Algebra 2. 2005/2006 ősz
13. gyakorlat: Galois-bővítések, véges testek

Legyen K/F véges bővítés. Ekkor $\mathrm{Gal}\,(K/F)$ *Galois-csoport* a K test F test elemeit fixen hagyó összes automorfizmusaiból áll.

A K/F véges bővítés *Galois-bővítés*, ha $|\mathrm{Gal}\,(K/F)| = [K : F]$. Ez azzal ekvivalens, hogy K/F normális és szeparábilis.

Tétel. Legyen K/F normális bővítés, $\alpha \in K$ és $\alpha' \in K$ az α minimálpolinomjának egy gyöke. Ekkor van olyan $\sigma \in \mathrm{Gal}\,(K/F)$, amelyre $\sigma(\alpha) = \alpha'$.

1. Határozzuk meg a K/F bővítés Galois-csoportját és a bővítés közbülső testeit, ahol K az $f(x)$ polinom F feletti felbontási teste és $F = \mathbb{Q}$, $f(x) = x^3 - 7$. Oldjuk meg ugyanezt a feladatot $F = \mathbb{F}_2$, $f(x) = x^6 + 1$ esetén is.

2. Mennyi a $\mathrm{Gal}\left(\mathbb{F}_p(\sqrt[p]{t})/\mathbb{F}_p(t)\right)$ és a $\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$ csoportok elemszáma?

3. Bizonyítsuk be, hogy $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ bővítés Galois-csoportja izomorf $(\mathbb{Z}_n)^*$-gal, ahol ε primitív n-edik egységgyök. (Felhasználhatjuk, hogy ε minimálpolinomjának gyökei pontosan a primitív n-edik egységgyökök.)

$*$ 4. Lássuk be, hogy minden véges Ábel-csoport előáll mint valamely $K/\mathbb{Q}$ bővítés Galois-csoportja. (Híres megoldatlan probléma, hogy tetszőleges véges csoporttal igaz-e ugyanez.)

• 5. Tegyük fel, hogy $n \geq 2$ egész, F test, amely karakterisztikája nem osztja n-et, F tartalmaz ε primitív n-edik egységgyököt, továbbá $f(x) = x^n - a \in F[x]$ irreducibilis polinom. Határozzuk meg $\mathrm{Gal}\,(K/F)$ csoportot, ahol K az $f(x)$ felbontási teste.

6. Lássuk be, hogy ha $K \supseteq F$ véges testek, akkor K az F egyszerű bővítése.
(Útmutatás: használjuk, hogy K multiplikatív részcsoportja ciklikus)

7. Mutassuk meg, hogy tetszőleges F véges test és n egész szám esetén van F felett n fokú irreducibilis polinom.

• 8. (*Primitív elem tétel*) Igazoljuk, hogy minden véges szeparábilis bővítés egyszerű.
(Útmutatás: mutassuk meg, hogy a bővítésnek csak véges sok közbülső teste van, ennek segítségével pedig lássuk be, hogy ha F elemszáma végtelen, $\alpha, \beta \in K$, akkor van két különböző $\lambda_1, \lambda_2 \in F$, amelyre $F(\lambda_1\alpha + \beta) = F(\lambda_2\alpha + \beta)$. Ebből következtessünk arra, hogy $F(\lambda_1\alpha + \beta) = F(\alpha, \beta)$.)

9. (a) Legyen $f(x) \in \mathbb{F}_p[x]$ n-edfokú irreducibilis polinom, aminek α egy gyöke. Igazoljuk, hogy $\mathbb{F}_p(\alpha)$ egy p^n elemű test.

   (b) Legyen $\mathbb{F}_{p^n}$ egy p^n elemű test. Mutassuk meg, hogy $\mathbb{F}_{p^n}$ a felbontási teste $x^{p^n} - x$ polinomnak. (Ezek szerint p^n elemű testből egyetlen egy van.)

   (c) Bizonyítsuk be, hogy tetszőleges n-edfokú $\mathbb{F}_p$ együtthatós irreducibilis polinom lineáris tényezőkre esik szét $\mathbb{F}_{p^n}$-ben.

10. (a) Mutassuk meg, hogy $\mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_p)$ n-edrendű ciklikus csoport, amelynek a Frobenius-automorfizmus $(a \mapsto a^p)$ generátora.

    (b) Határozzuk meg a bővítés L résztesteit és írjuk le az $L/\mathbb{F}_p$ és $\mathbb{F}_{p^n}/L$ részbővítések Galois-csoportjait is.

• 11. Bizonyítsuk be, hogy tetszőleges n-edfokú $\mathbb{F}_{p^k}$ együtthatós irreducibilis polinom lineáris tényezőkre esik szét $\mathbb{F}_{p^{kn}}$-ben.

• 12. Határozzuk meg $K/\mathbb{F}_8$ Galois-csoportját, ahol K az $x^2 + x + 1$ polinom $\mathbb{F}_8$ feletti felbontási teste.