1. *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.

2. *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 az 1. a) feladat állításának.

3. *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.

4. *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.

5. *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.

6. *Keressük meg az $f(x) = x^8 - 1$ polinom felbontási testének résztesteit!*

Megoldás: Az $x^8 - 1$ felbontási teste $\mathbb{Q}$ fölött $\mathbb{Q}(\varepsilon)$, ahol $\varepsilon = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$ 8-adik primitív egységgyök. Mivel $\varphi(8) = 4$, ez 4-edfokú bővítés, tehát a G Galois-csoport 4-edrendű. A bővítés felírható $\varepsilon + \varepsilon^3 = \sqrt{2}$-vel és $\varepsilon^2 = i$-vel való bővítésként is, amelyben $\mathbb{Q}(\sqrt{2})$ és $\mathbb{Q}(i)$ is másodfokú a $\mathbb{Q}$ fölött, tehát G-ben van legalább két 2 indexű, így másodrendű részcsoport, ezért $G \cong C_2 \times C_2$. Ebben összesen három valódi részcsoport van, tehát csak egy közbülső testet kell még találni, és ez $\mathbb{Q}(i\sqrt{2})$.

7. *Bizonyítsuk be, hogy az $x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinom Galois-csoportja S_5-tel izomorf. (Útmutatás: Lássuk be, hogy a polinomnak pontosan 3 valós gyöke van, így van a Galois-csoportnak olyan eleme, ami transzpozícióként hat a polinom gyökein.)*

Megoldás: Az $f(x) = x^5 - 4x + 2$ polinom irreducibilis a Schönemann–Eisenstein-kritérium miatt, és függvényvizsgálattal megállapíthatjuk, hogy pontosan 3 valós gyöke van, így a maradék kettő egymás konjugáltja. A felbontási test foka osztható 5-tel, így a G Galois csoport rendje is 5-tel osztható, ezért van benne ötödrendű elem. A G csoportot úgy tekinthetjük, mint S_5 részcsoportját, és ebben egy ötödrendű elem csak egy 5-ciklus lehet.

Továbbá a komplex konjugálás mint $\mathbb{C}$ egy automorfizmusa egymás között permutálja $f(x)$ gyökeit, tehát önmagába viszi a felbontási testet is, ezért a felbontási testre való megszorítása G-nek olyan eleme, ami a gyökökön egy 2-ciklus. Egy 5-ciklus és egy 2-ciklus pedig mindenképpen kigenerálja az egész S_5-öt.

Hf1. *Adjuk meg az* $x^3 - 2$ *polinom* $\mathbb{Q}$ *fölötti felbontási testének összes résztestét!*

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