1. *Csoportot alkotnak-e az összeadásra vagy a szorzásra nézve*
a) a pozitív determinánsú $n \times n$-es valós mátrixok;
b) a $\mathbb{Z}$ fölötti $n \times n$-es mátrixok;
c) a $\mathbb{Z}$ fölötti nem 0 determinánsú $n \times n$-es mátrixok;
d) a $\mathbb{Z}$ fölötti 1 determinánsú $n \times n$-es mátrixok;
e) az $n \times n$-es valós felső háromszögmátrixok?

Megoldás: Mivel $\mathbb{R}^{n\times n}$ gyűrű, az asszociativitást egyik példában sem kell ellenőrizni, csak azt, hogy zárt a műveletre nézve, és van benne egységelem és inverz.

a) Az összeadásra nem, pl. $n = 2$-re $|I| = |-I| = 1 > 0$, de $|I + (-I)| = |O| = 0$. A szorzásra viszont igen: a determinánsok szorzástétele miatt két pozitív determinánsú mátrix szorzata is ilyen. $|I| = 1 > 0$, és ha $|A| > 0$, akkor A invertálható, és $|A^{-1}| = 1/|A| > 0$.

b) Az összeadásra nézve csoportot alkotnak, mert egész elemű mátrixok összege is, negatívja is egész elemű, és a O mátrix is ilyen. A szorzásra nézve I az egységelem, viszont nincs mindennek multiplikatív inverze (pl. a O mátrixnak), tehát a szorzásra nézve nem alkotnak csoportot.

c) Az összeadásra nem zárt, ld. az a) ellenpéldáját. A szorzásra ugyan zárt, de nincs minden elemének multiplikatív inverze a halmazban (pl. $2I$-nek nincs).

d) Az összeadásra nem zárt (ld. az a) 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 csoportot, a szorzásra igen.

e) Az összeadásra csoportot alkot (sőt alterét alkotja az $\mathbb{R}^{n\times n}$-nek), de a szorzásra nem: zárt ugyan a szorzásra, és az I egységelem is benne van, a pl. a O-nak nincs inverze. (Viszont a nemnulla determinánsú valós felső háromszögmátrixok már csoportot alkotnak a szorzásra nézve.)

2. *Hány eleme van a következő geometriai alakzatok egybevágósági csoportjának? Mik ezek az egybevágóságok?*
a) téglalap;
b) négyzet alapú egyenes hasáb (ami nem kocka);
c) szabályos háromszög;
d) egyenlőszárú háromszög;
e) paralelogramma;
f) kör.

Megoldás: a) A négyzetről tudjuk, hogy 8-elemű az egybevágósági csoportja, tehát elég olyan téglalapot nézni, amelynek két szomszédos oldala $a \neq b$ hosszú. Egy csúcsot el lehet vinni egybevágósággal bármely másik csúcsba (helyben hagyás, a két középvonalra való tükrözés, illetve 180°-os forgatás segítségével), viszont ennek a csúcsnak a képe már meghatározza a két szomszédjáét: egyetlen a távolságú, és egy b távolságú szomszéd van csak, és három nem kollineáris pont képe meghatározza az egybevágóságot. Tehát csak az előbb felsorolt négy egybevágóság létezik.

b) Itt legyen az alapnégyzet oldalhossza a, a magasság b. Az alap egy csúcsát átvihetjük a másik nyolc csúcs bármelyikébe (az alapba a függőleges tengely körüli forgatásokkal, a fedőlapba először egy vízszintes síkra való tükrözéssel jutunk, majd az előbbi forgatásokkal elérjük a célba vett csúcsot). Az kiinduló csúcs b távolságú szomszédjának a képe egyértelmű, viszont a két a távolságú szomszédot minden esetben kétféle eloszlásban is belevihetjük a képcsúcs két ilyen szomszédjába: a képcsúcson

átmenő négyzetátlón átfektetett, az alaplapra merőleges síkra való tükrözéssel. Ez a négy csúcs már meghatározza az egybevágóságot. Tehát $4 \cdot 2 = 8$ elemű az egybevágósági csoport.

c) A három csúcs képe $3 \cdot 2 \cdot 1 = 6$-féle lehet, és ennyi egybevágóság van is: három forgatás és három tükrözés.

d) A szabályos háromszöget a c) pontban tárgyaltuk. Ha az egyenlőszárú háromszög nem egyenlőoldalú, akkor a szimmetriatengelyen levő csúcsot csak önmagába vihetjük, az alapcsúcsokat pedig legfeljebb csak felcserélhetjük a szimmetriatengelyre való tükrözéssel. Tehát ez a csoport kételemű, a Z_2-vel izomorf.

e) Ha a paralelogramma se nem téglalap, se nem rombusz, akkor a középpontos tükrözés az egyetlen nem triviális egybevágóság, mert a hegyesszögnél levő csúcsot csak a másik ugyanilyenbe képezhetjük, és a másik két csúcs képét meghatározza az ettől való (különböző) távolsága. Tehát ez az egybevágósági csoport is Z_2-vel izomorf.

A speciális esetek közül a téglalap szerepelt az a) pontban. A (nem négyzet) rombusz egybevágósági csoportja megegyezik egy (szintén nem négyzet) téglalap egybevágósági csoportjával: az oldalközéppontok által alkotott téglalapéval, tehát az is négyelemű (izomorf $\mathbb{F}_2^2$-vel, mert minden 1-től különböző eleme másodrendű).

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 $(\mathbb{R} \setminus \{0\}, \cdot)$ csoportban;
b) az $\mathbb{R}$ additív csoportjában;
c) a $(\mathbb{C} \setminus \{0\}, \cdot)$ csoportban;
d) $GL_2(\mathbb{R})$-ben;
e) $GL_2(\mathbb{Q})$-ban, ahol $GL_n(K) = \{ A \in K^{n \times n} \mid |A| \neq 0 \}$ a szorzással?*

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. *a) Keressünk olyan geometriai alakzatot, amelynek az egybevágósági csoportja, illetve olyan gráfot, amelynek automorfizmuscsoportja izomorf Z_3-mal.*
b) Adjunk meg olyan (végtelen) gráfot, amelynek az automorfizmuscsoportja végtelen.
Egy gráf automorfizmusa egy olyan $\varphi : V(G) \to V(G)$ bijekció, amelyre $(a, b) \in E(G) \Leftrightarrow (a\varphi, b\varphi) \in E(G)$.

Megoldás: a) Egy szabályos háromszögből indulunk ki, és azt egészítjük ki olyan módon, hogy a középpont körüli 120°-os forgatás továbbra is egybevágóság legyen, de a tükrözések ne. Például mindegyik élre rárakhatunk még egy-egy egybevágó, nem egyenlő szárú háromszöget, ugyanúgy irányítva.
A gráfautomorfizmusnál is érdemes a háromszöggel kezdeni, aztán új csúcsok és élek hozzáadásával elrontani a tükrözéseket. Plusz 6 csúccsal ez már megvalósítható: minden él mellett vezetünk egy új, három hosszú utat is, és minden eredeti csúcsot hozzákötünk a belőle pozítív irányban induló új út távolabbi belső pontjához. Így az eredeti csúcsok lesznek csak 5 fokúak, és csak egy irányban tudunk belőlük a következőig rendre egy 2 és egy 3 fokú ponton keresztülmenve 3 hosszú úton eljutni.
Irányított gráfból persze sokkal kisebbet is találunk, egyetlen három hosszú irányított kör is megfelel.
b) Egy mindkét irányban végtelen (irányítatlan) útnak minden eltolás automorfizmusa, és minden élhez tartozik egy "tükrözés" is.

7. *Bizonyítsuk be, hogy a $G_1 = (\mathbb{Z}_8, +)$, $G_2 = (\mathbb{Z}_{16}^*, \cdot)$, és $G_3 = (\mathbb{F}_2^3, +)$ 8-adrendű Abel-csoportok páronként nem izomorfak. (Mennyi az elemek rendje ezekben a csoportokban?)*

Megoldás: G_3 minden eleme 1 vagy 2 rendű. A másik két csoportnak az elemrendjeit a következő táblázatok mutatják.

G_1:

g	0	1	2	3	4	5	6	7
$o(g)$	1	8	4	8	2	8	4	8

G_2:

g	1	3	5	7	9	11	13	15
$o(g)$	1	4	4	2	2	4	4	2

Izomorf csoportok megfelelő elemei azonos rendűek, itt pedig még csak nem is ugyanazok a rendek fordulnak elő, tehát semelyik két csoport nem lehet izomorf egymással.

8. *Az alábbi szorzástáblákkal megadott struktúrák közül melyik csoport? Amelyik nem, abban melyik axióma nem teljesül?*

$\cdot$	a	b
a	a	a
b	b	b

$\cdot$	a	b
a	a	b
b	b	b

$\cdot$	a	b
a	a	b
b	b	a

$\cdot$	a	b	c
a	a	b	c
b	b	b	a
c	c	a	c

Megoldás: Csak a harmadik struktúra csoport, izomorf a $(\{\pm 1\}, \cdot)$ csoporttal (vagyis másodrendű ciklikus csoport). Az első kettő asszociatív (az elsőnél egy akárhogy zárójelezett, többtényezős szorzat a bal szélső elemet veszi föl értékként, a másodiknál pedig minden ilyen szorzat értéke b, ha legalább egy b-t tartalmaz, és a, ha csak a-kból áll), viszont az elsőben nincs egységelem, a másodikban ugyan van egységelem, az a, de b nem invertálható: pl. a sorában nem szerepel az a. Így az első kettő csak félcsoport, az első izomorf például az $\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ félcsoporttal, a második az $\{1, 0\}$-val a szorzásra nézve.

A negyedikben van egységelem (a) és inverz is ($a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$), tehát ha asszociatív lenne, akkor csoport is lenne. De akkor minden sorban (és oszlopban) minden elem szerepelne, ez pedig láthatóan nem teljesül, így ez a struktúra nem asszociatív.

9. *Legyen g egy csoportelem, g rendje $o(g) = n$, és $k, m \in \mathbb{Z}$. Lássuk be, hogy*

a) $g^m = 1 \Leftrightarrow n \mid m$;

b) $o(g^k) = \dfrac{n}{(n,k)}$.

Fogalmazzuk meg és bizonyítsuk be a megfelelő állításokat végtelen rendre!

Milyen rendű elemek vannak Z_n-ben és Z-ben?

Megoldás: a) $\Rightarrow$: Osszuk el az m-et maradékosan n-nel: $m = nq + r$. Ekkor $1 = g^m = (g^n)^q g^r = 1^q g^r = g^r$, de $r < n$, tehát $r = 0$, így $n \mid m$.

$\Leftarrow$: $m = qn \Rightarrow g^m = (g^n)^q = 1^q = 1$.

b) Az a) rész miatt $(g^k)^m = g^{km} = 1 \Leftrightarrow n \mid km \Leftrightarrow \frac{n}{(n,k)} \mid \frac{k}{(n,k)} m \Leftrightarrow \frac{n}{(n,k)} \mid m$, mivel $\frac{n}{(n,k)}$ és $\frac{k}{(n,k)}$ relatív prímek. Így a g^k legkisebb 1 értékű pozitív hatványa az $\frac{n}{(n,k)}$-adik.

Végtelen rendre a megfelelő állítások: Ha $o(g) = \infty$, akkor

$g^m = 1 \Leftrightarrow m = 0$;

$o(g^k) = \infty$, ha $k \neq 0$.

Az első nyilvánvaló a végtelen rend definíciójából, a második pedig az elsőből következik: ha $(g^k)^m = g^{km} = 1$, akkor $km = 0$, így $m = 0$.

A b) állításból látszik, hogy Z_n minden elemének a rendje osztója n-nek, és minden $d \mid n$ osztóra van is d-edrendű elem: ha $o(a) = n$, akkor $o(a^{n/d}) = d$. Z-nek pedig minden eleme 1 vagy ∞ rendű.

Hf1. *Csoportot alkotnak-e a $(-1, 1)$ nyílt intervallum elemei az $a * b = \dfrac{a+b}{1+ab}$ műveletre mint szorzásra nézve? Ne felejtsük el azt is ellenőrizni, hogy az ilyen elemek szorzata értelmezve van, és benne van az intervallumban!)*

Hf2. *Bizonyítsuk be, hogy $o(ab) = o(ba)$ egy G csoport tetszőleges a, b elemeire.*