Matematikus gyakorlat, második évfolyam, második félév
Első alkalom

1. *Bontsuk fel a $\mathbb{Z}_2$ test felett az $x^8 - x$ polinomot irreducibilisek szorzatára, és adjuk meg, hogy a $\mathbb{Z}_2[z]/(z^3 + z + 1)$ nyolcelemű test mely elemeinek mi lesz a minimálpolinomja.*

2. *Hány négyzet- illetve köbelem van a 27-elemű testben?*

3. *Határozzuk meg $x^2 + x + 1$ felbontási testét $GF(121)$ és $GF(125)$ fölött.*

4. *Mutassuk meg, hogy minden véges test felett van akármilyen fokú irreducibilis polinom.*

5. *Pistike szerint „a $\mathbb{Z}_2$ felett az $x^3 - x$ polinom gyökei (e polinom felbontási testében) résztestet alkotnak, ezért ez egy háromelemű test". Mit szólt ehhez a tanító néni?*

6. *Határozzuk meg az $x^{11} - 1$ polinom felbontási testét $\mathbb{Z}_2$ fölött. Általánosítsunk.*

7. *Mutassuk meg, hogy ha p prím, akkor $x^{p^n} - x$ az összes olyan $\mathbb{Z}_p$ fölött irreducibilis polinomom szorzata, melyek foka n-nek osztója.*

8. *Hány nyolcad- illetve 12-edfokú irreducibilis polinom van $\mathbb{Z}_2$ fölött?*

9. *Legyenek p és q prímek és n pozitív egész. Bizonyítsuk be, hogy $\mathbb{Z}_p$ fölött a q^n-edfokú irreducibilis polinomok száma $(p^{q^n} - p^{q^{n-1}})/q^n$.*

10. *Legyen $K = GF(p^n)$, ahol p prím, és g a K multiplikatív csoportjának generátoreleme. Mutassuk meg, hogy ha K két elemének minimálpolinomja megegyezik, akkor multiplikatív rendjük ugyanaz. Igazoljuk, hogy a $g = h^i$ elem $\mathbb{Z}_p$ feletti minimálpolinomjának a foka éppen a p rendje modulo m, ahol $m = (p^n - 1)/(p^n - 1, i)$ a h elem multiplikatív rendje. Igazoljuk, hogy ez a fok pontosan akkor n, ha i nem osztható $(p^n - 1)/(p^d - 1)$-gyel semmilyen $d < n$ esetén. Következik-e ebből, hogy h rendje $p^n - 1$?*

11. *Legyen p prím, és K a $\mathbb{Z}_p[z]$ hányadosteste. Mutassuk meg a Schönemann-Eisenstein kritérium felhasználásával, hogy az $x^p - z$ polinom irreducibilis K felett, de a K algebrai lezártjában vannak többszörös gyökei (és így K nem tökéletes test).*

12. *Legyen p prím, és K egy p karakterisztikájú test. Bizonyítsuk be az alábbi állításokat.*
- a) *Ha K-ban a p-edik gyökvonás elvégezhető, akkor egyértelmű.*
- b) *Egy K felett irreducibilis f polinomnak pontosan akkor van többszörös gyöke K egy bővítésében, ha f-ben csupa p-vel osztható kitevőjű tag szerepel.*
- c) *A K pontosan akkor tökéletes, ha minden eleméből vonható K-ban p-edik gyök.*
- d) *Minden véges test tökéletes.*
- e) *Tökéletes test minden algebrai bővítése is tökéletes.*

13. *Legyen K (kommutatív) test, és G egy véges részcsoportja K multiplikatív csoportjának. Mutassuk meg, hogy ha k pozitív osztója G rendjének, akkor G-ben legfeljebb $\varphi(k)$ darab k rendű elem lehet. Ebből, és a $\sum_{k|n} \varphi(k) = n$ azonosságból, de a véges Abel-csoportok alaptételének felhasználása nélkül lássuk be, hogy G ciklikus. Igazoljuk azt is, hogy véges Abel-csoportban mindig van olyan elem, aminek a rendje a csoport exponense.*

14. *Igazoljuk, hogy ha K test, akkor*
- a) *K pontosan akkor algebrailag zárt, ha minden algebrai bővítése elsőfokú;*
- b) *a K algebrai lezártja K feletti izomorfizmus erejéig egyértelmű.*