Alg. strukture – drugi kolokvij - rješenja i bodovanje
27. lipnja 2023.

1. *Neka je $\mathcal{S}$ skup svih matrica $A \in M_2(\mathbb{Z})$ takvih da je $AX = XA$, gdje je matrica $X = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$. Je li $\mathcal{S}$ prsten s jedinicom uz standardne operacije zbrajanja i množenja matrica? Je li $\mathcal{S}$ komutativan prsten?*

(1+2 boda) Ako su $A, B \in \mathcal{S}$, onda je $AX = XA$ i $BX = XB$. I zato imamo

$$(A-B)X = AX-BX = XA-XB = X(A-B) \quad \text{i} \quad (AB)X = A(BX) = A(XB) = (AX)B = X(AB),$$

iz čega zaključujemo da su $A - B \in \mathcal{S}$ i $AB \in \mathcal{S}$. Tojest, $\mathcal{S}$ je potprsten od $M_2(\mathbb{Z})$.

(1 bod) Jer je očito i jedinična matrica $I \in \mathcal{S}$, imamo da je $\mathcal{S}$ potprsten s jedinicom od $M_2(\mathbb{Z})$; i zato je to prsten s jediniccom.

(4 boda) Za provjeru komutativnosti, nađimo oblik matrica $A \in \mathcal{S}$. Ako je $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, onda

$$AX = XA \quad \Leftrightarrow \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix} a-b & 2a-b \\ c-d & 2c-d \end{pmatrix} = \begin{pmatrix} a+2c & b+2d \\ -a-c & -b-d \end{pmatrix}.$$

Usporedbom matričnih koeficijenata u zadnjoj jednakosti imamo: $b = -2c$, $a = b + d$, $a = d - 2c$ i $b = -2c$. Slijedi: $A = \begin{pmatrix} d-2c & -2c \\ c & d \end{pmatrix}$. Sada, za tu matricu A i neku matricu $B = \begin{pmatrix} y-2x & -2x \\ x & y \end{pmatrix} \in \mathcal{S}$ lako provjerimo da je $AB = BA$. (Treba napisati detalje!) Zaključak: $\mathcal{S}$ je komutativan prsten.

Napomena. Krivo argumentiran, ili uopće ne argumentiran, zaključak da je $\mathcal{S}$ nekomutativan prsten nosi 0 bodova.

---

2. *Definirajmo preslikavanje $f : \mathbb{Z}[X] \to M_2(\mathbb{Z})$ s $f(p(X)) := \begin{pmatrix} p(1) & p(1)-p(-1) \\ 0 & p(-1) \end{pmatrix}$. Je li f homomorfizam prstena? Je li f homomorfizam prstena s jedinicom? Ako da, izračunajte jezgru od f i posebno utvrdite je li f monomorfizam prstena.*

(3 boda) Za polinome $p, q \in \mathbb{Z}[X]$ imamo

$$f(pq) = \begin{pmatrix} (pq)(1) & (pq)(1)-(pq)(-1) \\ 0 & (pq)(-1) \end{pmatrix},$$

i isto tako (napisati detalje!)

$$f(p)f(q) = \begin{pmatrix} p(1) & p(1)-p(-1) \\ 0 & p(-1) \end{pmatrix}\begin{pmatrix} q(1) & q(1)-q(-1) \\ 0 & q(-1) \end{pmatrix} = \cdots = \begin{pmatrix} p(1)q(1) & p(1)q(1)-p(-1)q(-1) \\ 0 & p(-1)q(-1) \end{pmatrix}.$$

Zaključujemo da je $f(pq) = f(p)f(q)$. Analogno, ali još jednostavnije, vidi se da imamo i $f(p+q) = f(p) + f(q)$; i zato je f homomorfizam prstena.

(1 bod) Za polinom konstante $j(X) = 1$, koji je jedinica u prstenu $\mathbb{Z}[X]$, imamo da je $f(j) = \begin{pmatrix} j(1) & j(1) - j(-1) \\ 0 & j(-1) \end{pmatrix} = \begin{pmatrix} 1 & 1-1 \\ 0 & 1 \end{pmatrix} = I$, jedinica u prstenu $M_2(\mathbb{Z})$. Dakle, f je homo. prstena s jedinicom.

(1 bod) Tvrdimo da f nije monomorfizam. Naime, jezgra od f je

$$\ker f = \{p \in \mathbb{Z}[X] \mid f(p) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} = \{p \in \mathbb{Z}[X] \mid p(1) = 0 = p(-1)\}.$$

Očito je npr. polinom $X^2 - 1$ u jezgri; pa jee jezgra netrivijalna i zato f nije monomorfizam.

(3 boda) Tvrdimo da je jezgra $\ker f$ jednaka glavnom idealu $G = (X^2 - 1)$. Naime, jer znamo da jezgra od f jest ideal i primijetili smo da je $X^2 - 1 \in \ker f$, slijedi inkluzija $G \subseteq \ker f$. Za obratnu inkluziju, uzmimo proizvoljan $p(X) \in \ker f$. Kako je $p(1) = 0 = p(-1)$, po Bezoutovom teoremu za polinome znamo da i $X - 1$ i $X + 1 = X - (-1)$ dijele polinom $p(X)$. Znači da je $p(X) = (X-1)(X+1)h(X) = (X^2-1)h(X)$, za neki polinom $h(X) \in \mathbb{Z}[X]$. Zaključujemo da je $p(X) \in G$; i zato slijedi inkluzija $\ker f \subseteq G$.

---

3. *Ako neki takvi postoje, odredite sve prirodne brojeve k za koje je skup*

$$B_k := \{ka + 3b\sqrt{6} \mid a, b \in \mathbb{Z}\}$$

ideal u prstenu $A = \mathbb{Z}[\sqrt{6}]$. Postoji li barem jedan takav k za koji je ideal B_k glavni?

(1 bod) Za svaki $k \in \mathbb{N}$ i elemente $w_i = ka_i + 3b_1\sqrt{6} \in B_k$ očito je $w_1 - w_2 \in B_k$; tj., $(B_k, +)$ je aditivna podgrupa grupe $(A, +)$.

(2 bod) Da bi skup B_k bio ideal u prstenu A mora za proizvoljne $x + y\sqrt{6} \in A$ i $ka + 3b\sqrt{6} \in B_k$ biti

$$(x + y\sqrt{6})(ka + 3b\sqrt{6}) = kax + 18by + (3bx + kay)\sqrt{6}$$

element iz B_k. Tu primijetimo kako je A komutativan prsten pa su pojam lijevog ideala i desnog ideala jedno te isto.

(4 boda) No onda to posebno znači da nužno imamo ove uvjete djeljivosti:

$$k|18by \quad \text{i} \quad 3|kay, \qquad \text{za sve } a, b, x, y \in \mathbb{Z}.$$

Posebno za $a = b = x = y = 1$ imamo: $k|18$ i $3|k$. Zaključujemo da dobivamo 4 vrijednosti za k za koje je pripadni skup B_k ideal; to su $k \in \{3, 6, 9, 18\}$.

(1 bod) Primijetimo da je $B_3 = (3)$, glavni ideal.

---

4. *Neka je I ideal u prstenu racionalnih polinoma $A = \mathbb{Q}[X]$ generiran polinomima $2X^3 + 2X$ i $X^3 + X^2 + X + 1$. Je li I glavni ideal? Je li I prost ideal? Je li kvocijentni prsten A/I polje?*

Označimo $f = f(X) = 2X^3 + 2X$ i $g = g(X) = X^3 + X^2 + X + 1$.

(1 bod) Jer je $\mathbb{Q}$ polje, po teoremu s predavanja znamo da je $\mathbb{Q}[X]$ PGI, i zato je posebno ideal $I = (f, g)$ glavni.

(1 bod) Zapravo, jer je $X^2 + 1 = \frac{1}{2}g - f \in I$ te $f = 2X(X^2 + 1)$ i $g = (X + 1)(X^2 + 1)$, zaključujemo da je $I = (X^2 + 1)$.

(4 boda) Tvrdimo da je ideal I maksimalan. Jasno, $I \neq A$. Sada pretpostavimo da postoji neki ideal $M \trianglelefteq A$ takav da je $I \subseteq M \subseteq A$. Zbog činjenice da je A PGI posebno je $M = (m)$, za neki polinom $m = m(X) \in A$. A onda bi posebno bilo $X^2 + 1 \in M$, iz čega slijedi da m dijeli $X^2 + 1$. Ali kako je $X^2 + 1$ ireducibilan polinom u A, jedino je moguće da je $m \in \mathbb{Q}^\times$ ili $m \sim X^2 + 1$ (tj., m i $X^2 + 1$ su asocirani). No ako je prvo, onda je $M = A$; a ako je drugo, onda je $M = I$. No to, po definiciji maksimalnog ideala znači da je ideal I maksimalan.

(1 bod) Na predavanjima smo dokazali ekvivalenciju: Ideal $I \trianglelefteq A$ je maksimalan ako i samo ako je kvocijentni prsten A/I polje. Znači; A/I jest polje.

(1 bod) Na predavanjima smo dokazali da je svaki maksimalan ideal ujedno i prost. Dakle, ideal I je prost.

---

5. *Neka su R i S komutativni prsteni s jedinicama i neka je $\phi : R \to S$ neki epimorfizam.*

   (a) Ako je Y prost ideal u prstenu S, mora li nužno praslika $X := \phi^{-1}(Y)$ biti prost ideal u R? Svoju tvrdnju treba dokazati.

   (b) Ako je R prsten glavnih ideala, mora li i S nužno biti prsten glavnih ideala? Svoju tvrdnju treba dokazati.

(a) **(1 bod)** Znamo da je u komutativnom prstenu ideal prost ako i samo ako je on potpuno prost.

(1 bod) Tvrdimo da je X (potpuno) prost ideal. Prvo, lako vidimo da X jest ideal. Nadalje je $X \neq R$, jer bismo u suprotnom imali $S = \phi(R) = \phi(X) = Y$; što nije jer je Y prost ideal pa po definiciji mora biti $Y \neq S$. (Za zadnju napisanu jednakost koristili smo da je ϕ surjekcija.)

(2 boda) Sada pretpostavimo da su $r_1, r_2 \in R$ takvi da je $r_1 r_2 \in X$. Onda, jer je ϕ homomorfizam i surjekcija, imamo

$$\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(X) = Y.$$

Budući je Y (potpuno) prost ideal, imamo $\phi(r_1) \in Y$ ili $\phi(r_2) \in Y$; i onda $r_1 \in \phi^{-1}(Y) = X$ ili $r_2 \in X$. Po definiciji, X je (potpuno) prost ideal.

(b) **(4 boda)** Tvrdimo da S jest nužno PGI. Da to vidimo, neka je $J \trianglelefteq S$ bilo koji ideal. Tada znamo da je $I := \phi^{-1}(J)$ ideal u R. Jer je R PGI, postoji neki $x_0 \in R$ takav da je $I = (x_0) = Rx_0$. Ali onda, jer je ϕ surjekcija, imamo da je

$$J = \phi(I) = \phi(Rx_0) = \phi(R)\phi(x_0) = S\phi(x_0) = \big(\phi(x_0)\big);$$

tj., J je glavni ideal generiran elementom $\phi(x_0)$.