

Algebrai struktúrák

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Melyek gyűrűk, integritási tartományok, ill. testek az alábbiak közül? Amelyik nem igaz, ott mely tulajdonság nem teljesül?
a) $\mathbb{N}$, b) $\mathbb{Z}$, c) $\mathbb{Q}$, d) $\mathbb{R}$, e) $\mathbb{C}$,
f) $2\mathbb{Z}$, g) $2\mathbb{Z} + 1$, h) $\mathbb{Q} \setminus \mathbb{Z}$,
i) $\mathbb{Z}_2$, j) $\mathbb{Z}_3$, k) $\mathbb{Z}_4$, l) $\mathbb{Z}_5$,
m) $\mathbb{R}[x]$, n) $\mathbb{Z}[x]$, o) $\mathbb{Z}_7[x]$, p) $\mathbb{Z}_8[x]$,
q) $\mathbb{Q}^{5 \times 5}$, r) $\mathbb{R}^{4 \times 4}$, s) $\mathbb{Z}^{2 \times 3}$.
2. Mi a nullelem, ill. egységelem (ha van) az alábbi gyűrűkben:
a) $\mathbb{Z}$, b) $\mathbb{Z}_3$, c) $2\mathbb{Z}$, d) $\mathbb{Z}^{3 \times 3}$, e) $\mathbb{Z}[x]$?
3. Mit jelent a nullosztó? Adjunk rá példát *két* különböző gyűrűben.
4. Milyen m -ekre nullosztómentes $\mathbb{Z}_m$? Ha nem az, mely elemek nullosztók?
5. Adjunk meg az alábbi elemek multiplikatív inverzét, ha létezik:
a) $4 \in \mathbb{Q}$, b) $-1 \in \mathbb{Z}$, c) $2 \in \mathbb{Z}$, d) $i \in \mathbb{C}$, e) $\bar{3} \in \mathbb{Z}_5$, f) $\bar{3} \in \mathbb{Z}_6$, g) $\bar{1} \in \mathbb{Z}_7$,
h) $2x^2 \in \mathbb{R}[x]$, i) $2 \in \mathbb{R}[x]$, j) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$, k) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$.
6. a) Legfeljebb hány gyöke lehet egy másodfokú polinomnak $\mathbb{Z}_5[x]$ -ben?
b) Legfeljebb hány gyöke lehet egy másodfokú polinomnak $\mathbb{Z}_6[x]$ -ben?
7. Számítsuk ki azt a $p \in \mathbb{Z}_7[x]$ másodfokú polinomot, amelyre $p(\bar{2}) = \bar{4}$, $p(\bar{3}) = \bar{2}$ és $p(\bar{4}) = \bar{6}$.

Programozási feladatok

8. Végezzük el egy tetszőleges bemenő gyűrűn az alábbi feladatokat. Minden részfeladatra írjunk egy-egy függvényt, amelyek egyetlen listát várnak, a gyűrű elemeit. (Tehát **nem** Sage algebrai struktúrát várnak, pl. `Zmod(10)`, hanem az elemek listáját, pl. `list(Zmod(10))`.) Az elemekről **semmi mást** ne használjunk, csak a gyűrű két műveletét ($a + b$ és $a * b$) és egyenlőségvizsgálatot ($a == b$ és $a != b$), valamint azt az absztrakt tényt, hogy gyűrűt alkotnak.
- a) Döntsük el, hogy a gyűrű kommutatív-e.
Próbáljuk ki $\mathbb{Z}_{10}$ -re (`list(Zmod(10))`) és $\mathbb{Z}_3^{2 \times 2}$ -re (`list(Mat(Zmod(3), 2))`).
 - b) Adjuk vissza a gyűrű nullelemét.
Próbáljuk ki $\mathbb{Z}_{10}$ -re és $\mathbb{Z}_3^{2 \times 2}$ -re.
 - c) Adjuk vissza a gyűrű egységelemét, ha van, különben adjunk `None`-t.
Próbáljuk ki $\mathbb{Z}_{10}$ -re, $2\mathbb{Z}_{20}$ -ra és $2\mathbb{Z}_{10}$ -re. (Itt $2\mathbb{Z}_m$ a $\mathbb{Z}_m$ páros elemeiből álló gyűrűt jelenti, és például így állítható elő: `list(Zmod(10))[:2]`.) Meglepő eredményt kapunk?
 - d) Keressünk nullosztót a gyűrűben, és ha van, adjunk vissza egyet, különben adjunk `None`-t.
Próbáljuk ki $\mathbb{Z}_5$ -re és $\mathbb{Z}_6$ -ra.
 - e) Döntsük el, hogy a gyűrű integritási tartomány-e.
 $\mathbb{Z}_1$ -től $\mathbb{Z}_{20}$ -ig melyek azok?
9. Állítsuk elő azt a $p \in \mathbb{Z}_{11}[x]$ polinomot, melynek minden $c \in \mathbb{Z}_{11}$ gyöke, kivéve ezt a kettőt: $\bar{0}, \bar{1} \in \mathbb{Z}_{11}$. Minden gyöke egyszeres, kivéve a $c = \bar{2}$ -t, amely kétszeres.
10. Keressünk olyan másodfokú polinomot $\mathbb{Z}_6[x]$ -ben, melynek $\mathbb{Z}_6$ mind a hat eleme gyöke. (Tipp: a másodfokú polinomok $ax^2 + bx + c$ alakúak, és minden együttható csak véges sokféle lehet.)
11. Tudjuk, hogy $1/x$ nem polinom. Sőt, nincs is olyan polinom, amely minden nemnulla x -re ugyanazt az értéket venné föl, mint $1/x$ – legalábbis számpolinomok esetén. De véges gyűrűk fölött lehetséges. Állítsuk elő azt a $p \in \mathbb{Z}_{97}[x]$ polinomot, melyre $\deg p = 95$ és $\forall a \in \mathbb{Z}_{97} \setminus \{\bar{0}\} : p(a) = 1/a = a^{-1}$.
12. a) Írjuk át az előző feladatsorból a Shamir-féle titokmegosztást (13. feladat) $\mathbb{Z}_p$ -re, ahol p egy prímszám, amely szintén legyen paramétere a titokrészeket generáló függvénynek. Az együtthatók tetszőleges $\mathbb{Z}_p$ -beli véletlen számok legyenek.
- b) Ismételjük meg az előző feladatsorban szereplő tesztet a Shamir-féle titokmegosztás biztonságára vonatkozóan (14. feladat), ezúttal $\mathbb{Z}_{89}$ -ben (értelemszerűen változtatva y_5 lehetséges értékeit). Biztonságosabb lett?