

Izbrana poglavja iz matematike

Kolobarji

- (1) Poišči vse obrnljive elemente in vse delitelje nič v kolobarjih $\mathbb{Z}_{10}$ in $M_2(\mathbb{R})$.

Rešitev: Kolobar je algebraična struktura, ki jo tvori množica K skupaj z operacijama seštevanja in množenja, ki zadoščata pogojem:

- za seštevanje je K komutativna grupa z enoto 0,
- za množenje je K polgrupa,
- operaciji seštevanja in množenja sta povezani z distributivnostnima zakonoma:

$$a(b + c) = ab + ac,$$

$$(a + b)c = ac + bc,$$

ki morata veljati za vse $a, b, c \in K$.

V splošnem ne zahtevamo komutativnosti množenja ali obstoja enote za množenje. Če ima kolobar K enoto 1, rečemo, da je element $x \in K$ *obrnljiv*, če obstaja tak element $x^{-1} \in K$, da velja

$$xx^{-1} = x^{-1}x = 1.$$

Neničeln element $x \in K$ je *delitelj nič*, če obstaja neničeln element $y \in K$, da je $xy = 0$ ali $yx = 0$.

Kolobar $\mathbb{Z}_{10}$:

V kolobarju ostankov $\mathbb{Z}_{10}$ so obrnljivi elementi $\{1, 3, 7, 9\}$. Vsi ostali elementi pa so delitelji nič, kar sledi iz naslednjih kongruenc:

$$2 \cdot 5 \equiv 0 \pmod{10},$$

$$4 \cdot 5 \equiv 0 \pmod{10},$$

$$6 \cdot 5 \equiv 0 \pmod{10},$$

$$8 \cdot 5 \equiv 0 \pmod{10}.$$

Kolobar $M_2(\mathbb{R})$:

V kolobarju 2×2 realnih matrik so obrnljive natanko matrike z neničelno determinanto. Matrike, ki imajo determinanto enako nič, pa so obenem delitelji nič. Vsaka taka matrika A ima namreč vzporedni vrstici in je zato oblike

$$\begin{bmatrix} ka & kb \\ la & lb \end{bmatrix}$$

za neka realna števila a, b in k, l . Potem lahko preverimo, da velja

$$\begin{bmatrix} ka & kb \\ la & lb \end{bmatrix} \cdot \begin{bmatrix} b & b \\ -a & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Opomba: Kolobarju, v katerem so vsi neničelni elementi obrnljivi, rečemo *obseg*. Znani so obsegi racionalnih, realnih in kompleksnih števil in pa obsegi ostankov po praštevilske

modulu. Ti obsegi so vsi komutativni. Poleg teh se pogosto uporabljajo še Galoisovi obsegi (ti so končni in komutativni) ter obseg kvaternionov (ta obseg je nekomutativen).

Cel kolobar je komutativen kolobar z enoto brez netrivialnih deliteljev nič. Celi kolobarji so posplošitve celih števil, tipični predstavniki pa so kolobarji polinomov s koeficienti v nekem komutativnem obsegu. $\square$

- (2) Opiši grupi obrnljivih elementov v kolobarjih $M_2(\mathbb{Z})$ in $M_2(\mathbb{Z}_2)$.

Rešitev: Kolobar $M_2(\mathbb{Z})$:

Najprej se spomnimo na formulo za inverz 2×2 matrike

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Od tod sklepamo, da je za $A \in M_2(\mathbb{Z})$, ki ima $\det(A) = \pm 1$, tudi njen inverz $A^{-1} \in M_2(\mathbb{Z})$. Sedaj bomo pokazali, da je matrika $A \in M_2(\mathbb{Z})$ obrnljiva v $M_2(\mathbb{Z})$ natanko takrat, ko je $\det(A) = \pm 1$. Pa denimo, da je matrika A obrnljiva in, da je $A^{-1} \in M_2(\mathbb{Z})$. Ker so koeficienti matrik A in A^{-1} cela števila, je tudi $\det(A), \det(A^{-1}) \in \mathbb{Z}$. Iz multiplikativne lastnosti determinante pa od tod dobimo

$$\det(A) \det(A^{-1}) = 1,$$

kar pomeni, da je $\det(A) = \det(A^{-1}) = \pm 1$.

Kolobar $M_2(\mathbb{Z}_2)$:

Kolobar $M_2(\mathbb{Z}_2)$ sestoji iz 16 matrik, obrnljive pa so tiste, ki imajo determinanto enako 1. Takšnih je 6, in sicer so to matrike

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, c = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, d = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, f = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Obrnljivi elementi kolobarja $M_2(\mathbb{Z}_2)$ tvorijo grupo s 6 elementi in enoto e . Preverimo lahko, da velja

$$a^2 = d^2 = f^2 = b^3 = c^3 = e,$$

od koder sklepamo, da je ta grupa izomorfna simetrični grupi S_3 . Množica $\{e, b, c\}$ tvori podgrupo te grupe, če ji dodamo še ničelno matriko, pa je dobljena množica zaprta tudi za seštevanje. Od tod sledi, da je množica

$$F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

obseg s 4 elementi. To je primer končnega obsega, ki ni oblike $\mathbb{Z}_p$ za neko praštevilo p . $\square$

- (3) Naj bo $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ kolobar Gaussovih celih števil.

(a) Poišči vse obrnljive elemente $\mathbb{Z}[i]$.

(b) Poišči vse razcepe števila $2 \in \mathbb{Z}[i]$ na produkt nerazcepnih elementov $\mathbb{Z}[i]$.

Rešitev: (a) Vzemimo poljubno neničelno Gaussovo celo število $a + bi$ in ga za trenutek smatrajmo kot kompleksno število. Njegova obratna vrednost je potem

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

Če hočemo, da bo število $a + bi$ obrnljivo v kolobarju $\mathbb{Z}[i]$, morata biti $\frac{a}{a^2+b^2}$ in $\frac{b}{a^2+b^2}$ celi števili. Hitro se lahko prepričamo, da tem pogojem ustrezajo samo štiri števila

$$1, -1, i, -i.$$

(b) Naj bo $x \neq 0$ Gaussovo celo število, ki ni obrnljivo. Potem rečemo, da je x *nerazcepno*, če iz razcepa $x = yz$ sledi, da je ali y ali pa z obrnljiv element. Nerazcepni elementi so posplošitev praštevil. Število 2 lahko razcepimo na naslednje načine

$$2 = (1 + i)(1 - i) = (-1 - i)(-1 + i).$$

Vidimo, da lahko faktorje v posameznem razcepu množimo z ustreznimi obrnljivimi elementi kolobarja, da dobimo nov razcep. Elementom, ki jih dobimo z množenjem elementa x z obrnljivimi elementi, rečemo, da so *asociirani* elementu x . Elementu $1 + i$ so tako asociirani elementi

$$-1 - i, i - 1, -i + 1.$$

□

(4) Pokaži, da je liho praštevilo $p \in \mathbb{N}$ razcepno v $\mathbb{Z}[i]$ natanko takrat, ko je oblike $p = 4k + 1$.

Rešitev: Ker so naravna števila hkrati tudi Gaussova cela števila, nas bo zanimalo, katera naravna števila lahko razcepimo v kolobarju $\mathbb{Z}[i]$. Če lahko neko naravno število razcepimo v celih številih, je ta razcep dober tudi v kolobarju Gaussovih celih števil, zato so potencialni nerazcepni elementi samo praštevila. Števili 2 in 5 lahko razcepimo v obliki

$$\begin{aligned} 2 &= (1 + i)(1 - i), \\ 5 &= (1 + 2i)(1 - 2i), \end{aligned}$$

kar pomeni, da vsa praštevila niso nerazcepna. V nadaljevanju bomo pokazali, da je liho praštevilo p nerazcepno v $\mathbb{Z}[i]$ natanko takrat, ko je oblike $p = 4k + 3$.

($\Leftarrow$) Denimo sedaj, da je praštevilo p razcepno, kar pomeni, da ga lahko zapišemo v obliki

$$p = (a + ib)(c + id),$$

za neki neobrnljivi Gaussovi celi števili $a + ib$ in $c + id$. Če izračunamo kvadrat absolutnih vrednosti obeh strani, pridemo do enačbe

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Iz predpostavke neobrnljivosti sledi, da faktorja na desni strani nista enaka ena, od tod pa nadalje sledi, da je

$$p = a^2 + b^2 = c^2 + d^2.$$

Ker dajo kvadrati naravnih števil pri deljenju s 4 ostanek bodisi 0 bodisi 1, torej število p ne more biti oblike $p = 4k + 3$, zato je oblike $p = 4k + 1$.

($\Leftarrow$) Denimo, da je praštevilo p oblike $p = 4k + 1$ za neko naravno število k . Pokazali bomo, da lahko potem p razcepimo kot produkt dveh neobrnljivih Gaussovih celih števil. Pokazali smo že, da ima polinom $q(x) = x^2 + 1$ ničlo v $\mathbb{Z}_p$. To pomeni, da obstaja $a \in \mathbb{Z}_p$, da velja

$$a^2 + 1 = np$$

za neko naravno število n . Če bi torej p bil nerazcepen, bi iz enakosti

$$(a + i)(a - i) = np$$

sledilo, da p deli bodisi $a + i$ bodisi $a - i$, kar pa ne gre. Število p je torej razcepeno. $\square$

- (5) Poišči največji skupni delitelj Gaussovih celih števil 30 in $-2 + 6i$ in ju nato zapiši kot produkt nerazcepnih elementov.

Rešitev: Na kolobarju Gaussovih celih števil $\mathbb{Z}[i]$ lahko definiramo normo s predpisom

$$N(a + bi) = a^2 + b^2$$

za poljuben $a + bi \in \mathbb{Z}[i]$. Z uporabo norme lahko definiramo *največji skupni delitelj* števil $z, w \in \mathbb{Z}[i]$ kot število $\gcd(z, w) \in \mathbb{Z}[i]$, ki deli z in w in ima največjo normo izmed vseh skupnih deliteljev. Največji skupni delitelj je določen do obrnljivega elementa natančno.

Za izračun največjega skupnega delitelja uporabljamo prirejen Evklidov algoritem, ki temelji na dejstvu, da lahko za vsak par Gaussovih celih števil z in w zapišemo

$$z = kw + r.$$

Pri tem mora veljati $N(z) > N(w)$, število r pa lahko izberemo tako, da je $N(r) < N(w)$. Po končnem številu takšnih korakov pridemo do največjega skupnega delitelja danih števil. V našem primeru je $N(30) = 900$ in $N(-2 + 6i) = 40$, zato bomo izbrali $z = 30$ in $w = -2 + 6i$. Sledi

$$\frac{30}{-2 + 6i} = \frac{30(-2 - 6i)}{40} = -\frac{3}{2} - \frac{9}{2}i.$$

Kvocienit ni Gaussovo celo število, kar pomeni, da z ni deljiv z w . Kot količnik v takem primeru vzamemo Gaussovo celo število, ki je najbližje številu z/w . Če jih je več, lahko izberemo katerokoli izmed njih. Izberimo na primer $k = -2 - 5i$. Potem je

$$r = z - kw = 30 - (-2 - 5i)(-2 + 6i) = 30 - 4 + 12i - 10i - 30 = -4 + 2i.$$

V naslednjem koraku sedaj postopek ponovimo za par števil w in r . Velja

$$\frac{-2 + 6i}{-4 + 2i} = \frac{(-2 + 6i)(-4 - 2i)}{20} = \frac{8 - 24i + 4i + 12}{20} = 1 - i.$$

Kvocienit je sedaj Gaussovo celo število, kar pomeni, da je

$$-2 + 6i = (-4 + 2i)(1 - i) + 0,$$

zato lahko postopek končamo. Največji skupni delitelj danih števil je torej

$$\gcd(30, -2 + 6i) = -4 + 2i.$$

Razcep števil z in w kot produkt nerazcepnih faktorjev pa je enak

$$\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 = (1 + i)(1 - i)3(-2 + i)(-2 - i), \\ -2 + 6i &= 2(-1 + 3i) = (1 + i)(1 - i)(1 - i)(-2 + i). \end{aligned}$$

$\square$

(6) Poišči vse ideale in maksimalne ideale v kolobarjih $\mathbb{Z}_8$, $\mathbb{Z}_{15}$ in $\mathbb{C}[x]$.

Rešitev: Podmnožica I komutativnega kolobarja K je *ideal*, če zadošča pogoja:

- I je podkolobar K ,
- za poljubna elementa $i \in I$ in $k \in K$ je $ki \in I$.

To pomeni, da je množica I zaprta za seštevanje, odštevanje, množenje ter poljubne večkratnike. Tipični primeri idealov so *glavni* ideali. To so množice večkratnikov nekega danega elementa $k \in K$. Če vzamemo na primer polinom $x \in \mathbb{C}[x]$, je pripadajoči glavni ideal

$$(x) = \{p \in \mathbb{C}[x] \mid p(x) = a_1x + a_2x^2 + \dots + a_nx^n\}$$

množica vseh polinomov z ničelnim konstantnim členom. Ideal I je *maksimalen*, če je $I \neq K$ in je K edini ideal kolobarja K , ki strogo vsebuje I .

Kolobar $\mathbb{Z}_8$:

Kolobar $\mathbb{Z}_8$ ima poleg $\{0\}$ in $\mathbb{Z}_8$ še ideale $I_1 = \{0, 4\} = (4)$ in $I_2 = \{0, 2, 4, 6\} = (2)$. Od teh dveh je I_2 maksimalen, I_1 pa ne.

Kolobar $\mathbb{Z}_{15}$:

V kolobarju $\mathbb{Z}_{15}$ sta zanimiva ideala $I_1 = \{0, 3, 6, 9, 12\} = (3)$ in $I_2 = \{0, 5, 10\} = (5)$, ki sta oba maksimalna.

Kolobar $\mathbb{C}[x]$:

Pokazali bomo, da je vsak ideal I kolobarja $\mathbb{C}[x]$ oblike $I = (p)$ za nek polinom $p \in \mathbb{C}[x]$. Vzemimo torej poljuben netrivialen ideal I in neničeln polinom $p \in I$, ki ima izmed vseh polinomov v I najnižjo stopnjo. Takšnih polinomov je več, izberemo pa lahko poljubnega izmed njih. Naj bo sedaj $q \in I$ poljuben polinom. Po izreku o deljenju polinomov obstajata polinoma $k, r \in \mathbb{C}[x]$, da velja

$$q = kp + r,$$

kjer je $r = 0$ ali pa ima stopnjo nižjo od stopnje p . Ker je $q \in I$ in $kp \in I$, mora biti tudi $r \in I$. Iz predpostavke o minimalnosti stopnje polinoma p od tod sledi, da je $r = 0$ oziroma, da je $q = kp$, kar smo želeli pokazati.

Opišimo sedaj še maksimalne ideale $\mathbb{C}[x]$. Če je polinom $p = st$ produkt dveh nekonstantnih polinomov s in t , je ideal (p) strogo vsebovan v idealih (s) in (t) in torej ne more biti minimalen. Edini kandidati za maksimalne ideale so torej ideali oblike

$$(x - a)$$

za poljuben $a \in \mathbb{C}$.

Opomba: V kolobarju polinomov $F[x]$, kjer je F komutativen obseg, so vsi ideali glavni. Maksimalni ideali pripadajo natanko nerazcepnim polinomom. $\square$

(7) Poišči vse ideale in maksimalne ideale v kolobarjih $M_2(\mathbb{R})$ in $M_2(\mathbb{Z})$.

Rešitev: V primeru nekomutativnih kolobarjev je treba definicijo ideala malce posplošiti. Podmnožica I v nekomutativnem kolobarju K je *ideal*, če je podkolobar in če za poljubna elementa $i \in I$ in $k \in K$ velja $ki \in I$ in $ik \in I$. Preveriti moramo torej, da je množica I zaprta za leve in desne večkratnike.

Ideali kolobarja $M_2(\mathbb{R})$:

Pokazali bomo, da kolobar realnih matrik $M_2(\mathbb{R})$ vsebuje samo dva ideala $I_1 = \{0\}$ in $I_2 = M_2(\mathbb{R})$. Denimo torej, da je I nek netrivialen ideal v $M_2(\mathbb{R})$ in izberimo neničelno matriko

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in I.$$

Po definiciji ideala so potem v I tudi matrike:

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} &= \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 0 & d \end{bmatrix}. \end{aligned}$$

Ker je matrika A neničelna, je vsaj ena od štirih matrik na desni neničelna. Denimo, da je to matrika $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$. Z uporabo permutacijskih matrik lahko to matriko prevedemo na matrike:

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}, \\ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}. \end{aligned}$$

Z množenjem z večkratniki identične matrike in seštevanjem lahko sedaj iz dobljenih matrik izrazimo poljubno matriko v $M_2(\mathbb{R})$. Torej je $I = M_2(\mathbb{R})$.

V nekomutativnih kolobarjih poleg idealov obravnavamo tudi leve in desne ideale. Gre za podgrupe, ki so zaprte samo za množenje z leve ali desne. V kolobarju $M_2(\mathbb{R})$ sta primera levih idealov ideala:

$$\begin{aligned} L_1 &= \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \mid a, c \in \mathbb{R} \right\}, \\ L_2 &= \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{R} \right\}, \end{aligned}$$

primera desnih pa:

$$\begin{aligned} L_1 &= \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \right\}, \\ L_2 &= \left\{ \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} \mid c, d \in \mathbb{R} \right\}. \end{aligned}$$

Ideali kolobarja $M_2(\mathbb{Z})$:

V tem primeru bomo imeli več idealov kot v primeru realnih matrik. Razlog je v tem, da sta v $\mathbb{Z}$ obrnljivi samo števili ± 1 . Denimo, da je I netrivialen ideal $M_2(\mathbb{Z})$ in naj bo n najmanjše naravno število, ki se pojavi v koeficientih vseh matrik v I . Trdimo, da potem velja

$$I = M_2(n\mathbb{Z}).$$

S podobnimi računi kot v prejšnjem primeru lahko pokažemo, da je $M_2(n\mathbb{Z}) \subset I$, zato moramo dokazati še inkluzijo v obratno smer. Denimo, da je

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in I$$

Če tej matriki prištejemo ustrezen večkratnik matrike

$$\begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix}$$

lahko dosežemo, da imamo v zgornjem levem kotu število med 0 in $n - 1$. Ker je po predpostavki n najmanjše naravno število, ki se pojavi v matrikah iz I , mora torej to število biti 0, kar pa pomeni, da je a večkratnik n . Podobno lahko sklepamo tudi za ostale 3 koeficiente. $\square$

- (8) Opiši kvocientna kolobarja $\mathbb{Z}[x]/(x^2 - 3)$ in $\mathbb{Q}[x]/(x^2 - 3)$.

Rešitev: Kolobar $\mathbb{Z}[x]/(x^2 - 3)$ je kolobar ostankov pri deljenju s polinomom $x^2 - 3$, kar pomeni, da je

$$\mathbb{Z}[x]/(x^2 - 3) = \{a_0 + a_1x \mid a_0, a_1 \in \mathbb{Z}\}.$$

Ostanke lahko seštevamo in odštevamo kot običajno, za produkt pa velja

$$(a_0 + a_1x)(b_0 + b_1x) = a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2 = (a_0b_0 + 3a_1b_1) + (a_0b_1 + a_1b_0)x.$$

Pri tem smo upoštevali, da velja v kolobarju $\mathbb{Z}[x]/(x^2 - 3)$ enakost $x^2 = 3$. Preverimo lahko, da je dani kolobar izomorfen kolobarju števil

$$\mathbb{Z}[\sqrt{3}] = \{a_0 + a_1\sqrt{3} \mid a_0, a_1 \in \mathbb{Z}\}.$$

V primeru kolobarja $\mathbb{Q}[x]/(x^2 - 3)$ dobimo na podoben način kolobar ostankov, ki je izomorfen kolobarju števil

$$\mathbb{Q}[\sqrt{3}] = \{a_0 + a_1\sqrt{3} \mid a_0, a_1 \in \mathbb{Q}\}.$$

Računsko lahko preverimo, da je ta kolobar v resnici obseg. Abstraktno pa to na primer sledi iz dejstva, da je polinom $p(x) = x^2 - 3$ nerazcepen v $\mathbb{Q}[x]$, od koder sledi, da je ideal $(x^2 - 3)$ maksimalen.

Opomba: V kolobarju $\mathbb{Z}[x]$ ideal $(x^2 - 3)$ ni maksimalen, saj je na primer vsebovan v idealu $(x^2 - 3, 3) \neq \mathbb{Z}[x]$. Kolobar $\mathbb{Z}[x]/(x^2 - 3)$ posledično ni obseg. Če je namreč K komutativen kolobar z enoto, je kvocientni kolobar K/I obseg natanko takrat, ko je I maksimalen ideal. $\square$

- (9) Zapiši tabeli za seštevanje in množenje v kvocientnem kolobarju $K = \mathbb{Z}[i]/(2)$.

Rešitev: Definicija ideala I v kolobarju K je narejena tako, da je kvocientna množica K/I spet kolobar. Elementi množice K/I so ekvivalenčni razredi oblike $a + I$ za $a \in K$, seštevanje in množenje pa sta definirani s predpisoma:

$$(a + I) + (b + I) = (a + b) + I, \\ (a + I)(b + I) = ab + I.$$

V našem primeru je $I = (2)$ ideal večkratnikov števila 2 v kolobarju Gaussovih celih števil. Ta ideal si lahko predstavljamo kot kvadratno mrežo v kompleksni ravnini, ki sestoji iz vseh števil oblike $z = 2(x + iy) = 2x + 2iy$ za $x, y \in \mathbb{Z}$. V tem primeru ni na prvi pogled jasno, katero množico bi vzeli za množico ostankov, zato bomo na elemente K/I gledali kot na ekvivalenčne razrede. Tako dobimo

$$K/I = \{0 + I, 1 + I, i + I, 1 + i + I\}.$$

Na krajše lahko te štiri ekvivalenčne razrede opišemo z njihovimi predstavniki

$$\{0, 1, i, 1 + i\}.$$

Pri seštevanju in množenju pa moramo biti pozorni, saj vsota in produkt dveh predstavnikov ni nujno predstavnik. V takšnih primerih moramo ugotoviti, v katerem ekvivalenčnem razredu leži vsota in produkt. Tako dobimo na primer:

$$(i + I) + (i + I) = (2i) + I = 0 + I \implies i + i = 0, \\ (i + I)(i + I) = -1 + I = 1 + I \implies i^2 = 1.$$

Tako dobimo tabeli za seštevanje in množenje:

+	0	1	i	$1 + i$	·	0	1	i	$1 + i$
0	0	1	i	$1 + i$	0	0	0	0	0
1	1	0	$1 + i$	i	1	0	1	i	$1 + i$
i	i	$1 + i$	0	1	i	0	i	1	$1 + i$
$1 + i$	$1 + i$	i	1	0	$1 + i$	0	$1 + i$	$1 + i$	0

□

- (10) Naj bo K komutativen kolobar z enoto. Pokaži, da je P praideal v K natanko takrat, ko je K/P cel kolobar.

Rešitev: Ideal P v kolobarju K je *praideal*, če je $P \neq K$ in če za vsaka $a, b \in K$ iz pogoja $ab = P$ sledi, da je bodisi $a \in P$ bodisi $b \in P$.

Denimo najprej, da je P praideal v K . Če je $(a+P)(b+P) = 0$ za neka $a+P, b+P \in K/P$, od tod sledi, da je $ab+P = 0+P$ oziroma $ab \in P$. Po definiciji praideala lahko sklepamo, da je bodisi $a \in P$ bodisi $b \in P$, kar pa pomeni, da je $a+P = 0$ bodisi $b+P = 0$ v K/P . Naj bo sedaj K/P cel kolobar. Če je $ab \in P$, je torej $(a+P)(b+P) = ab+P = 0$ v K/P . Ker po predpostavki K/P nima netrivialnih deliteljev nič, od tod sklepamo, da je bodisi $a+P = 0$ bodisi $b+P = 0$ v K/P . To pa z drugimi besedami pomeni, da je bodisi $a \in P$ bodisi $b \in P$.

Opomba: Vsak maksimalen ideal je tudi praideal, obratno pa ne velja zmeraj. Pri prejšnji analogi smo videli, da je v kolobarju $\mathbb{Z}[x]$ ideal $(x^2 - 3)$ praideal, ki ni maksimalen ideal. □

(11) Poišči vse homomorfizme kolobarjev $\phi : \mathbb{Q} \rightarrow \mathbb{Q}$.

Rešitev: Homomorfizem kolobarjev $\phi : K \rightarrow K'$ je preslikava, ki zadošča pogojema:

$$\begin{aligned}\phi(x + y) &= \phi(x) + \phi(y), \\ \phi(xy) &= \phi(x)\phi(y),\end{aligned}$$

za vsaka $x, y \in K$. Iščemo torej aditivne in multiplikativne preslikave.

Če v zgornji enačbi zaporedoma vstavimo $x = y = 0$ in $x = y = 1$, od tod sledi $\phi(0) = 0$ in $\phi(1) = \phi(1)^2$. V primeru, ko je $\phi(1) = 0$, dobimo ničelni homomorfizem, zato se bomo v nadaljevanju osredotočili na homomorfizme, za katere je $\phi(1) = 1$.

Izberimo sedaj poljuben $n \in \mathbb{N}$. Potem lahko pišemo

$$n = \underbrace{1 + 1 + \dots + 1}_n,$$

zato iz aditivnosti preslikave ϕ sledi

$$\phi(n) = \phi(\underbrace{1 + 1 + \dots + 1}_n) = \underbrace{\phi(1) + \phi(1) + \dots + \phi(1)}_n = \underbrace{1 + 1 + \dots + 1}_n = n.$$

Naj bo sedaj $y = -x$. Potem velja $\phi(0) = \phi(x) + \phi(-x)$ oziroma

$$\phi(-x) = -\phi(x),$$

kar pomeni, da je ϕ liha funkcija. Torej mora biti $\phi(k) = k$ za vsak $k \in \mathbb{Z}$.

Sedaj vzemimo $x = n$ ter $y = \frac{1}{n}$. Iz druge zveze tako dobimo pogoj

$$1 = \phi(1) = \phi(n \cdot \frac{1}{n}) = \phi(n)\phi(\frac{1}{n}) = n\phi(\frac{1}{n}).$$

Torej je

$$\phi(\frac{1}{n}) = \frac{1}{n}$$

za vsako naravno število n . Če je tudi m naravno število, pa velja

$$\phi(\frac{m}{n}) = \phi(m \cdot \frac{1}{n}) = \phi(m)\phi(\frac{1}{n}) = \frac{m}{n}.$$

Skupaj z lihostjo funkcije ϕ od tod sledi, da je

$$\phi(q) = q$$

za vsako racionalno število q . □

(12) Poišči vse homomorfizme kolobarjev:

(a) $\phi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$,

(b) $\phi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_{15}$.

Rešitev: Pri tej nalogi bomo študirali homomorfizme med kolobarji, ki vsebujejo delitelje ničla. V tem primeru še vedno zmeraj velja $\phi(0) = 0$ in $\phi(1) = \phi(1)^2$, lahko pa se zgodi, da ima enačba za $\phi(1)$ več kot dve rešitvi.

Homomorfizmi $\mathbb{Z}_6 \rightarrow \mathbb{Z}_6$:

Enačba $x^2 - x = 0$ ima v kolobarju $\mathbb{Z}_6$ rešitve $x \in \{0, 1, 3, 4\}$. Poleg identitete in ničelnega homomorfizma imamo tako še dva homomorfizma, ki ju lahko podamo v obliki:

$$\phi_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 3 & 0 & 3 & 0 & 3 \end{pmatrix},$$

$$\phi_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 0 & 4 & 2 \end{pmatrix}.$$

Njuni sliki sta izomorfni kolobarjema $\mathbb{Z}_2$ in $\mathbb{Z}_3$.

Homomorfizmi $\mathbb{Z}_6 \rightarrow \mathbb{Z}_{15}$:

V tem primeru si nekoliko olajšamo delo, če upoštevamo, da je $1 + 1 + 1 + 1 + 1 + 1 = 0$ v $\mathbb{Z}_6$. Torej mora biti $6 \cdot \phi(1) = 0$ v $\mathbb{Z}_{15}$. Kandidati za $\phi(1)$ so torej le $\{0, 5, 10\}$. Ker $5 \neq 5^2$ v $\mathbb{Z}_{15}$, sta možnosti le $\phi(1) = 0$ in $\phi(1) = 10$. V prvem primeru dobimo ničelni homomorfizem, v drugem pa

$$\phi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 10 & 5 & 0 & 10 & 5 \end{pmatrix}.$$

Slika ϕ je izomorfna kolobarju $\mathbb{Z}_3$. □

(13) Pokaži, da je preslikava $\phi : \mathbb{C} \rightarrow M_2(\mathbb{R})$ s predpisom

$$\phi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

injektiven homomorfizem kolobarjev.

Rešitev: Aditivnost preslikave ϕ sledi iz definicije seštevanja matrik, zato bomo preverili samo multiplikativnost. Po eni strani je

$$\phi((a + ib)(c + id)) = \phi(ac - bd + i(bc + ad)) = \begin{bmatrix} ac - bd & -bc - ad \\ bc + ad & ac - bd \end{bmatrix},$$

po drugi pa

$$\phi(a + ib)\phi(c + id) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -bc - ad \\ bc + ad & ac - bd \end{bmatrix}.$$

Sedaj bomo pokazali, da homomorfizem ϕ kompleksnemu številu priredi kvadratno realno matriko, ki ustreza množenju s tem številom. Naj bo torej $z = a + ib \in \mathbb{C}$ in $(x, y) \in \mathbb{R}^2$. Če vektor (x, y) identificiramo s kompleksnim številom $x + iy$, lahko definiramo linearno preslikavo $\phi(z) : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ s predpisom

$$\phi(z)(x, y) = z(x + iy) = (a + ib)(x + iy) = (ax - by) + i(bx + ay).$$

Preslikavi $\phi(z)$ potem pripada matrika

$$\phi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Če število z zapišemo v polarni obliki $z = |z|e^{i\phi}$, lahko linearno preslikavo $\phi(z)$ geometrično interpretiramo kot kompozicijo rotacije za kot ϕ okoli $(0, 0)$ in središčnega raztega za faktor $|z|$ s središčem v $(0, 0)$. $\square$

(14) Pokaži, da obstaja natanko en homomorfizem kolobarjev $\phi : M_2(\mathbb{R}) \rightarrow \mathbb{R}$.

Rešitev: Ker je ϕ homomorfizem kolobarjev, mora veljati je $\phi(0) = 0$ in $\phi(I)^2 = \phi(I)$. Torej je lahko bodisi $\phi(I) = 0$ ali pa $\phi(I) = 1$.

(1) Če je $\phi(I) = 0$, od tod sledi, da je $\phi(A) = 0$ za vsako matriko A , kar pomeni, da je ϕ ničelni homomorfizem.

(2) Sedaj bomo pokazali, da nas pogoj $\phi(I) = 1$ pripelje v protislovje. Ker je preslikava ϕ aditivna, je $\phi(-I) = -1$. Matriko $-I$ lahko faktoriziramo v obliki

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

kjer matrika na desni predstavlja rotacijo za 90° . Če to rotacijsko matriko označimo z R , dobimo enakost

$$-1 = \phi(-I) = \phi(R^2) = \phi(R)^2,$$

kar pa ni mogoče v obsegu realnih števil. $\square$

(15) Za poljubno končno množico S definiramo Booleov kolobar $K = \mathcal{P}(S)$ z operacijama:

$$\begin{aligned} A + B &= (A \setminus B) \cup (B \setminus A), \\ A \cdot B &= A \cap B \end{aligned}$$

za poljubni $A, B \subset S$.

(a) Zapiši tabeli za seštevanje in množenje v $\mathcal{P}(S)$, če je $S = \{1, 2\}$.

(b) Konstruiraj izomorfizem kolobarjev $\mathcal{P}(\{1, 2, \dots, n\}) \rightarrow \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_n$.

Rešitev: (a) Kolobar $\mathcal{P}(\{1, 2\})$ ima elemente $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. V duhu izomorfizma, ki ga bomo obravnavali malo kasneje, jih bomo označili z binarnimi besedami dolžine 2 na naslednji način:

$$\begin{aligned} \emptyset &\leftrightarrow 00, \\ \{1\} &\leftrightarrow 10, \\ \{2\} &\leftrightarrow 01, \\ \{1, 2\} &\leftrightarrow 11. \end{aligned}$$

Glede na te oznake lahko zapišemo tabeli za seštevanje in množenje na naslednji način:

+	00	10	01	11	.	00	10	01	11
00	00	10	01	11	00	00	00	00	00
10	10	00	11	01	10	00	10	00	10
01	01	11	00	10	01	00	00	01	01
11	11	01	10	00	11	00	10	01	11

Opazimo lahko, da pri obeh operacijah pravzaprav računamo na vsaki komponenti posebej v obsegu $\mathbb{Z}_2$. Zato je $\mathcal{P}(\{1, 2\}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Naj bo $S = \{1, 2, \dots, n\}$. Potem lahko podmnožice množice S enačimo z binarnimi besedami dolžine n . Če je na i -tem mestu v besedi 1, je element i v podmnožici, sicer pa ne. Tako dobimo bijekcijo

$$w : \mathcal{P}(\{1, 2, \dots, n\}) \rightarrow \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_n.$$

Pokažimo, da je ta bijekcija izomorfizem kolobarjev. Če sta $A, B \subset S$, je $x_i \in A + B$ natanko takrat, ko je $x_i \in A \setminus B$ ali $x_i \in B \setminus A$. Torej je $w(A + B)_i = 1$ natanko takrat, ko je $w(A)_i = 1$ in $w(B)_i = 0$ ali pa $w(A)_i = 0$ in $w(B)_i = 1$. Od tod sledi, da je preslikava w aditivna. Za dokaz multiplikativnosti pa najprej opazimo, da je $x_i \in A \cdot B$ natanko takrat, ko je $x_i \in A$ in $x_i \in B$. Torej je $w(A \cdot B)_i = 1$ natanko takrat, ko je $w(A)_i = 1$ in $w(B)_i = 1$.

Opomba: Boolovi kolobarji so komutativni kolobarji z enico, v katerih je vsak element idempotent. Da se dokazati, da je vsak končen Booleov kolobar izomorfen kolobarju $\mathcal{P}(S)$ za neko končno množico S . $\square$