**1.** *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 gyökteszttel 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.

**2.** *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.

**3.** *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.

**4.** *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.

**5.** *Legyen $L|K$ egy Galois-bővítés, $M$ és $N$ pedig olyan közbülső testek, amelyekre az $M|K$ és $N|K$ bővítések normálisak, továbbá legyen $S$ az $L$-nek az $M$ és $N$ által generált részteste. Bizonyítsuk be, hogy ha* $\mathrm{Gal}(M|K)$ *és* $\mathrm{Gal}(N|K)$ *feloldható, akkor* $\mathrm{Gal}(S|K)$ *is feloldható.*

*Megoldás:* Mivel $M|K$ és $N|K$ normális bővítések, a Galois-csoport $M^*$ és $N^*$ részcsoportjai normálosztók. A tartalmazást megfordító Galois-kapcsolatból következik, hogy $S^* = M^* \cap N^*$. Két normálosztó metszete is normálosztó, így az $M \cap N$ és $S$ bővítés is normális $K$ fölött. Továbbá $Gal(S|K) \cong K^*/S^* = G/(M^* \cap N^*)$, ha $G = Gal(L|K)$. Tudjuk, hogy $Gal(M|K) \cong G/M^*$ és $Gal(N|K) \cong G/N^*$ feloldható. Így $M^*/(M^* \cap N^*) \cong M^*N^*/N^* \le G/N^*$ feloldható, és $(G/(M^* \cap N^*))/(M^*/(M^* \cap N^*) \cong G/M^*$ is az, így $Gal(S|K) \cong G/(M^* \cap N^*)$ is feloldható.

**6.** *Legyen $H$ egy nem üres részhalmaza az $R$ gyűrűnek. Lássuk be, hogy a $H$ által generált jobbideál $\{\sum n_i h_i + h_i r_i \mid n_i \in \mathbb{Z},\ h_i \in H,\ r_i \in R\}$. Írjuk föl hasonló módon a $H$ által generált ideál elemeit is!*

*Megoldás:* Legyen $J = \{\sum n_i h_i + h_i r_i \mid n_i \in \mathbb{Z},\ h_i \in H,\ r_i \in R\}$. Ekkor $H \subseteq S$, és $S$ zárt az összeadásra és a gyűrűelemekkel való jobbszorzásra nézve: $(\sum n_i h_i + h_i r_i) + (\sum n_i' h_i + h_i r_i') = \sum (n_i + n_i')h_i + h_i(r_i + r_i')$, és $(\sum n_i h_i + h_i r_i)r' = \sum h_i(n_i r' + r_i r')$, tehát $J$ jobbideál. Végül minden $H$-t tartalmazó jobbideál tartalmazza az $n_i h_i$ és $h_i r_i$ alakú elemeket, és ezek összegét is, tehát $J$ benne van minden ilyen jobbideálban, és ezért $J$ a generált jobbideál. Ugyanígy lehet ellenőrizni, hogy a generált ideál

$$\left\{ \sum n_i h_i + h_i r_i + s_i h_i + s_i' h_i r_i' \mid n_i \in \mathbb{Z},\ h_i \in H,\ r_i, s_i, r_i', s_i' \in R \right\}$$

**7.** *Bizonyítsuk be, hogy az $R$ egységelemes gyűrű $a$ eleme által generált jobbideál az $aR$ komplexusszorzat. Miért nem igaz, hogy egy tetszőleges $H$ részhalmaz által generált jobbideál a $HR$ komplexusszorzat?*

*Megoldás:* Az $aR = \{ar \mid r \in R\}$ halmaz zárt az összeadásra és az $R$-beli elemekkel való jobbszorzásra nézve: $ar + as = a(r+s)$ és $(ar)r' = a(rr')$, és $1 \in R$ miatt $a = a \cdot 1 \in aR$, tehát $aR$ egy $a$-t tartalmazó jobbideál. Továbbá minden $a$-t tartalmazó jobbideál az $ar$ alakú elemeket is tartalmazza, így $aR$ az $a$ által generált jobbideál. Tetszőleges $HR$ komplexusszorzatban viszont megtörténhet, hogy $hr, h'r' \in HR$, de $hr + h'r'$ nem írható $h''r''$ alakban.

**8.** *Adjuk meg a $K[x,y]$ gyűrű (ahol $K$ kommutatív test) $x$ és $y^2$ által generált ideáljának elemeit. Adjuk meg a faktorgyűrűt az ideál mellékosztályainak egy alkalmas reprezentánsrendszerével. Mik az ideáljai a faktorgyűrűnek?*

*Megoldás:* A generált ideál az olyan $\sum\limits_{i,j} a_{i,j} x^i y^j$ polinomokból áll, amelyekben $a_{0,0} = a_{0,1} = 0$. Ugyanis minden olyan $x^i y^j$ benne van a generált ideálban, amelyre $i \ge 1$, vagy

$j \geq 2$, és így az ilyenek $K$-együtthatós kombinációi is, az ilyen polinomok pedig valóban ideált alkotnak (se az összeadás, se a $K$ elemével vagy $x$-szel vagy $y$-nal való szorzás nem visz ki ebből a részhalmazból). Az ideál egy mellékosztályában azok a polinomok vannak amelyeknek $a_{0,0}$ és $a_{0,1}$ együtthatójuk megegyezik, így reprezentánsrendszert alkotnak az $a + by$ alakú polinomok. Ha $a \neq 0$, akkor $(a + by)\frac{1}{a^2}(a - by) \equiv 1$ a faktorgyűrűben, tehát valódi ideálban csak $by$ alakú elemek lehetnek. Viszont ha $b \neq 0$, akkor $by$ kigenerálja az $(y)$ ideált, tehát a teljes faktorgyűrűn és a triviális ideálon kívül csak az $y$ generálta ideál van a faktorgyűrűben.

**9.** *Bizonyítsuk be, hogy ha egy gyűrűnek minden eleme idempotens, akkor a gyűrű kommutatív. Hány eleme lehet egy ilyen tulajdonságú véges gyűrűnek? Adjunk meg ilyen végtelen gyűrűt is!*

*Megoldás:* Tetszőleges $x \in R$-re $x+x = (x+x)^2 = x^2+x^2+x^2+x^2 = x+x+x+x$, amiből $x+x = 0$ minden $x$-re. $x, y \in R$-re $x+y = (x+y)^2 = x^2+xy+yx+y^2 = x+y+xy+yx$, így $xy + yx = 0$. Viszont $xy + xy = 0$ is igaz, ezért $xy = yx$.

Ha a gyűrű véges, akkor az additív csoportjában minden elem rendje 1 vagy 2, tehát a véges Abel-csoportok alaptétele szerinti felbontásban csupa másodrendű ciklikus szerepel. Így a gyűrű rendje 2-hatvány.

Ilyen tulajdonságú a $\mathbb{Z}_2$ akárhány (akár végtelen sok) példányban vett direkt összege.

**10.** *Legyen $K$ test. Bizonyítsuk be, hogy a $K$ fölötti $n \times n$-es fölső háromszögmátrixok gyűrűjében ideált alkotnak azok, amelyeknek átlójában csupa 0 áll. Mi az ehhez az ideálhoz tartozó faktorgyűrű? Keressük meg $n = 3$-ra az összes ideált.*

*Megoldás:* Legyen $R$ a fölső háromszögmátrixok gyűrűje, és ebben $I$ a szigorú fölső háromszögmátrixok részhalmaza (amelyeknek átlójában csupa 0 van). Könnyű ellenőrizni, hogy $I$ ideál $R$-ben. Az $I$ mellékosztályaiban azok a mátrixok vannak, amelyeknek az átlójában ugyanazok az elemek állnak. Reprezentánsrendszert adnak a diagonális mátrixok, sőt, ezek zártak is a gyűrűműveletekre nézve, így $R/I$ a diagonális mátrixok részgyűrűjével izomorf, ez viszont $K$ $n$ példányának direkt összege.

Az $R$ gyűrűt az olyan $E_{ij}$ mátrixok lineáris kombinációi alkotják, amelyekre $i \leq j$ (az $E_{ij}$ mátrix az, amelyiknek az $ij$ pozíciójában 1 van, a többiben 0). Ha $I$ ideál, és $A \in I$ mátrix, akkor $E_{ij}AE_{k\ell} \in I$ minden $i \leq j$ és $k \leq \ell$-re. $E_{ij}AE_{k\ell} \in I$ $i\ell$ pozíciójában $a_{jk}$ áll, mindenhol máshol 0, tehát ha $a_{jk} \neq 0$ (ez csak $j \leq k$ esetén lehet), akkor $E_{i\ell} \in I$ minden $i \leq j \leq k \leq \ell$-re (ugyanis még az $\frac{1}{a_{jk}}I$ mátrixszal is beszorozhatunk). Ezek pontosan a $jk$ pozíciótól kezdődő jobb felső téglalaphoz tartozó $E_{i\ell}$-ek, és ha az $A$ minden nem nulla eleméhez vesszük ezeket az $E_{i\ell}$ mátrixokat, akkor azok lineáris kombinációjaként az $A$ is előáll. Tehát $R$ ideáljait úgy kapjuk meg, ha kijelölünk néhány jobb felső téglalapot, és az azokhoz tartozó $E_{i\ell}$ mátrixok lineáris kombinációit vesszük (az ilyenek valóban ideált alkotnak). Ennek alapján a következő ideálokat kapjuk a $3 \times 3$-as fölső háromszögmátrixok gyűrűjében (a $*$ azt jelenti, hogy oda akármilyen $K$-elemet írhatunk):

$$\begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix} \quad \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix} \quad \begin{bmatrix} * & * & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix} \quad \begin{bmatrix} * & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix}$$

$$\begin{bmatrix} 0 & * & * \\ 0 & * & * \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} * & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix} \quad \begin{bmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

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

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