1. *Legyen $L = \mathbb{Q}(\sqrt[4]{2}, i)$, és $G = \mathrm{Gal}(L|\mathbb{Q})$. Legyen g elemei közül f az a "forgatás", amelyre $\sqrt[4]{2}f = i\sqrt[4]{2}$ és $if = i$, és t az a "tükrözés", amelyre $\sqrt[4]{2}t = \sqrt[4]{2}$ és $it = -i$. Határozzuk meg H^*-ot $H = \langle f \rangle$-re, és M^*-ot $M = \mathbb{Q}(i\sqrt{2})$-re.*

Megoldás: $(L : \mathbb{Q}) = (\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}) \cdot (L : \mathbb{Q}(\sqrt[4]{2})) = 4 \cdot 2 = 8$, mert $\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}$ fölött $x^4 - 2$, és ezután az i hozzáadása egy másodfokú bővítés, mivel $i \notin \mathbb{R} \geq \mathbb{Q}(\sqrt[4]{2})$. Tetszőleges $g \in G$ testautomorfizmusra $\sqrt[4]{2}g \in \{ \pm\sqrt[4]{2}, \pm i\sqrt[4]{2} \}$, míg $ig \in \{ \pm i \}$, és az összes lehetőség előfordul a 8-elemű Galois-csoportban (amelyről könnyen látható, hogy D_4-gyel izomorf, például mert beágyazható S_4-be). Tehát a G Galois-csoportban valóban léteznek a megadott f és t automorfizmusok.

$|G : H| = 2$ miatt $(H^* : K) = (H^* : G^*) = 2$, tehát H^* meghatározásához elég egy K fölött másodfokú elemet találni, amelyet H helyben hagy. f megadásából láthatjuk, hogy $if = i$, tehát $H^* = \mathbb{Q}(i)$.

$(M : \mathbb{Q}) = 2$ miatt $|G : M^*| = |\mathbb{Q}^* : M^*| = 2$, azaz $|M^*| = 4$. Mivel $(i\sqrt{2})f = -i\sqrt{2}$, és $(i\sqrt{2})t = -i\sqrt{2}$, nyilván ft és f^2 is helyben hagyja M-et, és ezek együtt már egy $C_2 \times C_2$-vel izomorf negyedrendű részcsoportot generálnak. Így $M^* = \langle ft, f^2 \rangle = \{ 1, ft, f^2, f^3t \}$.

2. *Keressünk olyan $p(x) \in \mathbb{Q}[x]$ polinomokat, melyeknek a Galois-csoportjai rendre:*
a) C_3; *b) C_2^n;* *c) S_3.*

Megoldás: a) Mint láttuk a 2/Hf2. feladat megoldásánál, a $\mathbb{Q}$-nak $\cos 40°$-kal való bővítése normális, tehát minimálpolinomjának, $8x^3 - 6x + 1$-nek a felbontási teste $\mathbb{Q}$ fölött 3-adfokú, és így a Galois-csoportja csak C_3 lehet.

b) Legyenek $p_1, p_2, \ldots, p_n$ különböző pozitív prímek. Belátjuk, hogy ekkor a $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ bővítés Galois-csoportja (azaz az $(x^2 - p_1) \cdots (x^2 - p_n)$ polinom Galois-csoportja), G izomorf C_2^n-nel. Egyszerű számolás mutatja, hogy ha $u, v, uv \in \mathbb{N}$ nem négyzetszámok, akkor $\sqrt{u} \notin \mathbb{Q}(\sqrt{v})$, tehát K-ban van $2^n - 1$ olyan közbülső test, amelyek mindegyike másodfokú $\mathbb{Q}$ fölött ($\{ p_1, \ldots, p_n \}$ bármelyik nem üres részhalmazában levő számok szorzatának a négyzetgyökével való bővítés). Ez azt jelenti, hogy a G Galois-csoportnak van legalább $2^n - 1$ különböző 2 indexű normálosztója: N_i $(i = 1, \ldots, 2^n - 1)$. Legyen N ezen normálosztók metszete. G/N-ben minden elem négyzete 1, ugyanis minden N_i-ben benne van a négyzetük. Ebből következik, hogy G/N Abel-csoport, sőt C_2^k alakú. C_2^k — additív írásmódra áttérve — egy k dimenziós vektortér $\mathbb{F}_2$ fölött, és ebben a $k - 1$ dimenziós alterek száma megegyezik a nem triviális k-változós lineáris egyenletek számával, $2^k - 1$-gyel. Tehát G/N-ben, és így G-ben is $2^k - 1$ darab 2 indexű részcsoport van, ezért $k \geq n$, amiből $|G/N| \geq 2^n$ következik. Másrészt $(K : \mathbb{Q}) \leq 2^n$ miatt $|G| \leq 2^n$, tehát $N = 1$, és $G \cong C_2^n$.

c) $x^3 - 2$ Galois-csoportja S_3-mal izomorf, ahogy láttuk a 3/9.b) feladat megoldásában.

3. *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.

4. *Bizonyítsuk be, hogy ha az $L|K$ Galois-bővítés páros fokú, akkor L megkapható egy résztestének egy elem négyzetgyökével való bővítéseként.*

Megoldás: Ha G a bővítés Galois-csoportja, akkor $|G| = (L : K)$ páros, így G-nek van másodrendű eleme, tehát másodrendű részcsoportja is. Legyen ez H. Ekkor $K \leq H^* \leq L$ úgy, hogy $(L : H^*) = 2$, azt pedig korábban láttuk, hogy egy másodfokú bővítés mindig megadható egy elem négyzetgyökével való bővítésként.

5. *Ha egy racionális együtthatós polinom Galois-csoportja a kvaterniócsoporttal izomorf, akkor legalább hányadfokú a polinom?*

Megoldás: Ha a polinom n-edfokú, akkor G felfogható S_n részcsoportjaként (a polinom gyökein ható permutációcsoportként), tehát csak olyan n jöhet szóba, amelyre S_n-nek van Q-val izomorf részcsoportja. $n < 4$ esetén $|S_n|$ nem is osztható 8-cal. $n = 4, 5$ esetén egy 8-adrendű részcsoport S_n-nek Sylow-részcsoportja, tehát az összes ilyen izomorf egymással, viszont tudjuk, hogy S_4-ben (és így S_5-ben is) benne van a D_4 diédercsoport, tehát a 2-Sylow nem izomorf Q-val. S_6 2-Sylow-részcsoportjai $D_4 \times C_2$-vel izomorfak (ugyanis egy Sylowot megkaphatunk úgy, hogy vesszük az $\{1, 2, 3, 4\}$ halmazon ható szimmetrikus csoport 2-Sylow-részcsoportját, és a vele felcserélhető $\langle(56)\rangle$ részcsoporttal megszorozzuk). Ha lenne S_6-ban Q-val izomorf részcsoport, az beágyazható lenne egy 2-Sylowba, de $D_4 \times C_2$-be biztosan nem lehet beágyazható, mert abban minden negyedrendű elem felcserélhető egymással. S_7-ben ugyanígy nem lehet Q-val izomorf részcsoport. S_8-ba viszont már beágyazható a Cayley-reprezentációval (Q saját magán hat a jobbról való szorzással). Tehát a keresett polinom foka legalább 8. (Ilyen polinom egyébként létezik is, de ezt itt nem bizonyítjuk.)

6. *Melyik n egészekre szerkeszthető n fokos szög?*

Megoldás: $\frac{2\pi}{n}$ akkor és csak akkor szerkeszthető, ha az n-edik primitív egységgyökkel való bővítés foka 2-hatvány, azaz ha $n = p_1 \cdots p_r \cdot 2^k$, ahol $p_1, \ldots, p_r$ különböző Fermat-prímek, és $k \geq 0$ tetszőleges. Az is nyilvánvaló, hogy $2\pi \cdot \frac{k}{n}$ (ahol $(k, n) = 1$) akkor és csak akkor szerkeszthető, ha $\frac{2\pi}{n}$ szerkeszthető. Fokokban kifejezve: ahhoz, hogy egy n fokos szög szerkeszthető legyen, az kell, hogy $\frac{n}{360} \cdot 2\pi$ szerkeszthető legyen, vagyis hogy n 3-mal osztható szám legyen.

7. *Megszerkeszthető-e egy tetszőlegesen megadott szög ötödrésze?*

Megoldás: Felhasználva, hogy $\cos 5\alpha = 16\cos^5\alpha - 20\cos^3\alpha + 5\cos\alpha$, egy c koszinuszú szög ötödrészének koszinusza kielégíti a $16x^5 - 20x^3 + 5x - c = 0$ egyenletet. Ha például az adott szög koszinusza $\frac{5}{6}$, akkor az ötödének a minimálpolinomja $96x^5 - 120x^3 + 30x - 5$, amely kielégíti a Schönemann–Eisenstein-kritériumot $p = 5$-tel, tehát irreducibilis. Ez azt jelenti, hogy például az $\arccos\frac{5}{6}$ szög ötödét nem lehet megszerkeszteni, mert az ehhez tartozó bővítés 5-ödfokú.

Másképpen: ha lehetne szöget ötödölni, akkor nemcsak szabályos ötszöget, hanem szabályos huszonötszöget is tudnánk szerkeszteni, pedig tudjuk, hogy csak olyan szabályos n-szög szerkeszthető, amelyre $\varphi(n)$ 2-hatvány.

8. *Határozzuk meg* $\cos(2\pi/n)$ *fokát* $\mathbb{Q}$ *fölött.*

Megoldás: Legyen $\alpha = \cos(2\pi/n)$, és $\varepsilon = \cos(2\pi/n) + i\sin(2\pi/n)$. Ekkor tudjuk, hogy $(\mathbb{Q}(\varepsilon) : \mathbb{Q}) = \varphi(n)$, és $\alpha = \varepsilon + (1/\varepsilon)$, tehát $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\varepsilon)$. Viszont ε kifejezhető, mint $\alpha + \sqrt{\alpha^2 - 1}$, tehát $(\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)) \leq 2$, és nem lehet 1, minthogy $\mathbb{Q}(\alpha) \leq \mathbb{R}$, de $\varepsilon \notin \mathbb{R}$, ha $n \geq 3$. Következésképpen α foka $\mathbb{Q}$ fölött $\varphi(n)/2$, ha $n \geq 3$, és $n = 1, 2$-re nyilván 1.

9. *Egy egységnyi hosszúságú szakasz két végpontjából kiindulva megszerkeszthető-e az* 1 *térfogatú, szabályos tetraéder élhossza?*

Megoldás: Könnyen kiszámítható, hogy egy a élhosszúságú szabályos tetraéder térfogata $\frac{\sqrt{2}}{12}a^3$, tehát az 1 térfogatú tetraéder a élhosszára $a = \sqrt{2}\sqrt[3]{3}$. Ez azt jelenti, hogy az a-val való bővítésben benne van $a^3/6 = \sqrt{2}$, és így $\sqrt[3]{3}$ is, pedig az utóbbinak a foka $\mathbb{Q}$ fölött 3, így nem lehet megszerkeszteni ennek a tetraédernek az élhosszát.

Hf1. *Adjuk meg* $x^8 - x^4 - 2$ *felbontási testét* $\mathbb{Q}$ *egyszerű bővítéseként!*

Hf2. *Legyen* $f(x) = g(x^k) \in \mathbb{Q}[x]$, *ahol* $\deg g = t$ *és* $k > 1$. *Bizonyítsuk be, hogy* $|\mathrm{Gal}(f)| \leq (k-1) \cdot t! \cdot k^t$.

Hf3. *Határozzuk meg az* $f(x) = x^4 + x^2 + 1$ *polinom Galois-csoportját* $\mathbb{Q}$ *fölött.*