1. *Legyen α az x^3-2 polinom egyik nem valós gyöke. Határozzuk meg α fokát $\mathbb{Q}(\sqrt[3]{2})$ fölött, és határozzuk meg a $\mathbb{Q}(\alpha)\cap\mathbb{R}$ résztestet! Igaz-e, hogy ha $K\le L\le M$, és $\alpha\in M$, akkor α L fölötti foka osztója α K fölötti fokának?*

Megoldás: Mivel $\alpha=\sqrt[3]{2}\,\varepsilon$, ahol ε primitív harmadik egységgyök, α foka $L=\mathbb{Q}(\sqrt[3]{2})$ fölött legfőljebb 2, de ε nincs benne L-ben, ezért a foka pontosan 2. Legyen $K=\mathbb{Q}$ és M az x^3-2 felbontási teste $\mathbb{Q}$ fölött.
Az előbb láttuk, hogy ekkor $K\le L\le M$, $\alpha\in M$, α foka L fölött 2, de K fölött 3, mivel α minimálpolinomja K fölött harmadfokú. Tehát az α elem M fölötti foka nem feltétlenül osztja a kisebb, K test fölötti fokát.
A $\mathbb{Q}\le\mathbb{Q}(\alpha)\cap\mathbb{R}\le\mathbb{Q}(\alpha)$ bővítéssorozatban a két bővítés fokának szorzata, $(\mathbb{Q}(\alpha):\mathbb{Q})=3$, és a második bővítés nem triviális (ugyanis $\alpha\notin\mathbb{R}$), tehát a másodk foka 3, és az elsőé csak 1 lehet.

2. *Bizonyítsuk be, hogy minden másodfokú bővítés normális!*

Megoldás: Ha bővítünk egy másodfokú irreducibilis polinom egyik gyökével, akkor az ehhez tartozó gyöktényező a bővebb test fölött kiemelhető a polinomból, és így a megmaradó, elsőfokú polinom gyöke is benne lesz ebben a testben.

3. *Igaz-e, hogy normális bővítés normális bővítése normális az eredeti test fölött?*

Megoldás: Nem igaz. Tekintsük a $\mathbb{Q}\le\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\sqrt[4]{2})$ bővítéssorozatot. Mindkét bővítés másodfokú (x^2-2, illetve $x^2-\sqrt{2}$ a minimálpolinomok), így normális, de $\sqrt[4]{2}$ $\mathbb{Q}$ fölötti minimálpolinomjának, x^4-2-nek nem valós gyökei is vannak, és ezek még a bővebb testben sincsenek benne.

4. *Legyen $L|K$ egy testbővítés, M és N pedig olyan közbülső testek, amelyekre az $M|K$ és $N|K$ bővítések normálisak. Legyen S az L-nek az M és N által generált részteste és $T=M\cap N$. Bizonyítsuk be, hogy az $S|K$ és $T|K$ bővítések mindegyike normális.*

Megoldás: Legyen $\alpha\in S$. Ekkor α előállítható véges sok M-beli és N-beli elem K fölötti racionális törtfüggvényeként, azaz $\alpha\in K(\beta_1,\dots,\beta_m,\gamma_1,\dots,\gamma_n)$, ahol $\beta_i\in M$ és $\gamma_j\in N$ minden i,j-re. Legyenek $f_1,\dots,f_m,g_1,\dots,g_n$ az $\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n$ minimálpolinomjai K fölött. Ezek a polinomok lineáris faktorokra bomlanak S-ben, mert $M|K$ és $N|K$ normális bővítések, így ezeknek a polinomoknak a szorzata, f is lineáris faktorokra bomlik. Legyen F az f felbontási teste K fölött. Ekkor $F|K$ normális bővítés, így α K fölötti minimálpolinomja lineáris faktorokra bomlik F-ben, és az F-et tartalmazó S-ben is.

Ha $\alpha\in T=M\cap N$, és f az α normált minimálpolinomja K fölött, akkor f az M és N fölött is gyöktényezőkre bomlik, és az L fölötti normált irreducibilisekre bontás egyértelműsége miatt a két felbontás megegyezik, vagyis a kapott gyökök $M\cap N$-beliek, így f $M\cap N$ fölött is felbomlik.

5. *Hányadfokú x^4-x^2+1 felbontási teste $\mathbb{Q}$ fölött, illetve $\mathbb{F}_p$ fölött, ha p prím?*

Megoldás: $f(x):=x^4-x^2+1=\dfrac{x^6+1}{x^2+1}=\dfrac{x^{12}-1}{(x^6-1)(x^2+1)}$ a 12-edik körosztási polinom, tehát irreducibilis, és egyetlen gyökének (egy primitív 12-edik egységgyöknek) a hatványaként előáll az összes többi, így egy gyökével való bővítés már a teljes felbontási test. Ebből következik, hogy a felbontási test $\mathbb{Q}$ fölött 4-edfokú.

(Az irreducibilitás bizonyítható úgy is, hogy az $x^4 - x^2 + 1 = (x^2+1)^2 - 3x^2 = (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$ $\mathbb{R}[x]$-beli irreducibilisekre bontásból látható, hogy $\mathbb{Q}$ fölött irreducibilis az $f(x)$, mert az 1 főegyütthatós irreducibilis faktorokra való felbontás egyértelműsége miatt a $\mathbb{Q}$ fölötti felbontás is csak ebből a felbontásból rakható össze.)
Ha $p \neq 2, 3$, akkor $x^{12} - 1$ minden gyöke különböző a felbontási testében ($(x^{12}-1)' = 12x^{11} \neq 0$ és relatív prím $x^{12}-1$-hez), ezért $f(x)$ gyökei csak a 12-edrendű elemek lehetnek. Sőt, ha van a ciklikus $\mathbb{F}_{p^n}^\times$ csoportban 12-edrendű elem (azaz ha $12 \mid (p^n - 1)$), akkor pontosan $\varphi(12) = 4$ darab van, és ezek $f(x)$ gyökei, vagyis a felbontási test $\mathbb{F}_{p^n}$, ahol n a minimális olyan kitevő, amelyre $12 \mid (p^n - 1)$. Ha $p \equiv 1 \pmod{12}$, akkor a felbontási test elsőfokú, a többi esetben pedig másodfokú, mert $12 \mid (p-1)(p+1)$ igaz, ha $p \neq 2, 3$ prím. Végül $\mathbb{F}_2$ fölött $x^4 - x^2 + 1 = (x^2 + x + 1)^2$ irreducibilisekre bontás, $\mathbb{F}_3$ fölött pedig $x^4 - x^2 + 1 = x^4 + 2x^2 + 1 = (x^2+1)^2$, tehát ezekben az esetekben is másodfokú a bővítés.

6. *Igaz-e, hogy egy $K = \mathbb{F}_p(\alpha)$ ($\alpha \notin \mathbb{F}_p$) testben α szükségképpen generátoreleme a K multiplikatív csoportjának?*

Megoldás: Nem igaz: például $\mathbb{F}_9^\times \cong C_8$-ban egy 4-edrendű α elemre $\alpha \notin \mathbb{F}_3$, tehát $\mathbb{F}_3(\alpha) = \mathbb{F}_9$, de α nem generálja a 8-adrendű ciklikus csoportot.

7. *Bizonyítsuk be, hogy tökéletes test minden véges bővítése is tökéletes.*

Megoldás: Tegyük fel, hogy K tökéletes, azaz K fölött minden irreducibilis polinom szeparábilis, és legyen az $L|K$ bővítés véges. Legyen továbbá $f(x) \in L[x]$ irreducibilis, és α az f egyik gyöke f felbontási testében, F-ben. Ha $g(x)$ az α minimálpolinomja K fölött, akkor $f(x)$ osztója $g(x)$-nek $F[x]$-ben, és ott $g(x)$ minden gyöke egyszeres, így $f(x)$ gyökei is egyszeresek.

8. *a) Tegyük fel, hogy α és β algebrai elemek K fölött, és a minimálpolinomjuk gyökei $\alpha = \alpha_1, \dots, \alpha_n$, illetve $\beta = \beta_1, \dots, \beta_m$ mind különbözők. Legyen továbbá $c, d \in K \setminus \{0\}$ olyan, hogy $(i,j) \neq (1,1)$ esetén $c\alpha + d\beta \neq c\alpha_i + d\beta_j$. Lássuk be a szeparábilis bővítés egyszerűségéről szóló tétel bizonyítása alapján, hogy $K(c\alpha + d\beta) = K(\alpha, \beta)$.*

b) Alkalmazzuk az a) részben bizonyított tételt $(\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q})$, illetve $(\mathbb{Q}(\sqrt[3]{2} + \sqrt{2}) : \mathbb{Q})$ kiszámítására.

Megoldás: a) Legyen $f(x), g(x) \in K[x]$ az α, illetve β minimálpolinomja, és $\gamma = c\alpha + d\beta$. Ekkor $g(x), f(\frac{1}{d}\gamma - \frac{c}{d}x) \in K(\gamma)[x]$ is lineáris faktorokra bomlanak az $f(x)g(x)$ felbontási testében, F-ben. Mivel egyik polinomnak sincs többszörös gyöke, és a feltétel miatt egyetlen közös gyökük M-ben a β, a $g(x)$ és $f(\frac{1}{d}\gamma - \frac{c}{d}x)$ legnagyobb közös osztója $F[x]$-ben $x - \beta$, s mivel az euklideszi algoritmus végig $K(\gamma)[x]$-ben marad, ott is ugyanez. Ebből következik, hogy $\beta \in K(\gamma)$.

b) A $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ esetében azt kell ellenőrizni, hogy a $\pm\sqrt{2}$ és $\pm\sqrt{3}$ páronkénti összegei közül csak egy egyenlő $\sqrt{2} + \sqrt{3}$-mal, és ez nyilvánvalóan igaz. A $\mathbb{Q}(\sqrt[3]{2} + \sqrt{2})$ esetében pedig az $\varepsilon^k \sqrt[3]{2}$ ($k = 0, 1, 2$, ε primitív harmadik egységgyök) és $\pm\sqrt{2}$ páronkénti összegeiről kell belátni ugyanezt. Nyilván elég csak azokat nézni, ahol az első és a második tag is különböző, tehát az $\varepsilon\sqrt[3]{2} - \sqrt{2}$ és $\varepsilon^2\sqrt[3]{2} - \sqrt{2}$ alakúakat, ezek pedig nem lehetnek $\sqrt[3]{2} + \sqrt{2}$-vel egyenlők, mert nem valósak.

9. *Adjuk meg az $\mathbb{F}_2(\alpha, \beta)$ bővítést egyszerű bővítésként, ahol α az $x^2 + x + 1$, β az $x^3 + x + 1$ polinom egy-egy gyöke.*

Megoldás: $\mathbb{F}_2(\alpha,\beta) = \mathbb{F}_{64}$, mert $(\mathbb{F}_2(\alpha,\beta) : \mathbb{F}_2)$ 2-vel és 3-mal is osztható, így legalább 6, másrészt $\mathbb{F}_{64}$-nek részteste $\mathbb{F}_4$ és $\mathbb{F}_8$ is, tehát itt x^2+x+1 és x^3+x+1 is lineáris faktorokra bomlik, következésképpen $\alpha,\beta \in \mathbb{F}_{64}$. Mivel α a háromelemű $\mathbb{F}_4^\times$ csoport nem triviális eleme, α rendje 3, és hasonlóan β a hételemű $\mathbb{F}_8^\times$ csoport nem triviális eleme, így β rendje 7. A kommutatív $\mathbb{F}_{64}^\times$ csoportban két relatív prím rendű elem szorzatának rendje a rendek szorzata, tehát $\alpha\beta$ rendje 21. Ez azt jelenti, hogy $\alpha\beta$ nem lehet benne $\mathbb{F}_{64}$ semelyik valódi résztestében, mert azok 21-nél kisebb elemszámúak, így $\mathbb{F}_2(\alpha,\beta) = \mathbb{F}_2(\alpha\beta)$.

Hf1. *Adjuk meg x^4-2 felbontási testét $\mathbb{Q}$ egyszerű bővítéseként!*

Hf2. *Bizonyítsuk be, hogy $\mathbb{Q}(\cos 40^\circ)$ normális bővítése $\mathbb{Q}$-nak!*