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

Megoldás: $(i\sqrt{3})^2 = -3$, tehát $i\sqrt{3}$ gyöke az x^2+3 polinomnak, és ez irreducibilis, ezért ez az $i\sqrt{3}$ minimálpolinomja. Következésképpen $(\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}) = 2$.
Legyen $\alpha = i+\sqrt{3}$. Az $\alpha - \sqrt{3} = i$ egyenlőséget négyzetre emelve látjuk, hogy $\sqrt{3} \in \mathbb{Q}(\alpha)$, és akkor $i = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$ is teljesül, amiből $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, i)$. A $\mathbb{Q} \le \mathbb{Q}(\sqrt{3}) \le \mathbb{Q}(\sqrt{3}, i)$ bővítéssorozat egyik lépése sem triviális ($\sqrt{3}$ nem racionális, és i nem valós), viszont mindegyik bővítő elem gyöke egy másodfokú polinomnak, ezért a $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ bővítés foka csak $2 \cdot 2 = 4$ lehet.

2. *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)* $\mathbb{Q}(\sqrt[3]{2}+\sqrt{2})$

Megoldás: a) $\sqrt{2}$ minimálpolinomja x^2-2, ezért a bővítés foka 2.

b) $\sqrt[3]{2}$ minimálpolinomja x^3-2 (irreducibilis például a Schönemann–Eisenstein-kritérium miatt), így a bővítés foka 3.

c) Legyen $\alpha = \sqrt[3]{2}+\sqrt[3]{4}$. Mivel $\alpha = \sqrt[3]{2} + (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$, felírhatjuk a következő bővítéssorozatot:

$$\mathbb{Q} \le \mathbb{Q}(\alpha) \le \mathbb{Q}(\sqrt[3]{2}).$$

Itt $3 = (\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = (\mathbb{Q}(\alpha) : \mathbb{Q}) \cdot (\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\alpha))$, és a második bővítés foka legföljebb 2, mert $\sqrt[3]{2}$ gyöke az $x^2+x-\alpha$ polinomnak, tehát a második bővítés csak triviális lehet, és így $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 3$.

Egy $f(x) \in K[x]$ polinom felbontási teste $L \ge K$, ha L-ben f lineáris faktorokra bomlik, és ha itt f gyökei $\alpha_1, \dots, \alpha_n$, akkor $L = K(\alpha_1, \dots, \alpha_n)$. (Ez izomorfia erejéig egyértelmű.)

3. *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) A felbontási testet megkapjuk, ha egyetlen primitív 6-dik egységgyököt adjungálunk $\mathbb{Q}$-hoz (akkor a többi hatványa is, tehát x^6-1 összes gyöke belekerül a testbővítésbe), ennek a minimálpolinomja pedig $\Phi_6(x) = x^2-x+1$, ezért x^6-1 felbontási teste 2-odfokú $\mathbb{Q}$ fölött.

b) x^6-2 gyökei $\sqrt[6]{2}$ és ennek hatodik egységgyökszörösei. Másrészt ha ε primitív 6-odik egységgyök, akkor $\varepsilon = (\varepsilon\sqrt[6]{2})/\sqrt[6]{2}$ a polinom két gyökének hányadosa, tehát ε is benne van a felbontási testben. Ebből azt kaptuk, hogy $F = \mathbb{Q}(\sqrt[6]{2}, \varepsilon)$, amit a $\mathbb{Q} \le \mathbb{Q}(\sqrt[6]{2}) \le \mathbb{Q}(\sqrt[6]{2}, \varepsilon)$ bővítéssorozattal is megkaphatunk. Ebben az első bővítés foka 6, mert x^6-2 irreducibilis a Schönemann–Eisenstein-kritérium miatt, és a második bővítés egyrészt nem triviális (ε nem valós, de a második test része $\mathbb{R}$-nek), másrészt legföljebb másodfokú (az x^2-x+1 gyöke), így pontosan másodfokú. Ebből adódóan $(F : \mathbb{Q}) = 6 \cdot 2 = 12$.

c) x^6-1-nek gyöke $\mathbb{F}_7$ összes nemnulla eleme, és ezekből éppen hat van, tehát maga $\mathbb{F}_7$ a felbontási test, vagyis az F/K bővítés foka 1.

d) 2 köbszám modulo 5, ezért $x^6-2 = x^6-3^3 = (x^2-3)(x^4+3x^2+9)$. A második tényezőt megpróbálhatjuk két teljes négyzet különbségére bontani az x^2-es vagy a

konstans tagnak az első teljes négyzetbe rakásával: $x^4+3x^2+9 = x^4+4x^2+4-x^2 = (x^2+2)^2-x^2 = (x^2-x+2)(x^2+x+2)$, vagyis

$$x^6-2 = (x^2-3)(x^2-x+2)(x^2+x+2),$$

ahol a másodfokú faktorok már irreducibilisek, mert nincs gyökük $\mathbb{F}_5$-ben. Mivel $\mathbb{F}_5$ egy másodfokú bővítésében már minden másodfokú, $\mathbb{F}_5$ fölött irreducibilis polinom lineáris faktorokra bomlik (ld. a 9. feladatot), elég az egyiknek egy gyökét adjungálni $\mathbb{F}_5$-höz, hogy megkapjuk a felbontási testet. Tehát $(F:\mathbb{F}_5)=2$.
Másképpen: Nevezzük $\sqrt{3}$-nak az x^2-3 egyik gyökét. Ekkor a másik két irreducibilis polinom gyökei, a másodfokú megoldóképlet szerint $(\pm 1 \pm \sqrt{3})/2$, szintén benne vannak az $\mathbb{F}_5(\sqrt{3})$-ban, így a felbontási test a $\sqrt{3}$-mal való 2-odfokú bővítés.

4. *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: Az x^3+x+1 irreducibilis, tehát $(\mathbb{Q}(\alpha):\mathbb{Q})=3$. Keressük meg az $x^2+x+\alpha$ polinom β gyökének minimálpolinomját $\mathbb{F}_2$ fölött! Mivel $\alpha=\beta^2+\beta$ gyöke az x^3+x+1-nek, $0=(\beta^2+\beta)^3+(\beta^2+\beta)+1 = \beta^6+\beta^5+\beta^4+\beta^3+\beta^2+\beta+1$, tehát β minimálpolinomja osztója az $f(x)=x^6+x^5+x^4+x^3+x^2+x+1$ polinomnak. Ennek $\mathbb{F}_2$-beli gyöke nincs, és könnyen ellenőrizhető, hogy az egyetlen másodfokú irreducibilis polinom, x^2+x+1 sem osztója $f(x)$-nek, viszont a harmadfokú x^3+x+1 igen: $f(x)=(x^3+x+1)(x^3+x^2+1)$ az irreducibilisekre bontása. Ebből következik, hogy $(\mathbb{F}_2(\beta):\mathbb{F}_2)=3$, viszont $\mathbb{F}_2 \le \mathbb{F}_2(\alpha) \le \mathbb{F}_2(\alpha,\beta)=\mathbb{F}_2(\beta)$, és ebben az első bővítés is harmadfokú, tehát $(K(\beta):K)=1$, azaz az $x^2+x+\alpha$ polinom nem lehet irreducibilis K fölött. (Konkrétan ellenőrizhető, hogy α^2 és α^2+1 a gyökei.)

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

Megoldás: Legyen $\alpha \in R$ tetszőleges nem nulla elem. Ekkor a $K[\alpha] := \{\, f(\alpha) \,|\, f(x) \in K[x] \,\}$ részgyűrű R-ben. Másrészt $\alpha \in L$ miatt $K(\alpha)$ véges fokú testbővítés K fölött (mert $L|K$ algebrai), így $K(\alpha)$ minden eleme, így α^{-1} is előáll α polinomjaként, vagyis benne van $K[\alpha]$-ban, és ezzel R-ben is. Beláttuk, hogy R az invertálásra is zárt, tehát részteste L-nek.

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

Megoldás: Legyen $c \in M \setminus K$. Ekkor $c=\dfrac{f(t)}{g(t)}$ valamely $f(x)=a_nx^n+\ldots+a_0,\ g(x)=b_mx^m+\ldots+b_0 \in K[x]$, $g \neq 0$ polinomokkal. Tehát t gyöke a $h(x)=f(x)-cg(x) \in K(c)$ polinomnak. Ez a polinom nem triviális, ugyanis $g(x) \neq 0$ miatt g-nek van nem nulla együtthatója, mondjuk, $b_k \neq 0$, és akkor $h(x)$-ben az x^k együtthatója a_k-cb_k, ami nem lehet 0, mert különben $c=a_k/b_k \in K$ volna. Ezzel azt kaptuk, hogy t algebrai M fölött, azaz a $K(t)=M(t)$ bővítés algebrai M fölött.

7. *Tegyük fel, hogy $\alpha,\beta,\gamma \in \mathbb{C}$ olyanok, hogy $\alpha\beta\gamma$, $\alpha\beta+\alpha\gamma+\beta\gamma$ és $\alpha+\beta+\gamma$ is algebrai számok $\mathbb{Q}$ fölött. Bizonyítsuk be, hogy α, β és γ is algebraiak.*

Megoldás: Legyen $f(x)=(x-\alpha)(x-\beta)(x-\gamma)=x^3+a_2x^2+a_1x+a_0$. A feltétel szerint $a_0=-\alpha\beta\gamma,\ a_1=\alpha\beta+\alpha\gamma+\beta\gamma,\ a_2=-(\alpha+\beta+\gamma)$ algebraiak $\mathbb{Q}$ fölött, így a

$\mathbb{Q}(a_0, a_1, a_2)|\mathbb{Q}$ bővítés is algebrai. Viszont α, β, γ gyökei a $0 \neq f(x) \in \mathbb{Q}(a_0, a_1, a_2)[x]$ polinomnak, tehát algebraiak $\mathbb{Q}(a_0, a_1, a_2)$ fölött. Mivel algebrai bővítések egymásutánja is algebrai, azt kaptuk, hogy α, β, γ algebraiak $\mathbb{Q}$ fölött is.

8. *Bizonyítsuk be, hogy ha p prím, és K egy p^n elemű test, akkor*
a) K-nak minden részteste p^d elemű az n valamely d osztójára;
b) n minden d osztójára van K-nak pontosan egy p^d elemű részteste;
c) $\mathrm{Aut}(K)$ egy n elemű ciklikus csoport, amelynek generátoreleme az $x \mapsto x^p$ $(x \in K)$ automorfizmus.

Megoldás:
a) Ha M részteste K-nak, akkor K vektortér M fölött, ezért $|M| = m$ esetén $p^n = m^k$ valamely k-ra. Ebből következik, hogy $|M| = p^d$, és $dk = n$, azaz $d \mid n$.
b) Tudjuk az 1. feladatsor 7.b) feladatából, hogy az $x^{p^d} - x$ polinom gyökei résztestet alkotnak K-ban, s mivel $(x^{p^d} - x) \mid (x^{p^n} - x)$ különböző gyöktényezők szorzata K-ban, ez a résztest éppen p^d-elemű.
c) $(K : \mathbb{F}_p) = n$, és $K|\mathbb{F}_p$ egyszerű bővítés ($K^\times$ generátoreleme generálja a testbővítést is), így $|\operatorname{Aut} K| \leq n$.
A $\sigma : x \mapsto x^p$ leképezés művelettartó az 1/7.a) miatt, és nyilván injektív, ezért K végessége miatt szürjektív is. Ennek az automorfizmusnak a k. hatványa a $\sigma^k : x \mapsto x^{p^k}$ leképzés, ami az identitás $k = n$-re, ugyanis K minden eleme gyöke az $x^{p^n} - x$ polinomnak (ld. 1/7.c)), viszont kisebb k-ra nem, ugyanis az $x^{p^k} - x$-nek legföljebb p^k gyöke van. Vagyis $o(\sigma) = n$. Mivel $|\operatorname{Aut} K| \leq n$, azt kaptuk, hogy $\operatorname{Aut} K = \langle\sigma\rangle \cong C_n$.

9. *Legyen K az $x^{p^n} - x$ felbontási teste $\mathbb{F}_p$ fölött, ahol p prím. Bizonyítsuk be, hogy*
a) $|K| = p^n$;
b) K megkapható $\mathbb{F}_p$ egyszerű algebrai bővítéseként;
c) $x^{p^d} - x$ osztója $(x^{p^n} - x)$-nek az n minden d osztójára;
d) $(x^{p^n} - x)$-nek osztója minden olyan irreducibilis polinom, amelynek foka osztója n-nek;
e) minden p^n elemű test izomorf egymással.

Megoldás: a) A felbontási testben $x^{p^n} - x$ gyökei résztestet alkotnak, tehát ez a résztest a teljes felbontási test. Másrészt ennek a polinomnak minden gyöke egyszeres, mert $\left((x^{p^n} - x)',\ x^{p^n} - x\right) = \left(-1,\ x^{p^n} - x\right) = 1 \neq 0$, tehát a felbontási test p^n elemű.
b) A $K^\times$ multiplikatív csoport α generátorelemére $\mathbb{F}_p(\alpha) = K$. Mivel K véges, ez szükségképpen algebrai bővítés.
c) Ha $n = dk$, akkor $p^d - 1 \mid (p^d)^k - 1 = p^n - 1 \Rightarrow (x^{p^d-1} - 1) \mid (x^{p^n-1} - 1) \Rightarrow (x^{p^d} - x) \mid (x^{p^n} - x)$.
d) Legyen $f(x) \in \mathbb{F}_p$ irreducibilis, ahol $\deg f = d \mid n$, és $M = \mathbb{F}_p(\alpha)$ az f egy α gyökével való bővítés. Ekkor $|M| = p^d \Rightarrow \alpha$ gyöke $x^{p^d} - x$-nek $\Rightarrow f(x) \mid (x^{p^d} - x)$, és az utóbbi a c) rész miatt osztója $(x^{p^n} - x)$-nek.
e) Tegyük fel, hogy a K és az L test elemszáma is p^n. Mindkettő megkapható az $\mathbb{F}_p$ egyszerű algebrai bővítéseként (pl. a multiplikatív csoport egy generátorelemével): $K = \mathbb{F}_p(\alpha)$ és $L = \mathbb{F}_2(\beta)$, ahol α minimálpolinomja $f(x)$, β minimálpolinomja $g(x)$ n-edfokú irreducibilis polinomok $\mathbb{F}_p$ fölött. K-ban az $x^{p^n} - x$ polinom lineáris faktorokra bomlik (K mind a p^n eleme gyöke ennek a polinomnak), és a d) rész szerint

$g(x)$ is osztója $x^{p^n} - x$-nek, tehát $g(x)$-nek van egy γ gyöke K-ban is. Mivel $g(x)$ irreducibilis, $(\mathbb{F}_p(\gamma) : \mathbb{F}_p) = n$, és így $K = \mathbb{F}_p(\gamma)$. Mivel β és γ ugyanannak az $\mathbb{F}_p$ fölötti irreducibilis polinomnak a gyökei más-más testbővítésben, $K = \mathbb{F}_p(\gamma) \cong \mathbb{F}_p(\beta) = L$. (Vegyük észre, hogy az egyértelműség bizonyításához itt nem használtuk a felbontási test egyértelműségét.)

Hf1. *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!*

Hf2. *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?*