# Diskretna matematika 2

## Zadaća 9

March 19, 2025

Borna Gojšić

---

1. Napišite tablice množenja i zbrajanja u polju $(\mathbb{Z}_7, +_7, \cdot_7)$.

**Rj:**

| $+_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| $\cdot_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

2. a) Izračunajte $3(2^3+5)^{-1}+6$ u polju $(\mathbb{Z}_7, +_7, \cdot_7)$.
   b) Riješite jednadžbu $(2x+9)(3x+1)^{-1} = 7$ u polju $(\mathbb{Z}_{11}, +_{11}, \cdot_{11})$.
   c) Riješite jednadžbu $x^2 + 4(x^{-1}+2x+1) = 2$ u polju $(\mathbb{Z}_5, +_5, \cdot_5)$.

**Rj:**

a) $3(2^3+5)^{-1}+6 = 3(1+5)^{-1}+6 = 3\cdot 6^{-1}+6 = 3+6 = 2.$

b) Znamo da $3x+1 \neq 0$ pa imamo $3x \neq 10 = -1$, tj. $x \neq -3 = 8$.

$$\begin{aligned}(2x+9)(3x+1)^{-1} &= 7\\ 2x+9 &= 7(3x+1)\\ 2x+9 &= 9x+7\\ 9x-2x &= 7-9\\ 7x &= 9\end{aligned}$$

Očito je $x = 6$. Budući da je $(\mathbb{Z}_{11}, +_{11}, \cdot_{11})$ polje, rješenje je jedinstveno.

c) Budući da imamo $x^{-1}$ u jednadžbi, znamo da je $x \neq 0$.

$$x^2 + 4(x^{-1}+2x+1) = 2 \implies x^2 + 4x^{-1} + 3x + 4 = 2$$
$$x^2 - x^{-1} + 3x = 3$$

Sada možemo provjeriti sve elemente iz $\{1, 2, 3, 4\}$.

$$\begin{aligned}1^2 - 1^{-1} + 3\cdot 1 &= 1 - 1 + 3 = 3 \quad \checkmark\\ 2^2 - 2^{-1} + 3\cdot 2 &= 4 - 3 + 1 = 2 \neq 3\\ 3^2 - 3^{-1} + 3\cdot 3 &= 4 - 2 + 4 = 1 \neq 3\\ 4^2 - 4^{-1} + 3\cdot 4 &= 1 - 4 + 2 = 4 \neq 3\end{aligned}$$

Dakle, jedino rješenje je $x = 1$.

3. Na skupu racionalnih brojeva definirane su operacije $\triangle$ i $\square$ na sljedeći način:

$$x\triangle y = x + y + 1, \quad x\square y = xy + x + y.$$

Dokažite da je $(\mathbb{Q}, \triangle, \square)$ prsten.

**Rj:** Trebamo dokazati da je $(\mathbb{Q}, \triangle)$ abelova grupa i $(\mathbb{Q}, \square)$ polugrupa te da vrijedi distributivnost.

1. Zatvorenost operacije $\triangle$ slijedi iz zatvorenosti zbrajanja u $\mathbb{Q}$. Imamo

$$(x\triangle y)\triangle z = (x + y + 1) + z + 1 = x + y + z + 2 = x + (y + z + 1) + 1 = x\triangle(y\triangle z)$$

pa vrijedi asocijativnost. Neutralni element je $-1$ jer je

$$x\triangle -1 = x + (-1) + 1 = x = -1 + x + 1 = -1\triangle x$$

Inverz elementa $x$ je $-(x + 2)$ jer je

$$x\triangle(-(x + 2)) = x + (-(x + 2)) + 1 = -1 = -(x + 2) + x + 1 = -(x + 2)\triangle x$$

Također, imamo komutativnost jer je

$$x\triangle y = x + y + 1 = y + x + 1 = y\triangle x$$

Dakle, $(\mathbb{Q}, \triangle)$ je abelova grupa.

2. Zatvorenost operacije $\square$ slijedi iz zatvorenosti množenja i zbrajanja u $\mathbb{Q}$. Imamo

$$(x\square y)\square z = (xy + x + y)z + xy + x + y + z = xyz + xz + yz + xy + x + y + z$$
$$x\square(y\square z) = x(yz + y + z) + x + yz + y + z = xyz + xy + xz + x + yz + y + z$$

pa je $(\mathbb{Q}, \square)$ polugrupa.

3. Još trebamo provjeriti samo distributivnost. Imamo

$$\begin{aligned} x\square(y\triangle z) &= x\square(y + z + 1) = x(y + z + 1) + x + y + z + 1 = xy + x + y + xz + x + z + 1 \\ &= (x\square y) + (x\square z) + 1 = (x\square y)\triangle(x\square z) \end{aligned}$$

$$\begin{aligned} (x\triangle y)\square z &= (x + y + 1)\square z = (x + y + 1)z + x + y + z + 1 = xz + x + z + yz + y + z + 1 \\ &= (x\square z) + (y\square z) + 1 = (x\square z)\triangle(y\square z) \end{aligned}$$

Dakle, $(\mathbb{Q}, \triangle, \square)$ je prsten.

4. Neka su $a \oplus b = a + b - 1$ i $a \otimes b = -\frac{ab}{2}$ binarne operacije na skupu $\mathbb{R}$. Ispitajte ima li $(\mathbb{R}, \oplus, \otimes)$ strukturu prstena.

**Rj:** Trebamo dokazati da je $(\mathbb{R}, \oplus)$ abelova grupa i $(\mathbb{R}, \otimes)$ polugrupa te da vrijedi distributivnost.

1. Zatvorenost operacije $\oplus$ slijedi iz zatvorenosti zbrajanja u $\mathbb{R}$. Imamo

$$(a \oplus b) \oplus c = (a + b - 1) + c - 1 = a + b + c - 2 = a + (b + c - 1) - 1 = a \oplus (b \oplus c)$$

pa vrijedi asocijativnost. Neutralni element je 1 jer je

$$a \oplus 1 = a + 1 - 1 = a = 1 + a - 1 = 1 \oplus a$$

Inverz elementa $a$ je $2 - a$ jer je

$$a \oplus (2 - a) = a + (2 - a) - 1 = 1 = 2 - a + a - 1 = (2 - a) \oplus a$$

Također, imamo komutativnost jer je

$$a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$$

Dakle, $(\mathbb{R}, \oplus)$ je abelova grupa.

2. Zatvorenost operacije $\otimes$ slijedi iz zatvorenosti množenja u $\mathbb{R}$. Imamo

$$(a \otimes b) \otimes c = -\frac{ab}{2} \otimes c = -\frac{\frac{-ab}{2} \cdot c}{2} = \frac{abc}{4} = -\frac{a \cdot \frac{-bc}{2}}{2} = -\frac{a \cdot (b \otimes c)}{2} = a \otimes (b \otimes c)$$

pa je $(\mathbb{R}, \otimes)$ polugrupa.

3. Još trebamo provjeriti samo distributivnost. Imamo

$$a \otimes (b \oplus c) = a \otimes (b + c - 1) = -\frac{a(b + c - 1)}{2} = -\frac{ab + ac - a}{2}$$

ali je

$$(a \otimes b) \oplus (a \otimes c) = -\frac{ab}{2} \oplus -\frac{ac}{2} = -\frac{ab}{2} - \frac{ac}{2} - 1 = -\frac{ab + ac + 2}{2}$$

pa distributivnost ne vrijedi.

Dakle, $(\mathbb{R}, \oplus, \otimes)$ nije prsten.

5. Dokažite da matrice oblika $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$, gdje su $a$ i $b$ racionalni brojevi, uz uobičajeno zbrajanje i množenje matrica čine polje.

**Rj:** Neka je $\mathcal{Q} = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$ Tada je

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} + \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ 2(b+d) & a+c \end{bmatrix} \in \mathcal{Q}$$
$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{bmatrix} \in \mathcal{Q}$$

Dakle, $\mathcal{Q}$ je zatvoren na zbrajanje i množenje matrica. Vrijedi asocijativnost zbrajanja i množenja iz asocijativnosti zbrajanja i množenja matrica. Neutralni element je $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, a inverz od $A = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ je $A^{-1} = \begin{bmatrix} -a & -b \\ -2b & -a \end{bmatrix}$. Distributivnost množenja nad zbrajanjem proizlazi iz distributvnosti matričnog množenja nad zbrajanjem. Dakle, $(\mathcal{Q}, +, \cdot)$ je prsten. Jedinica je očito $I$. Dakle, trebamo provjeriti da postoje inverzi u $(\mathcal{Q} \setminus \{0\}, \cdot)$. Imamo:

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Dakle,

$$ac + 2bd = 1$$
$$ad + bc = 0 \implies c = -\frac{ad}{b}$$
$$a\left(-\frac{ad}{b}\right) + 2bd = 1 \implies d\left(-\frac{a^2}{b} + 2b\right) = 1$$
$$d = \frac{b}{2b^2 - a^2}, \quad c = \frac{-a}{2b^2 - a^2}$$

Budući da je $a, b \neq 0$, to je $2b^2 - a^2 \neq 0$, tj. $\frac{1}{2b^2-a^2} \begin{bmatrix} -a & b \\ 2b & -a \end{bmatrix} \in \mathcal{Q}$. Dakle, $(\mathcal{Q}, +, \cdot)$ je tijelo. Za polje još trebamo dokazati komutativnost množenja:

$$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \begin{bmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{bmatrix} = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix}$$

Dakle, $(\mathcal{Q}, +, \cdot)$ je polje

6. Zadan je skup $T = \{a + b\sqrt{10}\ ;\ a, b \in \mathbb{Q}\}$.
   a) Dokažite da je skup $T$ polje uz uobičajeno zbrajanje i množenje realnih brojeva.
   b) Je li polje $T$ izomorfno polju racionalnih brojeva $(\mathbb{Q}, +, \cdot)$?
   c) Odredite inverz elementa $x = -3 + 2\sqrt{10}$ s obzirom na množenje.

**Rj:**

a) Neka su $x = a + b\sqrt{10}, y = c + d\sqrt{10} \in T$. Tada imamo

$$\begin{aligned} x + y &= (a + c) + (b + d)\sqrt{10} \in T \\ x \cdot y &= (ac + 10bd) + (ad + bc)\sqrt{10} \in T \end{aligned}$$

Dakle, $T$ je zatvoren na zbrajanje i množenje. Vrijedi asocijativnost zbrajanja i množenja jer vrijedi asocijativnost zbrajanja i množenja realnih brojeva. Neutralni element zbrajanja je $0 \in \mathbb{R}$, a neutralni element množenja je $1 \in \mathbb{R}$. Inverz od $x = a + b\sqrt{10}$ s obzirom na zbrajanje je $-a - b\sqrt{10}$. Inverz od $x = a + b\sqrt{10}$ s obzirom na množenje je $\frac{a}{a^2-10b^2} - \frac{b}{a^2-10b^2}\sqrt{10}$ jer je

$$(a + b\sqrt{10})\left(\frac{a}{a^2 - 10b^2} - \frac{b}{a^2 - 10b^2}\sqrt{10}\right) = \frac{a^2}{a^2 - 10b^2} - \frac{10b^2}{a^2 - 10b^2} = 1$$

Distributivnost množenja nad zbrajanjem slijedi iz distributivnosti množenja realnih brojeva nad zbrajanjem. Dakle, $(T, +, \cdot)$ je polje.

b) Neka je $\varphi : T \to \mathbb{Q}$ izomorfizam polja. Tada je $\varphi(0 + 0\sqrt{10}) = 0$ i $\varphi(1 + 0\sqrt{10}) = 1$ jer su to neutralni elementi zbrajanja i množenja. Tada imamo:

$$\begin{aligned} \varphi(2) &= \varphi(1 + 1) = \varphi(1) + \varphi(1) = 2 \\ \varphi(4) &= \varphi(2 + 2) = \varphi(2) + \varphi(2) = 4 \\ \varphi(8) &= \varphi(4 + 4) = \varphi(4) + \varphi(4) = 8 \\ \varphi(10) &= \varphi(8 + 2) = \varphi(8) + \varphi(2) = 10 \end{aligned}$$

ali ako definiramo $q = \varphi(\sqrt{10})$, tada s druge strane imamo:

$$\varphi(10) = \varphi(\sqrt{10} \cdot \sqrt{10}) = \varphi(\sqrt{10}) \cdot \varphi(\sqrt{10}) = q^2 = 10$$

Ali ne postoji $q \in \mathbb{Q}$ takav da je $q^2 = 10$. Dakle, $\varphi$ nije izomorfizam.

c) Neka je $x = -3 + 2\sqrt{10}$. Tada je prema a) dijelu

$$x^{-1} = \frac{-3}{(-3)^2 - 10 \cdot 2^2} - \frac{2}{(-3)^2 - 10 \cdot 2^2}\sqrt{10} = \frac{3}{31} + \frac{2}{31}\sqrt{10}$$

7. Dokažite da je skup $P = \{a + bi \ ; \ a, b \in \mathbb{Z}\}$ prsten uz uobičajeno zbrajanje i množenje kompleksnih brojeva. Je li skup $P$ polje? Obrazložite!

**Rj:** Neka su $z = a + bi, w = c + di \in P$. Tada imamo:

$$\begin{aligned} z + w &= (a + c) + (b + d)i \in P \\ z \cdot w &= (ac - bd) + (ad + bc)i \in P \end{aligned}$$

Dakle, $P$ je zatvoren na zbrajanje i množenje. Vrijedi asocijativnost zbrajanja i množenja jer vrijedi asocijativnost zbrajanja i množenja kompleksnih brojeva. Neutralni element zbrajanja je $0 \in \mathbb{C}$. Inverz od $z = a + bi$ s obzirom na zbrajanje je $-a - bi$. Komutativnost zbrajanja slijedi iz komutativnosti zbrajanja kompleksnih brojeva. Distributivnost množenja nad zbrajanjem slijedi iz distributivnosti množenja kompleksnih brojeva nad zbrajanjem. Dakle, $(P, +, \cdot)$ je prsten. Skup $P$ nije polje jer nema nužno inverz za množenje. Na primjer, $1 + i \in P$ nema inverz jer

$$\begin{aligned} (1 + i)(a + bi) &= 1 \\ (a - b) + (a + b)i = 1 &\implies a = \frac{1}{2}, b = -\frac{1}{2} \end{aligned}$$

ali $a, b \notin \mathbb{Z}$.

8. a) Dokažite da je skup $P = \{a+bi \ ; \ a, b \in \mathbb{Q}\}$ polje uz uobičajeno zbrajanje i množenje kompleksnih brojeva.
   b) Je li polje $P$ izomorfno standardnom polju racionalnih brojeva? Obrazložite!

**Rj:**

a) Neka su $z = a + bi, w = c + di \in P$. Tada imamo:

$$\begin{aligned} z + w &= (a + c) + (b + d)i \in P \\ z \cdot w &= (ac - bd) + (ad + bc)i \in P \end{aligned}$$

Dakle, $P$ je zatvoren na zbrajanje i množenje. Vrijedi asocijativnost zbrajanja i množenja jer vrijedi asocijativnost zbrajanja i množenja kompleksnih brojeva. Neutralni element zbrajanja je $0 \in \mathbb{C}$, a neutralni element množenja je $1 \in \mathbb{C}$. Inverz od $z = a+bi$ s obzirom na zbrajanje je $-a-bi$. Komutativnost zbrajanja i množenja slijedi iz komutativnosti zbrajanja kompleksnih brojeva. Distributivnost množenja nad zbrajanjem slijedi iz distributivnosti množenja kompleksnih brojeva nad zbrajanjem. Inverz od $z = a+bi$ s obzirom na množenje je $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$ jer je

$$(a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\right) = \frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2} = 1$$

pa je $(P, +, \cdot)$ polje.

b) Pretpostavimo da postoji izomorfizam $\varphi : P \to \mathbb{Q}$. Tada je $\varphi(1) = 1$ jer je 1 neutralni element množenja. Također, $\varphi(1) = \varphi(-1 \cdot -1) = \varphi(-1) \cdot \varphi(-1) = 1$, pa je $\varphi(-1) = -1$. Ali, $\varphi(1) = \varphi(i^4) = \varphi(i)^4 = 1$ pa je $\varphi(i) = \pm 1$. Dakle, $\varphi$ nije pa nije ni izomorfizam. Dakle, $P$ nije izomorfno standardnom polju racionalnih brojeva.

9. Je li skup $T = \{a + b\sqrt[4]{2} \ ; \ a, b \in \mathbb{Q}\}$ prsten uz uobičajeno zbrajanje i množenje realnih brojeva?

**Rj:** Ne, jer $\sqrt{2} = \sqrt[4]{2} \cdot \sqrt[4]{2}$ nije u skupu $T$. Pretpostavimo suprotno, neka je $a + b\sqrt[4]{2} \in T$ i $a + b\sqrt[4]{2} = \sqrt{2}$. Tada imamo

$$\begin{aligned} a + b\sqrt[4]{2} &= \sqrt{2} \\ a - \sqrt{2} &= -b\sqrt[4]{2} \\ a^2 - 2a\sqrt{2} + 2 &= b^2\sqrt{2} \\ a^2 + 2 &= (b^2 + 2a)\sqrt{2} \end{aligned}$$

Lijeva strana je racionalna, a desna strana je iracionalna, što je kontradikcija. Dakle, $\sqrt{2} \notin T$.

10. Je li prsten $(\mathbb{Z}_{143}, +_{143}, \cdot_{143})$ integralna domena? Ukoliko jest, dokažite tu tvrdnju, a ukoliko nije navedite odgovarajući kontraprimjer.

**Rj:** Prsten $(\mathbb{Z}_{143}, +_{143}, \cdot_{143})$ nije integralna domena jer je $11 \cdot_{143} 13 = 0$.

11. Dokažite da je skup

$$P = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Z}\}$$

prsten uz uobičajeno zbrajanje i množenje realnih brojeva. Je li taj skup polje? Detaljno obrazložite!

**Rj:** Da bi $(P, +, \cdot)$ bio prsten, $(P, +)$ treba biti abelova grupa i $(P, \cdot)$ polugrupa.

$$\begin{aligned} (a + b\sqrt[3]{3} + c\sqrt[3]{9}) + (d + e\sqrt[3]{3} + f\sqrt[3]{9}) &= (a + d) + (b + e)\sqrt[3]{3} + (c + f)\sqrt[3]{9} \in P \\ (a + b\sqrt[3]{3} + c\sqrt[3]{9}) \cdot (d + e\sqrt[3]{3} + f\sqrt[3]{9}) &= (ad + 3bf + 9ce) \\ &\quad + (ae + bd + 3cf)\sqrt[3]{3} + (af + be + 3cd)\sqrt[3]{9} \in P \end{aligned}$$

Dakle $P$ je zatvoren na zbrajanje i množenje. Komutativnost i asocijativnost slijede iz asocijativnosti i komutativnosti zbrajanja i množenja realnih brojeva. Neutralni element zbrajanja je $0 \in P$, a neutralni element množenja je 1. Inverz od elementa $x = a + b\sqrt[3]{3} + c\sqrt[3]{9}$ s obzirom na zbrajanje je $-a - b\sqrt[3]{3} - c\sqrt[3]{9}$. Distributivnost množenja nad zbrajanjem slijedi iz distributivnosti množenja realnih brojeva nad zbrajanjem. Dakle, $(P, +, \cdot)$ je prsten. Neka je $x = \sqrt[3]{3}$ Tada bi njegov invez s obzirom na množenje bio $x^{-1} = a + b\sqrt[3]{3} + c\sqrt[3]{9}$ za koji je

$$1 = \sqrt[3]{3}(a + b\sqrt[3]{3} + c\sqrt[3]{9}) = 3c + a\sqrt[3]{3} + b\sqrt[3]{9} \implies a = 0, b = 0, c = \frac{1}{3}$$

ali $c \notin \mathbb{Z}$, pa $(P, +, \cdot)$ nije polje.