1. *Csoportot (esetleg félcsoportot) alkotnak-e*
a) $\mathbb{R}^3$ *elemei a vektoriális szorzásra nézve*
b) a valós 2×2*-es invertálható mátrixok az* $A * B := AB^T$ *műveletre nézve;*
az alábbi mátrixhalmazok a mátrixok szokásos összeadására vagy szorzására nézve?
c) az 1 *determinánsú* $n \times n$*-es valós mátrixok;*
d) a pozitív determinánsú $n \times n$*-es valós mátrixok;*
e) a $\mathbb{Z}$ *fölötti* $n \times n$*-es mátrixok;*
f) a $\mathbb{Z}$ *fölötti nem* 0 *determinánsú* $n \times n$*-es mátrixok;*
g) a $\mathbb{Z}$ *fölötti* 1 *determinánsú* $n \times n$*-es mátrixok;*
h) az $n \times n$*-es valós felső háromszögmátrixok.*

Megoldás: a) A vektoriális szorzás nem asszociatív (pl. $(\mathbf{i} \times \mathbf{i}) \times \mathbf{j} = \mathbf{0}$, de $\mathbf{i} \times (\mathbf{i} \times \mathbf{j}) = \mathbf{i} \times \mathbf{k} = -\mathbf{j}$), tehát még csak nem is félcsoport.

b) Ez sem asszociatív: $(A * B) * C = AB^TC^T$, de $A * (B * C) = ACB^T$, és ezek nem egyenlők pl. az $A = B = I$, és $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ mátrixokra.

Mivel $\mathbb{R}^{n \times n}$ gyűrű, a további példáknál az asszociativitást egyik műveletre sem kell ellenőrizni, csak azt, hogy az adott részhalmaz zárt a műveletre nézve, és van benne egységelem és inverz. Az egységelem elvileg lehetne egy a teljes gyűrű egységelemétől különböző elem is, de ha az eredeti egységelem benne van, akkor más egységeleme már nem lehet, és akkor az inverz is csak az eredeti inverz lehet.

c) Az összeadásra nem zárt, így nem is félcsoport, pl. $|I + I| = |2I| = 2^n \neq 1$, de a szorzásra nézve csoport: nem üres, I benne van, $|AB| = |A| \cdot |B|$ miatt zárt a szorzásra, és $|A^{-1}| = |A|^{-1}$ miatt az inverzre is.

d) Az összeadásra nem, pl. $n = 2$-re $|I| = |-I| = 1 > 0$, de $|I + (-I)| = |0| = 0$. A szorzásra viszont igen, ugyanazért, mint az előző.

e) Az összeadásra nézve csoportot alkotnak, mert egész elemű mátrixok összege is, negatívja is egész elemű, és a 0 mátrix is ilyen. A szorzásra is zárt, tehát az asszociativitás miatt félcsoport is, továbbá I az egységeleme, viszont nincs mindennek multiplikatív inverze (pl. $2I$ inverze nem egész elemű), tehát a szorzásra nézve nem alkotnak csoportot.

f) Az összeadásra nem zárt, ld. a d) ellenpéldáját. A szorzásra ugyan zárt, és így félcsoport, és I is benne van, de nincs minden elemének multiplikatív inverze a halmazban (pl. $2I$-nek nincs).

g) Az összeadásra nem zárt (ld. az c) rész ellenpéldáját), a szorzásra igen, benne van az I egységelem, és minden elemének van multiplikatív inverze, ugyanis az $A^{-1} = \frac{1}{|A|}\mathrm{adj}A$ formula itt egész együtthatós mátrixot ad, és persze $|A^{-1}| = |A|^{-1} = 1$ is teljesül. Tehát az összeadásra nem alkot félcsoportot sem, a szorzásra viszont csoportot alkot.

h) Az összeadásra csoportot alkot (sőt alterét alkotja az $\mathbb{R}^{n \times n}$ vektortérnek), de a szorzásra csak félcsoport: zárt ugyan a szorzásra, és az I egységelem is benne van, de pl. a 0-nak nincs inverze.

2. *Bizonyítsuk be, hogy egy egységelemes félcsoportban*
a) ha a *és* b *invertálható, akkor* ab *és* ba *is invertálható;*
b) ha ab *és* ba *invertálható, akkor* a *és* b *is invertálható.*
Adjunk példát arra, hogy ab *invertálhatóságából nem feltétlenül következik* a *vagy* b *invertálhatósága.*

Megoldás: a) Könnyen ellenőrizhető, hogy $(ab)^{-1} = b^{-1}a^{-1}$: $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$, és $b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$; és ugyanígy $(ba)^{-1} = a^{-1}b^{-1}$.

b) $b(ab)^{-1}$ az a jobb inverze: $ab(ab)^{-1} = e$, és $(ba)^{-1}b$ az a bal inverze: $(ba)^{-1}ba = e$. Viszont általában is igaz az, hogy ha egy elemnek van jobb inverze: x-hez van x', hogy $xx' = e$ és bal inverze is: x'', hogy $x''x = e$, akkor ezek egyenlők, így inverze is van: $x'' = x''e = x''xx' = ex' = x'$. A b inverzének létezése ugyanígy bizonyítható.

Tekintsük az $\mathbb{N}$ halmazon ható leképezések (kompozícióra nézve vett) félcsoportjában az $f : n \mapsto n+1$, illetve a $g : n+1 \mapsto n$, $0 \mapsto 0$ $(n \geq 0)$ elemeket. Ekkor $g \circ f : n \mapsto n$ $(n \geq 0)$ az identikus leképezés, és így önmaga inverze. Viszont f és g közül egyik sem invertálható, mert f nem szürjektív, g pedig nem injektív.

3. *Bizonyítsuk be, hogy ha egy csoportban $x^2 = 1$ minden x elemre, akkor a csoport kommutatív!*

Megoldás: Tetszőleges a, b elemre $1 = (ab)^2 = abab$, és ha ezt megszorozzuk balról a-val, jobbról pedig b-vel, akkor azt kapjuk, hogy $ab = aababb = 1ba1 = ba$.

4. *Hányadrendű elemek vannak*

a) az $\mathbb{R}^* := (\mathbb{R} \setminus \{0\}, \cdot)$ csoportban;
b) az $\mathbb{R}$ additív csoportjában;
c) a $\mathbb{C}^* := (\mathbb{C} \setminus \{0\}, \cdot)$ csoportban;
d) $GL_2(\mathbb{R})$-ben, azaz a 2×2-es invertáható valós mátrixok csoportjában;
e) $GL_2(\mathbb{Q})$-ban?*

Megoldás: a) Mivel az $x^n = 1$ egyenletnek $n > 0$-ra csak 1, és (páros n esetén) -1 a megoldása, más véges rendű elem nem lehet. Így a rendek $1, 2, \infty$.

b) Ha $a \neq 0$, akkor nincs olyan $n > 0$ egész szám, amelyre $na = 0$. Így minden nem nulla elem végtelen rendű, azaz a rendek csak 1 és ∞.

c) Itt a végtelen rendűek (pl. 2), mellett minden véges rend is előfordul, pl. $\cos(2\pi/n) + i\sin(2\pi/n)$ rendje n.

d) Itt is vannak végtelen rendű elemek, pl. $2I$, és tetszőleges véges rendűek is: a $2\pi/n$ szögű origó körüli forgatás mátrixának a rendje n.

e) Végtelen rendűek itt is vannak. Ha egy mátrix véges rendű, a minimálpolinomja osztója valamely $x^n - 1$ polinomnak. Az utóbbi az n osztóihoz tartozó körosztási polinomok szorzata, amelyekről ismert, hogy $\mathbb{Q}$ fölött irreducibilisek. Mivel egy 2×2-es mátrix minimálpolinomja legföljebb másodfokú, az $(x^n - 1)$-nek vagy a lineáris faktoraiból, $(x-1)$-ből és $(x+1)$-ből áll össze (és akkor a mátrix rendje 1 vagy 2), vagy megegyezik egy másodfokú körosztási polinommal, Φ_d-vel, és akkor a rendje d. Viszont ehhez az kell, hogy $\varphi(d) = 2$ legyen. A φ függvény kanonikus alakjából, $\varphi(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_r - 1)p_r^{\alpha_r - 1}$-ből látható, hogy ekkor d minden prímosztója 2 vagy 3, és ha van 3, akkor $d = 3$ vagy 6, ha nincs, akkor $d = 4$. Tehát a lehetséges véges rendek $1, 2, 3, 4, 6$. Ilyen rendű racionális mátrixok valóban vannak:

$$o(I) = 1,\ o(-I) = 2,\ o\left(\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\right) = 3,\ o\left(\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}\right) = 6,\ o\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) = 4$$

(az utolsó hármat a $\Phi_3(x) = x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$ és $\Phi_4(x) = x^2 + 1$ polinomok kísérőmátrixaiként kaphatjuk meg).

5. *Bizonyítsuk be, hogy egy páros elemszámú véges csoportban mindig van másodrendű elem!*

Megoldás: Állítsuk párba az elemeket az inverzükkel. Mivel az inverz inverze az eredeti elem, ezek valóban diszjunkt párokat alkotnak, kivéve, ha az elem inverze önmaga, azaz ha az elem az 1, vagy pedig másodrendű. Összesen páros sok elem van, és az 1 egyedül van, tehát van még legalább egy elem egyedül, és az szükségképpen másodrendű.

6. *Van-e nemtriviális (azaz nem minden elemet az egységelembe vivő) homomorfizmus*
a) $\mathbb{C}^*$*-ból* $\mathbb{R}^*$*-ba;*
b) $\mathbb{R}^*$*-ból* $\{1, -1\} \leq \mathbb{R}^*$*-ba;*
c) $(\mathbb{Z}_5, +)$*-ból* $(\mathbb{Z}_2, +)$*-ba;*
d) $GL_n(\mathbb{R})$*-ből* $\mathbb{R}^*$*-ba, illetve ennek a pozitív valós számokból álló részcsoportjába?*

Megoldás: a) Pl. $z \mapsto |z|$ ilyen, mert $|z| \in \mathbb{R}^*$, ha $z \neq 0$, és $|uv| = |u||v|$.
b) Legyen $f(a) = 1$, ha $a > 0$, és $f(a) = -1$, ha $a < 0$. Könnyen ellenőrizhető, hogy ez a leképezés szorzattartó.
c) Nincs ilyen, ugyanis ha φ homomorfizmus, akkor tetszőleges $a \in \mathbb{Z}_5$-re $a + a + a + a + a = 0$, viszont $\mathbb{Z}_2$-ben $\varphi(a) + \varphi(a) + \varphi(a) + \varphi(a) + \varphi(a) = \varphi(a)$, ezért minden a-ra $\varphi(a) = \varphi(0) = 0$.

7. *Lássuk be, hogy ha egy* $\varphi : G \to H$ *homomorfizmus bijektív (azaz* φ *izomorfizmus), akkor* $\varphi(g)$ *rendje megegyezik* g *rendjével minden* $g \in G$*-re.*

Megoldás: Ha $o(g) = n$, akkor $\varphi(g)^n = \varphi(g^n) = \varphi(1) = 1$, viszont $0 < k < n$-re nem lehet $\varphi(g)^k = 1$, ugyanis akkor $\varphi(g^k) = \varphi(1)$, de φ bijekció, így ebből $g^k = 1$ következne, ellentmondva annak, hogy g rendje n.

8. *a) Milyen rendű elemből hány van a* D_4 *diédercsoportban és a* Q *kvaterniócsoportban?*
b) Adjunk meg egy nemtriviális homomorfizmust D_4*-ből* Q*-ba.*
c) Bizonyítsuk be, hogy D_4 *és* Q *nem izomorfak.*
d) Bizonyítsuk be, hogy a pozitív valós számok multiplikatív csoportja izomorf a valós számok additív csoportjával.

Megoldás: a) D_4-ben a négy forgatás $(1, \frac{\pi}{2}, \pi, 3\frac{\pi}{2})$ rendje $1, 4, 2, 4$, a tengelyes tükrözéseké pedig 2, tehát egy elsőrendű, öt másodrendű, és két negyedrendű eleme van D_4-nek. Q-ban viszont $\pm i, \pm j, \pm k$ mindegyike negyedrendű, és -1 másodrendű, így egy elsőrendű, egy másodrendű és hat negyedrendű eleme van.
b) Rendeljük hozzá az irányítástartó transzformációkhoz (a forgatásokhoz) az 1-et, az irányításváltókhoz (tengelyes tükrözésekhez) pedig a -1-et. Mivel két irányítástartó, illetve két irányításváltó transzformáció kompozíciója irányítástartó, míg egy irányítástartó és egy irányításváltó kompozíciója bármelyik sorrendben irányításváltó, ez a leképezés művelettartó, azaz homomorfizmus lesz.
c) Az a) részben láttuk, hogy nem ugyanannyi van a különféle rendű elemekből a két csoportban, tehát nincs olyan bijekció a két nyolcelemű csoport között, amelyik rendtartó lenne. A 7. feladat szerint így nincs köztük izomorfizmus sem.
d) Mivel az első csoport művelete a szorzás, a másodiké pedig az összeadás, itt egy φ függvény művelettartása azt jelenti, hogy $\varphi(ab) = \varphi(a) + \varphi(b)$ minden a, b-re. A logaritmusfüggvény épp ilyen tulajdonságú, szigorúan monoton növő, így injektív függvény, értelmezési tartománya $(0, +\infty)$, értékkészlete pedig $\mathbb{R}$, így művelettartó bijekció, azaz izomorfizmus a két csoport között.

Hf1. *a) Bizonyítsuk be, hogy az* $a * b = \dfrac{a+b}{1+ab}$ *művelet értelmezve van az* $I = (-1, 1) \subseteq \mathbb{R}$ *nyílt intervallum minden elemén, és az eredménye is az intervallumba esik.*
b) Lássuk be, hogy $(I, *)$ *csoport.* *(3 pont)*

Hf2. *Milyen rendű elemek vannak a* D_6 *diédercsoportban (a szabályos hatszög egybevágóságainak csoportjában), és melyik rendhez hány olyan rendű elem van?* *(2 pont)*