# 5. feladatsor – Véges testek

**5.1. Feladat.** Döntsük el, hogy a megadott $T$ test, és ezen test feletti $f$ polinom esetén $T[x]/\langle f\rangle$ testet alkot-e. Ha igen, határozzuk meg az így kapott test elemszámát, karakterisztikáját, prímtestét.

(a) $T = \mathbb{Z}_2,\ f = x^2 + x + 1$;
(b) $T = \mathbb{Z}_2,\ f = x^2 + 1$;
(c) $T = \mathbb{Z}_3,\ f = x^2 + 1$;
(d) $T = \mathbb{Z}_3,\ f = x^3 + 2x^2 + 2$;
(e) $T = \mathbb{Z}_3,\ f = x^3 + 2x + 1$;
(f) $T = \mathbb{Z}_2,\ f = x^4 + x^3 + 1$;
(g) $T = \mathbb{Z}_2,\ f = x^4 + x^2 + 1$.

**5.2. Feladat.** Adjuk meg a $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 2\rangle$ test alábbi elemeit:

(a) $\overline{x+2} + \overline{x^2+2x+1}$;
(b) $\overline{x^2+2x+1} \cdot \overline{x+2}$;
(c) $\overline{x^2+2x+1} \cdot \overline{x^2+2}$;
(d) $\overline{x+2}^{-1}$.

**5.3. Feladat.** Végezzük el a műveleteket a megadott $K$ véges testekben.

(a) $K = \mathbb{Z}_{17}$; $\quad 16 \cdot 10, \quad 3^{-1}$;
(b) $K = \mathbb{Z}_{19}$; $\quad 17 \cdot 9, \quad 6^{-1}$;
(c) $K = \mathbb{Z}_2[x]/\langle x^4 + x^3 + 1\rangle$; $\quad \overline{x^3+x+1} \cdot \overline{x^2+1}, \quad \overline{x^3+x^2}^{-1}$;
(d) $K = \mathbb{Z}_3[x]/\langle x^3 + 2x^2 + x + 1\rangle$; $\quad \overline{x^2+2x+1} \cdot \overline{x^2+2}, \quad \overline{x^2+2x+1}^{-1}$;
(e) $K = \mathbb{Z}_3[x]/\langle x^3 + x^2 + 2x + 1\rangle$; $\quad \overline{x^2+x+1} \cdot \overline{x^2+2x}, \quad \overline{x^2+x+1}^{-1}$.

**5.4. Feladat.** Határozzuk meg a $K$ testben az $\alpha$ elem (multiplikatív) rendjét. Döntsük el, hogy primitív-e az adott elem a $K$ testben.

(a) $K = \mathbb{Z}_5,\ \alpha = 2$;
(b) $K = \mathbb{Z}_7,\ \alpha = 4$;
(c) $K = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle,\ \alpha = \overline{x+1}$;
(d) $K = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle,\ \alpha = \overline{x^2+1}$;
(e) $K = \mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle,\ \alpha = \overline{x+1}$;
(f) $K = \mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle,\ \alpha = \overline{x+1}$.

**5.5. Feladat.** Határozzuk meg az $\alpha \in K$ elem minimálpolinomját.

(a) $K = \mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle,\ \alpha = \overline{x+1}$;
(b) $K = \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle,\ \alpha = \overline{x+1}$;
(c) $K = \mathbb{Z}_2[x]/\langle x^4 + x^3 + 1\rangle,\ \alpha = \overline{x^2+1}$.