POLINOM FELBONTÁSI TESTE. VÉGES TESTEK TULAJDONSÁGAI. SZÁMOLÁS VÉGES TESTEKBEN.

1. Döntse el,hogy a megadott $\mathbf{F}$ test, és ezen test feletti f polinom esetén $\mathbf{F}[x]/(f)$ testet alkot-e. Ha igen, akkor határozzuk meg az így kapott test karakterisztikáját és prímestét.

(a) $\mathbf{F} = \mathbb{Z}_2$, $f \in \{x^2+x, x^2+x+\overline{1}, x^3+x^2+\overline{1}, x^4+x^2+\overline{1}, x^4+x^3+\overline{1}\}$;

(b) $\mathbf{F} = \mathbb{Z}_3$, $f \in \{x^2+\overline{1}, x^2+x+\overline{1}, x^3+\overline{2}x+\overline{1}\}$;

(c) $\mathbf{F} = \mathbb{Z}_4$, $f \in \{\overline{3}x^2+\overline{3}, \overline{2}x^2+x-\overline{1}, x^3+\overline{2}x+\overline{1}\}$.

2. Adjuk meg a $\mathbb{Z}_3[x]/(x^3+x^2+\overline{2})$ test alábbi elemeit $\overline{h} = h + (x^3+x^2+\overline{2})$ alakban, ahol $h \in \mathbb{Z}_3[x]$ és $h^* \leqslant 2$:

$$\overline{x^3+\overline{2}}, \quad \overline{x^3+\overline{2}} + \overline{\overline{2}x^3+\overline{1}x^2+\overline{1}}, \quad \overline{x^3+\overline{2}} \cdot \overline{\overline{2}x^3+\overline{1}x^2+\overline{1}}, \quad \overline{x^3+\overline{2}}^{-1}.$$

3. Igazolja, hogy az $f = x^4+x+\overline{1} \in \mathbb{Z}_2[x]$ polinom irreducibilis $\mathbb{Z}_2$ felett. Írja fel az

$$\left(\overline{x^3+x+\overline{1}} + \overline{x^2+x+\overline{1}}\right)^{-1} \cdot \overline{x^5}$$

elemet $\overline{h}$ alakban, ahol $h \in \mathbb{Z}_2[x]$ és $h^* \leqslant 3$.

4. Határozza meg az $\mathbf{F}$ testben az a elem rendjét, majd döntse el, hogy a primitív-e.

(a) $\mathbf{F} = \mathbb{Z}_{17}$, $a \in \{\overline{2}, \overline{3}, \overline{4}\}$;

(b) $\mathbf{F} = \mathbb{Z}_2[y]$, $a \in \left\{\overline{y}, \overline{y+\overline{1}}\right\}$;

(c) $\mathbf{F} = \mathbb{Z}_3[y]$, $a \in \left\{\overline{y+\overline{1}}, \overline{y^2+\overline{1}}\right\}$;

5. Határozza meg az $f = x^4 - 5x^2 + 6$ polinom felbontási testét $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ és $\mathbb{R}$ felett.

6. Határozza meg az $f = x^4 - 10x^2 + 1$ polinom felbontási testét $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ és $\mathbb{R}$ felett.

7. Határozza meg a $\mathbb{Z}_2[x]$ polinomgyűrűben a másod- és harmadfokú irreducibilis polinomokat.

8. Legyen $K = \mathbb{Z}_2[x]/(x^4+x^3+\overline{1})$. Határozza meg az $\overline{x^2+\overline{1}} \in K$ elem minimálpolinomját $\mathbb{Z}_2$ felett.

9. Legyen $\alpha \in \mathrm{GF}(2^3)$ gyöke az $f = x^3+x^2+\overline{1} \in \mathbb{Z}_2[x]$ polinomnak. Határozza meg az $n = 2010$ egész szám $Z(n)$ Zech-logaritmusát.[1]

10. Legyen $\alpha \in \mathrm{GF}(q)$ primitív elem, ahol q prímhatvány. Igazolja, hogy tetszőleges m és n egészekre

$$\alpha^m + \alpha^n = \alpha^{n+Z(n-m)}$$

teljesül, ha $Z(n-m)$ definiált.

11. Határozza meg az összes primitív elemet a $\mathbb{Z}_3[x]/(x^4+x+\overline{2})$ testben.

SZORGAMI FELADAT(OK)

18. Legyen $\mathbf{E} = (E; +, \cdot)$ egységelemes gyűrű az e egységelemmel. Definiáljuk a $*$ 2-változós műveletet E-n a következőképpen:

$$a * b = a + b - a \cdot b.$$

[1] Legyen α primitív elem az $\mathbf{F}$ véges testben. Ekkor az n egész szám *Zech-logaritmusa* az a $Z(n)$ egész szám, amelyre $\alpha^{Z(n)} = 1 + \alpha^n$.

Legyen G mindazon E-beli a elemek halmaza, amelyekhez van olyan $w \in E$, hogy $a * w = w * a = 0$. Bizonyítsa be, hogy $(G; *)$ csoport, és $a \in E$ pontosan akkor eleme G-nek, ha $e - a$ invertálható **E**-ben.

19. Legyen

$$R = \left\{ \begin{pmatrix} a & b\sqrt{5} \\ -b\sqrt{5} & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\},$$
$$I = \left\{ \begin{pmatrix} x & (3y+x)\sqrt{5} \\ -(3y+x)\sqrt{5} & x \end{pmatrix} \mid x, y \in \mathbb{Z} \right\}.$$

Mutassuk meg, hogy

(a) $\mathbf{R} = (R; +, \cdot)$ részgyűrűje $(\mathbb{R}^{2\times 2}; +, \cdot)$-nak;

(b) I ideál **R**-ben, de nem főideál.

20. Legyen $P_n = \{f \in \mathbb{Z}_2[x] \mid f^* = n$ és f irreducibilis$\}$ $(n \in \mathbb{N})$. Határozza meg a $P_1, P_2, \cdots, P_8$ halmazok elemszámát.

21. Legyen α primitív elem a $\mathrm{GF}(p^k)$ testben (p prímszám, $k \in \mathbb{N}$). Igazolja, hogy az α elem $\mathbb{Z}_p$ feletti minimálpoinomja k-adfokú.

22. Van-e olyan $\mathbb{Z}_2$ feletti f negyedfokú irreducibilis polinom, amelyre a $\mathbb{Z}_2[x]/(f)$ test $\overline{f}$ eleme nem primitív?
