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 legföljebb 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.

2. *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.

3. *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.

4. *Adjuk meg a következő bővítéseket egyszerű bővítésként:*
a) x^4-2 felbontási teste $\mathbb{Q}$ fölött;
b) $\mathbb{F}_2(\alpha,\beta)$, ahol α az x^2+x+1, β az x^3+x+1 polinom egy-egy gyöke.

Megoldás: b) $\mathbb{F}_2(\alpha,\beta)=\mathbb{F}_{64}$, 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 $\mathbb{F}_2(\alpha,\beta)=\mathbb{F}_2(\alpha\beta)$.

5. *Hányadfokú az x^6+3 polinom felbontási teste $\mathbb{Q}$ fölött?*

Megoldás: Ha x^6+3 egyik gyöke α, akkor a többi gyök $\alpha\varepsilon^k$, ahol $\varepsilon = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ primitív hatodik egységgyök, és $k = 0, 1, \ldots, 5$. Ebből látszik, hogy x^6+3 felbontási teste $\mathbb{Q}(\alpha, \varepsilon)$ (ε-t megkapjuk két gyök hányadosaként). Viszont $\alpha^3 = i\sqrt{3}$ vagy $-i\sqrt{3}$, tehát $\varepsilon \in \mathbb{Q}(\alpha)$. Így a felbontási test $\mathbb{Q}(\alpha)$, amelynek foka $\mathbb{Q}$ fölött 6, mivel x^6+3 irreducibilis a Schönemann–Eisenstein-kritérium miatt.

6. *a) Bizonyítsuk be, hogy $\mathbb{R}$ automorfizmuscsoportja egyelemű. (Útmutatás: Lássuk be, hogy $\mathbb{R}$ minden automorfizmusa rendezéstartó.)*

b) Hány automorfizmusa van $\mathbb{Q}(\sqrt[3]{2})$-nek? (Miért nem mond ez ellent a Galois-elmélet főtételének?)

c) Mutassunk példát olyan véges normális (de nem szeparábilis!) bővítésre, melynél a relatív automorfizmusok csoportja 1-elemű.

Megoldás: a) $\mathbb{R}$-ben egy elem pontosan akkor pozitív, ha nem 0, és $\mathbb{R}$-ben van négyzetgyöke. Ezt a tulajdonságot megtartja $\mathbb{R}$ minden automorfizmusa, tehát pozitív számokat pozitívakba, negatívakat negatívakba visznek az $\mathbb{R}$ automorfizmusai. Ebből az is következik, hogy az automorfizmus rendezéstartó, mivel $a < b$ akkor és csak akkor igaz, ha $b - a > 0$. $\mathbb{Q}$ elemeit az automorfizmusok helyben hagyják ($1 \mapsto 1$, $-1 \mapsto -1$, $n \mapsto n$ $\forall n \in \mathbb{Z}$, $\frac{1}{n} \mapsto \frac{1}{n}$ és végül $\frac{m}{n} \mapsto \frac{m}{n}$). Ezután tetszőleges $\alpha \in \mathbb{R}$-re $\alpha = \sup\{ r \in \mathbb{Q} \mid r \leq \alpha \}$, tehát α képe a $\mathbb{Q}$ ugyanazon részhalmazának szuprémuma $\mathbb{R}$-ben, azaz α is önmagába képződik.

b) $\sqrt[3]{2}$ csak önmagába képződhet, mert az x^3-2-nek csak egy gyöke van ebben a testben (a másik kettő nem valós). Mivel $\mathbb{Q}$ elemeit szükségképpen helyben hagyják az automorfizmusok, így a racionálisak és $\sqrt[3]{2}$ segítségével kifejezhető összes elem is helyben marad, vagyis $\mathbb{Q}(\sqrt[3]{2})$-nek csak a triviális automorfizmusa van. Bár $(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = 3$, a relatív automorfizmusok csoportjának nem kell 3 eleműnek lennie, mert a $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ bővítés nem normális.

c) Legyen $\operatorname{char} K = p$, és $K(t)$ a K egy egyszerű transzcendens bővítése. A 2. feladatsor 11. feladatában láttuk, hogy az $x^p - t$ egy gyökével való bővítés normális, de nem szeparábilis, és itt $x^p - t$-nek csak egy (p-szeres) gyöke van, tehát a bővítés tetszőleges relatív automorfizmusa ezt a gyököt, és így a bővítés minden elemét is helyben hagyja.

7. *Bizonyítsuk be, hogy $\mathbb{R}$ nem áll elő egy valódi résztestének véges fokú normális bővítéseként.*

Megoldás: Egy ilyen bővítés Galois-csoportjának az elemszáma a bővítés fokával lenne egyenlő, tehát akkor $\mathbb{R}$-nek lenne nem triviális automorfizmusa, ami ellentmond a 6. a) feladat állításának.

8. *Határozzuk meg a $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \mid \mathbb{Q}$ bővítés Galois-csoportját.*

Megoldás: Az 1. feladatsor 5. d) feladatában láttuk, hogy $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, és a bővítés foka 4. Mivel $L|\mathbb{Q}$ Galois-bővítés (L az $(x^2-2)(x^2-3)$ polinom felbontási teste), a Galois-csoportja, G is 4 elemű, tehát vagy $C_2 \times C_2$-vel, vagy C_4-gyel izomorf. $\mathbb{Q}$ és L között legalább két közbülső test van: $\mathbb{Q}(\sqrt{2})$ és $\mathbb{Q}(\sqrt{3})$, tehát G-nek is van legalább két valódi részcsoportja. Ezért G nem lehet C_4-gyel izomorf, csak $C_2 \times C_2$-vel.

9. *Határozzuk meg a következő polinomok Galois-csoportját $\mathbb{Q}$ fölött és $\mathbb{F}_3$ fölött*

a) $x^4 - 3x^2 + 4$ *b)* $x^3 - 2$ *c)* $x^3 + 2x^2 + 2$

Megoldás: a) $x^4-3x^2+4=(x^2+2)^2-7x^2=(x^2-\sqrt{7}x+2)(x^2+\sqrt{7}x+2)$ a polinomnak az $\mathbb{R}$ fölötti irreducibilis tényezőkre bontása (tovább már nem bontható, mert a másodfokú polinomok gyökei nem valósak). Ez a felbontás a $\mathbb{Q}$ fölötti felbontás finomítása kell, hogy legyen, de a tényezők nem $\mathbb{Q}[x]$-beliek, tehát a negyedfokú polinom irreducibilis $\mathbb{Q}[x]$-ben, következésképpen a felbontási teste legalább 4-edfokú. A polinom gyökei a fönti felbontás alapján $\pm\frac{\sqrt{7}}{2}\pm\frac{1}{2}i$, így a felbontási teste, $F\leq\mathbb{Q}(\sqrt{7},i)$, és az utóbbi is negyedfokú $\mathbb{Q}$ fölött, tehát $F=\mathbb{Q}(\sqrt{7},i)$. Innentől kezdve a 8. feladat bizonyítását alkalmazhatjuk erre az esetre is, és azt kapjuk, hogy a Galois-csoport $C_2\times C_2$-vel izomorf.
$\mathbb{F}_3$ fölött $x^4-3x^2+4=x^4-2x^2+1-x^2=(x^2-1)^2-x^2=(x^2-x-1)(x^2+x-1)$, és ezek a másodfokú polinomok már irreducibilisek, a polinom felbontási teste pedig $\mathbb{F}_9$ (minden $\mathbb{F}_3$ fölött irreducibilis másodfokú polinom lineáris faktorokra bomlik $\mathbb{F}_9$ fölött). Mivel $(\mathbb{F}_9:\mathbb{F}_3)=2$, a polinom Galois-csoportja kételemű, így C_2-vel izomorf.

b) x^3-2 felbontási teste $F=\mathbb{Q}(\sqrt[3]{2},\varepsilon)$, ahol ε harmadfokú primitív egységgyök, és a $\mathbb{Q}\leq\mathbb{Q}(\sqrt[3]{2})\leq F$ bővítéssorozat 3-ad- és 2-odfokú bővítések egymásutánja, tehát x^3-2 Galois-csoportja 6 elemű. Másrészt a Galois-csoport elemei leírhatók az x^3-2 polinom gyökein megadott permutációhatásukkal, ezért a Galois-csoport beágyazható S_3-ba, és a mérete miatt ekkor izomorf S_3-mal.
$\mathbb{F}_3$ fölött $x^3-2=x^3+1=(x+1)^3$, tehát a Galois-csoport 1.

c) Az $f(x)=x^3+2x^2+2$ irreducibilis polinomra $f'(x)=3x^2+4x$ gyökei $-\frac{4}{3}$ és 0, és mindkét helyen pozitív az f értéke, tehát f-nek egyetlen valós gyöke van, és két nem valós. Így Galois-csoportja a 10. feladat szerint S_3-mal izomorf.
$\mathbb{F}_3$ fölött $x^3+2x^2+2=(x+1)(x^2+x-1)$, és x^2+x-1 irreducibilis, így az a) részhez hasonlóan 2-odfokú a felbontási teste, és a Galois-csoportja C_2-vel izomorf.

10. *Bizonyítsuk be, hogy ha egy harmadfokú, racionális együtthatós, irreducibilis polinomnak nem mindegyik gyöke valós, akkor a Galois-csoportja S_3-mal izomorf.*

Megoldás: A két nem valós gyök szükségképpen egymás konjugáltja, tehát a komplex konjugálás, ami $\mathbb{C}$-nek automorfizmusa a polinom gyökeit nem triviális módon permutálja. Ebből következik, hogy ez az automorfizmus helyben hagyja a polinom felbontási testét, és másodrendű automorfizmusként hat rajta, ezért a Galois-csoport rendje osztható 2-vel. Másrészt a bővítés foka osztható 3-mal, tehát a Galois-csoport rendje is osztható vele. Így a Galois-csoport legalább 6-odrendű, és a gyökökön való hatása által az S_3-ba ágyazható, ezért izomorf S_3-mal.

Hf1. *Bizonyítsuk be, hogy egy nem 2 karakterisztikájú K test minden másodfokú bővítése megkapható $K(\sqrt{d})$ alakban, valamely $d\in K$-val!*

Hf2. *Ha egy testnek van egy 8 elemű és egy 16 elemű részteste, akkor hány elemű ezeknek a metszete, illetve az általuk generált résztest?*

Hf3. *Tegyük fel, hogy egy α algebrai szám minimálpolinomja $\mathbb{Q}$ fölött x^3-2x+2. Hányadfokú $\mathbb{Q}$-nak az α^2-tel való bővítése? Adjuk meg α^2 minimálpolinomját $\mathbb{Q}$ fölött!*