Mat-alkmat gyakorlat, első évfolyam első félév

Nyolcadik alkalom (2003 nov. 10–12)

1. *Az alábbi struktúrák gyűrűk-e? Ha igen, kommutatívak-e, egységelemesek-e, nullosztómentesek-e, testek-e? A kommutatív gyűrűkben határozzuk meg az invertálható elemeket.*

a) $\{a+bi \mid a,b \in \mathbb{Q}\}$, $\{a+bi \mid a,b \in \mathbb{Z}\}$, $\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, $\{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Q}\}$ *a szokásos összeadásra és szorzásra nézve.*

b) $\mathbb{C}[x]$ *páros fokú elemei és a* 0 *a polinomok szokásos összeadására és szorzására nézve.*

c) $\mathbb{R}[x]$ *legalább huszadfokú elemei és a* 0 *a szokásos összeadásra és szorzásra nézve.*

d) $\mathbb{C}[x]$ *elemei a szokásos összeadásra, és a kompozícióra, mint szorzásra.*

e) Tetszőleges Abel-csoport, a szorzást úgy definiáljuk, hogy minden szorzat nulla.

f) Egy X *halmaz összes részhalmaza, ahol az összeadás a szimmetrikus differencia képzése, a szorzás pedig a metszetképzés.*

2. *Bizonyítsuk be az alábbi állításokat.*

a) Ha $\circ$ *kétváltozós művelet egy* A *halmazon, akkor csak egy neutrális eleme lehet.*

b) Ha e *neutrális elem a* $\circ$ *kétváltozós asszociatív műveletre nézve, akkor minden elemnek legfeljebb egy (kétoldali) inverze lehet (*e*-re nézve).*

c) Ha S *gyűrű, és* 0 *az összeadás neutrális eleme (azaz* S *nulleleme), akkor tetszőleges* $s,t \in S$ *esetén* $s*0 = 0*s = 0$ *és* $(-s)*t = s*(-t) = -(s*t)$.

d) Egy egységelemes R *gyűrű invertálható elemei a szorzásra nézve csoportot alkotnak.*

3. *Legyen* p *prímszám, és* R *gyűrű, amelyben minden elem* p*-szerese nulla. Mutassuk meg, hogy* $(r+s)^p = r^p + s^p$ *teljesül minden* $r,s \in R$ *esetén. Vezessük le ebből a kis Fermat-tételt.*

4. *Végezzük el* $\mathbb{Z}_{17}$*-ben a* $2/3$ *és az* $5/12$ *osztásokat. Mutassuk meg, hogy ez egy test.*

5. *Mutassuk meg, hogy a* $\mathbb{Z}_n$ *gyűrű akkor és csak akkor nullosztómentes, ha* n *prímszám, és ebben az esetben test is.*

6. *Mely* m*-ekre van* $\mathbb{Z}_m[x]$*-ben olyan polinom, amelynek több gyöke van, mint a foka?*

7. *Határozzuk meg a legfeljebb negyedfokú irreducibilis polinomokat* $\mathbb{Z}_2$ *felett.*

8. *Bontsuk az* $x^{12}-1$ *polinomot irreducibilisek szorzatára* $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ *és* $\mathbb{Z}_5$ *felett.*

9. *Az* $x^4+x^3+x^2+1$ *polinomot* $\mathbb{Z}_2$ *felett vizsgálva igazoljuk, hogy irreducibilis* $\mathbb{Q}$ *felett.*

10. *Irreducibilisek-e az alábbi polinomok?*

a) $\mathbb{Z}_2$ *felett* x^8+x^2+1, x^5+x+1, $x^5+x^4+x^3+1$, x^5+x^3+1.

b) $\mathbb{Z}_{17}$ *felett* x^2+1, x^4+1, x^8+1, $x^{17}+1$, $x^{17}+2$.

c) $\mathbb{Z}$ *felett* $x^4+2x+27$, $3x^7+6x-18$, x^6+1, x^3+7x-3, $x^4+3x^3+x^2+1$.

11. *Legyen* $\varphi : G \to H$ *művelettartó leképezés a* G *illetve* H *csoportok között. Mutassuk meg, hogy* φ *a* G *csoport egységelemét a* H *egységelemébe képzi, és ha* $g \in G$, *akkor* g *inverzének képe ugyanaz, mint* g *képének inverze (vagyis* φ *az inverzképzést is tartja).*

12. *Döntsük el az alábbi $\varphi : G_1 \to G_2$ leképezésekről, hogy művelettartóak-e.*
a) $G_1 = G_2 = \mathbb{C}^+$, $\varphi(x) = |x|$ *(abszolút érték).*
b) $G_1 = G_2 = \mathbb{C}^\times$, $\varphi(x) = |x|$ *(abszolút érték).*
c) $G_1 = \mathbb{R}^+$, $G_2 = \mathbb{R}^\times$, $\varphi(x) = e^x$.
d) $G_1 = \mathbb{R}^+$, $G_2 = \mathbb{C}^\times$, $\varphi(x) = \cos x + i \sin x$.
e) $G_1 = \mathbb{Z}_{100}^+$, $G_2 = \mathbb{Z}_{100}^+$, $\varphi(x) = 60x$.
f) $G_1 = \mathbb{R}[x]$ *mint gyűrű,* $G_2 = \mathbb{C}$ *mint gyűrű,* $\varphi(f) = f(i)$.

13*. *Igazoljuk, hogy az $\{a + bi \mid a, b \in \mathbb{Q}\}$ és $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ testek nem izomorfak (a műveletek mindkét esetben a szokásos $\mathbb{C}$-beli összeadás és szorzás).*

14. *Mutassuk meg, hogy a mod m maradékképzés $\mathbb{Z}$-ből $\mathbb{Z}_m$-be művelettartó (mindkét gyűrűműveletre). Vezessük le ebből, hogy $\mathbb{Z}_m$ gyűrű.*

15. *Ha R és S gyűrűk, és $\varphi : R \to S$ gyűrűhomomorfizmus, akkor mutassuk meg, hogy $a_0 + a_1x + \cdots + a_nx^n \mapsto \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$ is homomorfizmus $R[x]$-ből $S[x]$-be.*

16. *Legyen $f \in \mathbb{Z}[x]$ egy n-edfokú polinom, ahol $n \geq 1$, p egy prímszám, és $0 < k < n$. Legyen $\overline{f} \in \mathbb{Z}_p[x]$ az f modulo p véve. Az alábbi állítások közül melyek igazak?*
a) Ha f irreducibilis $\mathbb{Z}$ felett, akkor $\overline{f}$ irreducibilis $\mathbb{Z}_p$ felett.
b) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ felett, akkor f irreducibilis $\mathbb{Z}$ illetve $\mathbb{Q}$ felett.
c) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ felett, és $\overline{f}$ foka n, akkor f irreducibilis $\mathbb{Q}$ felett.
d) Ha f-nek van $\mathbb{Z}$ felett k-adfokú tényezője, akkor $\overline{f}$-nak is van k-adfokú tényezője.
e) Az előző állítás akkor, ha azt is tudjuk, hogy $\overline{f}$ foka n.
Adjunk az első Gauss-lemmára és a Schönemann-Eisenstein-tételre új bizonyítást a polinom mod p vizsgálatával.

17. *Fogalmazzuk meg precízen, és bizonyítsuk is be, milyen értelemben egyértelmű egy egész együtthatós polinom felbontása egy egész szám és egy primitív polinom szorzatára. Mennyiben egyértelmű egy racionális együtthatós polinom felbontása egy racionális szám, és egy (egész együtthatós) primitív polinom szorzatára?*

18. *Mutassuk meg, hogy az $f, g \in \mathbb{Z}[x]$ polinomok $\mathbb{Z}[x]$-beli legnagyobb közös osztója a következő módon határozható meg. Alkalmazzuk az euklideszi algoritmust $\mathbb{Q}$ felett, a kapott racionális együtthatós polinomot írjuk fel rh alakban, ahol $r \in \mathbb{Q}$ és $h \in \mathbb{Z}[x]$ primitív polinom. Határozzuk meg f és g együtthatóinak legnagyobb közös osztóját, az eredmény ennek a számnak a h-szorosa. Hogyan módosítható ez az eljárás, ha két $\mathbb{C}[x, y]$-beli polinom legnagyobb közös osztóját keressük?*

19. *Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Mutassuk meg a következőket.*
a) a^{-n} *az* a^n *inverze (az* a^{-n} *definíció szerint* $((a^{-1})^n$*, ha* n *poiztív egész).*
b) $a^m a^n = a^{m+n}$.
c) $(a^m)^n = a^{mn}$.
d) Ha a és b felcserélhető, azaz $ab = ba$, akkor $(ab)^n = a^n b^n$.

20. *Legyen $\circ$ asszociatív művelet az A halmazon, és $a, b, c, d, e \in A$.*
a) Mutassuk meg, hogy $[(a \circ b) \circ (c \circ d)] \circ e = a \circ [\{(b \circ c) \circ d\} \circ e]$.
b) Mutassuk meg, hogy tetszőleges szorzat értéke független a zárójelezéstől.*