Algebra4 matematikus szakirány

4. gyakorlat

2019. március 7.

1. Legyenek $\mathbb{F}_4$ elemei $0, 1, a, a^2$. Adjuk meg ezen elemek segítségével $\mathbb{F}_4$ összeadástábláját.

2. Az $f(x) = x^3 + x + 1$ és a $g(x) = x^3 + x^2 + 1$ polinomok egyaránt irreducibilisek $\mathbb{F}_2$ fölött. Legyen K az f egy gyökével való bővítése $\mathbb{F}_2$-nek, F pedig a g gyökével. Adjunk meg egy izomorfizmust F és K között.

3. Legyen $\alpha \in \mathbb{F}_9$ a multiplikatív csoportnak egy generátoreleme. Mi α minimálpolinomja $\mathbb{F}_3$ felett?

4. Legyen $\beta \in \mathbb{F}_8$ multiplikatív csoportjának generátoreleme. Mi β minimálpolinomja $\mathbb{F}_2$ felett?

5. Jelölje $F_d(x)$ az összes $\mathbb{F}_p$ fölött irreducibilis, d-edfokú, 1-főegyütthatójú polinom szorzatát, N_d pedig az ilyen polinomok számát. Igazoljuk az alábbiakat:

   (a) $x^{p^n} - x = \prod_{d|n} F_d(x)$;

   (b) $p^n = \sum_{d|n} dN_d$;

   (c) $N_n = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$. (Itt $\mu(n) = (-1)^r$ ha $n = \prod_{i=1}^{r} p_i$ négyzetmentes, és $\mu(n) = 0$, ha $n \in \mathbb{N}$ nem négyzetmentes.)

6. Határozzuk meg az $x^{11} - 1$ polinom felbontási testét $\mathbb{F}_2$ és $\mathbb{F}_{11}$ fölött.

7. Legyen ε egy primitív nyolcadik egységgyök egy K testben (azaz $\varepsilon \in K^\times$ 8-adrendű elem). Igazoljuk, hogy $(\varepsilon + \varepsilon^7)^2 = 2$. (Először lássuk ezt be $K = \mathbb{C}$ esetén.) Vezessük le ebből a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ képletet.

8. Legyen p egy prímszám és $p \nmid n$. Jelölje k a p rendjét modulo n (vagyis p rendét a $(\mathbb{Z}/n\mathbb{Z})^\times$ multiplikatív csoportban). Bizonyítsuk be az alábbi állításokat:

   (a) $\mathbb{F}_{p^m}$ akkor és csak akkor tartalmaz n rendű elemet, ha $k \mid m$.

   (b) $\mathbb{F}_{p^m}$ minden n rendű elemének az $\mathbb{F}_p$ feletti minimálpolinomja k-adfokú.

   (c) Az $x^n - 1$ és a $\Phi_n(x)$ polinomoknak az $\mathbb{F}_p$ feletti felbontási teste $\mathbb{F}_{p^k}$.

   (d) A Φ_n körosztási polinom az $\mathbb{F}_p$ test fölött felbomlik k-adfokú, $\mathbb{F}_p$ fölött irreducibilis polinomok szorzatára.

9. Legyen $\alpha \in \mathbb{F}_{p^n}$.

   (a) Igazoljuk, hogy az $f(x) = (x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \dots (x - \alpha^{p^{n-1}})$ polinom együtthatói $\mathbb{F}_p$-ből valók.

   (b) Legyen $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{n-1}}$ az α nyoma. Igazoljuk, hogy $\mathrm{Tr}\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ egy $\mathbb{F}_p$-lineáris szürjektív leképezés.

   (c)* Mutassuk meg, hogy az $x^p - x - \alpha \in \mathbb{F}_{p^n}[x]$ polinom vagy irreducibilis, vagy lineáris faktorokra bomlik. Az utóbbi eset pontosan akkor áll fenn, ha $\mathrm{Tr}(\alpha) = 0$.

Nehezebb feladatok

10. Igazoljuk, hogy minden A Abel-csoportra van olyan K véges Galois-bővítése $\mathbb{Q}$-nak, melynek $\mathrm{Gal}(K/\mathbb{Q})$ Galois-csoportja A-val izomorf. (Használjuk fel Dirichlet tételét a számtani sorozatokban levő prímszámokról.) Híres megoldatlan probléma, hogy igaz-e ez minden G csoportra (inverz Galois-probléma). Ha G feloldható, akkor igaz, és ez Safarevics (1958) tétele. Sőt, igaz minden véges egyszerű csoportra is.