da je $k_k^n = k! s_k^n$ (Posledica 3.1.29). Takođe je

$$n^k = |\{f \mid f\colon n \to k\}| = \left| \bigcup_{i=1}^n \{f \mid f\colon n \to k, |\mathrm{codom}(f)| = i\} \right| = \sum_{i=1}^n \binom{n}{i} k_i^n.$$

Pošto su matrice $A$ i $B$ uzajamno inverzne dobijamo jednakost $k_i^n = \sum_{j=1}^n (-1)^{i-j}\binom{n}{j} j^n$ (kao u zadatku 3.19), i konačno $s_k^n = \frac{1}{k!}\sum_{j=1}^n (-1)^{i-j}\binom{n}{j} j^n$. $\square$ **c.** Brojevi sa leve i desne strane jednakosti predstavljaju broj particija skupa sa $n+1$ elemenata na $k+1$ delova. $\diamondsuit$

**3.23** Posmatrajmo niz brojeva $10, 10^2, \ldots, 10^{n^2+1}$ i niz ostataka $r_1, \ldots, r_{n^2+1}$ dobijenih pri deljenju ovih brojeva sa $n$. Među tim ostacima ima $n$ jednakih (Dirišleov princip), neka su to $r_{i_1}, \ldots, r_{i_n}$. Tada je broj $\sum_{j=1}^n 10^{i_j}$ deljiv sa $n$. $\diamondsuit$

**3.26** U rešenju koristimo činjenicu da je zapis broja u sistemu sa osnovom 4 jedinstven. **a.** Ukoliko je $n = 4^a + 4^b + 4^c + 4^d$ i važi $a < b < c < d$, broj $n$ možemo zapisati u obliku $a_i + a_j$ $(i \neq j)$ na sledeća tri načina:

$$(*) \qquad (4^a + 4^b) + (4^c + 4^d), \qquad (4^a + 4^c) + (4^b + 4^d), \qquad \text{i} \qquad (4^a + 4^d) + (4^b + 4^c).$$

Ako su neki od brojeva $a, b, c, d$ jednaki, broj reprezentacija se smanjuje na 1 ili 0. $\square$
**b.** Definišimo funkciju $f\colon [N]^2 \to r+1$ sa: $f(i,j) = k$ akko $4^i + 4^j \in A_k$. Po Ramzejevoj teoremi (3.5.11) postoji beskonačan $X \subset N$ i $l \leq r$ takvi da je $4^i + 4^j \in A_l$ za sve $i, j \in X$. Svaki broj oblika $4^a + 4^b + 4^c + 4^d$ $(a, b, c, d$ su različiti elementi skupa $X)$ se može zapisati u obliku $a_i + a_j$ $(a_i, a_j \in A_l)$ na tačno tri načina (kao u $(*)$). $\diamondsuit$

**3.27** Evo najpre nekoliko definicija. Za familiju $\langle A_i \mid i \in I \rangle$ različitih elemenata parcijalno uređenog skupa $\mathbf{X} = (X, \leq)$ kažemo da čini *antilanac* ako su svaka dva različita člana te familije međusobno neuporediva. Podskup $L \subseteq X$ je *lanac* u $\mathbf{X}$ ako su svaka dva člana iz $L$ međusobno uporediva u odnosu na $\leq$. Najzad, podskup $L \subseteq X$ je *maksimalan lanac* ako $L$ nije sadržan kao pravi podskup niti u jednom lancu od $\mathbf{X}$. $\square$

Dokažimo sledeće tvrđenje.

**Teorema** *Neka je* $A_1, A_2, \dots, A_m$ *antilanac parcijalno uređenog skupa* $(P(X), \subseteq)$, *gde je* $X$ *skup od* $n$ *elemenata; dakle* $A_i \subseteq X$ *i važi uslov:* $A_i \not\subseteq A_j$, $1 \le i \ne j \le m$. *Tada za* $r_i = |A_i|$ *važi nejednakost:* $\displaystyle\sum_{i=1}^{m} 1/\binom{n}{r_i} \le 1.$

**Dokaz** Neka je $C_0 \subseteq C_1 \subseteq \dots \subseteq C_n$ maskimalan lanac u $P(X)$. Tada je $|C_k| = k$, i ako je $X = \{a_1, a_2, \dots, a_n\}$, onda je $C_i - C_{i-1} = \{a_{p(i)}\}$, $i = 1, 2, \dots, n$, gde je $p$ permutacija skupa $\{1, 2, \dots, n\}$. S druge strane, za bilo koju permutaciju $q$ skupa $\{1, 2, \dots, n\}$ i $S_k(q) = \{a_{q(1)}, a_{q(2)}, \dots, a_{q(k)}\}$, dobijamo jedan maksimalan lanac $S(q) = \langle S_k(q) \,|\, k \le n\rangle$ $(S_0 = \emptyset)$. Ako su $p$ i $q$ različite permutacije, na primer ako je $i$ najmanji prirodan broj takav da je $p(i) \ne q(i)$, onda $S_i(p) \ne S_i(q)$, tj. lanci $S(p)$ i $S(q)$ su različiti. Dakle, maksimalnih lanaca u $P(X)$ ima tačno $n!$.

Neka je $A \subseteq X$, gde je $|A| = r$. Tada svaki maksimalan lanac $C_i$, $0 \le i \le n$, koji "prolazi" kroz $A$ izgleda: $C_0 \subseteq C_1 \subseteq \dots \subseteq C_{r-1} \subseteq A \subseteq C_{r+1} \subseteq \dots \subseteq C_n$.

Argumentom kao u prvom delu dokaza nalazimo da lanaca $C_0 \subseteq C_1 \subseteq \dots \subseteq C_{r-1}$ ima tačno $r!$, dok lanaca $C_{r+1} \subseteq \dots \subseteq C_n$ ima tačno $(n-r)!$. Dakle ukupan broj maksimalnih lanaca koji "prolaze" kroz $A$ ima tačno $r!(n-r)!$. Neka je $B \subset X$ neuporediv sa $A$. Ako je $C_i$ lanac koji prolazi kroz $A$, i $S_i$ je lanac koji prolazi kroz $B$, onda su ti lanci međusobno različiti. Zaista, u suprotnom $A$ i $B$ bi pripadali istom lancu, dakle bili bi međusobno uporedivi, suprotno pretpostavci da nisu uporedivi.

Kako su prema uslovu teoreme $A_i$, $i = 1, \dots, m$ međusobno neuporedivi, prema prethodnom broj svih maksimalnih lanaca koji prolaze kroz neki $A_i$ manji je ili jednak od broja svih maksimalnih lanaca od $P(X)$, dakle

$\displaystyle\sum_{i=1}^{m} r_i!(n-r_i)! \le n!,$ odakle sledi tvrđenje teoreme. □

Nije teško proveriti da za $n > 2$ važi

$\binom{2n}{0} < \binom{2n}{1} < \dots < \binom{2n}{n}$; $\binom{2n-1}{0} < \binom{2n-1}{1} < \dots < \binom{2n-1}{n-1}$.

što znači da za fiksirano $n$, niz $\binom{n}{k}$ raste za $k \le [n/2]$, dok za $k \ge [n/2]$ opada (s obzirom na jednakost $\binom{n}{k} = \binom{n}{n-k}$). Prema tome, za bilo koji $A \subseteq X$, za $r = |A|$ važi $\binom{n}{r} \le \binom{n}{[n/2]}$.
□ Prelazimo na sam dokaz Špernerove teoreme. Prema pretpostavci teoreme i prema prethodno dokazanoj teoremi nalazimo: (1) $\displaystyle\sum_{i=1}^{k} 1/\binom{n}{r_i} \le 1$, gde je $r_i = |A_i|$. Prema prethodno utvrđenoj oceni za $\binom{n}{r}$, nalazimo $\binom{n}{r_i} \le \binom{n}{[n/2]}$. Prema (1) sledi $k/\binom{n}{[n/2]} \le 1$.

**Napomena** *Špernerova teorema daje ocenu za broj elemenata maksimalnog antilanca u* $P(X)$. ♢

**3.28** Da bi odredili broj $D_n$ iskoristićemo formulu uključivanja–isključivanja, sa $A_i = \{f \,|\, f$ je permutacija skupa $n$ i $f(i) = i\}$. Za različite brojeve $i_j$ $(j = 1, \dots, k)$ je $\left|\bigcap_{j=1}^{k} A_{i_j}\right| = \binom{n}{k}(n-k)! = n!/k!$. Dobijamo $D_n = n!\displaystyle\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}$. ♢

**3.29** Ako su $n, m \in N$ neka je $A_{nm} = \dfrac{1}{n} + \dots + \dfrac{1}{m}$. Označimo sa $k$ najveći ceo broj takav da je $\dfrac{1}{2^k} \le \dfrac{1}{m}$. Ako je $\dfrac{1}{2^k} < n$, onda je $A_{nm} = \sum_{i=n}^{m} \dfrac{1}{i} < \dfrac{m-n}{2^k} < 1$, i $A_{nm}$ nije ceo. U protivnom je ($A = \mathrm{NZS}(n, n+1, \ldots, m)$):

$$A_{nm} = \sum_{i=n}^{m} \frac{1}{i} = \sum_{i=n}^{m} \frac{a_i}{A} = \frac{1}{A} \sum_{i=n}^{m} a_i.$$

Pošto je $2^k$ jedini broj iz intervala $[n, m]$ koji je deljiv sa $2^k$ svi brojevi $a_i$ ($i \neq 2^k$) su parni, dok je $a_{2^k}$ neparan. Dakle broj $\sum_{i=n}^{m} a_i$ je neparan; pošto je $k > 0$ broj $A_{nm}$ nije ceo. $\diamondsuit$

**3.31** **a.** Neka je $i = \max\{j \mid [x + j/n] = [x]\}$; tada je $[x] + 1 = x + i/n + r$ za neko $r \in [0, 1/n)$, pa $nx = n[x] + n - i - nr$, odakle $[nx] == [n[x] + n - i - nr] = n[x] + n - i - 1$, jer $0 \leq nr < 1$; s druge strane,

$$\sum_{j=0}^{n-1} [x + j/n] = \sum_{j=0}^{i} [x + j/n] + \sum_{j=i+1}^{n-1} [x + j/n] = (i+1)[x] + (n - i - 1)([x] + 1) = [nx]. \quad \square$$

**b.** Leva nejednakost je trivijalna. S druge strane imamo $\sqrt[k]{x} < [\sqrt[k]{x}] + 1$ i $x < ([\sqrt[k]{x}] + 1)^k = \sum_{j=0}^{k} \binom{k}{j} [\sqrt[k]{x}]^{k-j}$. Pošto za cele brojeve $m < n \Rightarrow m \leq n - 1$, imamo $x \leq \sum_{j=0}^{k-1} \binom{k}{j} [\sqrt[k]{x}]^{k-j}$. $\diamondsuit$

**3.33** Dokaz teče kao jedan smer dokaza Primera 3.3.11. $\diamondsuit$

**3.34** Ako je $Y$ linearno uređen skup i $a, b \in Y$, sa $(a, b)_Y$ označavamo interval $\{x \in Y \mid a < x < b\}$; slično se definišu i $(a, \infty)_Y = \{x \in Y \mid a < x\}$ i i $(-\infty, a)_Y = \{x \in Y \mid x < a\}$. Na primer, ako je $Y = (a, b)_X$ i $c \in (a, b)_X$, onda je $(c, \infty)_Y = (c, b)_X$. Ako je $Y$ linearno uređen skup, kažemo da je "skup $Y$ univerzalan" ako se u njega može utopiti svaki prebrojiv dobro uređen skup (ili ekvivalentno – svaki ordinal $\alpha < \omega_1$). Ako su $X$ i $Y$ dobro uređeni skupovi, onda $X \preceq Y$ označava činjenicu da se $X$ može utopiti u $Y$ kao početni komad. Koristićemo sledeće tvrđenje:

*Ako su $X$ i $Y$ dobro uređeni skupovi, onda je ili $X \preceq Y$ ili $Y \preceq X$.*

**Dokaz** Neka je $X_0 = \bigcup\{Z \subset X \mid Z$ je početni komad i $Z \preceq Y\}$; tada je i $X_0 \preceq Y$ (jer se svaka dva utapanja početnog komada skupa $X$ u početni komad skupa $Y$ poklapaju na preseku svojih domena). Ukoliko je $X_0 = X$, imamo $X \preceq Y$. U protivnom, neka je $x_0 = \min\{x \in X \mid x \notin X_0\}$. Ukoliko je početni komad $Y_0$ skupa $Y$ koji je izomorfan sa $X_0$ jednak $Y$, tvrđenje je dokazano; u protivnom proširujemo izomorfizam $f \colon X_0 \to Y_0$ sa $f(x_0) = \min\{y \in Y \mid y \notin Y_0\}$, dakle $X_0 \cup \{x_0\} \subset X_0$ – kontradikcija.

Na osnovu prethodnog tvrđenja, svaka familija dobro uređenih skupova $\{X_i \mid i \in N\}$ je linearno uređena relacijom $\preceq$, i možemo govoriti (uz primenu teoreme 2.2.5) o supremumu ove familije – najmanjem dobro uređenom skupu $Y$ takvom da je $X_i \preceq Y$ za sve $i \in N$. Skup $Y$ označavamo sa $\sup_{i \in N} X_i$. $\square$ Sledeće tvrđenje je korak ka definisanju gusto uređenog podskupa skupa $X$.

*Ako je skup $Y$ univerzalan, onda postoji $F(Y) = c \in Y$ takav da su $(-\infty, c)_Y$ i $(c, \infty)_Y$ univerzalni.*

**Dokaz** Neka je

$$C_l = \{x \in Y \mid \text{ interval } (-\infty, x)_Y \text{ nije univerzalan}\}, \quad \text{i}$$
$$C_d = \{x \in Y \mid \text{ interval } (x, \infty)_Y \text{ nije univerzalan}\}.$$

(Uočimo da je $C_l$ početni, a $C_d$ završni komad skupa $Y$). Pretpostavimo da tvrđenje nije tačno; dakle $C_l \cup C_d = Y$. Svakom $x \in C_l$ pridružimo $\alpha_{xl}$ – prebrojiv, dobro uređen skup koji se ne može utopiti u $(-\infty, x)_Y$, a svakom $x \in C_d$ pridružimo $\alpha_{xd}$ – prebrojiv, dobro uređen skup koji se ne može utopiti u $(x, \infty)_Y$. Neka je $\alpha_l = \sup_{x \in C_l} \alpha_{xl}$ i $\alpha_d = \sup_{x \in C_d} \alpha_{xd}$; $\alpha_l$ i $\alpha_d$ su prebrojivi. Posmatrajmo skup $Z = (\{0\} \times \alpha_l \cup \{1\} \times \alpha_d, <_{\mathrm{Lex}})$ (ovaj skup se označava i sa $\alpha_l + \alpha_d$, to je uređenje koje dobijemo kada na kraj $\alpha_l$ "zalepimo" $\alpha_d$). Ovaj skup je dobro uređen, i po pretpostavci zadatka postoji utapanje $f: Z \to Y$. Uočimo element $c = f((1, \min \alpha_d))$. Tada $(-\infty, c)_Y$ nije u $C_l$ (pošto je $f(\{0\} \times \alpha_l) \subset (-\infty, c)_Y$); slično $(c, \infty)_Y$ nije u $C_d$ – kontradikcija.

*Skup $X$ sadrži gusto uređen podskup.*

**Dokaz** Definišemo rastući niz skupova $\langle A_i \mid i \in N \rangle$ elemenata skupa $Y$ i niz intervala $B_i$ sa:

$$
\begin{aligned}
A_0 &= \{F(X)\}, \\
B_n &= \{(a,b)_Y \mid a, b \in A_n \cup \{-\infty, \infty\},\ (a,b)_Y \cap A_n = \emptyset\} \\
A_{n+1} &= A_n \cup \{F(B) \mid B \in B_n\}.
\end{aligned}
$$

Skup $\bigcup_{n \in N} A_n$ je gust, jer se između svaka dva elementa skupa $A_n$ nalazi element skupa $A_{n+1}$. Pošto svaki gust prebrojiv linearno uređen skup sadrži izomorfnu kopiju od $(Q, <)$, v. Primer 3.3.11, ovim je dokaz završen. $\diamondsuit$

**3.36** *(Napomena: ovde racionalni brojevi igraju dvostruku ulogu – oni su istovremeno vektori i elementi polja).* **a.** Svaki vektorski prostor ima bazu (uz AC). $\square$ **b.** Neka je $H$ neki skup realnih brojeva kardinalnosti $\kappa < 2^{\aleph_0}$. Tada je

$\mathcal{L}(H) = \{r_1 q_1 + \cdots + r_n q_n \mid n \in N, r_j \in H, q_j \in Q (j = 1, \ldots, n)\}$

kardinalnosti najviše $|H||Q| = \kappa < 2^{\aleph_0}$, dakle ne pokriva $\mathbf{R}$. $\square$ **c.** Sledeći dokaz je, u suštini, uobičajena konstrukcija baze datog vektorskog prostora. Pošto konstruišemo jednu Hamelovu nazu, pokazaćemo kako da se od nje napravi $2^{2^{\aleph_0}}$ različitih baza. To je dovoljno, pošto podskupova realnih brojeva ima ukupno $2^{2^{\aleph_0}}$. Konstruisaćemo familiju $\langle A_\alpha, B_\alpha, r_\alpha \mid \alpha \text{ je ordinal}, \alpha < 2^{\aleph_0} \rangle$ takvu da je za sve $\alpha < 2^{\aleph_0}$:

**i.** $B_\alpha \subset \mathbf{R}$ i $B_\alpha = \mathcal{L}(\{r_\beta \mid \beta < \alpha\})$,
**ii.** $A_\alpha = \mathbf{R} \setminus B_\alpha$, i
**iii.** $r_\alpha \in A_\alpha$.

Ukoliko ovakva familija postoji, tada važi $r_\alpha \notin B_\alpha$, pa je $B_\alpha \subsetneq B_\beta \subset \mathbf{R}$ i skup vektora $H = \{r_\alpha \mid \alpha < 2^{\aleph_0}\}$ je linearno nezavisan. Da bi osigurali da skup $H$ bude baza, izaberemo bijekciju $f: \mathbf{R} \to 2^{\aleph_0}$ i uvek biramo $r_\alpha \in A_\alpha$ tako da ordinal $f(r_\alpha)$ bude minimalan.

Uzmimo $A_0 = \mathbf{R}$, $B_0 = Q$ i $r_0 = 0$. Pretpostavimo da su $A_\beta$, $B_\beta$ i $r_\beta$ konstruisani za sve $\beta < \alpha$ tako da zadovoljavaju uslove **i.–iii.** i da je $\alpha < 2^{\aleph_0}$. Neka je $B_\alpha = \mathcal{L}(\{r_\beta \mid \beta < \alpha\})$ i $A_\alpha = \mathbf{R} \setminus B_\alpha$. Očigledno je (kao u dokazu za **b.**) i $|B_\alpha| = |\alpha|$, a pošto je $|A_\alpha| + |B_\alpha| = 2^{\aleph_0}$ imamo $|A_\alpha| = 2^{\aleph_0}$ za sve $\alpha < 2^{\aleph_0}$; izaberimo $r_\alpha \in A_\alpha$. Na osnovu principa transfinitne indukcije, ovakva familija postoji. $\square$ Za funkciju $g: 2^{\aleph_0} \to \{1, 2\}$ definišimo $H_g = \{g(\alpha) \cdot r_\alpha \mid \alpha \in 2^{\aleph_0}\}$. Pošto su vektori $r_\alpha$ i $2r_\alpha$ kolinearni, $H_g$ je Hamelova baza. Na osnovu konstrukcije skupa $H$ imamo $2r_\alpha \neq r_\beta$ za sve $\alpha \neq \beta$. Osim toga, ako je $\alpha$ takav da je $g(\alpha) = 1$ i $f(\alpha) = 2$ imamo $r_\alpha \in H_g \setminus H_f$. Dakle za $f \neq g$ skupovi $H_g$ i $H_f$ se razlikuju. $\square$ **d.** Koristićemo oznake $A - n = \{x - n \mid x \in A\}$, $qA = \{qx \mid x \in A\}$, i $A' = \{x - [x] \mid x \in A\}$. Neka je Hamelova baza $H$ merljiv skup; tada je skup $H_n = H \cap [n, n+1)$ takođe merljiv za sve $n \in Z$. Pretpostavimo da $H$ sadrži neki racionalan broj $q_H$ (ukoliko ovo nije tačno, zamenimo $H$ skupom $\frac{1}{r}H$ za neko $r \in H$ – ovo je Hamelova baza mere $m(H)/r$). Skupovi $H_n - n$ i $H_m - m$ su disjunktni za sve $m \neq n \in Z$ – inače bi za neke $r_\alpha, r_\beta \in H$ imali $r_\alpha - n = r_\beta - m$ i $r_\alpha - r_\beta + \dfrac{m-n}{q_H} q_H = 0$, tj. $\{r_\alpha, r_\beta, q_H\}$ bio bi linearno zavisan podskup od $H$. Neka je $H' = \bigcup_{n \in Z}(H_n - n)$. Primetimo da je $H_n - n \subseteq [0,1]$ za sve $n \in Z$, dakle i $H' \subseteq [0,1]$. Otuda imamo:

$$m(H') = \sum_{n \in Z} m(H_n - n) = \sum_{n \in Z} m(H_n) = m(H).$$

Ukoliko je $q \in Q \setminus \{0\}$, s obzirom da je Lebegova mera translatorno invarijantna, skupovi $H$ i $(H+q)$ su disjunktni i iste mere. Dakle, m(H')= m(H)= m(H+q)= m(H+q)', pa

$$1 = m([0,1]) \geq \sum_{q \in Q} m\left((H+q)'\right) = \sum_{q \in Q} m(H),$$

i prema tome je $m(H) = 0$. $\square$ Da bi dokazali da postoji Hamelova baza mere nula, dovoljno je da dokažemo sledeće:

*Postoji skup realnih brojeva $H$ mere nula takav da je $\mathcal{L}(H) = \mathbf{R}$.*

Neka je $H_1$ *Kantorov skup*, to jest skup svih realnih brojeva u intervalu $[0,1]$ u čijem se ternarnom razvoju ne pojavljuje cifra 1. Dakle,

$$H_1 = [0,1] \setminus \bigcup_{n \in N} \bigcup_{i=1}^{3^{n-1}-1} \left[\frac{3i+1}{3^n}, \frac{3i+2}{3^n}\right].$$

(Slikovitije rečeno, Kantorov skup dobijamo tako što iz intervala $[0,1]$ izbacimo srednju trećinu, zatim iz svakog od preostala dva intervala $[0,1/3]$ i $[2/3,1]$ izbacimo srednju trećinu, i tako u beskonačnost.) Skup $H_1$ je mere $\prod_{n=1}^{\infty} 2/3 = 0$. Neka je $H_2$ skup svih realnih brojeva iz intervala $[0,1]$ u čijem se zapisu ne pojavljuje cifra 2; ovaj skup je takođe mere nula. Za svaki $r \in [0,1]$ ternarni razvoj je $r = \sum_{i=1}^{\infty} a_i 3^i$. Neka je $S_1 = \{i \in N \mid a_i = 1\}$ i $S_2 = \{i \in N \mid i = 2\}$; tada imamo $r = \sum_{i \in S_1} 1/3^i + \sum_{i \in S_2} 2/3^i$, i $r$ je linearna kombinacija jednog vektora iz skupa $H_1$ i jednog vektora iz skupa $H_2$. Pošto je $[0,1] \subset \mathcal{L}(H_1 \cup H_2)$, lako se dobije da je i $\mathbf{R} \subset \mathcal{L}(H_1 \cup H_2)$. Ovim je dokaz završen. $\diamondsuit$

**3.37** Kao u rešenju zadatka 2.10 dokažemo da je $f(qa) = qf(a)$ za sve $q \in Q$ i $a \in R$. Funkcija $f^- = f \restriction Q$ je neprekidna i monotona na skupu $Q$ koji je gust u $R$, dakle proširenje funkcije $f^-$ na skup $R$ koje je neprekidno (ili monotono) je jednoznačno određeno, i imamo **a.** $\Leftrightarrow$ **b.** $\Leftrightarrow$ **c.** $\square$ Tvrđenja **a.** $\Rightarrow$ **d.** i **a.** $\Rightarrow$ **e.** su trivijalna. $\square$ Uočimo da iz sledećeg tvrđenja sledi $\neg$**d.** i $\neg$**e.**:

*Za svaki $b \in R$ i svaki $a \in R$ postoji niz $x_i$ takav da je $\lim_{i\to\infty} x_i = b$ i $\lim_{i\to\infty} f(x_i) = a$.*

Pošto $f$ zadovoljava Košijevu osobinu, ovo je ekvivalentno sa:

*Za svaki $a \in R$ postoji niz $x_i$ takav da je $\lim_{i\to\infty} x_i = 0$ i $\lim_{i\to\infty} f(x_i) = a$.*

Pretpostavimo da važi $\neg$**b.** Tada postoji niz tačaka $x_i$ i $c, d \in R$ takvi da je $\lim_{i\to\infty} x_i = c$ i $\lim_{i\to\infty} f(x_i) = d \neq f(c)$. Uzmimo $y_i = x_i - c$; tada je $\lim_{i\to\infty} y_i = 0$ i $\lim_{i\to\infty} f(y_i) = d - f(c) \neq 0$. Za svaki $q \in Q$ imamo $\lim_{i\to\infty} f(qx_i) = q(d - f(c))$, a skup $\{q(d-f(c)) \mid q \in Q\}$ je gust u $R$. Ovim je tvrđenje dokazano. $\diamondsuit$

**3.38** Pošto je $F$ beskonačno uređeno polje, ono sadrži potpolje $\mathbf{Q}_F$ izomorfno polju $\mathbf{Q}$. Dokažimo da se izomorfizam $f^-: Q_F \to Q$ može proširiti do izomorfnog utapanja.

*Svaki $a \in F$ je jednoznačno određen skupom $F_{<a} = \{q \in Q_F \mid q < a\}$.*

**Dokaz** Ako postoje $a < b \in F$ takvi da je $F_{<a} = F_{<b}$, onda za sve $n \in N$ imamo $b - a < (1/n)_F$ i $n \cdot 1/(b-a) < 1$; kontradikcija.

Preslikavanje $f: F \to R$ definišemo sa $f(a) = \sup\{q \mid q_F \in F_{<a}\}$. $\diamondsuit$

**Napomena** *Ovo znači da je svako arhimedovsko polje oblika $\mathbf{Q}(S)$, gde je $S$ neki skup iracionalnih brojeva.*

**3.39** Primetimo prvo da za $n \in Z$ element $a \in S$ definisan sa: $a_n = 1$, $a_i = 0$ za $i \neq n$ zadovoljava jednačinu $\epsilon^n = a_n$; prema tome, $S$ možemo da (neformalno) posmatramo kao skup beskonačnik redova oblika $a_{-k}\epsilon^{-k} + a_{-k+1}\epsilon^{-k+1} + \cdots + a_0 + a_1\epsilon + \cdots + a_n\epsilon^n + \ldots$. **a.** Dokazaćemo samo egzistenciju inverznog elementa za množenje; ostale osobine slede iz činjence da je $S$ podalgebra algebre $\mathbf{R}^Z$ i posledice 1.8.4. Neka je $a \in S$; uvedimo oznaku $k_a = \min\{n \in Z \mid a_n \neq 0\}$. Svaki $x \in S$ može da se predstavi kao $x' \cdot \epsilon^{k_x}$, gde je $x'$ takav da je $k_{x'} = 0$; dakle dovoljno je dokazati da svaki $a$ takav da je $k_a = 0$ ima inverzni element. $\square$ Neka je $a$ takav da je $k_a = 0$; dokazujemo da jednačina $a \cdot b = \mathbf{1}$ ima rešenje u $S$ takvo da je $k_b = 0$. Ova jednačina je ekvivalentna sistemu:

$$(*) \qquad a_0b_0 = 1, \qquad a_0b_1 + a_1b_0 = 0, \qquad \ldots, \qquad \sum_{i=0}^{n} a_ib_{n-i} = 0 \quad \text{za } n > 0.$$

Pošto je, po pretpostavci, $a_0 \neq 0$, sistem (*) je ekvivalentan sistemu rekurentnih formula $b_0 = -1/a_0$, $b_n = 1/a_0 \sum_{i=1}^{n} a_ib_{n-i}$ (za $n > 0$), i rešenje sistema je $b_0 = 1/a_0$, $b_1 = -a_1b_0/a_0 = a_1/a_0^2$, $b_2 = a_1/a_0^2(a_2 - a_1)$, ... $\square$ **b.** Utapanje $f: R \to S$ je definisano sa $(f(x))_0 = x$, $(f(x))_n = 0$ za $n \neq 0$. $\square$ **c.** Pošto je (uz $k_a$ definisano kao pod **a.**) $k_{ab} = k_ak_b$ i $(ab)_{k_{ab}} = a_{k_a}b_{k_b}$, množenje je saglasno sa relacijom $\leq$; ostalo je trivijalno. $\diamondsuit$

**3.40** **a.** Neka je $\mathbf{F} \subset \mathbf{G}$, $F$ je gusto u $\mathbf{G}$ i važi (*). Uzmimo $a \in G \setminus F$; neka je $X = \{x \in F \mid x < a\}$. Skup $F$ je gust u $G$, pa postoji $x \in F$ takav da je $a - \epsilon < x < a$. Pošto je $x + \epsilon > a$ skup $X$ ima supremum u $F$; označimo ga sa $a^F$. Ali $a^F < a$ i osim toga ne postoji $x \in F$ takav da je $a^F < x < a$ – kontradikcija. $\square$ Neka je $F$ uređeno polje za koje ne važi (*), i neka je $G$ skup svih ograničenih početnih komada skupa $F$. Na skupu $G$ definišemo operacije sa:

**i.** $X + Y = \{x + y \mid x \in X, y \in Y\}$;
**ii.** $-X = \{y \mid \forall x \in X\, y < -x\}$;
**iii.** Ako je $0^F \in X$ i $0^F \in Y$, onda $X \cdot Y = \{z \mid \exists x \in X\, \exists y \in Y\, x, y > 0 \land z < xy\}$; za ostale slučajeve se množenje definiše tako da se slaže sa unarnom operacijom "$-$".

Uz prirodno definisane $0^G$, $1^G$ i $<^G$, struktura $\mathbf{G}$ čini uređeno polje u kom je skup $F$ gust. ($\mathbf{G}$ nazivamo *Dedekindovim kompletiranjem* polja $F$.) Pošto u polju $\mathbf{F}$ ne važi (*) izaberimo početni segment $X$ koji je ograničen i nema supremum u $F$; $X$ odgovara elementu skupa $G$ koji nije u $F$. $\square$ **b.** Polje $\mathbf{G}$ iz **a.** je traženo polje, pošto zadovoljava uslov (*) i $F$ je gust u $G$. $\square$ **c.** Neka su $\mathbf{G}_1$ i $\mathbf{G}_2$ dva Scott–kompletna polja takva da je skup $F$ gust u svakom od njih. Definišemo izomorfizam $f: \mathbf{G}_1 \to \mathbf{G}_2$ sa $f(a) = a$ (za $a \in F$) i $F(\sup_{G_1} X) = \sup_{G_2} X$. $\diamondsuit$

**3.41** Pogledati napomenu posle rešenja zadatka 2.11. $\diamondsuit$

**3.42** **a.** Primer je dat u zadatku 3.39. **b.** Neka je $\mathbf{F}$ dato polje, i neka je $T = \mathrm{Th}(\mathbf{F}, \mathbf{a})_{a \in F} \cup \{n \cdot 1 < b \,|\, n \in N\}$ (ovde je $b$ novi konstantni simbol). Na osnovu Stava kompaktnosti ova teorija ima model. Ovaj model je nearhimedovsko polje u koje je $\mathbf{F}$ izomorfno uloženo. $\diamondsuit$

**3.45** **a.** Neka je $z_n^k = \cos\frac{k\pi}{n} + i \sin\frac{k\pi}{n}$. Imamo:

$$x^{2m+1} - 1 = \prod_{k=0}^{2m+1}\left(x - z_{2m+1}^k\right) = (x-1)\prod_{k=1}^{m}\left(x - z_{2m+1}^k\right)\prod_{k=1}^{m}\left(x - z_{2m+1}^{2m+1-k}\right)$$
$$= (x-1)\prod_{k=1}^{m}\left(x^2 - 2x\cos\tfrac{2\pi k}{2m+1} + 1\right) \qquad \diamondsuit$$

**3.47** Primetimo prvo da je polinom $\Phi_n(x)$ uvek moničan. Primetimo takođe da je $x^n - 1 = \prod_{d|n}\Phi_d(x)$, pošto za svaki koren $z$ jednačine $x^n = 1$ postoji jedinstven $d$ takav da je $z$ primitivan koren jednačine $z^d = 1$, i ovaj $d$ deli $n$. $\square$ Pretpostavimo da je $n$ najmanji $k$ takav da polinom $\Phi_k(x)$ nije sa celobrojnim koeficijentima. Imamo $x^n - 1 = \Phi_n(x)\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)$, dakle $\Phi_n(x) = (x^n-1)/(\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x))$, i polinom $\Phi_n(x)$ ima racionalne koeficijente. Dokažimo sledeće tvrđenje:

*Ako su $P(x) = p_{k_P}x^k + \cdots + p_0$, $Q(x) = q_{k_Q}x^{k_Q} + \cdots + q_0$ i $R(x) = x^{k_R} + r_{k_R-1}x^{m-1} + \cdots + r_0$ polinomi takvi da je $P(x) = Q(x)R(x)$, $P$ i $R$ imaju celobrojne koeficijente, $Q$ racionalne i $R$ je moničan, onda i $Q$ ima celobrojne koeficijente.*

**Dokaz** Neka je $l$ najveći broj takav da $q_l \notin Z$. Tada je $p_{l+k_R} = \sum_{i+j=l+k_R} q_i r_j = q_l \cdot 1 + \sum_{\substack{i+j=l+k_R\\ i\neq l}} q_i r_j$, i ovaj broj nije ceo kao zbir čisto racionalnog i celog broja – kontradikcija.

Ako uzmemo $x^n - 1$ za $P$, $\Phi_n(x)$ za $Q$ i $\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)$ za $R$ i iskoristimo tvrđenje, dokaz je završen. $\diamondsuit$

**3.48** Pošto $z = i$ nije rešenje, jednačina se svodi na (uz oznaku $z_n^k$ iz prethodnog rešenja):

$$\left(\frac{z+i}{z-i}\right)^n = -1, \quad \text{pa je} \quad \frac{z+i}{z-i} = z_n^{2k+1} \quad (k = 0, \ldots, n-1), \qquad \text{i}$$
$$z = \frac{2i}{z_n^{2k+1} - 1} = \frac{2i}{2z_{2n}^{2k+1}\cos\frac{2k+1}{2n}\pi} = \frac{iz_{2n}^{-(2k+1)}}{\cos\frac{2k+1}{2n}\pi} = \mathrm{tg}\,\frac{2k+1}{2n}\pi + i, \qquad k < n \qquad \diamondsuit$$

**3.49** Svaki koren polinoma $f$ mora biti parnog reda, dakle za neki polinom $f_1(x)$ koji je strogo pozitivan i neke $x_i$ $(i \leq n)$ imamo $f(x) = \prod_{i=1}^n (x - x_i)^{2k_i} f_1(x)$. Ukoliko je $f_1(x) = c$, uzmimo $g(x) = \sqrt{c}\prod_{i=1}^n (x - x_i)^{k_i}$ i $h(x) = 0$. U protivnom je

$$f_1(x) = c\prod_{i=0}^{m}(x - z_i)(x - \bar{z}_i) = c\prod_{i=0}^{m}(x - z_i)\prod_{i=0}^{m}(x - \bar{z}_i) = c\prod_{i=0}^{m}(x - z_i)\prod_{i=0}^{m}\overline{(x - z_i)}.$$

Dakle, za neke realne polinome $g_1(x)$ i $h_1(x)$ imamo

$$f_1(x) = (g_1(x) + ih_1(x))(g_1(x) - ih_1(x)) = g_1^2(x) + h_1^2(x),$$

Iz čega se dobija $g(x) = \prod_{i=1}^n (x - x_i)^{k_i} g_1(x)$ i $h(x) = \prod_{i=1}^n (x - x_i)^{k_i} h_1(x)$. $\diamondsuit$

**Napomena** *Tvrđenje prethodnog zadatka je tačno i za polinome sa više promenljivih. Ovo pitanje je postavio D. Hilbert u svojoj čuvenoj listi problema, a E. Artin kasnije rešio.*

## BIBLIOGRAFIJA

U bibliografiji se citiraju tri vrste pisanih dela:

- Knjige iz oblasti za koje se pretpostavlja da je čitalac sa njima već upoznat. To su, na primer, udžbenici iz linearne algebre.
- Dela koja su relevantna za ovu knjigu. U užem smislu to su knjige iz opšte algebre, u širem, iz teorije skupova.
- Knjige koje se preporučuju čitaocu za dalje izučavanje predmeta algebra. To su, uglavnom, sve knjige citirane u bibliografiji na stranom jeziku.

### Bibliografija na srpskom jeziku


[1] N. Božović, Ž. Mijajlović, *Uvod u teoriju grupa*, Naučna knjiga, Beograd, str. XIV + 399, 1983.

[2] D. Cvetković, M. Milić *Teorija grafova i njene primene*, BIGZ, Beograd, str. 126, 1971.

[3] R. Dedekind, *Neprekidnost i racionalni brojevi; Šta su i čemu služe brojevi?*; G. Cantor, *O proširenju jednog stava iz teorije trigonometrijskih redova*, prevod sa nemačkog Z. Mamuzić, **Klasični naučni spisi 2**, Matematički institut, str. 92, Beograd, 1976.

[4] V. Devide, *Zadaci iz apstraktne algebre*, **Matematički problemi i ekspozicije 1**, Naučna knjiga, Beograd, str. 114, 1968.

[5] G. Kalajdžić, *Algebra*, BS Procesor – Matematički fakultet, Beograd, str.X+205, 1992.

[6] Lj. Kočinac, *Linearna algebra i analitička geometrija*, Filozofski fakultet, Univerzitet u Nišu, Niš, str. 346, 1991.

[7] J.L. Krivine, prevod V. Devide, *Aksiomatička teorija skupova*, **Moderna matematika**, Školska knjiga, Zagreb, str. 120, 1978

[8] A. Kron, *Elementarna teorija skupova*, Matematički institut, Beograd, str. VI+150, 1992.

[9] Đ. Kurepa, *Teorija skupova*, Školska knjiga, Zagreb, str. XIX + 439, 1951.

[10] Đ. Kurepa, *Viša algebra 1–2*, Zavod za izdavanje udžbenika, Beograd, str. XXIII + 1342, 1971

[11] A. Lipkovski, *Linerna algebra i analitička geometrija*, Naučna knjiga, str. 238, 1992.

[12] M. Mihaljinec i drugi, *O brojevima*, Školska knjiga, Zagreb, 1984.

[13] S. Milić, *Elementi algebre*, Institut za matematiku, PMF, Univerzitet u Novom Sadu, str. VI+222, Novi Sad, 1984

[14] K. Milošević-Rakočević, *Prilozi teoriji i praksi Bernulijevih polinoma i brojeva*, Matematički institut, Beograd, str. 143, 1963.

[15] Ž. Mijajlović, Z. Marković, K.Došen, *Hilbertovi problemi i logika*, **Matematička biblioteka 34**, Zavod za izdavanje udžbenika, str. 168, 1986.

[16] V. Perić, *Algebra 1–2*, "SVJETLOST", Zavod za izdavanje udžbenika, Sarajevo, str. 410+180, 1980.

[17] M. Prešić i S. Prešić, *Uvod u matematičku logiku*, **Matematički vidici 2**, Matematički institut, Beograd, str. 398, 1979.

[18] S. Prešić, *Elementi matematičke logike*, **Matematička biblioteka 34**, Zavod za izdavanje udžbenika, str. 143, 1968.

### Bibliografija na stranom jeziku

[19] C.C. Chang, J. Keisler *Model theory*, North-Holland, Amsterdam, 1973.
[20] A. Clark, *Elements of Abstract algebra*, Dover Publications Inc., New York, 1984.
[21] P.M. Cohn, *Universal algebra*, D. Reidel Publ. Comp., Dordrecht, 1981.
[22] И.М. Гельфанд, *Лекции по линейной алгебре*, «Наука», Москва, 1966.
[23] И.М. Гельфанд, *Исчисление конечны разностей*, «Наука», Москва,1967.
[24] R. L. Graham, *Rudiments of Ramsey theory*, AMS, Providence, Rhode Island, 1983.
[25] Д. К. Фаддеев, И. С. Соминский, *Сборник задач по высшей алгебре*, Физматгиз, Москва, 1964.
[26] D. Grätzer, *Universal Algebra*, D. Von Nostrand Comp., Priceton, 1986.
[27] D. Knuth, *The art of computer programming 1–3*, Addison-Wesley Publ. Comp., Reading Massachusetts, 1973.
[28] K. Kuratowski, A. Mostowski, *Set theory*, PWN, Warszawa, 1976.
[29] А. Г. Курош *Лекции по общей алгебре*, Физматгиз, Москва, 1962.
[30] S. Lang, *Algebra*, Addison-Wesley Publ. Comp, Reading Massachusetts, 1965.
[31] Ž. Mijajlović, *An introduction to model theory*, Institute of Mathematics, Univ. of Novi Sad, Novi Sad, 1987.
[32] В.Н. Сачков, *Введение в комбинаторные методы дискретной математики*, «Наука», Москва, 1982.
[33] J. R. Shoenfield, *Mathematical logic*, Addison-Wesley Publ. Comp, Reading, Massachusetts, 1967.
[34] В. В. Воеводин, *Линейная алгебра*, «Наука», Москва, 1980.
[35] Van Der Waerden, *Algebra*, Springer Verlag, Berlin, 1967.
[36] S. Wolfram, *Mathematica*, Addison-Wesley Publ.Comp., Reading Massachusetts, 1991 (priručnik za programski paket *Mathematica*).

## Spisak aksioma i tvrđenja koja imaju nazive

# INDEKS SIMBOLA

| | |
|---|---|
| $f : A \to B$<br>$f = \langle f(x) \mid x \in A \rangle$<br>$f : x \mapsto f(x),\ x \in A$ | funkcija iz skupa $A$ u skup $B$ |
| $f(A)$, $f[A]$ | skup vrednosti funkcije $f$; $\{f(x) \mid x \in A\}$ |
| $A^B$, ${}^B A$ | skup svih funkcija iz skupa $B$ u skup $A$ |
| $P(X)$, $\mathbf{P}(X)$ | partitivni skup skupa $X$ |
| $f \circ g$, $fg$ | kompozicija (proizvod) funkcija $f$ i $g$ |
| $N^+$ | skup pozitivnih prirodnih brojeva |
| $Q^+$ | skup pozitivnih racionalnih brojeva |
| $Q_0^+$ | skup nenegativnih racionalnih brojeva |
| $R^+$ | skup pozitivnih realnih brojeva |
| $R_0^+$ | skup nenegativnih realnih brojeva |
| $m \mid n$ | $m$ deli $n$ |
| $m \not\mid n$ | $m$ ne deli $n$ |
| $\mathrm{rest}(x, n)$ | funkcija ostatka po modulu $n$ |
| $\mathbf{Z}_n$ | prsten ostataka po modulu $n$ |
| $\mathrm{NZD}(m, n)$ | Najveći zajednički delilac za $m$ i $n$ |
| $\mathrm{NZS}(m, n)$ | Najmanji zajednički sadržalac za $m$ i $n$ |
| $\mathbf{A}$ | algebra sa domenom $A$ |
| $\equiv$ | metajednakost |
| $\mathrm{Var}$ | skup promenljivih $v_0, v_1, \ldots$ |
| $L$ | jezik $L$ |
| $\mathrm{Const}_L$ | skup simbola konstanti jezika $L$ |
| $\mathrm{Fun}_L$ | skup operacijskih simbola jezika $L$ |
| $\mathrm{ar}(F)$ | arnost (dužina) funkcijskog znaka $F$ |
| $s^{\mathbf{A}}$ | interpretacija simbola $s$ u algebri (modelu) $\mathbf{A}$ |
| $\sigma\mathbf{A}$ | signatura algebre $\mathbf{A}$ |
| $\mathrm{Term}_L$ | skup terama jezika $L$ |
| $\mathrm{sl}(u)$ | složenost terma $u$ |
| $\mathrm{sl}(\varphi)$ | složenost formule $\varphi$ |
| $u^{\mathbf{A}}[\alpha]$ | vrednost terma $u$ u algebri $\mathbf{A}$ za valuaciju $\alpha$ |
| $\models$ | relacija zadovoljenja (istinitosti) |
| $\mathbf{A} \models u = v$ | algebra $\mathbf{A}$ zadovoljava algebarski zakon $u = v$ |
| $\mathbf{A} \models \varphi$ | model $\mathbf{A}$ zadovoljava rečenicu $\varphi$;<br>rečenica $\varphi$ je tačna (istinita) u $\mathbf{A}$ |

| | |
|---|---|
| $\mathfrak{M}(T)$ | algebarski varijetet algebarske teorije $T$; klasa modela teorije $T$. |
| $L_T$ | jezik teorije $T$ |
| Mon | algebarski varijetet monoida |
| Gp | algebarski varijetet grupa |
| Ab | algebarski varijetet abelovih grupa |
| Pk | algebarski varijetet komutativnih prstena |
| BA | algebarski varijetet Bulovih algebri |
| $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$ | skup homomorfizama iz algebre $\mathbf{A}$ u algebru $\mathbf{B}$ |
| $\cong$, $\xrightarrow{\sim}$ | relacija izomorfizma između algebri, modela |
| $\mathrm{Aut}(\mathbf{A})$ | skup automorfizama algebre (modela) $\mathbf{A}$ |
| $\mathbf{Aut}(\mathbf{A})$ | grupa automorfizama algebre (modela) $\mathbf{A}$ |
| $\mathrm{End}(\mathbf{A})$ | skup endomorfizama algebre (modela) $\mathbf{A}$ |
| $\mathbf{End}(\mathbf{A})$ | monoid endomorfizama algebre (modela) $\mathbf{A}$ |
| $\mathbf{A} \subseteq \mathbf{B}$ | $\mathbf{A}$ je podalgebra (podmodel, podstruktura) algebre $\mathbf{B}$ |
| $h : \mathbf{A} \to \mathbf{B}$ | $h$ je homomorfizam iz algebre $\mathbf{A}$ u algebru $\mathbf{B}$ |
| $\ker(h)$ | jezgro homomorfizma $h$ |
| $i_A$ | identičko preslikavanje domena $A$, inkluziono preslikavanje iz $A \subseteq B$ u $B$ |
| $h(\mathbf{A})$, $h\mathbf{A}$ | homomrfna slika algebre (strukture) $\mathbf{A}$ |
| $\mathbf{A} \times \mathbf{B}$ | proizvod algebri $\mathbf{A}$ i $\mathbf{B}$ |
| $\prod_{i \in I} \mathbf{A}_i$ | generalisani proizvod algebri $\mathbf{A}_i$, $i \in I$ |
| $\langle X \rangle_{\mathbf{A}}$ | podalgebra algebre $\mathbf{A}$ generisana skupom $X \subseteq A$ |
| $f\vert X$, $f \restriction X$ | restrikcija funkcije $f$ na skup $X$ |
| $A_\infty$ | skup svih skoro konstantnih valuacija domena $A$ |
| $\vert X\vert$ | kardinalni broj skupa $X$ |
| $\triangle_A$ | dijagonala skupa $A$ |
| $\sim$ | relacija ekvivalencije; relacija kongruencije |
| $a/\!\sim$ | klasa ekvivalencije (klasa kongruencije) elementa $a$ |
| $\mathbf{A}/\!\sim$ | količnička algebra algebre $\mathbf{A}$ |
| $=_n$ | kongruencija po modulu $n$ |
| $\mathrm{Rel}_L$ | skup relacijskih znakova jezika $L$ |
| $\mathrm{At}_L$ | skup atomičnih formula jezika $L$ |
| $\mathrm{For}_L$ | skup formula jezika $L$ |
| $\mathrm{Fv}(\varphi)$ | skup slobodnih promenljivih formule $\varphi$ |
| $\underline{a}$ | ime elementa $a$ |
| LO | teorija linearno uređenih skupova |
| PO | teorija parcijalno uređenih skupova |
| ZF | Zermelo-Fraenkelova teorija skupova |
| ZFC | ZF teorija skupova zajedno sa Aksiomom izbora |
| $\mathrm{ZF}_f$ | teorija striktno konačnih skupova |
| PA | Peanova aritmetika |
| FPA | Formalna aritmetika |
| $A(x, y, z)$ | Akermanova funkcija |
| $2^N$ | skup svih binarnih nizova |
| $\langle x, y \rangle_K$ | Kantorova funkcija nabrajanja |
| $L$, $R$ | projekcijske funkcije za Kantorovu funkciju |
| $C_k^n$, $\binom{n}{k}$ | binomni koeficijent |

| | |
|---|---|
| $S_k^n$ | Stirlingovi brojevi prve vrste |
| $s_k^n$ | Stirlingovi brojevi druge vrste |
| $\sigma_k^n$ | modifikovani Stirlingovi brojevi 1. vrste |
| $[x]$, $\lfloor x \rfloor$ | ceo deo od $x$ |
| $\lceil x \rceil$ | ceo deo "nagore" od $x$ |
| $\prod$, $\sum$ | operatori proizvoda i sumiranja |
| $\Delta_x$ | operator konačne razlike |
| $b_n$ | Bernulijevi brojevi |
| $V$ | skup svih striktno konačnih skupova |
| $(V, \in)$ | kombinatorni univerzum |
| $\mathrm{dom}(f)$ | domen funkcije $f$ |
| $\mathrm{codom}(f)$ | kodomen funkcije $f$ |
| $[X]^k$ | skup svih $k$-članih podskupova od $X$ |
| $\mathrm{RT}_v$ | konačna verzija Remzijeve teoreme |
| $\mathcal{C}$ | skup svih Košijevih racionalnih nizova |
| $\mathcal{C}_0$ | skup svih racionalnih nula nizova |
| $\sqrt[m]{x}$ | korenska funkcija |
| $\imath$ | imaginarna jedinica |
| $\mathrm{Re}(z)$ | realni deo kompleksnog broja $z$ |
| $\mathrm{Im}(z)$ | imaginarni deo kompleksnog broja $z$ |
| $\bar{z}$ | konjugacija kompleksnog broja $z$ |
| $e^{\imath\varphi}$ | $\cos(\varphi) + \imath \sin(\varphi)$ |

# INDEKS POJMOVA