Bsc algebra3a gyakorlat
Nyolcadik feladatsor

1. ***(K6.7.4)*** Igazoljuk, hogy a négyelemű test mindegyik eleme gyöke az $x^4 - x$ polinomnak.

2. ***(K384–386. oldal.)*** Legyen $L = \mathbb{Z}_2[x]/(x^3 + x + 1)$ a nyolcelemű test.

(1) Mutassuk meg, hogy L minden eleme gyöke az $x^8 - x$ polinomnak, majd bontsuk ezt irreducibilisek szorzatára $\mathbb{Z}_2$ fölött.
(2) Határozzuk meg a $\psi(x) = x^2$ Frobenius-automorfizmus ciklusait az L halmazon. Igazoljuk, hogy az egy ciklushoz tartozó elemek minimálpolinomja és rendje egyenlő.
(3) Határozzuk meg L mindegyik elemének a minimálpolinomját a prímtest fölött.
(4) Határozzuk meg L összes résztestét.

Végezzük el az analóg vizsgálatokat a 4, 9, 16 elemű test esetében is.

3. ***(K6.7.16)*** Hány négyzet-, illetve köbelem van az 27 elemű testben? Hány gyöke van itt az $x^4 + x^3 + x^2 + x + 1$, illetve az $x^2 - x + 1$ polinomnak?

4. ***(K6.7.17)*** Mi a 17 elemű test fölött az $x^2 + 1$ és az $x^2 - 3$ polinomok felbontási teste?

5. ***(K6.7.18)*** Határozzuk meg $x^2 + x + 1$ felbontási testét $\mathbb{F}_{121}$, illetve $\mathbb{F}_{125}$ fölött.

6. ***(K6.7.19)*** Határozzuk meg az $x^{11} - 1$ polinom felbontási testét $\mathbb{Z}_2$ és $\mathbb{Z}_{11}$ fölött.

7. ***(K6.7.20)*** Legyen p prím és $p \nmid n$, továbbá $k = o_n(p)$. Igazoljuk az alábbi állításokat.

(1) $\mathbb{F}_{p^m}$ akkor és csak akkor tartalmaz n rendű elemet, ha $k \mid m$.
(2) $\mathbb{F}_{p^m}$ minden n rendű elemének $\mathbb{Z}_p$ fölötti minimálpolinomja k-adfokú.
(3) Az $x^n - 1$ és a Φ_n polinomoknak a $\mathbb{Z}_p$ fölötti felbontási teste $\mathbb{F}_{p^k}$.
(4) A Φ_n körosztási polinomnak a $\mathbb{Z}_p$ fölötti irreducibilis tényetői k-adfokúak. Előfordulhat-e, hogy minden $\mathbb{Z}_p$ fölötti k-adfokú irreducibilis polinom osztója Φ_n-nek?

8. ***(K6.7.21)*** Legyen α a $K = \mathbb{F}_{p^m}$ test multiplikatív csoportjának generátoreleme, ahol p prím, és $\beta = \alpha^j$. Igazoljuk az alábbi állításokat.

(1) A β rendje a szorzásra $n = (p^m - 1)/(p^m - 1, j)$.
(2) A β elem $\mathbb{Z}_p$ fölötti foka éppen a p rendje modulo n.
(3) A β foka $\mathbb{Z}_p$ fölött pontosan akkor m, ha a $(p^m - 1)/(p^d - 1)$ szám semmilyen $d \mid m$, $d \neq m$ esetén sem osztója j-nek.

9. ***(K6.7.22, 9.3.9)*** Legyen α az $\mathbb{F}_{2^4}$ multiplikatív csoportjának egy generátoreleme. Határozzuk meg α^3 fokát a prímtest fölött. Mutassuk meg, hogy $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ **primitív** polinom, azaz mindegyik gyöke generálja a felbontási testének multiplikatív csoportját.

10. ***(K6.7.23)*** Hány 8, illetve 12 fokú irreducibilis polinom van $\mathbb{Z}_2$ fölött?

11. ***(K6.7.24**)*** Mutassuk meg, hogy a 16 csúcsú teljes gráf élei kiszínezhetők három színnel úgy, hogy ne keletkezzen egyszínű háromszög, de a 17 csúcsú teljes gráf élei már nem.

12. ***(K5.11.12, 5.11.7, 5.11.14)*** Határozzuk meg az $i + j + k$ és $1 + i + j$ kvaterniók négyzetét, inverzét és minimálpolinomját. Hányadfokú lehet egy kvaternió minimálpolinomja? Igazoljuk, hogy minden nem valós kvaterniónak pontosan két négyzetgyöke van $\mathbb{K}$-ban.

13. ***(K5.11.15*)*** Oldjuk meg $\mathbb{K}$-ban az $x^n = 1$ egyenletet.

14. ***(K5.11.13*)*** Igazoljuk, hogy a $p_m + q_m i + r_m j + s_m k \notin \mathbb{R}$ $(m = 1, 2)$ kvaterniók pontosan akkor generálják $\mathbb{K}$-nak ugyanazt a ($\mathbb{C}$-vel izomorf) részalgebráját, ha $(q_1, r_1, s_1) \parallel (q_2, r_2, s_2)$.