AS – drugi kolokvij (20.06.2025.) - rješenja i bodovanje

1. *Neka je S skup svih matrica $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Q})$ takvih da su $a+c$ i $b+d$ jednaki cijeli brojevi. Je li S prsten s obzirom na standardne operacije zbrajanja i množenja matrica? Je li S prsten s jedinicom?*

Rješenje. Neka su $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ i $B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ iz S. Onda su brojevi $\alpha := a+c = b+d$ i $\beta := x+z = y+w$ iz $\mathbb{Z}$.

- **(3 boda)** Računamo $A - B = \begin{pmatrix} a-x & b-y \\ c-z & d-w \end{pmatrix}$. I imamo

$$(a-x)+(c-z) = a+c-(x+z) = \alpha - \beta = b+d-(y+w) = (b-y)+(d-w).$$

Jer je i $\alpha - \beta \in \mathbb{Z}$, zaključujemo: $A - B \in S$.

- **(3 boda)** Računamo $AB = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix} := \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ i zatim

$$k_{11} + k_{21} = (ax+bz)+(cx+dz) = (a+c)x + (b+d)z = \alpha x + \alpha z = \alpha\beta \in \mathbb{Z}$$

te isto tako

$$k_{12} + k_{22} = \cdots = \alpha\beta.$$

Slijedi: $AB \in S$.

- **(1 bod)** Jer je $1+0 = 0+1 = 1 \in \mathbb{Z}$, očito je $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$.

- **(1 bod)** Po def. potprstena zaključujemo: S je potprsten s jedinicom prstena $M_2(\mathbb{Q})$.

Napomena. Veliki broj studenata je pri rješavanju zadatka ignorirao uvjet da u matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ iz S mora biti da je $a+c = b+d$ te da je to CIJELI broj. U tom slučaju je uzimano 1 ili 2 boda, ovisno o kontekstu rješavanja zadatka. Isto tako, ukoliko je zadatak rješavan kako je gore dano, trebalo je eksplicite navesti kako smo danim računom dobili da je S POTPRSTEN OD $M_2(\mathbb{Q})$; i stoga je, jasno, i sam prsten za standardne operacije zbrajanja i množenja matrica.

---

2. *Definirajmo preslikavanje $\phi : \mathbb{Q}[X] \to M_2(\mathbb{C})$ s $\phi(p(X)) := \begin{pmatrix} p(\sqrt{3}) & 2p(\sqrt{3}) - 2p(1) \\ 0 & p(1) \end{pmatrix}$. Je li ϕ homomorfizam prstena s jedinicom? Ako da, utvrdite je li ϕ monomorfizam.*

Rješenje. • **(1 bod)** Za $p_1, p_2 \in \mathbb{Q}[X]$ računamo

$$\phi(p_1 + p_2) = \begin{pmatrix} (p_1+p_2)(\sqrt{3}) & 2(p_1+p_2)(\sqrt{3}) - 2(p_1+p_2)(1) \\ 0 & (p_1+p_2)(1) \end{pmatrix} = \cdots = \phi(p_1) + \phi(p_2).$$

• **(3 boda)** Nadalje je

$$\phi(p_1p_2) = \begin{pmatrix} p_1(\sqrt{3})p_2(\sqrt{3}) & 2p_1(\sqrt{3})p_2(\sqrt{3}) - 2p_1(1)p_2(1) \\ 0 & p_1(1)p_2(1) \end{pmatrix}$$

te isto tako

$$\begin{aligned}\phi(p_1)\phi(p_2) &= \begin{pmatrix} p_1(\sqrt{3}) & 2p_1(\sqrt{3}) - 2p_1(1) \\ 0 & p_1(1) \end{pmatrix} \begin{pmatrix} p_2(\sqrt{3}) & 2p_2(\sqrt{3}) - 2p_2(1) \\ 0 & p_2(1) \end{pmatrix} \\ &= \begin{pmatrix} p_1(\sqrt{3})p_2(\sqrt{3}) & p_1(\sqrt{3})\big(2p_2(\sqrt{3}) - 2p_2(1)\big) + \big(2p_1(\sqrt{3}) - 2p_1(1)\big)p_2(1) \\ 0 & p_1(1)p_2(1) \end{pmatrix}.\end{aligned}$$

Nakon sređivanja posljednje dobivene matrice, odmah vidimo da je $\phi(p_1p_2) = \phi(p_1)\phi(p_2)$.

• **(1 bod)** Za polinom konstante $1_{\mathbb{Q}[X]} = 1$ imamo: $\phi(1_{\mathbb{Q}[X]}) = \begin{pmatrix} 1 & 2\cdot 1 - 2\cdot 1 \\ 0 & 1 \end{pmatrix} = I$.

• **(1 bod)** Zaključak: ϕ je homo. prstena s jedinicom.

• **(2 boda)** Računamo jezgru $\ker\phi = \{p \in \mathbb{Q}[X] \mid p(\sqrt{3}) = 0 = p(1)\}$. Ta jezgra je netrivijalan ideal jer je npr. polinom $f(X) := (X^2 - 3)(X - 1)$ u $\ker\phi$. Slijedi: ϕ nije monomorfizam.

Napomena. 1. Određeni broj studenata(precizno rečeno njih 8) još uvijek krivo koristi terminologiju pa pišu "homomorfizam s jedinicom" (ili "homomorfizam s 1"), namjesto ispravno napisanog "homomorfizam prstena s jedinicom". Za to nije uziman 1 bod; ali treba paziti da terminologija i notacija uvijek budu korektno napisani.

2. Ukoliko je napisano "polinom $(X - \sqrt{3})(X - 1)$ je u jezgri od ϕ i zato ϕ nije monomorfizam", to je nekorektna argumentacija za koju se dobije 0 bodova; jer taj polinom uopće NIJE u $\mathbb{Q}[X]$, pa ne može biti niti u jezgri od ϕ.

---

3. *Neka je W skup svih polinoma $f \in \mathbb{Z}[X]$ oblika $f(X) = a_0 + a_1X + \cdots + a_kX^k$, gdje je $k \in \mathbb{N}_0$, a_0 je djeljiv s 12 i a_1 je djeljiv s 3. Je li W ideal u $\mathbb{Z}[X]$? Ako da, je li W maksimalan ideal u $\mathbb{Z}[X]$?*

Rješenje. Neka je $f \in W$ kao u iskazu zadatka te $g(X) = b_1 + b_1X + \cdots + b_\ell X^\ell$ polinom iz $\mathbb{Z}[X]$.

• **(2 boda)** Ako je štoviše $g \in W$, onda posebno $12|a_0, b_0$ i $3|a_1, b_1$. No onda za

$$f - g = a_0 - b_0 + (a_1 - b_1)X + \text{“više potencije”}$$

imamo da $12|a_0 - b_0$ i $3|a_1 - b_1$. Slijedi: $f - g \in W$.

• **(3 boda)** Sada neka su $f \in W$ i $g \in \mathbb{Z}[X]$ proizvoljni. Računamo

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \text{“više potencije”}$$

Jer $12|a_0$, onda $12|a_0b_0$. Nadalje jer $12|a_0$ i $3|a_1$ slijedi da $3|(a_0b_1 + a_1b_0)$. Zaključujemo: $fg \in W$, i zato je $W \trianglelefteq \mathbb{Z}[X]$.

• **(3 boda)** Primijetimo da npr. skup $U \subseteq \mathbb{Z}[X]$ definiran kao skup svih $f(X) = a_0 + a_1X + \cdots + a_kX^k$ takvih da $6|a_0$ i $3|a_1$ je također ideal u $\mathbb{Z}[X]$. (Sasvim ista argumentacija kao i za W!) Nadalje je polinom konstante $C(X) = 6$ u U, ali nije u W; i očito je $W \subseteq U$. Slijedi (po def. maksimalnog ideala) da W nije maks. ideal.

Jednostavniji primjeri su kada za U uzmemo skup svih polinoma $f(X)$ napisanih kao gore, pri čemu je a_0 djeljiv s λ kada je λ jedan od brojeva iz skupa $\{2, 3, 4, 6, 12\}$ (Ima još primjera U t.d. je $W \subset U \subset \mathbb{Z}[X]$.)

---

4. *(a) Neka je A komutativan prsten s jedinicom te neka su K i L ideali u A takvi da je $K + L = A$. Je li moguće da su ideali $K \cap L$ i KL međusobno različiti?*

   (b) Pretpostavimo da je B komutativan prsten s jedinicom, da je $\mathbb{F}$ polje te da postoji neki surjektivan homomorfizam prstena s jedinicom $\alpha : B \to \mathbb{F}$. Je li B nužno polje?

Rješenje. (a) • **(5 bod.)** Znamo s predavanja kako je $KL \subseteq K \cap L$. Tvrdimo da sada vrijedi štoviše jednakost tih ideala. U tu svrhu uzmimo bilo koji $z \in K \cap L$; pa je onda $z \in K$ i $z \in L$. Zatim primijetimo, zbog uvjeta $K + L = A$ i jer znamo (propozicija s predavanja) da je $K + L = \{k + \ell \mid k \in K, \ \ell \in L\}$, kako postoje neki $k_0 \in K$ i $\ell_0 \in L$ t.d. je $k_0 + \ell_0 = 1_A$. No onda je

$$z = z\,1_A = z(k_0 + \ell_0) = zk_0 + z\ell_0 = k_0 z + z\ell_0.$$

Ali jer je $k_0 z \in KL$ i $z\ell_0 \in KL$, zaključujemo da je i $z \in KL$. Slijedi da je $K \cap L \subseteq KL$; pa onda i $K \cap L = KL$.

(b) • **(3 boda)** Neka je $B = \mathbb{Z}$. Znamo da je to komut. prsten s jedinicom te da nije polje. Uzmimo ideal $M := 2\mathbb{Z}$ u B. Znamo da je to maksimalan ideal u B. Po jednom teoremu s predavanja je onda kvocijentni prsten $\mathbb{F} := B/M = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ polje (od 2 elementa). Ako uzmemo da je α upravo kanonski epimorfizam $\pi_M : B \to \mathbb{F}$, onda smo u uvjetima (b) dijela zadatka. Zaključak: B nije nužno polje.

Ima još mnoštvo primjera. Npr. za $\mathbb{F}$ polje i bilo koju evaluaciju $\alpha : \mathbb{F}[X] \to \mathbb{F}$. Ili za $\mathbb{F}$ bilo koje polje i A bilo koji komut. prsten s jedinicom gledamo prvu projekciju $\alpha : \mathbb{F} \times A \to \mathbb{F}$, $\alpha(f, a) := f$. Ili...

Napomena. Iako je (a) dio zadatka bio dan kao domaća zadaća i na predavanjima i na vježbama, samo je jedna studentica iskazala da je nužno $KL = K \cap L$ te to "gotovo korektno dokazala". Onima koji su u korektnoj formi naveli da rečena jednakost nužno vrijedi, ali to nisu dokazali, dan je 1 bod.

U ovom zadatku, i (a) i u (b) dijelu, prilikom pokušaja rješavanja pisalo se "sve i svašta". Dobronamjeran je savjet da ukoliko nemamo niti ideju što bi moglo vrijediti i/ili nemamo ieju kako nešto dokazati, onda je uputnije niti ne pokušavati, a ne pisati potpune besmislice i/ili krive stvari pozivajući se na nepostojeće "teoreme".

---

5. *Je li polinom $p(X) = X + 1$ prost element u prstenu polinoma $\mathbb{Z}[X]$?*

Rješenje. Tvrdimo: *$p = p(X)$ je prost element u prstenu $\mathbb{Z}[X]$.*

• **(1 bod)** Jasno; p nije nul-polinom i nije invertibilan element, tako da imamo ispunjen prvi uvjet iz definicije prostog elementa. (Invertibilni elementi u $\mathbb{Z}[X]$ su samo konstantni polinomi 1 i -1.)

• **(7 bod.)** Pretpostavimo sada da su $g, h \in \mathbb{Z}[X]$ t.d. $p|gh$. Onda je $gh = p\varphi$, za neki $\varphi \in \mathbb{Z}[X]$. Slijedi, ako uvrstimo $X = -1$, da je

$$g(-1) \cdot h(-1) = p(-1) \cdot \varphi(-1) = 0 \cdot \varphi(-1) = 0 \quad \Rightarrow \quad g(-1) = 0 \text{ ili } h(-1) = 0.$$

Sada, ako je $g(-1) = 0$, onda $p|g$. Naime, po *Teoremu o dijeljenju s ostatkom za polinome*, postoje neki $q = q(X)$ i polinom konstante r iz $\mathbb{Z}[X]$ t.d. je $g(X) = q(X)p(X) + r$. (Bitno je primijetiti kako je vodeći koeficijent polinoma $p(X)$ jednak 1, što je invertibilan element u $\mathbb{Z}$; pa možemo dijeliti g polinomom p.) Ako i sada uvrstimo $X = -1$, i koristimo da je $g(-1) = 0 = p(-1)$, dobivamo da je $r = 0$. Slijedi da je $g = qp$ i zato doista $p|g$.

Ako je $h(-1) = 0$, analognim zaključivanjem dobijemo da $p|h$. Tako vidimo da vrijedi i drugi uvjet iz definicije prostog elementa.

Napomena. Kako znamo s predavanja, prsten $\mathbb{Z}[X]$ nije DGI. I zato nije moguće dokazati da je $p(X)$ prost element tako da pokažemo da je to ireducibilan element. (Znamo po jednoj propoziciji s predavanja da ako je prsten A ujedno i DGI, onda su pojmovi prostog elementa i ireducibilnog elementa ekvivalentni. No ako prsten A jest int. domena, ali nije i DGI, onda samo znamo da je svaki prost element nužno ireducibilan; ali ne nužno i obratno.)
