Véges testek és alkamazásaik / 2006 ősz / Küronya Alex

1. Házi feladat

1. ∘ Jelöljék $0, 1, a, b$ az $\mathbb{F}_4$ véges test elemeit. Adjuk meg a test szorzó- és összeadótábláját.

2. (a) Legyen G tetszőleges Abel-csoport, $a, b \in G$ véges rendű elemek. Mutassuk meg, hogy ha $\operatorname{ord} a = m$,$\operatorname{ord}(b) = n$, akkor van G-nek olyan c eleme, amelynek rendje (m, n).
(b) Igazoljuk, hogy ha G egy k-exponensű Abel-csoport, akkor van G-ben k-rendű elem.
(c) Igaz-e, hogy egy G csoportban bármely két véges rendű elem szorzata véges?

3. (a) Léteznek-e különböző karakterisztikájú testek között homomorfizmusok?
(b) Milyen esetben létezhet különböző karakterisztikájú integritási tartományok között homomorfizmus?

4. Van-e hatelemű integritási tartomány?

5. * Legyen p prímszám, n pozitív egész. Mutassuk meg, hogy
(a) egy $f \in \mathbb{F}_p[X]$ irreducibilis polinom pontosan akkor osztja az $X^{p^n} - X$ polinomot, ha $\deg f | n$;
(b) $X^{p^n} - X$ egyenlő az összes olyan egy főegyütthatós irreducibilis $\mathbb{F}_p[X]$-beli polinom szorzatával, amelyeknek a foka osztja n-et.

6. ** Igazoljuk, hogy a q-elemű véges test feletti n-edfokú egy főegyütthatós irreducibilis polinomok száma

$$\frac{1}{n} \sum_{k|n} \mu(k) q^{n/k} \ ,$$

ahol μ a Möbius-függvény.

7. * Legyen $\mathbb{K}$ test, $f, g \in \mathbb{K}[X]$ tetszőleges polinomok. Adjunk $\mathcal{O}((\operatorname{len} f)(\operatorname{len} g))$ $\mathbb{K}$-beli műveletet használó algoritmust annak eldöntésére, hogy $\bar{g} \in \mathbb{K}[X]/(f)$ invertálható-e, illetve ha igen, akkor (multiplikatív) inverzének kiszámítására.

8. ** (Kínai maradéktétel) (i) Legyen R tetszőleges (kommutatív) gyűrű, $I_1, \ldots, I_r \subseteq R$ páronként relatív prím ideálok (azaz minden $i \neq j$ esetén $I_i + I_j = R$). Jelölje $\pi_i : R \to R/I_i$ a kanonikus homomorfizmust. Ekkor a

$$\begin{aligned} \phi : R &\to R/I_1 \times \cdots \times R/I_r \\ x &\mapsto (\pi_1(x), \ldots, \pi_r(x)) \end{aligned}$$

homomorfizmus szürjektív, magja $\ker \phi = I_1 \cap \cdots \cap I_r$, és ily módon egy

$$R/\cap_{i=1}^r I_i \xrightarrow{\sim} \prod_{i=1}^r R/I_i$$

izomorfizmust indukál.
(ii) Legyenek $f_1, \ldots f_k, g_1, \ldots, g_k \in \mathbb{K}[X]$ tetszőleges polinomok, amelyekre igaz, hogy az f_i-k páronként relatív prímek, egyikük sem konstans, továbbá mindent $1 \leq i \leq k$ esetén $\deg(g_i) < \deg(f_i)$. Mutassuk meg, hogy $\mathcal{O}(\operatorname{len}(f)^2)$ $\mathbb{K}$-beli művelettel meg tudjuk határozni azt a $h \in \mathbb{K}[X]$ polinomot, amelyre

(1) $\deg(h) < \deg(f)$, és
(2) minden $1 \leq i \leq k$-ra $h \equiv g_i \pmod{f_i}$,

ahol $f \stackrel{\text{def}}{=} \prod_{i=1}^k f_i$.