1. *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 3/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 4/4.b) feladat megoldásában.

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

Megoldás: Az állítás akkor igaz, ha $\operatorname{char} K \neq 2$ (pl. $\mathbb{F}_2$-nek az $x^2 + x + 1$ polinom gyökével való bővítése másodfokú, de nem lehet négyzetgyökkel való bővítésként megkapni). Tegyük fel tehát, hogy $\operatorname{char} K \neq 2$.

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 $(L : H^*) = 2$, egy másodfokú bővítés pedig a megoldóképlet miatt (amelyben osztani csak 2-vel kell, tehát lehet is K-ban) mindig megadható a diszkrimináns négyzetgyökével való bővítésként.

3. *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 $D_4 \times C_2$-ben összesen négy negyedrendű elem

van, Q-ban viszont van hat is. 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.)

4. *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.

5. *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.

6. *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 $2\alpha = \varepsilon + (1/\varepsilon)$, 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.

7. *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.

8. *Megszerkeszthető-e egy egyenlőszárú háromszög, ha adott a szára és a beírt kör sugara?*

Megoldás: Legyen a beírt kör sugara 1, a háromszög szára a, és az ismeretlen alap x. Ekkor a területet kétféleképpen felírva azt kapjuk, hogy

$$\frac{2a + x}{2} = \frac{1}{2}x\sqrt{a^2 - \frac{x^2}{4}},$$

azaz $2(2a + x) = x\sqrt{4a^2 - x^2}$. Egyszerűsíthetünk a pozitív $\sqrt{2a + x}$-szel: $2\sqrt{2a + x} = x\sqrt{2a - x}$, és ebből négyzetre emelés és rendezés után: $x^3 - 2ax^2 + 4x + 8a$. Keressünk

olyan a-t, amelyre ez irreducibilis, de azért van 0 és $2a$ közötti valós gyöke! Például $a = 4$-re $f(x) = x^3 - 8x^2 + 4x + 32$-nek van gyöke 6 és 7 között, és a racionális gyöktesztel ellenőrizhetjük, hogy f-nek nincs racionális gyöke, így ez a harmadfokú polinom irreducibilis. Tehát a polinom gyökével való bővítés 3-adfokú, és így a háromszöget nem lehet megszerkeszteni.

9. *Tudjuk, hogy* $\mathbb{Q}(\cos 40°)$ *Galois-csoportja* 3*-elemű. Van-e olyan racionális szám, amelynek a köbgyökével való bővítés ugyanezt a testet adja?*

Megoldás: Nincs, ugyanis egy szám köbgyökével való bővítés vagy első, vagy harmadfokú, és az utóbbi esetben a minimálpolinomjának nem valós gyökei is vannak, tehát a felbontási test foka, és így a Galois-csoport rendje is 6.

10. *Bizonyítsuk be, hogy ha egy* $f(x) \in \mathbb{Q}[x]$ *irreducibilis polinom Galois-csoportja kommutatív, akkor a Galois-csoport rendje* $\deg f$*.*

Megoldás: Abel-csoport minden részcsoportja normálosztó, így a felbontási test minden közbülső teste normális bővítése $\mathbb{Q}$-nak. Ez azt jelenti, hogy a polinom egyetlen gyökével való bővítés (amely $\deg f$ fokú) már a teljes felbontási testet adja, az utóbbinak a foka pedig megegyezik a Galois-csoport rendjével.

11. *Az alábbiak közül melyik polinomok gyökeit lehet az alapműveletek és gyökvonás segítségével felírni?*

a) $x^4 + 2x^3 - 5x + 1$
b) $x^5 - 15x^4 + 6$
c) $x^6 - 2x^2 + 4$

Megoldás: Az a) és c) polinomét igen, a b)-ét nem.

a) A polinom Galois-csoportja permutációcsoportként hat a négy gyökön, tehát részcsoportja a feloldható S_4 csoportnak, és ezért maga is feloldható.

b) $f(x)$ irreducibilis (teljesíti a Schönemann–Eisenstein kritériumot $p = 3$-mal), és így minden gyöke különböző. Továbbá $f'(x) = 5x^4 - 60x^3 = 5x^3(x-12)$ 0-nál és 12-nél vált előjelet, $\lim_{x\to-\infty} f(x) = -\infty$, $f(0) = 6 > 0$, $f(12) = -3 \cdot 12^4 + 6 < 0$, és $\lim_{x\to\infty} f(x) = \infty$, tehát $f(x)$-nek pontosan három valós gyöke van. Ebből következik, hogy a Galois-csoport S_5-nek részcsoportja, és a komplex konjugálás mint transzpozíció benne van, továbbá 5-tel osztható a rendje, így egy 5-ciklus is van benne. Ezek együtt az egész S_5-öt kigenerálják, amely nem feloldható csoport.

c) A polinom gyökeit megkaphatjuk úgy, hogy először az $x^3 - 2x + 4$ harmadfokú polinom gyökeivel bővítünk; ez nyilván feloldható Galois-csoportot ad, majd mindegyik gyöknek a négyzetgyökével is. Az első bővítés normális, tehát a Galois-csoportban feloldható faktorú normálosztó tartozik hozzá. A négyzetgyökökkel való bővítés foka pedig 2-hatvány, így az előbbi normálosztó 2-hatvány elemszámú, tehát az is feloldható, és emiatt a teljes Galois-csoport is az. Másképpen: a Cardano-képlettel felírhatjuk a harmadfokú polinom gyökeit, és ezeknek a négyzetgyökei az eredeti polinom gyökei.

Hf1. *Hány elem áll elő négyzetszámként, illetve köbszámként* $\mathbb{F}_{27}$*-ben? Adjunk meg egy olyan irreducibilis polinomot* $\mathbb{F}_3$ *fölött, amelynek minden gyöke négyzetszám* $\mathbb{F}_{27} \setminus \mathbb{F}_3$*-ban!*

Hf2. *Határozzuk meg a* $\mathrm{Gal}(L|K)$ *Galois-csoportot, ahol* $K = \mathbb{Q}(i\sqrt{3})$ *és* $L = K(\sqrt[6]{7})$*.*