1. *Oldjuk meg az* $x^4 - 2x^3 + x^2 - 8x + 3 = 0$ *egyenletet* $\mathbb{C}$ *fölött!*

Megoldás: Írjuk fel az egyenletet két teljes négyzet különbségeként:

$$x^4 - 2x^3 + x^2 - 8x + 3 = (x^2 - x + u)^2 - (2ux^2 + (8 - 2u)x + (u^2 - 3)).$$

A második tag akkor teljes négyzet, ha a diszkriminánsa 0, azaz ha $(8-2u)^2 - 8u(u^2-3) = -8u^3 + 4u^2 - 8u + 64 = 0$, azaz $2u^3 - u^2 + 2u - 16 = 0$. Az utóbbit racionális gyökökre tesztelve látjuk, hogy $u = 2$ kielégíti az egyenletet. Ezzel az eredeti polinom

$$(x^2 - x + 2)^2 - (4x^2 + 4x + 1) = (x^2 - x + 2)^2 - (2x + 1)^2 = (x^2 + x + 3)(x^2 - 3x + 1),$$

aminek gyökei $-\frac{1}{2} \pm \frac{\sqrt{11}}{2}i$ és $\frac{3}{2} \pm \frac{\sqrt{5}}{2}$.

2. *Legyen* α *az* $x^2 - x + 1 \in \mathbb{Q}[x]$ *polinom egyik gyöke.*

a) Hány dimenziós $\mathbb{Q}(\alpha)$ *mint* $\mathbb{Q}$ *fölötti vektortér?*

b) Bizonyítsuk be, hogy α^7 *és* α *lineárisan összefüggnek ebben a vektortérben.*

Megoldás: a) 2 dimenziós; $\{1, \alpha\}$ bázisát adja a vektortérnek.

b) $\alpha^2 = \alpha - 1$, $\alpha^3 = \alpha^2 - \alpha = -1$, $\alpha^6 = 1$, $\alpha^7 = \alpha$.

3. *Bizonyítsuk be, hogy* $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[x]/(x^2 - 2x - 1)$.

Megoldás: Mindkét polinom irreducibilis, és az elsőnek $\sqrt{2}$, a másodiknak $1 + \sqrt{2}$ az egyik gyöke, tehát az első test $\mathbb{Q}(\sqrt{2})$-vel, a második $\mathbb{Q}(1 + \sqrt{2})$-vel izomorf, és $\mathbb{C}$-ben ez a két résztest nyilvánvalóan egybeesik, így izomorfak a feladatban megadott testek is.

4. *Adjuk meg* $\cos 20^\circ$ *minimálpolinomját* $\mathbb{Q}$ *fölött.*

Megoldás: A $\cos 3x = 4\cos^3 x - 3\cos x$ összefüggésből $\alpha = \cos 20^\circ$-ra $4\alpha^3 - 3\alpha = \cos 60^\circ = \frac{1}{2}$, tehát α gyöke a $8x^3 - 6x - 1$ polinomnak. Ez nyilván irreducibilis, mert harmadfokú, és nincs gyöke $\mathbb{Q}$-ban (a racionális gyökteszt szerint csak a $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ jöhetnek szóba). Tehát $8x^3 - 6x - 1$ az α minimálpolinomja.

5. *Adjuk meg* $\sqrt{2} + \sqrt{3}$ *minimálpolinomját* $\mathbb{Q}$*, illetve* $\mathbb{Q}(\sqrt{6})$ *fölött!*

Megoldás: Ha $\alpha = \sqrt{2} + \sqrt{3}$, akkor az $\alpha - \sqrt{2} = \sqrt{3}$ egyenlet négyzetre emelésével és átrendezésével azt kapjuk, hogy $\alpha^2 - 1 = 2\sqrt{2}\alpha$, majd ezt is négyzetre emelve és átrendezve $\alpha^4 - 10\alpha^2 + 1 = 0$, ezért a minimálpolinom osztója az $f(x) = x^4 - 10x^2 + 1$ polinomnak. A racionális gyöktesztből látjuk, hogy $f(x)$-nek nincs lineáris faktora $\mathbb{Q}[x]$-ben. Tehát ha nem irreducibilis, akkor csak két másodfokú irreducibilis polinom szorzata lehet. Az $f(x)$ polinomot faktorizálhatjuk $\mathbb{C}$ fölött: $f(x) = x^4 - 2x^2 + 1 - 8x^2 = (x^2 - 1)^2 - (2\sqrt{2}x)^2 = (x^2 + 2\sqrt{2}x - 1)(x^2 - 2\sqrt{2}x - 1) = (x + \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} - \sqrt{3})$. Tehát ha $\sqrt{2} + \sqrt{3}$ minimálpolinomja másodfokú lenne, akkor az $(x - \sqrt{2} - \sqrt{3})$ tényezőt valamelyik másikkal összeszorozva racionális együtthatós polinomot kapnánk. De a többivel való szorzatában:

$$x^2 - (5 + 2\sqrt{6})$$
$$x^2 - 2\sqrt{3}x + 1$$
$$x^2 - 2\sqrt{2}x - 1$$

valamelyik együttható nem racionális. Tehát f irreducibilis, és így az α minimálpolinomja.
Másik bizonyítás a testbővítések fokának felhasználásával:
Az $\alpha^2 - 1 = 2\sqrt{2}\alpha$ összefüggésből láthatjuk, hogy $\sqrt{2}$, és így $\sqrt{3}$ is benne van $\mathbb{Q}(\alpha)$-ban, másrészt $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, tehát $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Az utóbbi viszont két bővítés egymásutánjával kapható meg: $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2$, mert $\sqrt{2}$ minimálpolinomja az $x^2 - 2$ irreducibilis polinom, és $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})) > 1$, mert különben $\sqrt{3} = a + b\sqrt{2}$ valamely $a, b \in \mathbb{Q}$-ra, és $b = 0$ esetén $\sqrt{3}$, $a = 0$ esetén $\sqrt{3/2}$ racionális lenne, $a, b \neq 0$ esetén négyzetre emelés után azt kapnánk, hogy $\sqrt{2}$ racionális. Tehát a bővítés foka legalább 4, így az $f(x) = x^4 - 10x^2 + 1$ polinom szükségképpen a minimálpolinom.

6. *Legyen α az $x^3 - 2x^2 + x + 1 \in \mathbb{Q}[x]$ polinom egyik gyöke. Adjuk meg $\alpha^2 + 2$ reciprokát α legfőljebb másodfokú polinomjaként!*

Megoldás: Legyen $1/(\alpha^2 + 2) = A\alpha^2 + B\alpha + C$. Mivel

$$\begin{aligned}\alpha^3 &= 2\alpha^2 - \alpha - 1 \text{ és}\\ \alpha^4 &= \alpha(2\alpha^2 - \alpha - 1) = 2\alpha^3 - \alpha^2 - \alpha = 4\alpha^2 - 2\alpha - 2 - \alpha^2 - \alpha =\\ &= 3\alpha^2 - 3\alpha - 2,\end{aligned}$$

az $1 = (A\alpha^2 + B\alpha + C)(\alpha^2 + 2)$ egyenlet

$$1 = A\alpha^4 + B\alpha^3 + (2A + C)\alpha^2 + 2B\alpha + 2C = (5A + 2B + C)\alpha^2 + (-3A + B)\alpha + (-2A - B + 2C)$$

alakra hozható, és az

$$\begin{array}{rcrcrcl} 5A & + & 2B & + & C & = & 0\\ -3A & + & B & & & = & 0\\ -2A & - & B & + & 2C & = & 1 \end{array}$$

egyenletrendszer megoldásaként megkapjuk, hogy $A = \frac{1}{27}$, $B = -\frac{1}{9}$, $C = \frac{11}{27}$, azaz

$$\frac{1}{\alpha^2 + 2} = \frac{1}{27}(-\alpha^2 - 3\alpha + 11)$$

.

7. *Bizonyítsuk be, hogy egy p karakterisztikájú testben*
a) $(a + b)^{p^k} = a^{p^k} + b^{p^k}$ minden a, b elemre és k természetes számra;
b) $x^{p^k} - x$ gyökei résztestet alkotnak;
ha $|K| = p^n$, akkor
c) K minden eleme gyöke az $x^{p^n} - x$ polinomnak;
d) K minden elemének minimálpolinomja osztója $(x^{p^n} - x)$-nek.

Megoldás: a) $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$, ugyanis $0 < k < p$-re $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$ számlálója osztható p-vel, de a nevezője nem. A p-edik hatványozást k-szor alkalmazva azt kapjuk, hogy $(a + b)^{p^k} = a^{p^k} + b^{p^k}$.

b) Ha $a^{p^k} = a$ és $b^{p^k} = b$, akkor $(ab)^{p^k} = a^{p^k} b^{p^k} = ab$, és az a) rész miatt $(a + b)^{p^k} = a^{p^k} + b^{p^k} = a + b$, $(a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1}$, és $(-a)^{p^k} = (-1)^{p^k} a^{p^k} = -a$, tehát

a gyökök halmaza (ami nem üres, sőt tartalmazza az egész $\mathbb{F}_p$-t) zárt a szorzásra, összeadásra és a multiplikatív és az additív inverzre, tehát résztest.

c) $K^\times$ csoport, rendje $p^k - 1$, ezért minden $a \in K^\times$-ra $a^{p^k-1} = 1$, így $a^{p^k} = a$, és ez utóbbi az $a = 0$-ra is igaz, vagyis K minden elemére.

d) Ez közvetlen következménye a c)-nek.

Hf1. *Határozzuk meg a* $\mathbb{Q}(\sqrt{4-\sqrt{2}})$ *minimálpolinomját* $\mathbb{Q}$ *fölött!*

Hf2. *Legyen* $K = \mathbb{F}_2(\alpha)$ *a kételemű testnek az* $x^4 + x + 1 \in \mathbb{F}_2[x]$ *polinom* α *gyökével való bővítése. Írjuk fel az* $\frac{\alpha^2}{\alpha+1}$ *elemet* α *legföljebb harmadfokú polinomjaként!*