Linearna algebra

Mirko Primc

Sadržaj

Poglavlje 1. Polje realnih brojeva 5
1. Prirodni i cijeli brojevi 5
2. Polje racionalnih brojeva 6
3. Polje realnih brojeva $\mathbb{R}$ 9
4. Polje kompleksnih brojeva $\mathbb{C}$ 13
5. Pojam polja 15

Literatura 23

POGLAVLJE 1

Polje realnih brojeva

Mi pretpostavljamo poznavanje realnih brojeva. Svrha ovog kratkog poglavlja je sažeto ponavljanje svojstava operacija zbrajanja i množenja i relacije uređaja na skupu realnih brojeva.

1. Prirodni i cijeli brojevi

1.1. Zbrajanje i množenje. Na skupu prirodnih brojeva $\mathbb{N}$ i skupu cijelih brojeva $\mathbb{Z}$,

$$\mathbb{N} = \{1, 2, 3, \dots\} \subset \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\},$$

imamo operacije zbrajanja $+$ i množenja $\cdot$. Obje operacije su asocijativne, tj. (za sve brojeve k, m, n) vrijedi jednakost

$$k + (m + n) = (k + m) + n, \qquad k \cdot (m \cdot n) = (k \cdot m) \cdot n,$$

i komutativne, tj.

$$m + n = n + m, \qquad m \cdot n = n \cdot m,$$

i vrijedi distributivnost množenja u odnosu na zbrajanje, tj.

$$k \cdot (m + n) = k \cdot m + k \cdot n.$$

Broj 1 je neutralan element za množenje, a broj 0 u skupu $\mathbb{Z}$ je neutralni element za zbrajenje, tj.

$$1 \cdot n = n \cdot 1 = n, \qquad 0 + n = n + 0 = n.$$

U skupu $\mathbb{Z}$ svaki cijeli broj n ima jedinstveni suprotni element za zbrajanje $-n$, tj. broj $-n$ sa svojstvom

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

Tako, na primjer, broj -2 ima jedinstveni suprotni element 2, tj. $-(-2) = 2$.

U skupu prirodnih brojeva $\mathbb{N}$ i skupu cijelih brojeva $\mathbb{Z}$ element $n \neq 0$ općenito nema suprotni element za množenje[1], ali vrijedi zakon kraćenja s brojem $n \neq 0$, tj.

$$n \cdot m = n \cdot k \quad \text{povlači} \quad m = k.$$

[1]Za element $n \neq 0$ suprotni element za množenje obično zovemo recipročnim elementom kojeg zapisujemo kao $\frac{1}{n}$ ili n^{-1}.

1.2. Relacija uređaja. Na skupu prirodnih brojeva $\mathbb{N}$ i skupu cijelih brojeva $\mathbb{Z}$ imamo relaciju uređaja $\leq$. Ako je $m \leq n$ i $m \neq n$, onda pišeemo $m < n$ ili $n > m$. Tako je $2 \leq 3$, ali vrijedi i $2 < 3$.

Svaka su dva broja usporediva, tj. uvijek vrijedi $m \leq n$ ili $n \leq m$. Relacija uređaja je antisimetrična, tj.

$$n \leq m \quad \text{i} \quad m \leq n \qquad \text{vrijedi ako i samo ako je} \qquad n = m,$$

i tranzitivna, tj.

$$k \leq m \quad \text{i} \quad m \leq n \qquad \text{povlači} \qquad k \leq n.$$

Operacija uređaja je u skladu sa zbrajanjem, tj. za svaki broj n

$$k \leq m \qquad \text{povlači} \qquad k + n \leq m + n,$$

i u skladu je s množenjem, tj. za svaki broj $n > 0$

$$k \leq m \qquad \text{povlači} \qquad k \cdot n \leq m \cdot n.$$

1.3. Decimalni zapis prirodnih i cijelih brojeva. Navedena svojstva[2] zbrajanja, množenja i uređaja omogućuju nam da svaki prirodan (ili cijeli) broj možemo zapisati u decimalnom sustavu, npr. $1028 = 1 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10 + 8$, i da u tom zapisu možemo izvoditi operacije zbrajanja i množenja na uobičajeni način.

2. Polje racionalnih brojeva

2.1. Skup racionalnih brojeva. Skup racionalnih brojeva označavamo slovom $\mathbb{Q}$. Svaki racionalni broj $\alpha \in \mathbb{Q}$ predstavljen je razlomkom[3] $\frac{p}{q}$, gdje je $p \in \mathbb{Z}$ i $q \in \mathbb{N}$, i svaki razlomak predstavlja neki racionalni broj. Po definiciji dva razlomka $\frac{p}{q}$ i $\frac{p'}{q'}$ predstavljaju isti[4] racionalni broj α ako i samo ako je

$$p \cdot q' = p' \cdot q. \tag{2.1}$$

U tom slučaju pišemo

$$\frac{p}{q} = \frac{p'}{q'} = \alpha.$$

---

[2]Sva svojstva prirodnih brojeva, uključujći i operacije zbrajanja i množenja s navedenim svojstvima, mogu se izvesti iz Peanovih aksioma:

(1) 1 je prirodan broj.
(2) Svaki prirodan broj n ima točno jednog sljedbenika n^+ u skupu prirodnih brojeva.
(3) Uvijek je $n^+ \neq 1$, tj. 1 nije sljedbenik nijednog prirodnog broja.
(4) Iz $n^+ = m^+$ izlazi $n = m$, tj. prirodan broj može biti sljedbenik samo jednog ili nijednog prirodnog broja.
(5) *Princip potpune indukcije.* Svaki podskup M skupa prirodnih brojeva $\mathbb{N}$ koji sadrži broj 1 i koji sadrži sljedbenika svakog svojeg elementa, sadrži sve prirodne brojeve, tj. $M = \mathbb{N}$.

Operacija zbrajanja definirana je induktivno: $m + 1 = m^+$, $m + n^+ = (m + n)^+$. Nakon toga se induktivno definira i množenje: $m \cdot 1 = m$, $m \cdot n^+ = m \cdot n + m$, vidi [Md, Teorem 3, I. §3.1, str. 42] ili [B, I. §3, str. 25].

[3]Razlomak $\frac{p}{q}$ je u stvari uređeni par (p, q), pri čemu prvi član para p zovemo brojnikom, a drugi član para q zovemo nazivnikom razlomka (p, q).

[4]Pitanje: Ako razlomci $\frac{p}{q}$ i $\frac{p'}{q'}$ predstavljaju isti racionalni broj i ako razlomci $\frac{p'}{q'}$ i $\frac{p''}{q''}$ predstavljaju isti racionalni broj, da li onda i razlomci $\frac{p}{q}$ i $\frac{p''}{q''}$ predstavljaju isti racionalni broj? Odgovor je da, no koje nam je svojstvo prirodnih (cijelih) brojeva potrebno da to dokažemo?

Tako, na primjer, razlomci $\frac{1}{2}$, $\frac{2}{4}$ i $\frac{5}{10}$ predstavljaju isti racionalni broj "jedna polovina".

Fraza "racionalni broj predstavljen je razlomkom" ne kaže što racionalni broj "u stvari jest". Tu nedorečenost možemo izbjeći ako kažemo da je racionalni broj **skup** svih razlomaka "koji ga predstavljaju", npr. racionalni broj "jedna polovina" je skup[5]

$$\{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots, \frac{1037}{2074}, \dots\}.$$

2.2. Zbrajanje i množenje racionalnih brojeva. Zbrajanje i množenje definirano je formulama

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Pritom treba dokazati da zbroj $\alpha + \beta$ i produkt $\alpha \cdot \beta$ ne ovise o razlomcima kojima su racionalni brojevi α i β predstavljeni. Tako, na primjer,

$$\frac{1}{2} + \frac{2}{4} = \frac{1 \cdot 4 + 2 \cdot 2}{2 \cdot 4} = \frac{8}{8} \quad \text{i} \quad \frac{5}{10} + \frac{5}{10} = \frac{5 \cdot 10 + 5 \cdot 10}{10 \cdot 10} = \frac{100}{100}$$

predstavljaju isti rezultat $1 = \frac{1}{1}$.

2.3. Polje racionalnih brojeva. Primijetimo da su operacije zbrajanja i množenja racionalnih brojeva definirane pomoću zbrajanja i množenja cijelih brojeva.

Operacije zbrajanja i množenja racionalnih brojeva imaju niz svojstava naslijeđenih od svojstava zbrajanja i množenja cijelih brojeva: Obje su operacije asocijativne i komutativne i množenje je distributivno u odnosu na zbrajanje. Nadalje, obje operacije imaju neutralne elemente nulu $\frac{0}{1}$ i jedan $\frac{1}{1}$, a s obzirom na zbrajanje svaki $\alpha = \frac{p}{q}$ ima suprotni element $-\alpha = \frac{-p}{q}$.

---

[5]Neka je S skup. Binarna relacija $\sim$ na S je podskup od $S \times S$, tj. skup nekih uređenih parova (a, b) elemenata $a, b \in S$ za koje onda pišemo $a \sim b$. Kažemo da je $\sim$ *relacija ekvivalencije* ako vrijedi:

(1) $a \sim a$ za svaki $a \in S$ (refleksivnost),
(2) $a \sim b$ povlači $b \sim a$ (simetričnost),
(3) $a \sim b$ i $b \sim c$ povlači $a \sim c$ (tranzitivnost).

Za relaciju ekvivalencije $\sim$ definiramo *klase ekvivalencije* — podskupove od S oblika

$$E_a = \{x \in S \mid x \sim a\}.$$

Ako je presjek E_a i E_b neprazan, onda je $E_a = E_b$. Naime, za $c \in E_a \cap E_b$ imamo $c \sim a$ i $c \sim b$, pa je zbog simetričnosti i tranzitivnosti $a \sim b$. No onda je $E_a \subset E_b$ jer $x \sim a$ i $a \sim b$ povlači $x \sim b$. Slično dokazujemo $E_a \subset E_b$. To znači da su dvije klase ekvivalencije ili jednake ili disjunktne. Zbog refleksivnosti je $a \in E_a$ za svaki $a \in S$, pa je skup S disjunktna unija svih klasa ekvivalencije. Ukratko, svaki $a \in S$ nalazi se u jednoj i samo jednoj klasi ekvivalencije. Još kažemo da je a predstavnik klase kojoj pripada.

Skup čiji su elementi klase ekvivalencije zove se *kvocijentni skup* od S po relaciji $\sim$ (usp. [H1, §1.6]) kojeg obično zapisujemo kao $S/\sim$, tj.

$$S/\sim = \{E_a \mid a \in S\}.$$

Sada možemo reći da je racionalni broj α klasa ekvivalencije u skupu svih razlomaka $\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\} = \mathbb{Z} \times \mathbb{N}$ po relaciji ekvivalencije definiranoj relacijom (2.1):

$$\frac{p}{q} \sim \frac{p'}{q'} \quad \text{ako i samo ako je} \quad p \cdot q' = p' \cdot q.$$

Skup racionalnih brojeva $\mathbb{Q}$ je kvocijentni skup $(\mathbb{Z} \times \mathbb{N})/\sim$.

Međutim, operacija množenja ima svojstvo koje cijeli brojevi nemaju: svaki racionalni broj $\alpha = \frac{p}{q} \neq 0$ ima recipročni element α^{-1} (jednak $\frac{q}{p}$ za $p > 0$ ili $\frac{-q}{-p}$ za $p < 0$).

Zbog navedenih svojstava zbrajanja i množenja govorimo da je skup racionalnih brojeva polje (vidi niže definiciju 5.1).

2.4. Relacija uređaja. Za racinalne brojeve $\alpha = \frac{p}{q}$ i $\beta = \frac{m}{n}$ definiramo

$$\alpha \leq \beta \qquad \text{ako i samo ako je} \qquad p \cdot n \leq m \cdot q.$$

Naravno, prije svega bismo trebali provjeriti da ova definicija ne ovisi o razlomcima koji predstavljaju racionalne brojeve α i β.

Primijetimo da je relacija uređaja $\leq$ na skupu racionalnih brojeva definirana pomoću operacije množenja i relacije uređaja $\leq$ na skupu cijelih brojeva. Tako je

$$\frac{3}{7} < \frac{31}{71} \qquad \text{jer je} \qquad 3 \cdot 71 < 31 \cdot 7.$$

Relacija uređaja $\leq$ na skupu racionalnih brojeva ima niz svojstava naslijeđenih od relacije uređaja na skupu cijelih brojeva: svaka su dva racionalna broja usporediva i relacija je antisimetrična i tranzitivna. Nadalje, relacija je usklađena s operacijama zbrajanja i množenja na skupu racionalnih brojeva. Zbog svih navedeenih svojstava kažemo da je skup racionalnih brojeva $\mathbb{Q}$ uređeno polje.

2.5. Apsolutna vrijednost. Za racionalan broj α definiramo apsolutnu vrijednost $|\alpha|$ tako da je

$$|\alpha| = \begin{cases} \alpha & \text{ako je} \quad \alpha \geq 0, \\ -\alpha & \text{ako je} \quad \alpha < 0. \end{cases}$$

Očito je $|\alpha| \geq 0$ i $|\alpha| = 0$ ako i samo ako je $\alpha = 0$. S obzirom na zbrajanje imamo tzv. relaciju trokuta

$$|\alpha + \beta| \leq |\alpha| + |\beta|,$$

a s obzirom na množenje imamo jednakost

$$|\alpha \cdot \beta| = |\alpha| \cdot |\beta|.$$

2.6. Racionalni brojevi sadrže cijele brojeve. Cijele brojeve $n \in \mathbb{Z}$ možemo shvatiti kao racionalne brojeve predstavljene razlomcima $\frac{n}{1}$. Primijetimo da je identifikacija

$$n \longleftrightarrow \frac{n}{1}$$

u skladu s operacijama zbrajanja i množenja, s jedne strane na $\mathbb{Z}$, a s druge strane na $\mathbb{Q}$:

$$m + n \longleftrightarrow \frac{m+n}{1} = \frac{m}{1} + \frac{n}{1}\,, \qquad m \cdot n \longleftrightarrow \frac{m \cdot n}{1} = \frac{m}{1} \cdot \frac{n}{1}\,.$$

Ta je identifikacija u skladu i s relacijama uređaja: $m \leq n$ u $\mathbb{Z}$ ako i samo ako je $\frac{m}{1} \leq \frac{n}{1}$ u $\mathbb{Q}$. Zbog toga skup cijelih brojeva $\mathbb{Z}$ shvaćamo kao podskup racionalnih brojeva

$$\mathbb{Z} \subset \mathbb{Q}$$

s operacijama zbrajanja i množenja racionalnih brojeva i relacijom uređaja na racionalnim brojevima. Ponekad još kažemo da operacije zbrajanja i množenja i relacija uređaja na $\mathbb{Q}$ **proširuju** operacije zbrajanja i množenja i relacija uređaja na $\mathbb{Z}$.

2.7. Rješavanje linearnih jednadžbi. Promatrajmo linearnu jednadžbu

$$\alpha \cdot x + \beta = 0,$$

gdje su zadani racionalni brojevi $\alpha \neq 0$ i β, a traži se racionalni broj x (obično kažemo nepoznanica x) takav da vrijedi jednakost. Ako takav x postoji, onda dodavanjem suprotnog elementa $-\beta$ objema stranama dobivamo na lijevoj strani

$$(\alpha \cdot x + \beta) + (-\beta) = \alpha \cdot x + (\beta + (-\beta)) = \alpha \cdot x + 0 = \alpha \cdot x$$

(pri čemu smo koristili asocijativnost zbrajanja, svojstvo suprotnog elementa i svojstvo nule u polju racionalnih brojeva), a na desnoj strani dobivamo

$$0 + (-\beta) = -\beta$$

(pri čemu smo koristili svojstvo nule u polju racionalnih brojeva). Znači da je

$$\alpha \cdot x = -\beta.$$

Sada obje strane pomnožimo s recipročnim elementom α^{-1}, pa na lijevoj strani dobivamo

$$\alpha^{-1} \cdot (\alpha \cdot x) = (\alpha^{-1} \cdot \alpha) \cdot x = 1 \cdot x = x$$

(pri čemu smo koristili asocijativnost množenja, svojstvo recipročnog elementa i svojstvo jedinice u polju racionalnih brojeva), a na desnoj strani dobivamo

$$\alpha^{-1} \cdot (-\beta).$$

Znači da, ako postoji, rješenje x mora bit dano formulom

$$x = \alpha^{-1} \cdot (-\beta).$$

Sada "uvrstimo" taj x u lijevu stranu jednadžbe i provjerimo da je to zaista rješenje:

$$\alpha \cdot x + \beta = \alpha \cdot (\alpha^{-1} \cdot (-\beta)) + \beta = (\alpha \cdot \alpha^{-1}) \cdot (-\beta) + \beta = 1 \cdot (-\beta) + \beta = -\beta + \beta = 0$$

(pri čemu smo koristili asocijativnost množenja, svojstvo recipročnog elementa, svojstvo jedinice i svojstvo suprotnog elementa u polju racionalnih brojeva).

Poanta ovog razmatranja je dvostruka. Kao prvo, možemo zaključiti da linearna jednadžba "u polju racionalnih brojeva" uvijek ima jedinstveno rješenje koje dobivamo jednostavnim računom, koristeći pritom svojstva zbrajanja i množenja u polju racionalnih brojeva.

No također primijećujemo da kod našeg računa nije bilo bitno da se radi o racionalnim brojevima, već *da bi isti rezultat vrijedio za bilo kakve "brojeve" kod kojih operacije zbrajanja i množenja imaju ista svojstva!*

Jedan od osnovnih problema linearne algebre je riješavanje sistema jednadžbi s više nepoznanica. Vidjet ćemo da postupak riješavanja sistema nije bitno drugačiji od postupka riješavanja gornje jednadžbe. Zbog toga jedan dio linearne algebre neće ovisiti o "brojevima" s kojima računamo, već samo o svojstvima zbrajanja i množenja koja za te "brojeve" vrijede.

3. Polje realnih brojeva $\mathbb{R}$

Pitanje što su realni brojevi riješeno je na zadovoljavajući način tek krajem 19. i početkom 20. stoljeća[6]. Postoji više ekvivalentnih[7] pristupa:

[6]Za iscrpne komentare o razvoju pojma realnog broja kroz povijest vidi [Mk].

[7]vidi [Md, I. §4. Jedinstvenost i postojanje realnih brojeva]

3.1. Geometrijski pristup. Skup realnih brojeva je (bilo koji izabrani) pravac p u euklidskoj ravnini na kojem su izabrane (bilo koje) međusobno različite točke 0 i 1. Točke na tom pravcu p zovemo realnim brojevima.

Zbroj $\alpha + \beta$ realnih brojeva $\alpha, \beta \in p$ definiramo tako da odmjerimo usmjerenu dužinu (strelicu, vektor) $\overrightarrow{0\beta}$ i prenesemo njen početak na točku α, a kraj te prenesene usmjerene dužine proglasimo zbrojem $\alpha + \beta$.

Množenje realnih brojeva definiramo koristeći teorem o sličnosti trokuta: Neka su $\alpha, \beta \in p$. Odaberemo drugi pravac q, $q \neq p$, koji siječe pravac p u točki 0. Na pravcu q odaberemo točku $1'$ tako da su duljine $\overline{01}$ i $\overline{01'}$ jednake, te točku $\beta' \in q$ tako da su duljine $\overline{0\beta}$ i $\overline{0\beta'}$ jednake, pazeći pritom da su $1'$ i β' na istoj strani (zraci) pravca q u odnosu na 0 ako i samo ako su 1 i β na istoj strani (zraci) pravca p u odnosu na 0. Sada povučemo pravac r kroz točke $1' \in q$ i $\alpha \in p$ i njemu paralelan pravac s kroz točku $\beta' \in q$. Tada pravac s siječe pravac p u jednoj točki X, koju proglasimo umnoškom $X = \alpha \cdot \beta \in p$. Zbog teorema o sličnosti trokuta vrijedi $\overline{0\beta} : \overline{01} = \overline{0X} : \overline{0\alpha}$, što i jest motivacija naše definicije množenja.

Višekratnim nanošenjem usmjerene dužine $\overrightarrow{01}$, počevši od točke 0, dobit ćemo brojeve $1, 2, 3, \ldots$. Dakle $\mathbb{N} \subset \mathbb{R}$. Nanošenjem na drugu stranu usmjerene dužine $\overrightarrow{10}$ dobit ćemo $-1, -2, \ldots$. Dakle $\mathbb{Z} \subset \mathbb{R}$. Korištenjem teorema o sličnosti trokuta možemo konstruirati racionalne brojeve $\frac{1}{2}$, ili $\frac{3}{5}$, ili bilo koji $\frac{p}{q}$. Dakle

$$\mathbb{Q} \subset \mathbb{R},$$

pri čemu operacije zbrajanja i množenja na $\mathbb{R}$ proširuju operacije zbrajanja i množenja na $\mathbb{Q}$.

Geometrijski definirane operacije zbrajanja i množenja na $\mathbb{R}$ su asocijativne i komutativne i množenje je distributivno u odnosu na zbrajanje. Nadalje, obje operacije imaju neutralne elemente nulu i jedan. S obzirom na zbrajanje svaki realni broj α ima suprotni element $-\alpha$, a s obzirom na množenje svaki realni broj broj $\alpha \neq 0$ ima recipročni element α^{-1}.

Zbog navedenih svojstava zbrajanja i množenja govorimo da je skup realnih brojeva polje (vidi niže definiciju 5.1).

Za realan broj α pišemo $\alpha \geq 0$ ako i samo ako se nalazi na zraci s početkom u točki (broju) 0 koja prolazi točkom 1. Općenito pišemo $\alpha \geq \beta$ ako i samo ako

je $\alpha - \beta \geq 0$. To je relacija uređaja ne skupu realnih brojeva: svaka dva realna broja su usporediva i relacija uređaja je antisimetrična i tranzitivna i usklađena je s operacijama zbrajanja i množenja.

Apsolutna vrijednost realnog broja α definira se na isti način kao i u slučaju racionalnih brojeva:

$$|\alpha| = \begin{cases} \alpha & \text{ako je} \quad \alpha \geq 0, \\ -\alpha & \text{ako je} \quad \alpha < 0, \end{cases}$$

a geometrijsko značenje apsolutne vrijednosti $|\alpha - \beta|$ je udaljenost između točaka α i β.

Jedna od poteškoća s geometrijskom definicijom realnih brojeva je što pretpostavlja poznavanje euklidske geometrije. Među inim, jedno od svojstava pravaca u euklidskoj geometriji je i svojstvo potpunosti[8] koje glasi: *svaki Cauchyjev niz realnih brojeva je konvergentan* ili, ekvivalentno, *svaki neprazan odozdo omeđeni skup realnih brojeva A ima najveću donju među* $\inf A$.

3.2. Aksiomatski pristup. Drugi način da "definiramo" realne brojeve je da pobrojimo sva svojstva koja ih određuju (vidi [K2, §1.9 Skup realnih brojeva **R** kao potpuno uređeno polje] ili [Md, I. §2. Realni brojevi]). Svojstva operacija zbrajanja i množenja navedena u definiciji polja (vidi niže definiciju 5.1) je samo dio aksioma za realne brojeve. Motivacija za aksiome realnih brojeva dolazi iz njihove geometrijske interpretacije.

Iz aksioma za skup realnih brojeva $\mathbb{R}$ slijedi da $\mathbb{R}$ sadrži skup svih prirodnih brojeva, skup svih cijelih brojeva i skup svih racionalnih brojeva predstavljenih razlomcima. Posebno

$$\mathbb{Q} \subset \mathbb{R}.$$

3.3. Konstrukcija realnih brojeva iz racionalnih brojeva. Zamislimo si realne brojeve geometrijski, kao pravac u euklidskoj ravnini. Tada je "jasno" da je realan broj α u potpunosti određen skupom svih racionalnih brojeva većih od α, mogli bismo pisati

$$\alpha \longleftrightarrow \{r \in \mathbb{Q} \mid \alpha < r\}.$$

Ključna Dedekindova ideja[9] bila je da takve skupove proglasimo realnim brojevima. Evo Dedekindove definicije: Kažemo da je poskup $\alpha \subset \mathbb{Q}$ prerez[10] ako

(1) α nije prazan skup i α nije čitav skup $\mathbb{Q}$;
(2) ako je $r \in \alpha$ i $s > r$, $s \in \mathbb{Q}$, onda je $s \in \alpha$;
(3) u skupu α nema najmanjeg[11] broja.

Sada skup realnih brojeva $\mathbb{R}$ definiramo kao skup svih (Dedekindovih) prereza.

Zbroj $\alpha + \beta$ dva prereza α i β definiramo kao

$$\alpha + \beta = \{r + s \mid r \in \alpha, s \in \beta\}.$$

(Lako se vidi da je tako definirani skup ponovno prerez.) Primijetimo da u definiciji zbrajanja prereza koristimo zbrajanje racionalnih brojeva. Očito je da tako

[8] U euklidskoj geometriji to se svojstvo pretpostavlja, zovemo ga Cantorovim aksiomom potpunosti.

[9] vidi povijesni i geometrijski prikaz u [Mk, §18]

[10] usp. [B], [Md], [Mk]

[11] To znači da nema racionalnog broja $r \in \alpha$ takvog da je $r \leq s$ za svaki $s \in \alpha$.

definirano zbrajanje prereza naslijeđuje dva dobra svojstva zbrajanja racionalnih brojeva: asocijativnost i komutativnost. Neutralni element za zbrajanje je

$$0 = \{r \in \mathbb{Q} \mid r > 0\},$$

a nešto je teže vidjeti postojanje suprotnog elementa $-\alpha$ za zadani prerez α.

Za prerez α pišemo $\alpha \geq 0$ ako i samo ako je $r > 0$ za svaki $r \in \alpha$. Općenito pišemo $\alpha \geq \beta$ ako i samo ako je $\alpha - \beta \geq 0$. To je relacija uređaja ne skupu svih prereza: svaka dva prerza su usporediva i relacija uređaja je antisimetrična i tranzitivna i usklađena je s operacijom zbrajanja.

Apsolutna vrijednost prereza α definira se na isti način kao i u slučaju racionalnih brojeva:

$$|\alpha| = \begin{cases} \alpha & \text{ako je} \quad \alpha \geq 0, \\ -\alpha & \text{ako je} \quad \alpha < 0. \end{cases}$$

Produkt dva prereza $\alpha \geq 0$ i $\beta \geq 0$ definiramo kao

$$\alpha \cdot \beta = \{r \cdot s \mid r \in \alpha, s \in \beta\},$$

a općenito stavljamo

$$\alpha \cdot \beta = \begin{cases} \alpha \cdot \beta & \text{ako je} \quad \alpha \geq 0, \beta \geq 0, \\ -|\alpha| \cdot \beta & \text{ako je} \quad \alpha < 0, \beta \geq 0, \\ -\alpha \cdot |\beta| & \text{ako je} \quad \alpha \geq 0, \beta < 0, \\ |\alpha| \cdot |\beta| & \text{ako je} \quad \alpha < 0, \beta < 0. \end{cases}$$

Ovako definirano množenje je asocijativno i komutativno i ima jedinicu

$$1 = \{r \in \mathbb{Q} \mid r > 1\}.$$

Nadalje, svaki $\alpha \neq 0$ ima recipročni α^{-1}, množenje je distributivno u odnosu na zbrajanje i relacija uređaja je usklađena s množenjem.

Zbog svih navedenih svojstava kažemo da je skup svih prereza $\mathbb{R}$ uređeno polje. No taj skup ima i svojstvo potpunosti: za neprazan odozdo omeđeni skup realnih brojeva A najveća donja međa $\inf A$ dana je formulom[12]

$$\inf A = \bigcup_{\alpha \in A} \alpha.$$

Drugim riječima, u pristupu realnim brojevima pomoću Dedekindovih prereza svojstvo potpunosti se dokazuje, za razliku od aksiomatskog ili geometrijskog pristupa gdje se potpunost pretpostavlja. No u konstrukciji realnih brojeva pomoću Dedekindovih prereza pretpostavljamo neke druge stvari iz teorije skupova, pa na koncu ispada da su sva tri pristupa logički i matematički ekvivalentna.

Na kraju primijetimo da, u skladu s početnom idejom, svaki racionalni broj s određuje prerez

$$s \longleftrightarrow \{r \in \mathbb{Q} \mid s < r\},$$

pa racionalne brojeve moženo shvatiti kao prereze, a skup racionalnih brojeva kao podskup skupa realnih brojeva:

$$\mathbb{Q} \subset \mathbb{R},$$

[12]Simbol $\bigcup_{\alpha \in A} \alpha$ označava uniju svih skupova (prereza) α koji su elementi od A. Ta unija se sastoji od svih racionalnih brojeva r takvih da je $r \in \alpha$ za neki prerez $\alpha \in A$. Lako se vidi da je taj skup prerez.

pri čemu operacije zbrajanja i množenja na $\mathbb{R}$ proširuju operacije zbrajanja i množenja na $\mathbb{Q}$.

3.4. Realan broj $\sqrt{2}$. Opće je poznato da ne postoji postoji racionalan broj α takav da je $\alpha^2 = 2$. No postoji realan broj α takav da je $\alpha^2 = 2$, označavamo ga $\alpha = \sqrt{2}$. Egzistenciju tog broja možemo dokazati na razne načine:

U geometrijskom pristupu je broj $\sqrt{2}$, po Pitagorinom poučku, duljina dijagonale kvadrata sa stranicom duljine 1.

U aksiomatskom pristupu egzistencija broja $\sqrt{2}$ slijedi primjenom aksioma potpunosti: skup

$$A = \{r \in \mathbb{Q} \mid 2 < r^2\}$$

je neprazan odozdo omeđeni skup, pa po aksiomu potpunosti postoji $\inf A \in \mathbb{R}$. Lako je dokazati da je $\inf A = \sqrt{2}$, tj. da je $(\inf A)^2 = 2$.

U pristupu realnim brojevima pomoću Dedekindovih prereza realan broj $\sqrt{2}$ konstruiramo: skup

$$\alpha = \{r \in \mathbb{Q} \mid 2 < r^2\}$$

je prerez, tj. $\alpha \in \mathbb{R}$. Lako je dokazati da je $\alpha = \sqrt{2}$, tj. $\alpha^2 = 2$.

3.5. Zašto nam trebaju realni brojevi? Budući da su i $\mathbb{Q}$ i $\mathbb{R}$ polja, veliki dio linearne algebre vrijedi jednako i za racionalne i za realne brojeve. Međutim, ne postoji racionalan broj r takav da je $r^2 = 2$, pa ne postoji ni funkcija $x \mapsto \sqrt{x}$ definirana na skupu pozitivnih racionalnih brojeva s vrijednostima u $\mathbb{Q}$. S druge strane, aksiom potpunosti za realne brojeve osigurava egzistenciju funkcije $x \mapsto \sqrt{x}$ definirane na skupu pozitivnih realnih brojeva s vrijednosti u $\mathbb{R}$. Još je važnije da, zbog potpunosti, postoje trigonometrijske funkcije sin i cos i eksponencijalna funkcija exp na skupu realnih brojeva, tj. kao funkcije $\mathbb{R} \to \mathbb{R}$, a koje ne postoje na skupu racionalnih brojeva, tj. kao funkcije $\mathbb{Q} \to \mathbb{Q}$. Jedna je od posljedica egzistencije takvih funkcija da "realna ravnina" $\mathbb{R}^2$ ima rotacije oko ishodišta za svaki kut φ, dok "racionalna ravnina" $\mathbb{Q}^2$ ima rotacije samo za kuteve $\pm\frac{\pi}{2}$ i π. Stoga je geometrijska struktura $\mathbb{R}^2$ puno bogatija od geometrijske strukture $\mathbb{Q}^2$.

4. Polje kompleksnih brojeva $\mathbb{C}$

4.1. Skup kompleksnih brojeva. Kompleksni brojevi su uređeni parovi (α, β) realnih brojeva koje zapisujemo kao $z = \alpha + i\beta$. (Također pišemo $i = 0 + i \cdot 1$ te $i\beta = 0 + i \cdot \beta$.) Prvi član α zovemo realnim dijelom kompleksnog broja z, a drugi član para β zovemo imaginarnim dijelom kompleksnog broja z. Skup svih kompleksnih brojeva označavamo sa $\mathbb{C}$.

4.2. Zbrajanje i množenje. Operacije zbrajanja i množenja definirane su formulama

$$(\alpha + i\beta) + (\alpha' + i\beta') = (\alpha + \alpha') + i(\beta + \beta'),$$
$$(\alpha + i\beta) \cdot (\alpha' + i\beta') = (\alpha\alpha' - \beta\beta') + i(\alpha\beta' + \beta\alpha').$$

Skup $\mathbb{C}$ svih kompleksnih brojeva s tako definiranim operacijama zbrajanja i množenja je polje (vidi niže definiciju 5.1). Štoviše, ako identificiramo realan broj α s kompleksnim brojem $\alpha + i \cdot 0$, onda je $\mathbb{R} \subset \mathbb{C}$ i operacije zbrajanja i množenja na $\mathbb{C}$

proširuju operacije zbrajanja i množenja na $\mathbb{R}$. S obzirom na operacije zbrajanja i množenja, naše razmatranje možemo rezimirati formulom:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}. \tag{4.1}$$

4.3. Konjugiranje kompleksnog broja. Za kompleksan broj $z = \alpha + i\beta$ definiramo kompleksno konjugirani broj $\overline{z} = \alpha - i\beta$. Osnovna svojstva kompleksnog konjugiranja su:

(1) $\overline{\overline{z}} = z$,
(2) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
(3) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,
(4) $z \cdot \overline{z} = \alpha^2 + \beta^2$.

4.4. Apsolutna vrijednost realnog ili kompleksnog broja. Apsolutnu vrijednost kompleksnog broja $z = \alpha + i\beta$ definiramo kao

$$|z| = \sqrt{\alpha^2 + \beta^2}.$$

Imajući u vidu identifikaciju (4.1), apsolutna vrijednost realnog broja α je

$$|\alpha| = \sqrt{\alpha^2}.$$

Ovdje drugi korijen označava **realan broj** ≥ 0. Osnovna svojstva apsolutne vrijednosti su:

(1) $|z| \geq 0$, $|z| = 0$ ako i samo ako je $z = 0$,
(2) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$,
(3) $|z_1 + z_2| \leq |z_1| + |z_2|$ (nejednakost trokuta).

Na skupu kompleksnih brojeva nemamo uređaj koji bi bio analogan uređaju na skupu realnih brojeva. U slučaju kompleksnih brojeva, osim operacija zbrajanja i množenja, osnovnu ulogu igra apsolutna vrijednost. Štoviše, apsolutna vrijednost može preuzeti temeljnu ulogu i u proučavanju realnih brojeva[13]. No valja primijetiti da je osnovno svojstvo apsolutne vrijednosti — nejednakost trokuta — izraženo u terminima uređaja na $\mathbb{R}$.

4.5. Inverz kompleksnog broja različitog od nule. Budući da za kompleksan broj $z \neq 0$ imamo $|z| > 0$, to iz formule $z \cdot \overline{z} = |z|^2$ slijedi

$$z \cdot \frac{\overline{z}}{|z|^2} = 1.$$

Znači da je recipročni element z^{-1} (ili $\frac{1}{z}$) kompleksnog broja $z \neq 0$, kojeg obično zovemo inverznim elementom, dan formulom

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

[13]Koristeći apsolutnu vrijednost možemo definirati konvergentne i Cauchyjeve nizove racionalnih, realnih ili kompleksnih brojeva. Svojstvo potpunosti realnih brojeva naslijeđuje i $\mathbb{C}$: svaki Cauchyjev niz kompleksnih brojeva ima limes u skupu kompleksnih brojeva. Svojstvo potpunosti realnih i kompleksnih brojeva garantira egzistenciju eksponencijalne funkcije

$$\exp\colon \mathbb{C} \to \mathbb{C}, \quad z \mapsto e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!}.$$

Veza kompleksne eksponencijalne funkcije s realnim funkcijama dana je formulom

$$e^{\alpha+i\beta} = e^{\alpha}(\cos\beta + i\sin\beta).$$

4.6. Osnovni teorem algebre. Budući da je $\alpha^2+1 \geq 1$ za svaki realan broj α, to ne postoji realan broj x takav da je $P(x) = x^2+1 = 0$, obično kažemo da $\sqrt{-1}$ nije realan broj.

Naravno, u polju kompleksnih brojeva imamo $i^2+1=0$, pa je i nultočka polinoma $P(x) = x^2+1$, tj. $P(i) = 0$. Jedno od najvažnijih svojstava polja kompleksnih brojeva je da **svaki** polinom $P(x)$ s kompleksnim koeficijentima, stupnja ≥ 1, ima bar jednu nultočku u $\mathbb{C}$, tj. da postoji bar jedan $\lambda \in \mathbb{C}$ takav da je $P(\lambda) = 0$. To je tzv. osnovni teorem algebre, a neposredna posljedica je da za polinom oblika

$$P(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$$

postoje (ne nužno različiti) kompleksni brojevi $\lambda_1, \ldots, \lambda_n$ takvi da je

$$P(x) = (x-\lambda_1)\cdots(x-\lambda_n).$$

Na primjer, u slučaju $P(x) = x^2+1$ imamo $P(x) = (x-i)(x+i)$.

Već smo rekli da je jedan od osnovnih problema linearne algebre riješavanje sistema jednadžbi. Drugi osnovni problem linearne algebre je problem nalaženja nultočaka svojstvenog polinoma linearnog operatora. U rješavanju tog problema kompleksni brojevi i osnovni teorem algebre igraju presudnu ulogu.

5. Pojam polja

U linearnoj algebri, barem na početku, zanimaju nas prije svega algebarska svojstva realnih i kompleksnih brojeva, tj. svojstva operacija zbrajanja i množenja i njihove posljedice. Osnovna svojstva pobrojana su u definiciji polja.

5.1. Definicija polja. Kažemo da je skup K polje ako na tom skupu imamo definirane dvije binarne operacije, *zbrajanje* i *množenje*,

$$+\colon K \times K \to K, \qquad (\alpha,\beta) \mapsto \alpha+\beta,$$
$$\cdot\colon K \times K \to K, \qquad (\alpha,\beta) \mapsto \alpha\cdot\beta,$$

takve da vrijede sljedeća svojstva za sve elemente $\alpha, \beta, \gamma \in K$:

(1) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ (*asocijativnost zbrajanja*),
(2) postoji jedinstveni element $0 \in K$ takav da je $\alpha+0 = 0+\alpha = \alpha$ (*neutralni element za zbrajanje*),
(3) za svaki α postoji jedinstveni element $-\alpha \in K$ takav da je $\alpha+(-\alpha) = (-\alpha)+\alpha = 0$ (*suprotni element za zbrajanje*),
(4) $\alpha+\beta = \beta+\alpha$ (*komutativnost zbrajanja*)
(5) $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma)$ (*asocijativnost množenja*),
(6) postoji jedinstveni element $1 \in K$, $1 \neq 0$, takav da je $\alpha\cdot 1 = 1\cdot\alpha = \alpha$ (*neutralni element za množenje*),
(7) za svaki $\alpha \neq 0$ postoji jedinstveni element $\alpha^{-1} \in K$ takav da je $\alpha\cdot(\alpha^{-1}) = (\alpha^{-1})\cdot\alpha = 1$ (*recipročni element za množenje*),
(8) $\alpha\cdot\beta = \beta\cdot\alpha$ (*komutativnost množenja*),
(9) $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$, $\qquad(\beta+\gamma)\cdot\alpha = \beta\cdot\alpha+\gamma\cdot\alpha$ (*distributivnost množenja prema zbrajanju*).

5.2. Jedinstvenost neutralnog i suprotnog elementa. U našoj definiciji polja zahtijevali smo jedinstvenost neutralnog elementa i jedinstvenost suprotnog (odn. recipročnog) elementa za operaciju zbrajanja (odn. množenja). Pokažimo da je to bilo suvišno:

5.3. Lema. Neka je na skupu G zadana binarna asocijativna operacija

$$\star\colon G \times G \to G, \quad (a,b) \mapsto a \star b.$$

(1) U skupu G postoji najviše jedan element e takav da je

$$a \star e = e \star a = a \quad \text{za svaki} \quad a \in G.$$

(Ako postoji, zovemo ga *jedinicom* u G.)

(2) Neka je e jedinica u G. Za svaki element $a \in G$ postoji najviše jedan element $b \in G$ takav da je

$$a \star b = b \star a = e.$$

(Ako postoji, zovemo ga *inverzom* od a.)

Dokaz. Pretpostavimo da je $a \star e = e \star a = a$ i $a \star e' = e' \star a = a$ za svaki $a \in G$. Tada vrijedi $e' \star e = e \star e' = e'$ i $e \star e' = e' \star e = e$, što povlači $e' = e$.

Pretpostavimo da je e jedinica u G i da je $a \star b = b \star a = e$ i $a \star b' = b' \star a = e$. Tada je $b = b \star e = b \star (a \star b') = (b \star a) \star b' = e \star b' = b'$. □

5.4. Primjeri polja. Primjeri polja su polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$ i polje kompleksnih brojeva $\mathbb{C}$.

U algebri, teoriji brojeva i teoriji kodiranja postoje drugi važni primjeri polja. Najjednostavniji primjer (konačnog) polja je skup $\{0,1\}$; element 0 je "par", element 1 je "nepar". Na tom skupu zbrajanje definiramo kao par + par = par, par + nepar = nepar itd., a množenje kao nepar × nepar = nepar, par × nepar = par itd. Lako je provjeriti da je s tako definiranim zbrajanjem i množenjem skup $\{0,1\}$ polje koje se često označava[14] kao $\mathbb{Z}/2\mathbb{Z}$. Za to polje ne vrijede neka svojstva na koje smo naučeni na primjeru realnih brojeva. Tako, na primjer, u polju $\mathbb{Z}/2\mathbb{Z}$ imamo svojstvo da 1 je suprotan element od 1, tj. $-1 = 1$.

5.5. Injekcija, surjekcija, bijekcija. Neka su A i B dva skupa i f preslikavanje sa skupa A u skup B, pišemo $f\colon A \to B$.

Kažemo da je preslikavanje f *injekcija* ako za $x, y \in A$, $x \neq y$ vrijedi $f(x) \neq f(y)$. Drugim riječima, injekcija pridružuje različitim elementima iz A različite elemente u B.

Kažemo da je preslikavanje f *surjekcija* ako za svaki element $b \in B$ postoji neki element $a \in A$ takav daje $b = f(a)$. Drugim riječima, pri preslikavanju f je svaki element iz B slika nekog elementa iz A.

Kažemo da je preslikavanje f *bijekcija* ako je injekcija i surjekcija.

---

[14] Naime, radi se o kvocijentnom skupu $\mathbb{Z}/\sim$ od $\mathbb{Z}$ po relaciji ekvivalencije

$$n \sim m \quad \text{ako i samo ako je} \quad n - m \in 2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

za koju postoje samo dvije klase ekvivalencije

$$E_0 = \{\dots, -4, -2, 0, 2, 4, \dots\} \quad \text{i} \quad E_1 = \{\dots, -3, -1, 1, 3, \dots\}.$$

Definirajte zbrajanje i množenje klasa tako da zbrajate i množite predstavnike klasa, tj.

$$E_n + E_m = E_{n+m}, \qquad E_n \cdot E_m = E_{nm},$$

pritom treba pokazati da tako uvedene operacije ne ovise o predstavnicima klasa! Budući da za zbrajanje i množenje predstavnika vrijedi asocijativnost, komutativnost distributivnost itd., ta svojstva vrijede i za klase. Budući da $\mathbb{Z}$ općenito nema inverznih elemenata za množenje, taj dio svojstava za $\mathbb{Z}/2\mathbb{Z}$ treba posebno provjeriti.

Ako je f bijekcija, onda možemo identificirati elemente skupa A s elementima skupa B tako da element a identificiramo s njegovom slikom $f(a)$:

$$a \longleftrightarrow f(a).$$

Naime, zbog injektivnosti različite elemente $x, y \in A$ identificiramo s različitim elementima $f(x), f(y) \in B$, a zbog surjektivnosti smo svaki element $b \in B$ identificirali s nekim elementom $a \in A$. Grubo govoreći, ako je f bijekcija, onda skupovi A i B "izgledaju isto".

Ako je f bijekcija, onda postoji *inverzno preslikavanje* $g\colon B \to A$ koje elementima $f(a) \in B$ pridružuje elemente $a \in A$:

$$g\colon f(a) \mapsto a,$$

tj. ako je $b = f(a)$, onda je $g(b) = a$. Očito je inverzno preslikavanje također bijekcija i vrijedi

$$g(f(a)) = a, \qquad f(g(b)) = b.$$

Inverzno preslikavanje g označavamo s f^{-1}.

5.6. Definicija izomorfizma polja. Neka su K i F dva polja. Kažemo da je bijekcija $f\colon K \to F$ *izomorfizam polja* ako je

$$f(\alpha+\beta) = f(\alpha) + f(\beta) \quad \text{i} \quad f(\alpha\cdot\beta) = f(\alpha)\cdot f(\beta)$$

za sve $\alpha, \beta \in K$.

Drugim riječima, ako je f izomorfizam polja, onda možemo identificirati ne samo elemente skupova K i F:

$$\alpha \longleftrightarrow f(\alpha), \quad \beta \longleftrightarrow f(\beta),$$

nego i operacije na tim skupovima:

$$\alpha+\beta \longleftrightarrow f(\alpha+\beta) = f(\alpha)+f(\beta), \quad \alpha\cdot b \longleftrightarrow f(\alpha\cdot\beta) = f(\alpha)\cdot f(\beta).$$

Grubo govoreći, ako je f izomorfizam polja, onda ne samo skupovi K i F, nego i operacije na njima "izgledaju isto". Očito je i $f^{-1}\colon F \to K$ izomorfizam polja.

Kažemo da su dva polja K i F *izomorfna*[15] ako postoji neki izomorfizam polja $f\colon K \to F$. Tada obično pišemo $K \cong F$.

Primjer izomorfnih polja su dvije konstrukcije realnih brojeva: geometrijske i one pomoću Dedekindovih prereza.

Primjeri polja koja očito nisu izomorfna su $\mathbb{Q}$ i $\mathbb{Z}/2\mathbb{Z}$ (jer $\mathbb{Q}$ ima više od dva elementa), $\mathbb{Q}$ i $\mathbb{R}$ (jer $\mathbb{Q}$ nema $\sqrt{2}$), $\mathbb{R}$ i $\mathbb{C}$ (jer $\mathbb{R}$ nema $\sqrt{-1}$).

5.7. Množenje s 0 i -1 u polju. U polju K vrijedi $0\cdot\alpha = 0$ i $(-1)\cdot\alpha = -\alpha$ za svaki $\alpha \in K$.

Dokaz. Stavimo $\beta = 0\cdot\alpha$. Zbog svojstva (2) u definiciji polja 5.1 za nulu imamo $0+0 = 0$ i, koristeći distributivnost (9), imamo $0\cdot\alpha = (0+0)\cdot\alpha = 0\cdot\alpha + 0\cdot\alpha$, tj. $\beta = \beta+\beta$. Dodamo li objema stranama element $-\beta$, koji prema (3) postoji, dobivamo $0 = \beta+(-\beta) = (\beta+\beta)+(-\beta) = \beta+(\beta+(-\beta)) = \beta+0 = \beta$ (ovdje u prvoj jednakosti koristimo svojstvo suprotnog elementa (3), u trećoj asocijativnost zbrajanja (1), u četvrtoj ponovo (3) i u petoj jednakosti (2)). Dakle $\beta = 0$.

[15] izomorfan = istog oblika

Da bismo dokazali drugu tvrdnju, prvo primijetimo da (zbog već dokazane relacije $0 \cdot \alpha = 0$, svojstva suprotnog elementa i distributivnosti) imamo:

$$0 = 0 \cdot \alpha = (1 + (-1)) \cdot \alpha = \alpha + (-1) \cdot \alpha,$$
$$0 = 0 \cdot \alpha = ((-1) + 1) \cdot \alpha = (-1) \cdot \alpha + \alpha.$$

Budući da suprotni element od α mora biti jedinstven, to je $(-1) \cdot \alpha = -\alpha$. □

U slučaju polja $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$ znamo i za neka druga uobičajena pravila koja nisu popisana u definiciji polja. Tako, na primjer, općenito vrijedi $-(-\alpha) = \alpha$ i $(\alpha^{-1})^{-1} = \alpha$ zbog jedinstvenosti suprotnog i recipročnog elementa. Također preuzimamo običaj da pišemo $\alpha - \beta$ umjesto $\alpha + (-\beta)$. Naravno, vrijedi $-(\alpha + \beta) = -\alpha - \beta$.

5.8. Višestruke sume i produkti. Operacije zbrajanja i množenja u polju su binarne operacije, što znači da je definirano zbrajanje i množenje samo dva elementa polja. Imamo li više elemenata $\alpha_1, \alpha_2, \ldots \alpha_n$, onda definiramo

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = (\ldots((\alpha_1 + \alpha_2) + \alpha_3) + \ldots + \alpha_{n-1}) + \alpha_n,$$
$$\alpha_1 \cdot \alpha_2 \cdot \cdots \cdot \alpha_n = (\ldots((\alpha_1 \cdot \alpha_2) \cdot \alpha_3) \cdot \ldots \cdot \alpha_{n-1}) \cdot \alpha_n.$$

Na primjer, $1 + 2 + 3 + 4 = 3 + 3 + 4 = 6 + 4 = 10$. Primijetimo da je po definiciji

$$\begin{aligned}(\alpha_1 + \alpha_2 + \cdots + \alpha_n) + \alpha_{n+1} \\ = ((\ldots((\alpha_1 + \alpha_2) + \alpha_3) + \ldots + \alpha_{n-1}) + \alpha_n) + \alpha_{n+1} \\ = \alpha_1 + \alpha_2 + \cdots + \alpha_n + \alpha_{n+1}.\end{aligned} \tag{5.1}$$

5.9. Lema. Za sve prirodne brojeve n i m i elemente $\alpha_1, \ldots, \alpha_{n+m} \in K$ vrijedi

$$\begin{aligned}(\alpha_1 + \alpha_2 + \cdots + \alpha_n) + (\alpha_{n+1} + \alpha_{n+2} + \cdots + \alpha_{n+m}) \\ = \alpha_1 + \alpha_2 + \cdots + \alpha_n + \alpha_{n+1} + \alpha_{n+2} + \cdots + \alpha_{n+m}.\end{aligned} \tag{5.2}$$

Dokaz. Dokaz provodimo indukcijom po broju sumanada $n+m$. Za $n+m = 2$ imamo $(\alpha_1) + (\alpha_2) = \alpha_1 + \alpha_2$. Pretpostavimo da tvrdnja vrijedi kada je broj sumanada jednak $N - 1 \geq 2$ i pretpostavimo da je $n + m = N$. Ako je $m = 1$, onda je (5.2) upravo formula (5.1). Ako je $m \geq 2$, onda imamo (korištenjem (5.1), asocijativnosti za tri elementa, pretpostavke indukcije i (5.1)):

$$\begin{aligned}&(\alpha_1 + \alpha_2 + \cdots + \alpha_n) + (\alpha_{n+1} + \cdots + \alpha_{n+m-1} + \alpha_{n+m}) \\ &= (\alpha_1 + \alpha_2 + \cdots + \alpha_n) + ((\alpha_{n+1} + \cdots + \alpha_{n+m-1}) + \alpha_{n+m}) \\ &= ((\alpha_1 + \alpha_2 + \cdots + \alpha_n) + (\alpha_{n+1} + \cdots + \alpha_{n+m-1})) + \alpha_{n+m} \\ &= (\alpha_1 + \alpha_2 + \cdots + \alpha_n + \alpha_{n+1} + \cdots + \alpha_{n+m-1}) + \alpha_{n+m} \\ &= \alpha_1 + \alpha_2 + \cdots + \alpha_n + \alpha_{n+1} + \cdots + \alpha_{n+m-1} + \alpha_{n+m}.\end{aligned}$$

□

5.10. Asocijativnost za višestruke sume i produkte. Iz leme 5.9 slijedi da višestruka suma ne ovisi o redoslijedu[16] kojim izvodimo binarnu operaciju zbrajanja. Tako, na primjer

$$\begin{aligned}&\alpha_1+\alpha_2+\alpha_3+\alpha_4\\&=((\alpha_1+\alpha_2)+\alpha_3)+\alpha_4\\&=(\alpha_1+(\alpha_2+\alpha_3))+\alpha_4\\&=(\alpha_1+\alpha_2)+(\alpha_3+\alpha_4)\\&=\alpha_1+((\alpha_2+\alpha_3)+\alpha_4)\\&=\alpha_1+(\alpha_2+(\alpha_3+\alpha_4)).\end{aligned}$$

Na primjeru $(\alpha_1+\alpha_2)+(\alpha_3+\alpha_4)$ vidimo da je svejedno kojim smo redom računali brojeve $\beta=\alpha_1+\alpha_2$ i $\gamma=\alpha_3+\alpha_4$, no svakako smo sumu $\beta+\gamma$ računali na kraju. I u općem slučaju za sume elemenata $\alpha_1,\alpha_2,\ldots,\alpha_n$ s proizvoljno postavljenim zagradama postoji **jedinstvena** operacija zbrajanja koju izvodimo **na samom kraju**, ta zadnja operacija zbrajanja je oblika

($a_1,\ldots,a_s$ sa zagradama i zbrajanjem)+($a_{s+1},\ldots,a_n$ sa zagradama i zbrajanjem).

Po pretpostavci indukcije za manji broj sumanada zaključujemo da je to jednako

$$(a_1+\cdots+a_s)+(a_{s+1}+\cdots+a_n),$$

a primjenom leme 5.9 vidimo da je rezultat jednak $a_1+\cdots+a_n$.

5.11. Primjedba. Budući da smo u ovom razmatranju koristili samo svojstvo asocijativnosti binarne operacije $+$, to isti zaključak vrijedi i za svaku drugu asocijativnu binarnu operaciju, a posebno i za množenje brojeva:

5.12. Lema. Za sve prirodne brojeve n i m i elemente $\alpha_1,\ldots,\alpha_{n+m}\in K$ vrijedi

$$\begin{aligned}&(\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_n)\cdot(\alpha_{n+1}\cdot\alpha_{n+2}\cdot\ldots\cdot\alpha_{n+m})\\&=\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_n\cdot\alpha_{n+1}\cdot\alpha_{n+2}\cdot\ldots\cdot\alpha_{n+m}.\end{aligned}$$

5.13. Komutativnost za višestruke sume i produkte. Proučimo sada posljedicu komutativnosti zbrajanja u računanju višestrukih suma: Neka je $\sigma\colon\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ *permutacija*[17] skupa {1,2,...,n} — preslikavanje za koje je svaki $k\in\{1,2,\ldots,n\}$ slika $\sigma(j)$ jednog i samo jednog elementa $j\in\{1,2,\ldots,n\}$. Permutaciju σ možemo zapisati i kao niz $\sigma(1),\sigma(2),\ldots,\sigma(n)$. U tom zapisu je $1,3,2$ permutacija skupa $\{1,2,3\}$ za koju $1\mapsto1$, $2\mapsto3$, $3\mapsto2$.

---

[16]Po dogovoru, jedan par zagrada ( ) uvijek obuhvaća broj dobiven zbrajanjem već ranije izračunata dva broja. Na taj smo način zagradama označili redoslijed kojim izvodimo operaciju zbrajanja dva po dva broja, pritom ne mijenjajući poredak elemenata $\alpha_1,\alpha_2,\ldots,\alpha_n$ u zapisu operacija zbrajanja.

[17]Permutacija je drugi naziv za bijekciju $\sigma\colon A\to A$ na konačnom skupu A.

5.14. Lema. Za sve permutacije σ skupa $\{1, 2, \ldots, n\}$ i elemente $\alpha_1, \ldots, \alpha_n \in K$ vrijedi

$$\alpha_{\sigma(1)} + \alpha_{\sigma(2)} + \cdots + \alpha_{\sigma(n)} = \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

Dokaz. Za $n = 1$ je tvrdnja očigledna. Pretpostavimo sada da tvrdnja vrijedi za sume od $n-1$ sumanada. Označimo s k element kojeg permutacija σ preslikava u n, tj. $\sigma(k) = n$. Tada je, koristeći lemu 5.9,

$$\begin{aligned}
&\alpha_{\sigma(1)} + \alpha_{\sigma(2)} + \cdots + \alpha_{\sigma(n)} \\
&= (\alpha_{\sigma(1)} + \cdots + \alpha_{\sigma(k-1)}) + \alpha_{\sigma(k)} + (\alpha_{\sigma(k+1)} + \cdots + \alpha_{\sigma(n)}) \\
&= (\alpha_{\sigma(1)} + \cdots + \alpha_{\sigma(k-1)}) + \alpha_n + (\alpha_{\sigma(k+1)} + \cdots + \alpha_{\sigma(n)}) \\
&= (\alpha_{\sigma(1)} + \cdots + \alpha_{\sigma(k-1)}) + (\alpha_{\sigma(k+1)} + \cdots + \alpha_{\sigma(n)}) + \alpha_n \\
&= (\alpha_{\sigma(1)} + \cdots + \alpha_{\sigma(k-1)} + \alpha_{\sigma(k+1)} + \cdots + \alpha_{\sigma(n)}) + \alpha_n \\
&= (\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1}) + \alpha_n \\
&= \alpha_1 + \alpha_2 + \cdots + \alpha_n.
\end{aligned}$$

Komutativnost smo koristili u dokazu treće jednakosti, a predzadnja jednakost vrijedi zbog pretpostavke indukcije, jer je $\sigma(1), \ldots, \sigma(k-1), \sigma(k+1), \ldots, \sigma(n)$ neka permutacija skupa $\{1, 2, \ldots, n-1\}$. □

5.15. Primjedba. Budući da smo u ovom razmatranju koristili samo svojstva asocijativnosti i komutativnosti binarne operacije $+$, to isti zaključak vrijedi i za svaku drugu asocijativnu i komutativnu binarnu operaciju, a posebno i za množenje brojeva:

5.16. Lema. Za svaku permutaciju σ skupa $\{1, 2, \ldots, n\}$ i sve elemente $\alpha_1, \ldots, \alpha_n \in K$ vrijedi

$$\alpha_{\sigma(1)} \cdot \alpha_{\sigma(2)} \cdot \ldots \cdot \alpha_{\sigma(n)} = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n.$$

Na primjer, $\alpha_1 \cdot \alpha_2 \cdot \alpha_3 = \alpha_1 \cdot \alpha_3 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1 \cdot \alpha_3 = \alpha_2 \cdot \alpha_3 \cdot \alpha_1 = \alpha_3 \cdot \alpha_1 \cdot \alpha_2 = \alpha_3 \cdot \alpha_2 \cdot \alpha_1$.

5.17. Oznake za višestruke sume i produkte. Kasnije ćemo ponekad koristiti oznake

$$\sum_{k=1}^{n} \alpha_k = \alpha_1 + \alpha_2 + \cdots + \alpha_n, \qquad \prod_{k=1}^{n} \alpha_k = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n,$$

koje čitamo "suma (elemenata) alfa ka za ka ide od jedan do en" i "produkt (elemenata) alfa ka za ka ide od jedan do en".

U sumi $\sum_{k=1}^{n} \alpha_k$ indeks k zovemo indeksom sumacije. Taj indeks ima "pomoćni ulogu" — "pomaže" nam da označimo elemente koje sumiramo: α_k za $k = 1$ (tj. α_1), α_k za $k = 2$ (tj. α_2), …, α_k za $k = n$ (tj. α_n). Za tu ulogu mogli smo odabrati i neko drugo slovo. Na primjer, elemente koje sumiramo možemo označiti i ovako: α_j za $j = 1$ (tj. α_1), α_j za $j = 2$ (tj. α_2), …, α_j za $j = n$ (tj. α_n). Zato je

$$\sum_{k=1}^{n} \alpha_k = \sum_{j=1}^{n} \alpha_j.$$

Naravno, nije nužno da indeksi budu brojevi. Na primjer, imamo li indekse a, b, c, d pomoću kojih uvodimo "nova slova" α_a, α_b, α_c, α_d, onda nam oznaka

$$\sum_{k=a,b,c,d} \alpha_k$$

označava sumu elemenata α_k za $k = a$ (tj. α_a), α_k za $k = b$ (tj. α_b), α_k za $k = c$ i α_k za $k = d$ (tj. α_d), odnosno $\alpha_a + \alpha_b + \alpha_c + \alpha_d$.

5.18. U daljnjem (uglavnom) nećemo pisati množenje u polju kao $\alpha \cdot \beta$, već uobičajeno $\alpha\beta$.

5.19. Distributivnost množenja u odnosu na višestruke sume. Dokažite indukcijom da vrijedi distributivnost množenja u odnosu na višestruke sume:

$$\lambda \left(\sum_{k=1}^{n} \alpha_k \right) = \sum_{k=1}^{n} \lambda\alpha_k, \qquad \left(\sum_{k=1}^{n} \alpha_k \right) \lambda = \sum_{k=1}^{n} \alpha_k\lambda.$$

5.20. Produkti višestrukih suma. Uzastopnom primjenom distributivnosti za množenje višestrukih suma dobivamo

$$\left(\sum_{k=1}^{n} \alpha_k \right) \left(\sum_{j=1}^{m} \beta_j \right) = \sum_{k=1}^{n} \alpha_k \left(\sum_{j=1}^{m} \beta_j \right) = \sum_{k=1}^{n} \sum_{j=1}^{m} \alpha_k\beta_j = \sum_{\substack{k=1,\ldots,n \\ j=1,\ldots,m}} \alpha_k\beta_j.$$

Ponekad kažemo da smo primijenili pravilo množenja "svakog sa svakim": svaki α_k množili smo sa svim β_j i te produkte zbrojili.

5.21. Različiti indeksi kod produkta višestrukih suma. Valja primijetiti da

$$\left(\sum_{k=1}^{n} \alpha_k \right) \left(\sum_{k=1}^{n} \beta_k \right) = \sum_{k=1}^{n} \sum_{j=1}^{n} \alpha_k\beta_j \neq \sum_{k=1}^{n} \alpha_k\beta_k.$$

Stoga kod množenja višestrukih suma treba koristiti međusobno različite indekse. Na primjer,

$$\left(\sum_{k=1}^{n} \alpha_k \right)^r = \sum_{k_1,k_2,\ldots,k_r=1}^{n} \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_r} \ .$$

Ovdje smo međusobno različite indekse označili s $k_1, k_2, \ldots, k_r$.

5.22. Kroneckerov simbol. Često ćemo koristiti Kroneckerov simbol

$$\delta_{ij} = \begin{cases} 1 & \text{kad je} \quad i = j, \\ 0 & \text{kad je} \quad i \neq j. \end{cases}$$

Tako je, na primjer,

$$\sum_{k=1}^{n} \sum_{j=1}^{n} \delta_{kj}\alpha_k\beta_j = \sum_{k=1}^{n} \alpha_k\beta_k.$$

Literatura

[B] D. Blanuša, *Viša matematika*, I. dio, Tehnička knjiga, Zagreb, 1963.

[E] Neven Elezović, *Linearna algebra*, Element, Zagreb, 2001.

[H1] Krešimir Horvatić, *Linearna algebra*, I. dio, Matematički odjel PMF-a, Sveučilište u Zagrebu, Zagreb, 1995.

[H2] Krešimir Horvatić, *Linearna algebra*, II. dio, Matematički odjel PMF-a, Sveučilište u Zagrebu, Zagreb, 1995.

[H3] Krešimir Horvatić, *Linearna algebra*, III. dio, Matematički odjel PMF-a, Sveučilište u Zagrebu, Zagreb, 1995.

[Kr] Hrvoje Kraljević, *Vektorski prostori*, Sveučilište u Osijeku, Osijek, 2004.

[K1] Svetozar Kurepa, *Konačno dimenzionalni vektorski prostori i primjene*, Tehnička knjiga, Zagreb, 1967.

[K2] Svetozar Kurepa, *Matematička analiza (diferenciranje i integriranje)*, I. dio, Tehnička knjiga, Zagreb, 1989.

[Md] S. Mardešić, *Matematička analiza u n-dimenzionalnom realnom prostoru*, I. dio, Školska knjiga, Zagreb, 1991.

[Mk] Ž. Marković, *Uvod u višu analizu*, I. dio, Sveučilište u Zagrebu, Zagreb, 1961.