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

2. *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.

3. *Hányadfokú a $\mathbb{Q}(i\sqrt{3})$, illetve a $\mathbb{Q}(i+\sqrt{3})$ bővítés $\mathbb{Q}$ fölött?*

Megoldás: $i\sqrt{3}$ gyöke az x^2+3 irreducibilis polinomnak, tehát a vele való bővítés másodfokú.

A második bővítés nyilván benne van $\mathbb{Q}(\sqrt{3},i)$-ben. Másrészt, ha $\alpha=i+\sqrt{3}$, akkor $\alpha-\sqrt{3}=i$, amiből $-1=\alpha^2+3-2\sqrt{3}\alpha$, tehát $\sqrt{3}=\dfrac{\alpha^2+4}{2\alpha}\in\mathbb{Q}(\alpha)$, és ebből $i=\alpha-\sqrt{3}\in\mathbb{Q}(\alpha)$ is következik, tehát $\mathbb{Q}(i+\sqrt{3})=\mathbb{Q}(\sqrt{3},i)$. Az utóbbi két bővítés egymásutánjával kapható meg: $\mathbb{Q}\le\mathbb{Q}(\sqrt{3})\le\mathbb{Q}(\sqrt{3},i)$. A $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ bővítés nyilván másodfokú ($\sqrt{3}$ minimálpolinomja $\mathbb{Q}$ fölött x^2-3), a másodiknál i gyöke az x^2+1 polinomnak, tehát a bővítés legföljebb másodfokú, elsőfokú viszont nem lehet, mert $\mathbb{Q}(\sqrt{3})\le\mathbb{R}$, míg $i\notin\mathbb{R}$. Tehát $(\mathbb{Q}(i+\sqrt{3}):\mathbb{Q})=2\cdot2=4$.

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

Megoldás: A $\cos 3x=4\cos^3x-3\cos x$ 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 $\pm1,\pm\frac{1}{2},\pm\frac{1}{4},\pm\frac{1}{8}$ jöhetnek szóba). Tehát $8x^3-6x-1$ az α minimálpolinomja.

5. *Számítsuk ki a következő testbővítések fokait $\mathbb{Q}$ fölött!*

a) $\mathbb{Q}(\sqrt{2})$ *b)* $\mathbb{Q}(\sqrt[3]{2})$ *c)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{4})$ *d)* $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *e)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt{2})$

Megoldás: a) Másodfokú, mert x^2-2 irreducibilis.

b) Harmadfokú, mert x^3-2 irreducibilis polinom (pl. a Schönemann–Eisenstein-kritérium miatt).

c) Legyen $\alpha=\sqrt[3]{2}+\sqrt[3]{4}$. Ekkor $\alpha^3=2+3\sqrt[3]{16}+3\sqrt[3]{32}+4=6+6\sqrt[3]{2}+6\sqrt[3]{4}=6+6\alpha$, tehát α gyöke az x^3-6x-6 polinomnak, amely a Schönemann–Eisenstein-kritérium szerint irreducibilis, tehát α-nak minimálpolinomja. Következésképpen a bővítés harmadfokú. (Másképp: beláthatjuk, hogy $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt[3]{2})$.)

d) Legyen $\alpha=\sqrt{2}+\sqrt{3}$. Belátjuk, hogy $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Az előbbi nyilván benne van az utóbbiban, tehát csak a fordított tartalmazást kell megmutatni. Az $\alpha-\sqrt{2}=\sqrt{3}$ egyenletet négyzetre emelve a $\sqrt{2}$-t kifejezhetjük α-val: $\sqrt{2}=\dfrac{\alpha^2-1}{2\alpha}\in\mathbb{Q}(\alpha)$, és így $\sqrt{3}\in\mathbb{Q}(\alpha)$ is igaz. A $\mathbb{Q}\le\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\sqrt{2},\sqrt{3})$ bővítéssorozatból, az első nyilván másodfokú, a második legföljebb másodfokú, és pontosan másodfokú, ha $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. Az utóbbi pedig igaz, mert $\sqrt{3}=a+b\sqrt{2}$ $(a,b\in\mathbb{Q})$ esetén $3=a^2+2b^2+2ab\sqrt{2}$,

és a felírás egyértelműsége miatt ekkor $ab = 0$, $a^2 + 2b^2 = 3$ adódik, aminek könnyen ellenőrizhetően nincs racionális megoldása. Tehát $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 2 \cdot 2 = 4$.

e) Legyen $\alpha = \sqrt[3]{2} + \sqrt{2}$. A bővítés nyilván benne van a $\mathbb{Q}(\sqrt[6]{2})$ testben, ami $\mathbb{Q}$-nak 6-odfokú bővítése (a minimálpolinom $x^6 - 2$, ami a Schönemann–Eisenstein-kritérium miatt irreducibilis). Másrészt az $\alpha - \sqrt{2} = \sqrt[3]{2}$ egyenletet köbre emelve a $\sqrt{2}$-t ki tudjuk fejezni α racionális együtthatós racionális törtfüggvényeként, ezért $\sqrt{2} \in \mathbb{Q}(\alpha)$, ebből $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$, és $\sqrt[6]{2} = \sqrt{2}/\sqrt[3]{2} \in \mathbb{Q}(\alpha)$. Tehát $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[6]{2})$, és a foka $\mathbb{Q}$ fölött 6.

6. *Legyen α az $x^3 - 2x^2 + x + 1$ polinom egyik gyöke. Adjuk meg $\alpha - 1$ reciprokát α legfőljebb másodfokú polinomjaként!*

Megoldás: $0 = \alpha^3 - 2\alpha^2 + \alpha + 1 = \alpha(\alpha - 1)^2 + 1$, így $0 = \alpha(\alpha - 1) + (\alpha - 1)^{-1}$, azaz $(\alpha - 1)^{-1} = -\alpha^2 + \alpha$.

Általánosabb módszerrel megoldhatjuk úgy is, hogy keressük azt az ismeretlen együtthatós $A\alpha^2 + B\alpha + C$ polinomját α-nak, amelynek az $\alpha - 1$-gyel vett szorzata 1: $1 = (A\alpha^2 + B\alpha + C)(\alpha - 1) = A\alpha^3 + (B - A)\alpha^2 + (C - B)\alpha - C = A(2\alpha^2 - \alpha - 1) + (B - A)\alpha^2 + (C - B)\alpha - C = (A + B)\alpha^2 + (-A - B + C)\alpha - (A + C)$, ami az $A + B = 0$, $-A - B + C = 0$ és $A + C = -1$ egyenleteket adja, és az egyenletrendszer megoldása $A = -1$, $B = 1$, és $C = 0$.

7. *Hányadfokú az F/K bővítés, ha F az f felbontási teste, és*

a) $K = \mathbb{Q}$, $f = x^6 - 1$ *b)* $K = \mathbb{Q}$, $f = x^6 - 2$
c) $K = \mathbb{F}_7$, $f = x^6 - 1$ *d)* $K = \mathbb{F}_5$, $f = x^6 - 2$

Megoldás: a) Elég egyetlen primitív hatodik egységgyökkel bővíteni, és annak a minimálpolinomja a hatodik körosztási polinom, amelynek a foka $\varphi(6) = 2$ (a polinom egyébként $x^2 - x + 1$). Tehát a felbontási test 2-odfokú $\mathbb{Q}$ fölött.

b) A $\mathbb{Q}$-hoz adjungálandó gyökök $\sqrt[6]{2}$, és ennek a 6-odik egységgyökszörösei, tehát ezek hányadosaként a hatodik egységgyökök is belekerülnek a felbontási testbe. A valós 6-odik egységgyökkel való bővítés 6-odfokú ($x^6 - 2$ a minimálpolinomja), de ez még $\mathbb{R}$-ben van, tehát a primitív 6-odik egységgyök adjungálása efölött még egy másodfokú bővítést jelent, és ezzel az $x^6 - 2$ összes gyöke belekerül a bővebb testbe. Tehát a bővítés foka $6 \cdot 2 = 12$.

c) Az $\mathbb{F}_7$ összes nem 0 eleme kielégíti az $x^6 = 1$ egyenletet (elemei a 6-odrendű multiplikatív csoportnak), és ennél több gyöke az $x^6 - 1$ polinomnak nem is lehet, tehát a felbontási test maga az $\mathbb{F}_7$, a bővítés foka pedig 1.

d) $\mathbb{F}_5$-ben 2 nem négyzetszám, de köbszám: $3^3 = 2$, így $x^6 - 2 = x^6 - 3^3 = (x^2 - 3)(x^4 + 3x^2 + 9)$. Az utóbbi polinom szintén felbontható: $x^4 + 3x^2 + 9 = x^4 - 6x^2 + 9 + 9x^2 = x^4 - 6x^2 + 9 - x^2 = (x^2 - 3)^2 - x^2 = (x^2 - x - 3)(x^2 + x - 3)$. A kapott három másodfokú polinom mindegyike irreducibilis (mivel másodfokúak, elég ellenőrizni, hogy nincs gyökük $\mathbb{F}_5$-ben). Viszont az első polinom egy gyökével bővítve, a többiek gyökei is belekerülnek a bővítésbe (ha az első gyökeit $\pm\sqrt{3}$-mal jelöljük, akkor a másik kettőé $(\pm 1 \pm \sqrt{3})/2$ (a 2-vel való osztás $\mathbb{F}_5$-ben értelmezve van)), tehát a felbontási test foka $\mathbb{F}_5$ fölött 2.

8. *Legyen $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Irreducibilis-e ez a polinom? Ha $f(\theta) = 0$, ahol θ az f felbontási testének eleme, akkor mennyi lehet θ rendje a test multiplikatív csoportjában?*

Megoldás: x^4+x+1 irreducibilis, mert nincs gyöke $\mathbb{F}_2$-ben, és másodfokú irreducibilisek szorzataként csak az $(x^2+x+1)^2 = x^4+x^2+1$ áll elő, ugyanis $\mathbb{F}_2$ fölött egyetlen másodfokú irreducibilis polinom van. A felbontási test $2^4 = 16$ elemű, a multiplikatív csoportja 15 elemű, tehát θ rendje osztója 15-nek. Viszont $\theta^3 \neq 1$, mert akkor kisebb fokú lenne a minimálpolinomja, és $\theta^5 = \theta^2+\theta \neq 1$, így θ rendje csak 15 lehet.

9. *Legyen α az x^3+x+1 polinom egyik gyöke $\mathbb{F}_2$ fölött, és legyen $K = \mathbb{F}_2(\alpha)$. Irreducibilis-e az $x^2+x+\alpha$ polinom K fölött?*

Megoldás: Mivel az $x^2+x+\alpha$ polinom másodfokú, elég megnézni, hogy van-e gyöke $K = \mathbb{F}_2(\alpha)$-ban. Ha $A\alpha^2+B\alpha+C$ gyöke ennek a polinomnak, akkor $0 = (A\alpha^2+B\alpha+C)^2+(A\alpha^2+B\alpha+C)+\alpha = A^2\alpha^4+B^2\alpha^2+C^2+A\alpha^2+B\alpha+C+\alpha = A\alpha^4+B\alpha^2+C+A\alpha^2+B\alpha+C+\alpha = A(\alpha^2+\alpha)+B\alpha^2+C+A\alpha^2+B\alpha+C+\alpha = B\alpha^2+(A+B+1)\alpha$, amiből $A = 1$, $B = 0$, és C tetszőleges. Tehát az $x^2+x+\alpha$ polinom gyökei α^2 és α^2+1 mind K-ban vannak, ezért a polinom nem irreducibilis K fölött.

10. *Lássuk be, hogy ha $L|K$ algebrai testbővítés, és az R gyűrűre $K \leq R \leq L$, akkor R test!*

Megoldás: Tetszőleges $0 \neq \alpha \in R$ elem algebrai K fölött, így $K(\alpha)$ mint az L részteste α K fölötti polinomjaiból áll, és így $K(\alpha) \leq R$. Viszont $1/\alpha \in K(\alpha)$, tehát R-nek minden nem 0 eleme invertálható, vagyis R test.

11. *Legyen K tetszőleges test, $K(t)$ pedig K-nak egy egyszerű transzcendens bővítése. Legyen $K < M \leq K(t)$. Bizonyítsuk be, hogy $K(t)$ algebrai bővítése M-nek!*

Megoldás: Legyen $c \in M \setminus K$. Ekkor $c = f(t)/g(t)$ valamely $f(x), g(x) \in K[x]$ nem 0 polinomokra. Ebből azt kapjuk, hogy t gyöke a $h(x) = f(x)-cg(x) \in M[x]$ polinomnak. Azt kell csak belátni, hogy ez nem 0 polinom. Legyen $a \in K$ az $f(x)$, $b \in K$ a $g(x)$ polinom főegyütthatója. Ha $\deg f > \deg g$, akkor $h(x)$ főegyütthatója a, ha $\deg f < \deg g$, akkor $-cb$, nyilván egyik se 0. Végül ha $\deg f = \deg g = n$, akkor az x^n együtthatója h-ban $a-cb$, és ez sem 0, ugyanis különben $c = a/b \in K$ lenne.

Hf1. *Határozzuk meg a $\mathbb{Q}(\sqrt{3-\sqrt{2}})$ testbővítés fokát $\mathbb{Q}$ fölött!*

Hf2. *Legyen α az x^2+x-1 polinom egyik gyöke $\mathbb{F}_3$ fölött, és $K = \mathbb{F}_3(\alpha)$. Határozzuk meg az x^2+1 polinom összes gyökét K-ban mint az α lineáris polinomját!*

Hf3. *Tegyük fel, hogy $\alpha, \beta \in L$ elemekre $\alpha+\beta$ algebrai, $\alpha\beta$ pedig transzcendens a K résztest fölött. Hány lehet algebrai az α, β és $\alpha^2+\alpha$ közül?*