Feladat 1. Határozza meg a $\mathbb{Z}_2[x]/(x^4+x+1)$ testben a következőket ($a := x/(x^4+x+1)$):

- $(a^3+a)^{-1}$,
- $(a^2+1)^{68}$,
- $m_{\mathbb{Z}_2}(a^3+a^2+1)$.

Megoldás: Az a elem generálja a test multiplikatív csoportját: $a^4 = a+1$, $a^5 = a^2+a$, $a^6 = a^3+a^2$, $a^7 = a^4+a^3 = a^3+a+1$, $a^8 = a^4+a^2+a = a^2+1$, $a^9 = a^3+a$, $a^{10} = a^4+a^2 = a^2+a+1$, $a^{11} = a^3+a^2+a$, $a^{12} = a^4+a^3+a^2 = a^3+a^2+a+1$, $a^{13} = a^4+a^3+a^2+a = a^3+a^2+1$, $a^{14} = a^4+a^3+a = a^3+1$, $a^{15} = a^4+a = 1$. Ezt a sorozatot "logarlécként" használhatjuk.

- $(a^3+a)^{-1} = (a^9)^{-1} = a^6 = a^3+a^2$,
- $(a^2+1)^{68} = (a^8)^{68} = a^{544} = a^4 = a+1$
- a $b := a^3+a^2+1 = a^{13}$ elem hatványai: $b^2 = a^{11} = a^3+a^2+a$, $b^3 = a^9 = a^3+a$, $b^4 = a^7 = a^3+a+1$. Látható, hogy $b^4+b^3+1 = 0$. Mivel az x^4+x^3+1 polinom irreducibilis $\mathbb{Z}_2$ felett, ez lesz a minimálpolinom.

Feladat 2. Határozza meg a $\mathbb{Z}_3[x]/(x^3+2x+2)$ testben a következőket ($a := x/(x^3+2x+2)$):

- $(a^2+2a)^{-1}$,
- $(2a^2+a+1)^{68}$,
- $m_{\mathbb{Z}_3}(a^2+2a+1)$.

Megoldás:

- Euklideszi algoritmust végzünk $\mathbb{Z}_3[x]$-ben az $f := x^3+2x+2$ és a $g := x^2+2x$ polinomokra: $f = xg+x^2+2x+2 = (x+1)g+2$, így $1 = 2f-(2x+2)g$. Innen a testben

$$(a^2+2a)^{-1} = \frac{1}{a^2+2a} = \frac{2(a^3+2a+2)-(2a+2)(a^2+2a)}{a^2+2a} = \frac{-(2a+2)(a^2+2a)}{a^2+2a} = a+1.$$

- A test 27 elemű, tehát multiplikatív csoportjának rendje 26. Ezért

$$(2a^2+a+1)^{68} = (2a^2+a+1)^{16} = ((2a^2+a+1)^2)^8 = (4a^4+a^2+1+4a^3+4a^2+2a)^8 =$$
$$(a^2+a+a^2+1+a+1+a^2+2a)^8 = ((a+2)^2)^4 = ((a^2+a+1)^2)^2 = (a^4+a^2+1+2a^3+2a^2+2a)^2 =$$
$$(a^2+a+a^2+1+2a+2+2a^2+2a)^2 = (a^2+2a)^2 = a^4+a^3+a^2 = a^2+a+a+1+a^2 = 2a^2+2a+1.$$

- A $b = a^2+2a+1$ elem hatványai: $b^2 = a^4+4a^2+1+4a^3+2a^2+4a = a^2+2$, $b^3 = a^6+2a^3+1 = a^4+a^3+2a^3+1 = a^2+a+1$. Látható, hogy $b^3+b^2+b+2 = 0$. Mivel az x^3+x^2+x+2 poolinom irreducibilis $\mathbb{Z}_3$ felett (harmadfokú, és nincs gyöke), ez a minimálpolinom.

Feladat 3. Adja meg az $a = 2\sqrt[3]{12} - \sqrt[3]{3}$ szám minimálpolinomját $\mathbb{Q}$ fölött.

Megoldás: Kilencedfokú polinomot elvileg könnyű adni, aminek a gyöke. (Ha $\alpha = \alpha_1$ gyöke a $\Pi_i(x-\alpha_i)$, $\beta = \beta_1$ pedig a $\Pi_j(x-\beta_j)$ polinomnak, akkor $\alpha+\beta$ gyöke $\Pi_{i,j}(x-\alpha_i-\beta_j)$-nek, $\alpha\beta$ pedig $\Pi_{i,j}(x-\alpha_i\beta_j)$-nek. Belátható, hogy ha $\Pi_i(x-\alpha_i)$ és $\Pi_j(x-\beta_j)$ együthatói egy $\mathbf{K}$ testbe esnek, akkor $\Pi_{i,j}(x-\alpha_i-\beta_j)$ és $\Pi_{i,j}(x-\alpha_i\beta_j)$ együtthatói szintén.)

Ezt a következőképpen lehet megtenni ebben az esetben: $a = \sqrt[3]{3}(2\sqrt[3]{4} - 1)$, tehát $a^3 = 3(32 - 12\sqrt[3]{16} + 6\sqrt[3]{4} - 1)$, és $a^3 - 93 = 18\sqrt[3]{4} - 72\sqrt[3]{2}$. Legyen $d := \frac{a^3-93}{18} = \sqrt[3]{4} - 4\sqrt[3]{2}$. Ekkor

$$d^2 = \sqrt[3]{16} - 8\sqrt[3]{8} + 16\sqrt[3]{4} = 16\sqrt[3]{4} + 2\sqrt[3]{2} - 16,$$

míg

$$d^3 = 4 - 12\sqrt[3]{32} + 48\sqrt[3]{16} - 128 = -24\sqrt[3]{4} + 96\sqrt[3]{2} - 124.$$

Jól látható, hogy $\{1, d, d^2, d^3\}$ lineárisan függő halmaz $\mathbb{Q}$ felett, Gauss-eliminációval megkapható egy nemtriviális nullértékű lineáris kombináció. Ebben az esetben ránézésre is lehet látni, hogy $d^3 + 24d + 124 = 0$. Tehát a főpolinom, aminek a gyöke:

$$18^3((\frac{x^3 - 93}{18})^3 + 24\frac{x^3 - 93}{18} + 124).$$

Ahhoz, hogy belássuk, hogy ez a minimálpolinom, meg kell mutatni, hogy a nem gyöke kisebb fokú racionális együtthatós polinomnak. Az a benne van a $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ testben, ami a $\mathbb{Q}$ felett kilencedfokú (ez nem teljesen nyilvánvaló, feladtam feladatnak). Így a fokszáma a 9 osztója, tehát elég belátni, hogy a nem gyöke harmadfokú racionális polinomnak.

Tegyük fel, hogy $q_0 + q_1a + q_2a^2 + q_3a^3 = 0$, ekkor

$$q_0 + 3q_3(2\sqrt[3]{2} - 1)^3 + q_1(2\sqrt[3]{2} - 1)\sqrt[3]{3} + q_2(2\sqrt[3]{2} - 1)\sqrt[3]{9} = 0.$$

Mivel

$$\deg_{\mathbb{Q}(\sqrt[3]{2})} \sqrt[3]{3} = \frac{[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]} = 3,$$

az 1, $\sqrt[3]{3}$, $\sqrt{9}$ számok lineárisan függetlenek $\mathbb{Q}(\sqrt[3]{2})$ felett. Innen $q_0+3q_3(2\sqrt[3]{2}-1)^3 = 0$, amiből adódóan $(2\sqrt[3]{2} - 1)^3$ racionális. De $(2\sqrt[3]{2} - 1)^3 = 31 + 12\sqrt[3]{2} - 12\sqrt[3]{4}$, tehát ha $(2\sqrt[3]{2}-1)^3$ racionális volna, akkor $\sqrt[3]{2}$ gyöke volna egy $\mathbb{Q}$ feletti másodfokú polinomnak, ami képtelenség.

Feladat 4. Adja meg a $b = \sqrt[4]{3} + 5\sqrt{3} - 3$ szám minimálpolinomját $\mathbb{Q}$ fölött.

Megoldás: Mivel $b \in \mathbb{Q}(\sqrt[4]{3})$, b fokszáma 1, 2, vagy 4 lehet. Ha b elsőfú (vagyis racionális) volna, akkor $\sqrt[4]{3}) \in \mathbb{Q}(\sqrt[4]{3})$ másodfokú lenne. Mivel $b^2 = 84 + 10\sqrt[4]{27} - 29\sqrt{3} - 6\sqrt[4]{3}$, az 1, b, b^2 számok lineárisan függetlenek $\mathbb{Q}$ felett, tehát b nem másodfokú. Így elég olyan negyedfokú racionális polinomot találni, aminek b gyöke. Ez egyszerű:

$$\sqrt{3} = \sqrt[4]{3}^2 = (b - 5\sqrt{3} + 3)^2 = b^2 + (6 - 10\sqrt{3})b + 84 - 30\sqrt{3},$$

ahonnan

$$\sqrt{3(31 + 10b)} = b^2 + 6b + 84,$$

és

$$91 + 30b = (b^2 + 6b + 84)^2 = b^4 + 12b^3 + 204b^2 + 1008b + 7056,$$

tehát a minimálpolinom $x^4 + 12x^3 + 204x^2 + 978x + 6965$.

Feladat 5. Adja meg a $c = \sqrt[5]{2} - \sqrt{2}$ szám minimálpolinomját $\mathbb{Q}$ fölött.

Megoldás: Mivel

$$2 = (c+\sqrt{2})^5 = c^5 + 20c^3 + 20c + (5c^4 + 20c^2 + 4)\sqrt{2},$$
$$(2 - c^5 - 20c^3 - 20c)^2 = 2(5c^4 + 20c^2 + 4)^2,$$

tehát c gyöke az

$$x^{10} - 10x^8 + 40x^6 - 4x^5 + 720x^4 - 80x^3 + 80x^2 - 80x - 28$$

polinomnak.

Belátjuk, hogy ez a minimálpolinom. Ha c fokszáma 1 vagy 2 lenne, akkor $c+\sqrt{2}$ fokszáma nem lehetne több 4-nél. Így csak azt kell kizárni, hogy c ötödfokú. Tegyük fel, hogy $q_0 + \cdots + q_4c^4 + q_5c^5 = 0$. Ekkor

$$q_0 + q_1(\sqrt[5]{2} - \sqrt{2}) + q_2(\sqrt[5]{4} - 2\sqrt[5]{2}\sqrt{2} + 2) + q_3(\sqrt[5]{8} - 3\sqrt[5]{4}\sqrt{2} + 6\sqrt[5]{2} - 2\sqrt{2}) +$$
$$q_4(\sqrt[5]{16} - 4\sqrt[5]{8}\sqrt{2} + 12\sqrt[5]{4} - 8\sqrt[5]{2}\sqrt{2} + 4) +$$
$$q_5(2 - 5\sqrt[5]{16}\sqrt{2} + 20\sqrt[5]{8} - 20\sqrt[5]{4}\sqrt{2} + 20\sqrt[5]{2} - 4\sqrt{2}) = 0.$$

Mit lehet ezzel kezdeni? A bal oldal $u + v\sqrt{2}$ alakba írható, ahol $u, v \in \mathbb{Q}(\sqrt[5]{2})$. Viszont a $\mathbb{Q}(\sqrt[5]{2})$ testben nincs benne a $\sqrt{2}$, mert $\mathbb{Q}(\sqrt[5]{2})$ ötödfokú bővítése a $\mathbb{Q}$-nak, $\sqrt{2}$ viszont másodrendű. Ezért $u = v = 0$. Viszont u és v felírhatók az 1, $\sqrt[5]{2}$, $\sqrt[5]{4}$, $\sqrt[5]{8}$, $\sqrt[5]{16}$ számok racionális együtthatós lineáris kombinációjaként. Ezeknek az együtthatóknak így 0-knak kell lenniük. Ezzel tíz egyenletet kaptunk:

$$\begin{aligned}
q_0 + 2q_2 + 4q_4 + 2q_5 &= 0\\
q_1 + 6q_3 + 20q_5 &= 0\\
q_2 + 12q_4 &= 0\\
q_3 + 20q_5 &= 0\\
q_4 &= 0\\
-q_1 - 2q_3 - 4q_5 &= 0\\
-2q_2 - 8q_4 &= 0\\
-3q_3 - 20q_5 &= 0\\
-4q_4 &= 0\\
-5q_5 &= 0
\end{aligned}$$

Az utolsó egyenlet rögtön ellentmond annak, hogy c ötödfokú.