1. *Bizonyítsuk be, hogy egy H legalább kételemű halmaz részhalmazainak a halmaza, $P(H)$ nem alkot csoportot sem a metszet, sem az unió műveletére nézve, de csoportot alkot a szimmetrikus differenciára nézve ($A \triangle B := (A \cup B) \setminus (A \cap B)$)!*

Megoldás: Bár a metszet és az unió is asszociatív, és van rájuk nézve egységelem is (a metszetre a H, az unióra az $\emptyset$), az $\emptyset$ halmaznak nincs inverze a metszetre nézve, H-nak pedig nincs inverze az unióra nézve.
A szimmetrikus differencia a $P(H)$-n értelmezett kétváltozós művelet, amely átírható $A \triangle B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$ alakba. Az asszociativitás bizonyításához írjuk át az $A \triangle B$ halmaz komplementumát is. $\overline{A \triangle B} = \overline{A \cap \overline{B} \cap \overline{A} \cap B} = (\overline{A} \cup B) \cap (A \cup \overline{B}) = (\overline{A} \cap A) \cup (\overline{A} \cap \overline{B}) \cup (B \cap A) \cup (B \cap \overline{B}) = \emptyset \cup (\overline{A} \cap \overline{B}) \cup (A \cap B) \cup \emptyset = (\overline{A} \cap \overline{B}) \cup (A \cap B)$
A művelet asszociatív: $(A \triangle B) \triangle C = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)$, tehát $(A \triangle B) \triangle C$ pontosan azokból az elemekből áll, amelyek az A, B, C közül páratlan sokban vannak benne, és nyilván ugyanezt kapjuk az $A \triangle (B \triangle C) = (B \triangle C) \triangle A$ kifejtésénél is (itt használtuk azt is, hogy a $\triangle$ művelet láthatóan szimmetrikus is).
Van egységelem, az üres halmaz: $A \triangle \emptyset = \emptyset \triangle A = A$ minden A-ra,
továbbá minden halmaz önmaga inverze: $A \triangle A = \emptyset$.
Tehát $P(H)$ a szimmetrikus differencia műveletére csoportot, sőt Abel-csoportot alkot.

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

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

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

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

c) Az összeadásra nézve csoportot alkotnak, mert egész elemű mátrixok összege is, negatívja is egész elemű, és a 0 mátrix is ilyen. A szorzásra nézve I az egységelem, viszont nincs mindennek multiplikatív inverze (pl. $2I$ inverze nem egész elemű), tehát a szorzásra nézve nem alkotnak csoportot.

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

e) 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.

f) 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 0-nak nincs inverze.

3. *Bizonyítsuk be, hogy ha egy S félcsoportban*
van jobb oldali egységelem: $\exists e:\ xe = x\ \forall x$;
és minden elemnek van e-re nézve jobb oldali inverze: $\forall x\ \exists x':\ xx' = e$,
akkor S csoport.

Megoldás: Először belátjuk, hogy e kétoldali egységelem. A feltétel szerint $\exists x' \in S:\ xx' = e$, és $\exists x'' \in S:\ x'x'' = e$. De akkor $x = xe = xx'x'' = ex''$, amiből $ex = eex'' = ex'' = x$ következik.
Legyen megint tetszőleges $x \in S$-re x' és x'' olyan, hogy $xx' = e$ és $x'x'' = e$. Az elsőből következik, hogy $x'xx' = x'e = x'$, és ha ezt jobbról megszorozzuk x''-vel, akkor azt kapjuk, hogy $x'xx'x'' = x'x'' \Rightarrow x'xe = e \Rightarrow x'x = e$, tehát x' kétoldali inverze x-nek. Ezzel beláttuk, hogy minden elemnek van inverze.

4. *Bizonyítsuk be, hogy ha egy S félcsoport minden a, b elemére megoldható az $ax = b$ és az $ya = b$ egyenlet, akkor S csoport.*

Megoldás: Legyen $a \in S$ tetszőleges elem, és $x = e$ az $ax = a$ megoldása. Mivel minden b-re van megoldása az $ya = b$ egyenletnek, ezzel az y-nal $be = yae = ya = b$. Azt kaptuk, hogy e jobb oldali egységeleme a félcsoportnak. Ugyanígy van bal oldali egységelem is: ha valamely b-re az $y = f$ megoldása az $yb = b$ egyenletnek, és tetszőleges a-ra x olyan, hogy $bx = a$, akkor $fa = fbx = bx = a$, vagyis f bal egységelem. Végül $e = fe = f$ miatt e egységelem is.
A megoldhatósági feltételekből ezek után következik, hogy minden a-hoz van olyan a' és a'', amelyre $aa' = e$ és $a''a = e$, de akkor $a'' = a''e = a''aa' = ea' = a'$, vagyis $a' = a''$ az a-nak inverze.

5. *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.

6. *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 $ab = aababb = 1ba1 = ba$.

7. *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?*

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).

8. *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.

9. *Határozzuk meg az* $(1345)(236)(41)$ *permutáció rendjét!*

Megoldás: $(1345)(236)(41) = (1623)(45)$ az elem diszjunkt ciklusok szorzatára bontása, és ennek a rendje a ciklusok hosszánk legkisebb közös többszöröse, azaz 4.

10. *a) Hány tized- és negyedrendű elem van* S_{10}*-ben?*
b) Mi az elemek rendjének maximuma S_8*-ban?*

Megoldás: a) Ha egy elem tizedrendű, akkor vagy van a diszjunkt ciklusokra bontásában 10-ciklus, és akkor más ciklus már nem lehet, vagy van benne 5-ciklus és 2-ciklus(ok), tehát a lehetséges ciklusfelbontások: 10, 5+2+2+1, illetve $5 + 2 + 1 + 1 + 1$. Az első

fajtából $9! = 362880$ darab van, a másodikból $\binom{10}{5}4!\binom{5}{2}\binom{3}{2}\cdot\frac{1}{2} = 90720$, a harmadikból $\binom{10}{5}4!\binom{5}{2} = 60480$. Így összesen 514080 darab tizedrendű elem van S_{10}-ben.

Ha egy elem negyedrendű, akkor csak 4-ciklusokból, 2-ciklusokból és fixpontokból állhat, és van bennük 4-ciklus. Tehát ezek $k = 1$ vagy 2 darab 4-ciklus, és ℓ darab 2-ciklus szorzatai, ahol $0 \le \ell \le 5 - 2k$. Ezek száma összesen
$\binom{10}{4}3!\left(1 + \binom{6}{2} + \binom{6}{2}\binom{4}{2}\frac{1}{2!} + \binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{3!}\right) + \binom{10}{4}\binom{6}{4}\frac{1}{2}(3!)^2\left(1 + \binom{2}{2}\right) = 209160$

b) A maximális rendű elemről feltehetjük, hogy a ciklushosszai relatív prímek, mert ha van a és b hosszú ciklusa, ahol $(a, b) = d > 1$, akkor az a hosszú helyett vehetünk csak a/d hosszút (és a többi elemét fixen hagyjuk), és a rend ugyanannyi marad. Továbbá azt is feltehetjük, hogy a ciklushosszak prímhatványok, mert $xy \ge x + y$, ha $x, y \ge 2$, tehát egy xy hosszú ciklust, ahol x és y 1-nél nagyobb relatív prím számok, helyettesíthetünk egy x hosszúval és egy y hosszúval. Így a következő rendek jönnek szóba: 2^3, $2^2 \cdot 3$, $2 \cdot 5$, $3 \cdot 5$, 7, és ebből $3 \cdot 5 = 15$ a legnagyobb, így ez a maximális rend (egy diszjunkt 3-ciklus és 5-ciklus szorzatának rendje).

Hf1. *Csoportot alkotnak-e a* $(-1, 1)$ *nyílt intervallum elemei az* $a * b = \dfrac{a + b}{1 + ab}$ *műveletre mint szorzásra nézve?*

Hf2. *Hány* 6*-odrendű eleme van* S_7*-nek?*