4. FELADATLAP

Műveltek, monoidok, csoportok, csoportmorfizmusok

1. Legyen $(M,\cdot)$ egy monoid és $U(M)$ az invertálható elemek halmaza. Bizonyítsuk be, hogy $U(M)$ zárt részhalmaza M-nek és $(U(M),\cdot)$ csoportot alkot a leszűkített művelettel.

Megoldás. Legyen $e \in M$ az $(M,\cdot)$ monoid semleges eleme, vagyis minden $x \in M$ esetén $x \cdot e = e \cdot x = x$. Az $x \in M$ elem invertálható (van szimmetrikusa), ha létezik olyan $x' \in M$ elem, hogy $x \cdot x' = x' \cdot x = e$. Ekkor az invertálható eleme halmaza

$$U(M) = \{x \in M \,|\, \exists x' \in M \text{ ú.h. } x' \cdot x = x \cdot x' = e\}.$$

Az $U(M)$ zárt részhalmaza az M-nek, ha bármely $x, y \in U(M)$ esetén $x \cdot y \in U(M)$. Legyenek x', illetve y' az x, illetve y inverzei (szimmetrikusai) az M-ben. Belátjuk, hogy az $(x \cdot y)' := y' \cdot x'$ az $x \cdot y$ szimmetrikusa az M-ben, így $x \cdot y \in U(M)$. Valóban,

$$\begin{aligned}
(x\cdot y)\cdot(x\cdot y)' &= (x\cdot y)\cdot(y'\cdot x') \\
&= x \cdot \underbrace{y\cdot y'}_{e} \cdot x' && (y' \text{ az } y \text{ szimmetrikusa}) \\
&= \underbrace{x\cdot e}_{x} \cdot x' && (e \text{ semleges elem}) \\
&= x \cdot x' && (x' \text{ az } x \text{ szimmetrikusa}) \\
&= e,
\end{aligned}$$

$$\begin{aligned}
(x\cdot y)'\cdot(x\cdot y) &= (y'\cdot x')\cdot(x\cdot y) \\
&= y' \cdot \underbrace{x\cdot x'}_{e} \cdot y && (x' \text{ az } x \text{ szimmetrikusa}) \\
&= \underbrace{y'\cdot e}_{y'} \cdot y && (e \text{ semleges elem}) \\
&= y' \cdot y && (y' \text{ az } y \text{ szimmetrikusa}) \\
&= e.
\end{aligned}$$

Mivel beláttuk, hogy az $U(M)$ zárt részhalmaza az M-nek, ezért az M-en értelmezett „$\cdot$" művelet származtat egy szintén „$\cdot$"-tal jelölt műveletet az $U(M)$ halmazon. Be fogjuk látni, hogy $(U(M),\cdot)$ csoport, vagyis a származtatott (leszűkített) művelet szintén asszociatív, van semleges eleme és minden elemnek van szimmetrikusa (inverze).

- *Asszociativitás.* Mivel az M-en a „$\cdot$" művelet asszociatív, ezért $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ minden $x, y, z \in M$ esetén. Az $U(M) \subseteq M$ bennfoglaltatás miatt az előbbi reláció fennáll sajátosan az $x, y, z \in U(M)$ elemekre is. Tehát a származtatott (leszűkített) művelet is asszociatív az $U(M)$-en. Azt mondjuk, hogy az asszociativitás öröklődik a zárt részhalmazokra.
- *Semleges elem.* Elég belátni, hogy az M semleges eleme e is benne van $U(M)$-ben, mert így ő lesz az $(U(M),\cdot)$ semleges eleme. Valóban, az e-nek is van szimmetrikusa, éspedig $e' = e$, mivel a semleges elem tulajdonsága alapján $e \cdot e = e$. Tehát $e \in U(M)$, továbbá $e \cdot x = x \cdot e = x$, minden $x \in U(M) \subseteq M$ esetén.
- *Szimmetrikus (inverz) elem.* Értelmezés szerint minden $x \in U(M)$ esetén létezik $x' \in M$ úgy, hogy $x \cdot x' = x' \cdot x = e$. Elég belátni, hogy $x' \in U(M)$, vagyis létezik $(x')' \in M$ úgy, hogy $x' \cdot (x')' = (x')' \cdot x' = e$. Valóban, az $(x')' := x$ esetén teljesül az előbbi két reláció, mert x' az x szimmetrikusa. Tehát az $x \in U(M)$ elem M-beli és $U(M)$-beli szimmetrikusa (inverze) ugyanaz.

Ezzel beláttuk, hogy $(U(M), \cdot)$ csoport. $\square$

2. Határozzuk meg az invertálható elemenek halmazát a következő monoidok esetében:

(a) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$;

Megoldás. $U(\mathbb{N}, +) = \{0\}$; $U(\mathbb{N}, \cdot) = \{1\}$; $U(\mathbb{Z}, \cdot) = \{-1, 1\}$; $U(\mathbb{Q}, \cdot) = \mathbb{Q} \setminus \{0\} = \mathbb{Q}^*$; $U(\mathbb{R}, \cdot) = \mathbb{R} \setminus \{0\} = \mathbb{R}^*$; $U(\mathbb{C}, \cdot) = \mathbb{C} \setminus \{0\} = \mathbb{C}^*$. $\square$

(b) $(M^M, \circ)$, ahol M egy nemüres halmaz;

Megoldás. Az $M^M = \{f : M \to M \text{ függvény}\}$ halmazon a „$\circ$” művelet a függvények összetétele.

$$U(M^M, \circ) = \{f \in M^M \mid \exists g \in M^M \text{ ú.h. } g \circ f = f \circ g = id_M\},$$

ahol $id_M : M \to M$, $id_M(x) = x$ az identikus függvény az M halmazon (az $(M^M, \circ)$ monoid semleges eleme).

Ha $g \circ f = id_M$, vagyis minden $x \in M$ esetén $g(f(x)) = x$, akkor az f függvény injektív. Valóban, ha $f(x_1) = f(x_2)$, akkor behelyettesítve a g függvénybe kapjuk, hogy $g(f(x_1)) = g(f(x_2)) \Leftrightarrow x_1 = x_2$.

Ha $f \circ g = id_M$, vagyis minden $x \in M$ esetén $f(g(x)) = x$, akkor az g függvény szürjektív. Valóban, az f függvény tetszőleges $x \in M$ értéket felvesz a $g(x) \in M$ helyen.

Tehát, ha egy függvénynek van szimmetrikusa (inverze) az összetevésre nézve, akkor bijektív. Fordítva, ha egy függvény bijektív, akkor van inverze. Tehát

$$U(M^M, \circ) = \{f \mid f : M \to M \text{ bijektív függvény}\}.$$

$\square$

(c) $(\mathbb{Z}[i], \cdot)$, ahol $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$;

Első megoldás. A $z = a + ib \neq 0$ komplex szám inverze

$$z^{-1} = \frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a-ib)(a+ib)} = \frac{a-ib}{a^2+b^2} = \underbrace{\frac{a}{a^2+b^2}}_{a'} + i\underbrace{\frac{-b}{a^2+b^2}}_{b'} = a' + ib'$$

alakú. Tehát $z = a + ib \in U(\mathbb{Z}[i], \cdot)$, ha $a, b \in \mathbb{Z}$ ($(a, b) \neq (0, 0)$) és $a' = \dfrac{a}{a^2+b^2}$, $b' = \dfrac{-b}{a^2+b^2} \in \mathbb{Z}$.

1. eset. Ha $a, b \in \mathbb{Z}^*$, akkor

$$0 < |a'| = \frac{|a|}{a^2+b^2} < \frac{|a|}{a^2} = \frac{|a|}{|a|^2} = \frac{1}{|a|} \leq 1,$$

tehát ebben az esetben $a + ib \notin U(\mathbb{Z}[i], \cdot)$.

2. eset. Ha $a = 0$ és $b \neq 0$, akkor $a' = \dfrac{a}{a^2+b^2} = 0$ és

$$0 < |b'| = \left|\frac{-b}{a^2+b^2}\right| = \frac{|b|}{b^2} = \frac{|b|}{|b|^2} = \frac{1}{|b|} \leq 1.$$

Tehát ebben az esetben $b' \in \mathbb{Z}$ pontosan, akkor ha $b = \pm 1$.

3. eset. Ha $a \neq 0$ és $b = 0$, akkor $b' = \dfrac{-b}{a^2+b^2} = 0$ és

$$0 < |a'| = \left|\frac{a}{a^2+b^2}\right| = \frac{|a|}{a^2} = \frac{|a|}{|a|^2} = \frac{1}{|a|} \leq 1.$$

Tehát ebben az esetben $a' \in \mathbb{Z}$ pontosan, akkor ha $a = \pm 1$.

Összegezve, $U(\mathbb{Z}[i], \cdot) = \{\pm 1, \pm i\}$. $\square$

Második megoldás. A $z = r(\cos\alpha + i\sin\alpha) \neq 0$ trigonometrikus alakban felírt komplex szám inverze $z^{-1} = \frac{1}{r}(\cos(-\alpha) + i\sin(-\alpha))$. Ez alapján az invertálás a komplex számsík origó középpontú egységsugarú körön kívül lévő pontjait (vagyis azokat a $z = r(\cos\alpha + i\sin\alpha)$ komplex számokat, amelyekre $|z| = r > 1$) az egységsugarú kör belsejébe képezi (vagyis $z^{-1} = \frac{1}{r}(\cos(-\alpha) + i\sin(-\alpha))$ komplex számokba, amelyekre $|z^{-1}| = \frac{1}{r} < 1$). Az egységsugarú körön belül a $\mathbb{Z}[i]$ halmaznak csak a $0 = 0 + 0i$ pontja található, amely nem lehet inverz. Tehát az egységsugarú körön kívül és belül lévő komplex számok nem elemei az $U(\mathbb{Z}[i], \cdot)$-nek. Az egységsugarú körön a $\mathbb{Z}[i]$-nek négy eleme van, éspedig $-1, 1, -i, i$. Ezekre leellenőrizhető, hogy $1^{-1} = 1$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$ és $i^{-1} = -i$. Tehát $U(\mathbb{Z}[i], \cdot) = \{\pm 1, \pm i\}$. □

(d) $(\mathcal{M}_n(\mathbb{R}), \cdot)$, ahol $\mathcal{M}_n(\mathbb{R})$ az $n \times n$-es valós mátrixok halmaza;

Megoldás. Ha egy $(n \times n)$-es valós mátrix determinánsa nem nulla, akkor a mátrix invertálható és az inverze is egy $(n \times n)$-es valós mátrix. Ezért $U(\mathcal{M}_n(\mathbb{R}), \cdot) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) \neq 0\}$. □

(e) $(\mathbb{Z}_{10}, \cdot)$.

Megoldás. A $(\mathbb{Z}_{10}, \cdot)$ monoid semleges eleme $\hat{1}$. A $\mathbb{Z}_{10} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}, \hat{7}, \hat{8}, \hat{9}\}$ elemei közül csak az $\hat{1}$, $\hat{3}$, $\hat{7}$ és $\hat{9}$ invertálhatóak ($\hat{1} \cdot \hat{1} = \hat{1}$, $\hat{3} \cdot \hat{7} = \widehat{21} = \hat{1}$ és $\hat{9} \cdot \hat{9} = \widehat{81} = \hat{1}$), tehát $U(\mathbb{Z}_{10}, \cdot) = \{\hat{1}, \hat{3}, \hat{7}, \hat{9}\}$. □

3. Legyen $A = \{a_1, \ldots, a_n\}$. Határozzuk meg:

(a) az A halmazon értelmezhető műveletek számát;

Első megoldás. Egy $A \times A \to A$ művelet lényegében egy $A \times A \to A$ függvény, így az műveletek száma egyenlő a függvények számával:

$$|\{A \times A \to A \text{ művelet}\}| = |\{A \times A \to A \text{ függvény}\}| = |A|^{|A \times A|} = |A|^{|A| \cdot |A|} = n^{n \cdot n} = n^{n^2}.$$

□

Második megoldás. Egy $\cdot : A \times A \to A$ művelet megadható egy műveleti táblával, amelyben bármely két elemre elvégzett művelet eredményét tároljuk.

$\cdot$	a_1	a_2	$\ldots$	a_n
a_1	$a_1 \cdot a_1$	$a_1 \cdot a_2$	$\ldots$	$a_1 \cdot a_n$
a_2	$a_2 \cdot a_1$	$a_2 \cdot a_2$	$\ldots$	$a_2 \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
a_n	$a_n \cdot a_1$	$a_n \cdot a_2$	$\ldots$	$a_n \cdot a_n$

A „·” művelet táblája akkor adott, ha az $a_i \cdot a_j$, $i, j = 1, \ldots, n$ helyére mindenhova egy A-beli értéket írunk. Tehát a tábla $n \times n$ celláját (mivel ennyi $a_i \cdot a_j$ szorzat írható fel) kell kitölteni az n elemű A halmaz elemeivel. Ezt $n^{n \times n} = n^{n^2}$-féleképpen tehetjük meg, tehát n^{n^2} művelet van egy n elemű A halmazon. □

(b) az A halmazon értelmezhető kommutatív műveletek számát;

Megoldás. Egy $\cdot : A \times A \to A$ művelet kommutatív, ha $a_i \cdot a_j = a_j \cdot a_i$, minden $i, j = 1, \ldots, n$ esetén. Tehát egy kommutatív művelet műveleti táblája szimmetrikus a főátlóra nézve, vagyis ha a főátlót és a felette lévő cellákat kitöltjük, akkor a főátló alatti cellák kitöltése automatikus a kommutativitás tulajdonsága miatt.

$\cdot$	a_1	a_2	a_3	$\cdots$	a_{n-1}	a_n
a_1	$a_1\cdot a_1$	$a_1\cdot a_2$	$a_1\cdot a_3$	$\cdots$	$a_1\cdot a_{n-1}$	$a_1\cdot a_n$
a_2	$a_2\cdot a_1$	$a_2\cdot a_2$	$a_2\cdot a_3$	$\cdots$	$a_2\cdot a_{n-1}$	$a_2\cdot a_n$
a_3	$a_3\cdot a_1$	$a_3\cdot a_2$	$a_3\cdot a_3$	$\cdots$	$a_3\cdot a_{n-1}$	$a_3\cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$	$\vdots$
a_{n-1}	$a_{n-1}\cdot a_1$	$a_{n-1}\cdot a_2$	$a_{n-1}\cdot a_3$	$\cdots$	$a_{n-1}\cdot a_{n-1}$	$a_{n-1}\cdot a_n$
a_n	$a_n\cdot a_1$	$a_n\cdot a_2$	$a_n\cdot a_3$	$\cdots$	$a_n\cdot a_{n-1}$	$a_n\cdot a_n$

A fenti táblázatban a fehéren hagyott cellákban $a_i\cdot a_j$, $1\le i\le j\le n$ helyére kell egy A-beli értéket írni. Tehát összesen (soronként számolva) $n+(n-1)+\cdots+2+1=\dfrac{n(n+1)}{2}$ cellát kell kitöltenünk az A-beli elemekkel (a többi, zölddel jelölt cella automatikusan értéket kap a kommutativitás miatt). Ezt $n^{\frac{n(n+1)}{2}}$-féleképpen tehetjük meg, tehát ennyi kommutatív művelet van az n elemű A halmazon. $\square$

(c) az A halmazon értelmezhető semleges elemmel rendelkező műveletek számát;

Megoldás. Ha rögzítünk egy a_i elemet egységelemnek (vagyis $e=a_i$), akkor az a_i sora és oszlopa a műveleti táblában automatikusan kitölthető az $e\cdot a_j=a_j\cdot e=a_j$, minden $j=1,\ldots,n$-re összefüggések miatt.

$\cdot$	a_1	a_2	$\ldots$	$e=a_i$	$\ldots$	a_n
a_1	$a_1\cdot a_1$	$a_1\cdot a_2$	$\ldots$	a_1	$\ldots$	$a_1\cdot a_n$
a_2	$a_2\cdot a_1$	$a_2\cdot a_2$	$\ldots$	a_2	$\ldots$	$a_2\cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$	$\vdots$
$e=a_i$	a_1	a_2	$\cdots$	a_i	$\cdots$	a_n
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$	$\vdots$
a_n	$a_n\cdot a_1$	$a_n\cdot a_2$	$\ldots$	a_n	$\ldots$	$a_n\cdot a_n$

Tehát a fenti táblázatban a zöld cellákon kívül az összes többit ki kell tölteni A-beli elemekkel, összesen $n^2-n-(n-1)=n^2-2n+1=(n-1)^2$ cellát kell kitölteni. Így $n^{(n-1)^2}$ olyan műveletet kapunk, amikor a semleges elem $e=a_i$. Egy műveletnek csak egyetlen semleges eleme lehet, ha létezik.
Sorban megismételve $e=a_1,a_2,\ldots,a_n$ semleges elemekre kapjuk, hogy összesen

$$\underbrace{n^{(n-1)^2}}_{e=a_1\text{ esetén}}+\underbrace{n^{(n-1)^2}}_{e=a_2\text{ esetén}}+\cdots+\underbrace{n^{(n-1)^2}}_{e=a_n\text{ esetén}}=n\cdot n^{(n-1)^2}=n^{n^2-2n+2}$$

egységelemes művelet van az n elemű A halmazon. $\square$

(d) az A halmazon értelmezhető kommutatív és semleges elemmel rendelkező műveletek számát.

Megoldás. Ha a művelet kommutatív és egységelemes, akkor egy rögzített $e=a_i$ egységelemre csak a táblázat főátló és a feletti részét kell kitölteni ($\dfrac{(n+1)n}{2}$ cellát), sőt ezekből még n cella (az egységelem sorának és oszlopának főátlóra és fölé eső cellái) automatikusan kitöltődik az egységelem miatt. Tehát rögzített egységelemre $\dfrac{(n+1)n}{2}-n=\dfrac{n(n-1)}{2}$ cellát kell kitölteni az n elemű A halmaz elemeivel. Ezt $n^{\frac{n(n-1)}{2}}$-féleképpen tehetjük meg.

Ha egységelemnek sorban $e=a_1,a_2,\ldots,a_n$-et választunk, akkor azt kapjuk, hogy

$$\underbrace{n^{\frac{n(n-1)}{2}}}_{e=a_1\text{ esetén}}+\underbrace{n^{\frac{n(n-1)}{2}}}_{e=a_2\text{ esetén}}+\cdots+\underbrace{n^{\frac{n(n-1)}{2}}}_{e=a_n\text{ esetén}}=n\cdot n^{\frac{n(n-1)}{2}}=n^{\frac{n^2-n+2}{2}}$$

egységelemes, kommutatív művelet van az n elemű A halmazon. □

4. Legyen $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ egy művelet, ahol $x * y = x + y + xy$. Bizonyítsuk be, hogy:

(a) $(\mathbb{R}, *)$ kommutatív monoid;

Megoldás. A „$*$" egy művelet az $\mathbb{R}$ halmazon, mert a megadott szabály szerint $x * y \in \mathbb{R}$, minden $x, y \in \mathbb{R}$ esetén.

A „$*$" művelet asszociatív, mert minden $x, y, z \in \mathbb{R}$ esetén

$$\begin{aligned} x * (y * z) &= x + (y * z) + x(y * z) = x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + yz + xy + xz + xyz, \\ (x * y) * z &= (x * y) + z + (x * y)z = (x + y + xy) + z + (x + y + xy)z \\ &= x + y + xy + z + xz + yz + xyz, \end{aligned}$$

tehát $x * (y * z) = (x * y) * z$.

A „$*$" művelet kommutatív, mert minden $x, y \in \mathbb{R}$ esetén

$$x * y = x + y + xy = y + x + yx = y * x,$$

a valós számok összeadásának és szorzásának kommutativitása miatt.

Az e semleges elemet a következőképpen határozhatjuk meg.

$$e * x = x, \forall x \in \mathbb{R} \;\Leftrightarrow\; e + x + ex = x, \forall x \in \mathbb{R} \;\Leftrightarrow\; e(1 + x) = 0, \forall x \in \mathbb{R}.$$

Sajátosan $x = 0$-ra azt kapjuk, hogy $e = 0$. Az $e = 0$ esetén valóban teljesülnek az $0 * x = x \;\Leftrightarrow\; 0(1 + x) = 0$, minden $x \in \mathbb{R}$ összefüggések. Tehát $e = 0$ az $(\mathbb{R}, *)$ semleges eleme.

Ezzel beláttuk, hogy $(\mathbb{R}, *)$ egy kommutatív monoid. □

(b) a $[-1, \infty)$ intervallum zárt részhalmaza $\mathbb{R}$-nek a „$*$" műveletre nézve.

Megoldás. A $[-1, \infty)$ intervallum zárt részhalmaza $\mathbb{R}$-nek a „$*$" műveletre nézve, ha minden $x, y \in [-1, \infty)$ esetén $x * y \in [-1, \infty)$. Valóban, ha $x, y \in [-1, \infty)$, akkor $x \geq -1$ és $y \geq -1$, vagyis $x + 1 \geq 0$ és $y + 1 \geq 0$. Ezeket összeszorozva kapjuk, hogy

$$(x+1)(y+1) \geq 0 \;\Leftrightarrow\; x+y+xy+1 \geq 0 \;\Leftrightarrow\; x+y+xy \geq -1 \;\Leftrightarrow\; x*y \geq -1 \;\Leftrightarrow\; x*y \in [-1, \infty).$$

□

5. Határozzuk meg $(\mathbb{Z}, \cdot)$ véges zárt részhalmazait!

Megoldás. Ha az A nem üres véges halmaz a $(\mathbb{Z}, \cdot)$ monoid egy zárt részhalmaza, akkor minden $a \in A$ esetén az $a, a^2, \ldots, a^n, \ldots$ elemek is az A-ban vannak. Tegyük fel, hogy $a \neq 0$. Mivel A véges, ezért ez utóbbi elemek nem lehetnek mind különbözőek, vagyis léteznek $m > n \geq 1$ úgy, hogy $a^m = a^n$. Mindkét oldalt osztva a^n-nel kapjuk, hogy $a^{m-n} = 1$, ahol $m - n > 0$. Tehát a invertálható a $(\mathbb{Z}, \cdot)$ monoidban, mert $a \cdot a^{m-n-1} = 1$, ezért $a = \pm 1$. Ezzel beláttuk, hogy az A-nak csak $-1, 0, 1$ lehetnek az elemei, vagyis $\emptyset \neq A \subseteq \{-1, 0, 1\}$.

Ha $-1 \in A$, akkor $(-1)^2 = 1 \in A$, ezért $A = \{-1\}$, $A = \{-1, 0\}$ nem zárt részhalmazok. Így a következő zárt részhalmazokat kapjuk:

$$A = \{0\}, \quad A = \{1\}, \quad A = \{0, 1\}, \quad A = \{-1, 1\}, \quad A = \{-1, 0, 1\}.$$

□

6. Legyenek $(G, \cdot)$ és $(G', *)$ csoportok, 1 és $1'$ semleges elemekkel és a „$\circ$" művelet: $\circ : (G \times G') \times (G \times G') \to G \times G'$, $(g_1, g_1') \circ (g_2, g_2') = (g_1 \cdot g_2, g_1' * g_2')$, $\forall\, g_1, g_2 \in G$ és $\forall\, g_1', g_2' \in G'$. Bizonyítsuk be, hogy $(G \times G', \circ)$ csoport, ahol $(g^{-1}, (g')^{-1})$ az inverze egy (g, g') elemnek, és $(1, 1')$ a semleges elem.

Megoldás. A „$\circ$” művelet asszociatív: minden $(g_1, g_1'), (g_2, g_2'), (g_3, g_3') \in G \times G'$ esetén

$$\begin{aligned}(g_1, g_1') \circ \big[(g_2, g_2') \circ (g_3, g_3')\big] &= (g_1, g_1') \circ (g_2 \cdot g_3,\, g_2' * g_3') \\ &= \big(g_1 \cdot [g_2 \cdot g_3],\, g_1' * [g_2' * g_3']\big) \\ &\overset{(*)}{=} \big([g_1 \cdot g_2] \cdot g_3,\, [g_1' * g_2'] * g_3'\big) \\ &= (g_1 \cdot g_2,\, g_1' * g_2') \circ (g_3, g_3') \\ &= \big[(g_1, g_1') \circ (g_2, g_2')\big] \circ (g_3, g_3'),\end{aligned}$$

ahol a $(*)$ egyenlőségben felhasználtuk, hogy a „$\cdot$” és „$*$” műveletek asszociatívak.

Ha $1 \in G$ a „$\cdot$” és $1' \in G'$ a „$*$” művelet semleges elemei, akkor $(1, 1') \in G \times G'$ a „$\circ$” művelet semleges eleme. Valóban, minden $(g, g') \in G \times G'$ esetén

$$(1, 1') \circ (g, g') = (1 \cdot g, 1' * g') \overset{(\dagger)}{=} (g, g'), \qquad (g, g') \circ (1, 1') = (g \cdot 1, g' * 1') \overset{(\ddagger)}{=} (g, g'),$$

ahol a $(\dagger)$ és $(\ddagger)$ egyenlőségekben felhasználtuk, hogy 1 a „$\cdot$” és $1'$ a „$*$” művelet semleges eleme.

Ha g^{-1} a $g \in G$ elem inverze (a „$\cdot$” műveletre nézve) és $(g')^{-1}$ a $g' \in G'$ elem inverze (a „$*$” műveletre nézve), akkor $(g^{-1}, (g')^{-1}) \in G \times G'$ a (g, g') elem inverze (a „$\circ$” műveletre nézve), vagyis $(g, g')^{-1} = (g^{-1}, (g')^{-1})$. Valóban,

$$(g, g') \circ (g^{-1}, (g')^{-1}) = (g \cdot g^{-1}, g' * (g')^{-1}) \overset{(+)}{=} (1, 1'),$$

$$(g^{-1}, (g')^{-1}) \circ (g, g') = (g^{-1} \cdot g, (g')^{-1} * g') \overset{(\#)}{=} (1, 1'),$$

ahol a $(+)$ és $(\#)$ egyenlőségekben felhasználtuk, hogy g^{-1} a $g \in G$ elem inverze és $(g')^{-1}$ a $g' \in G'$ elem inverze. $\square$

7. Igazoljuk, hogy $H = \{z \in \mathbb{C} \mid |z| = 1\}$ részcsoportja $(\mathbb{C}^*, \cdot)$-nak, de nem részcsoportja $(\mathbb{C}, +)$-nak.

Megoldás. A $(H, \cdot)$ részcsoportja a $(\mathbb{C}^*, \cdot)$ csoportnak, mert:

(1) $H \neq \emptyset$, hiszen $1 \in H \;\Leftrightarrow\; |1| = 1$;

(2) minden $z_1, z_2 \in H$ (vagyis $|z_1| = |z_2| = 1$) esetén $|z_1 \cdot z_2| = |z_1| \cdot |z_2| = 1 \cdot 1 = 1$, tehát $z_1 \cdot z_2 \in H$;

(3) minden $z \in H$ (vagyis $|z| = 1$) esetén $|z^{-1}| = |z|^{-1} = 1^{-1} = 1$, tehát $z^{-1} \in H$.

A H nem részcsoportja a $(\mathbb{C}, +)$ csoportnak, mert $1 \in H$, de $1 + 1 = 2 \notin H$. $\square$

8. Legyen $n \in \mathbb{N}^*$, $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ az n-edrendű egységgyökök halmaza. Bizonyítsuk be, hogy $(U_n, \cdot)$ részcsoportja $(\mathbb{C}^*, \cdot)$-nak.

Megoldás.

(1) $U_n \neq \emptyset$, mert $1 \in U_n$, mivel $1^n = 1$, minden $n \in \mathbb{N}^*$ esetén.

(2) Minden $z_1, z_2 \in U_n$ esetén $z_1 \cdot z_2 \in U_n$. Valóban, $z_1, z_2 \in U_n$, vagyis $z_1^n = z_2^n = 1$, ezért

$$(z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1 \cdot 1 = 1,$$

tehát $z_1 \cdot z_2 \in U_n$.

(3) Minden $z \in U_n$ esetén $z^{-1} \in U_n$. Valóban, minden $z \in U_n$, vagyis $z^n = 1$ esetén

$$z^{-1} \cdot z = 1 \;\Leftrightarrow\; (z^{-1} \cdot z)^n = 1^n \;\Leftrightarrow\; (z^{-1})^n \cdot z^n = 1 \;\Leftrightarrow\; (z^{-1})^n \cdot 1 = 1 \;\Leftrightarrow\; (z^{-1})^n = 1,$$

ezért $z^{-1} \in U_n$.

A fentiek alapján U_n részcsoportja $(\mathbb{C}^*, \cdot)$ csoportnak. $\square$

9. Legyen $n \in \mathbb{N}$, $n \geq 2$. Bizonyítsuk be, hogy:

(a) $GL_n(\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) | \det(A) \neq 0\}$ zárt részhalmaz az $(\mathcal{M}_n(\mathbb{C}), \cdot)$ monoidban;

Megoldás. Minden $A, B \in GL_n(\mathbb{C})$ esetén $\det A \neq 0$, $\det B \neq 0$, így

$$\det(A \cdot B) = \det A \cdot \det B \neq 0,$$

ezért $A \cdot B \in GL_n(\mathbb{C})$. Tehát $GL_n(\mathbb{C})$ zárt részhalmaza az $(\mathcal{M}_n(\mathbb{C}), \cdot)$ monoidnak. $\square$

(b) $(GL_n(\mathbb{C}), \cdot)$ csoport;

Megoldás. Igazolni kell, hogy a szorzás asszociatív, van semleges elem és minden elemnek van inverze.

- A mátrixok szorzása asszociatív, ezért a nem nulla determinánsú mátrixok szorzása is asszociatív.
- Az I_n identikus mátrix főátlóján 1-sek vannak, míg a többi eleme 0 és $\det I_n = 1$, ezért $I_n \in GL_n(\mathbb{C})$.
- Minden $A \in GL_n(\mathbb{C})$ mátrix invertálható és az inverz mátrixa $A^{-1} = \frac{A^*}{\det A}$, ahol A^* az A adjungáltja. Ekkor $\det A^{-1} = (\det A)^{-1} \neq 0$, így $A^{-1} \in GL_n(\mathbb{C})$, továbbá $A \cdot A^{-1} = A^{-1} \cdot A = I_n$.

$\square$

(c) $SL_n(\mathbb{C}) \leq GL_n(C)$, ahol $SL_n(\mathbb{C}) = \{A \in \mathcal{M}_n(\mathbb{C}) \mid \det(A) = 1\}$.

Megoldás.

- $SL_n(\mathbb{C}) \neq \emptyset$, mert $\det I_n = 1$, ezért $I_n \in SL_n(\mathbb{C})$.
- Minden $A, B \in SL_n(\mathbb{C})$, vagyis $\det A = \det B = 1$ esetén

$$\det(A \cdot B) = \det A \cdot \det B = 1 \cdot 1 = 1,$$

  ezért $A \cdot B \in SL_n(\mathbb{C})$.
- Minden $A \in SL_n(\mathbb{C})$, vagyis $\det A = 1$ esetén

$$\det(A^{-1}) = (\det A)^{-1} = 1^{-1} = 1,$$

  ezért $A^{-1} \in SL_n(\mathbb{C})$.

A fentiek alapján az $SL_n(\mathbb{C})$ részcsoportja a $(GL_n(\mathbb{C}), \cdot)$ csoportnak. $\square$

10. Legyen G egy csoport és $H_1, H_2 \leq G$ részcsoportok. Bizonyítsuk be, hogy:

(a) $H_1 \cap H_2 \leq G$;

Megoldás. Jelölje $e \in G$ a $(G, \cdot)$ csoport semleges elemét.

- Mivel H_1 és H_2 a G részcsoportjai, ezért $e \in H_1$ és $e \in H_2$, tehát $e \in H_1 \cap H_2$, vagyis $H_1 \cap H_2 \neq \emptyset$.
- Ha $g, h \in H_1 \cap H_2$, akkor $g, h \in H_1$ és $g, h \in H_2$. Mivel H_1 részcsoportja G-nek, ezért $g \cdot h^{-1} \in H_1$. Hasonlóan, mivel H_2 részcsoportja G-nek, ezért $g \cdot h^{-1} \in H_2$. Mivel $g \cdot h^{-1}$ benne van a H_1-ben és H_2-ben is, ezért benne van a metszetükben is, vagyis $g \cdot h^{-1} \in H_1 \cap H_2$.

Ezzel igazoltuk, hogy $H_1 \cap H_2$ is részcsoportja G-nek. $\square$

(b) $H_1 \cup H_2 \leq G \iff H_1 \subseteq H_2$ vagy $H_2 \subseteq H_1$.

Megoldás.

$\boxed{\Leftarrow}$ Ha $H_1 \subseteq H_2$, akkor $H_1 \cup H_2 = H_2$, amely részcsoportja a G-nek a feltevés szerint. Hasonlóan, ha $H_2 \subseteq H_1$, akkor $H_1 \cup H_2 = H_1$, amely részcsoportja a G-nek a feltevés szerint.

$\boxed{\Rightarrow}$ Be kell még látni, hogy ha $H_1 \cup H_2$ a G-nek, akkor $H_1 \subseteq H_2$ vagy $H_2 \subseteq H_1$. Az ezzel egyenértékű következő állítást fogjuk belátni. Ha $H_1 \nsubseteq H_2$ és $H_2 \nsubseteq H_1$, akkor létezik $h_1 \in H_1 \setminus H_2$ és $h_2 \in H_2 \setminus H_1$. Ekkor $h_1 \cdot h_2 \notin H_1 \cup H_2$, tehát $H_1 \cup H_2$ nem részcsoportja G-nek. Valóban, ha $h_1 \cdot h_2 \in H_1 \cup H_2$, akkor $h_1 \cdot h_2 \in H_1$ vagy $h_1 \cdot h_2 \in H_2$. Az első esetben, ha $h_1 \cdot h_2 = h_1' \in H_1$, akkor $h_2 = h_1^{-1} \cdot h_1' \in H_1$, mivel H_1 részcsoport. De ez ellentmondáshoz vezet, mert $h_2 \in H_2 \setminus H_1$, így $h_2 \notin H_1$. Az második esetben, ha $h_1 \cdot h_2 = h_2' \in H_2$, akkor $h_1 = h_2' \cdot h_2^{-1} \in H_2$, mivel H_2 részcsoport. De ez ellentmondáshoz vezet, mert $h_1 \in H_1 \setminus H_2$, így $h_1 \notin H_2$.

□

11. Igazoljuk, hogy minden $m \in \mathbb{Z}$ esetén $m\mathbb{Z} = \{m \cdot z \mid z \in \mathbb{Z}\}$ részcsoportja a $(\mathbb{Z}, +)$ csoportnak. Adjuk meg a $m\mathbb{Z} \cap n\mathbb{Z}$ metszetcsoportot!

Megoldás. Rögzítjük az $m \in \mathbb{Z}$ számot és igazolni fogjuk, hogy $m\mathbb{Z}$ részcsoportja a $(\mathbb{Z}, +)$ csoportnak.

- $m\mathbb{Z} \neq \emptyset$, mert $0 = m \cdot 0 \in m\mathbb{Z} = \{m \cdot z \mid z \in \mathbb{Z}\}$.
- Minden $z_1, z_2 \in m\mathbb{Z}$ (vagyis léteznek $n_1, n_2 \in \mathbb{Z}$ úgy, hogy $z_1 = m \cdot n_1$, $z_2 = m \cdot n_2$) esetén
$$z_1 - z_2 = m \cdot n_1 - m \cdot n_2 = m \cdot \underbrace{(n_1 - n_2)}_{\in \mathbb{Z}} \in m\mathbb{Z}.$$

Ezzel igazoltuk, hogy $m\mathbb{Z}$ részcsoportja a $(\mathbb{Z}, +)$ csoportnak.

Be fogjuk látni, hogy $m\mathbb{Z} \cap n\mathbb{Z} = \text{lkkt}(m, n)\mathbb{Z}$, ahol $k = \text{lkkt}(m, n) > 0$ az m és n legkisebb közös többszöröse. Ezt az egyenlőséget két oldali bennfoglaltatással fogjuk belátni.
Mivel $m \mid k$, vagyis $k = m \cdot M$, $M \in \mathbb{Z}$, ezért ha $z \in k\mathbb{Z}$, vagyis $z = k \cdot p$, $p \in \mathbb{Z}$, akkor $z = (m \cdot M) \cdot p = m \cdot (M \cdot p) \in m\mathbb{Z}$. Tehát $k\mathbb{Z} = \text{lkkt}\,(m, n)\mathbb{Z} \subseteq m\mathbb{Z}$. Hasonlóan belátható, hogy $k\mathbb{Z} = \text{lkkt}\,(m, n)\mathbb{Z} \subseteq n\mathbb{Z}$. Ezek alapján $k\mathbb{Z} = \text{lkkt}\,(m, n)\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$.
Fordítva, minden $z \in \mathbb{Z}$ esetén ha $m \mid z$ és $n \mid z$, akkor $k \mid z$, vagyis ha $z \in m\mathbb{Z}$ és $z \in n \in \mathbb{Z}$, akkor $z \in k\mathbb{Z} = \text{lkkt}\,(m, n)\mathbb{Z}$. Ez alapján $m\mathbb{Z} \cap n\mathbb{Z} \subseteq \text{lkkt}\,(m, n)\mathbb{Z}$.

Mivel $\text{lkkt}\,(m, n)\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ és $m\mathbb{Z} \cap n\mathbb{Z} \subseteq \text{lkkt}\,(m, n)\mathbb{Z}$, így $m\mathbb{Z} \cap n\mathbb{Z} = \text{lkkt}\,(m, n)\mathbb{Z}$. □

12. Határozzuk meg a következő elemek rendjét $GL_2(\mathbb{C})$-ben:
$$X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad Z = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Megoldás. Egy $(G, \cdot)$ csoportban a $g \in G$ elem rendje a legkisebb olyan n pozitív egész szám, amelyre
$$g^n = \underbrace{g \cdot \dots \cdot g}_{n\text{-szer}} = 1,$$
ahol $1 \in G$ a csoport egységeleme (semleges eleme). Ha nem létezik ilyen elem, akkor az elem rendje végtelen.

Megjegyezzük, hogy a $(GL_2(\mathbb{C}), \cdot)$ csoport semleges eleme $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Az X elem rendjének kiszámításához elkezdjük kiszámolni az X mátrix hatványait:
$$X^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$
Mivel $X = X^{-1} \neq I_2$ és $X^2 = I_2$, ezért az $X \in GL_2(\mathbb{C})$ rendje 2.

Hasonlóan az Y elem rendjének kiszámításához elkezdjük kiszámolni az Y mátrix hatványait:

$$Y^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad Y^3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \quad Y^4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.$$

Indukcióval belátható, hogy $Y^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ minden $k \in \mathbb{N}^*$ esetén. Valóban,

$$Y^{k+1} = Y^k \cdot Y = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

Mivel csak $k = 0$ esetén lesz $Y^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = I_2$, ezért az $Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{C})$ elem rendje végtelen.

Végül a Z elem rendjének kiszámításához elkezdjük kiszámolni az Z mátrix hatványait:

$$Z^2 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \; Z^3 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}^3 = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}, \; Z^4 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Így a $Z = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$ elem rendje 4. □

13. Legyen $f : \mathbb{C}^* \to \mathbb{R}^*$, $f(z) = |z|$ és $g : \mathbb{C}^* \to GL_2(\mathbb{R})$, $g(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Bizonyítsuk be a következő állításokat:

(a) f csoportmorfizmus $(\mathbb{C}^*, \cdot)$ és $(\mathbb{R}^*, \cdot)$ csoportok között és határozzuk meg a magját;

Megoldás. Az $f : \mathbb{C}^* \to \mathbb{R}^*$, $f(z) = |z|$ leképezés jól értelmezett, mert $|z| = 0 \;\Leftrightarrow\; z = 0$. Az f egy csoportmorfizmus a $(\mathbb{C}^*, \cdot)$ csoportról a $(\mathbb{R})$ csoportra, mert

$$f(z_1 \cdot z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2| = f(z_1) \cdot f(z_2),$$

minden $z_1, z_2 \in \mathbb{C}^*$ esetén.

Az f morfizmus magja $\ker f = \{z \in \mathbb{C}^* \mid f(z) = 1\}$ (1 az $(\mathbb{R}^*, \cdot)$ csoport semleges eleme), tehát

$$\ker f = \{z \in \mathbb{C}^* \mid |z| = 1\} = \{z = \cos\varphi + i \sin\varphi \in \mathbb{C}^* \mid \varphi \in [0, 2\pi)\}.$$

□

(b) g csoportmorfizmus $(\mathbb{C}^*, \cdot)$ és $(GL_2(\mathbb{R}), \cdot)$ csoportok között.

Megoldás. A $g : \mathbb{C}^* \to GL_2(\mathbb{R})$, $g(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ jól értelmezett, mivel ha $z = a + ib \neq 0$, akkor $\det g(a+ib) = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 \neq 0$. Továbbá $g : \mathbb{C}^* \to GL_2(\mathbb{C})$ egy csoportmorfizmus, mivel minden $a_1 + ib_1,\; a_2 + ib_2 \in \mathbb{C}^*$ esetén

$$\begin{aligned} g((a_1+ib_1)\cdot(a_2+ib_2)) &= g(a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1)) \\ &= \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \\ &= g(a_1+ib_1) \cdot g(a_2+ib_2). \end{aligned}$$

$\square$

14. Legyen $n \in \mathbb{N}$, $n \geq 2$. Bizonyítsuk be, hogy $(\mathbb{Z}_n, +)$ és $(U_n, \cdot)$ csoportok izomorfak.

Megoldás. Értelmezzük az $f : \mathbb{Z}_n \to U_n$, $f(\hat{k}) = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$ függvényt. Ez a függvény jól értelmezett, mivel nem függ a $\hat{k} \in \mathbb{Z}_n$ maradék osztály k reprezentánsától, illetve $f(\hat{k}) \in U_n$. Valóban, ha $\hat{\ell} = \hat{k}$, akkor $\ell = k + p \cdot n$, ahol $p \in \mathbb{Z}$, és

$$\begin{aligned} f(\hat{\ell}) &= \cos\left(\frac{2\pi\ell}{n}\right) + i \sin\left(\frac{2\pi\ell}{n}\right) = \cos\left(\frac{2\pi(k+pn)}{n}\right) + i \sin\left(\frac{2\pi(k+pn)}{n}\right) \\ &= \cos\left(\frac{2\pi k}{n} + 2\pi p\right) + i \sin\left(\frac{2\pi k}{n} + 2\pi p\right) = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \\ &= f(\hat{k}). \end{aligned}$$

Végül $f(\hat{k}) = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \in U_n$, mivel

$$\left[\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)\right]^n = \cos\left(n \cdot \frac{2\pi k}{n}\right) + i \sin\left(n \cdot \frac{2\pi k}{n}\right) = \cos(2\pi k) + i \sin(2\pi k) = 1.$$

Az f függvény egy csoportmorfizmus, mert minden $\hat{k}, \hat{h} \in \mathbb{Z}_n$ esetén

$$\begin{aligned} f(\hat{k} + \hat{h}) = f(\widehat{k+h}) &= \cos\left(\frac{2\pi(k+h)}{n}\right) + i \sin\left(\frac{2\pi(k+h)}{n}\right) \\ &= \left[\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)\right] \cdot \left[\cos\left(\frac{2\pi h}{n}\right) + i \sin\left(\frac{2\pi h}{n}\right)\right] \\ &= f(\hat{k}) \cdot f(\hat{h}). \end{aligned}$$

Az f függvény injektív, mert a magja $\ker f = \{\hat{0}\}$:

$$f(\hat{k}) = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) = 1 \;\Leftrightarrow\; \frac{2\pi k}{n} \in 2\pi\mathbb{Z} \;\Leftrightarrow\; k \in n\mathbb{Z} \;\Leftrightarrow\; \hat{k} = \hat{0}.$$

Az $U_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$ halmaznak legfeljebb n eleme van, mert a $z^n - 1 = 0$ egyenletnek legfeljebb n különböző gyöke lehet a komplex számok halmazán. Ezenkívül

$$z_k = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right), \quad k = 0, 1, \ldots, n-1$$

különböző gyökei a $z^n - 1 = 0$ egyenletnek, így az U_n halmaznak pontosan n eleme van, éspedig $U_n = \left\{\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \,\middle|\, k = 0, 1, \ldots, n-1\right\}$. Minden $k = 0, 1, \ldots, n-1$ esetén $f(\hat{k}) = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$, tehát f szürjektív.

Mivel f bijektív csoportmorfizmus, ezért csoportizomorfizmus, így a $(\mathbb{Z}_n, +)$ és $(U_n, \cdot)$ csoportok izomorfak. $\square$

15. Legyenek $(G, *)$ és $(G', \circ)$ csoportok (a semleges elemek 1, illetve $1'$) és $f : G \to G'$ csoportmorfizmus. Bizonyítsuk be, hogy:

(a) $f(1) = 1'$ és minden $x \in G$ csoportelem esetén $f(x^{-1}) = [f(x)]^{-1}$;

Megoldás. Az f csoportmorfizmus, ezért $f(1) = f(1*1) = f(1)\circ f(1)$, vagyis $f(1) = f(1)\circ f(1)$. Ezt szorozva (balról vagy jobbról) az $f(1) \in G'$ elem inverzével (szimmetrikusával) kapjuk, hogy $1' = f(1)$.

Az f csoportmorfizmus, ezért minden $x \in G$ elem és az inverze, x^{-1} esetén

$$1' = f(1) = f(x * x^{-1}) = f(x) \circ f(x^{-1}),$$

amelyet szorozva balról az $f(x)^{-1} \in G'$ elemmel kapjuk, hogy $f(x)^{-1} = f(x^{-1})$. □

(b) $\ker f = \{x \in G \mid f(x) = 1'\} \leq G$ és $\operatorname{Im} f \leq G'$;

Megoldás. A $\ker f \neq \emptyset$, mivel $1 \in \ker f$ az (a) alpont alapján. Továbbá, ha $x, y \in \ker f$, vagyis $f(x) = f(y) = 1'$, akkor

$$f(x * y^{-1}) = f(x) \circ f(y^{-1}) = f(x) \circ f(y)^{-1} = 1' \circ (1')^{-1} = 1',$$

mert f csoportmorfizmus és $1' \in G'$ semleges elem, továbbá az (a) alpont alapján. Ezzel igazoltuk, hogy $\ker f$ részcsoportja G-nek.

Az $\operatorname{Im} f \neq \emptyset$, mert $1' = f(1) \in \operatorname{Im} f$ az (a) alpont alapján. Ha $x', y' \in \operatorname{Im} f$, vagyis $x' = f(x)$ és $y' = f(y)$ valamely $x, y \in G$ esetén, akkor az (a) alpont alapján

$$x' \circ (y')^{-1} = f(x) \circ [f(y)]^{-1} = f(x) \circ f(y^{-1}) = f(x * y^{-1}) \in \operatorname{Im} f$$

Ezzel igazoltuk, hogy $\operatorname{Im} f$ részcsoportja G'-nek. □

(c) $\ker f = \{1\}$ akkor és csakis akkor, ha f injektív;

Megoldás. Ha f injektív, akkor a $\ker f = f^{-1}(1')$ halmaznak 1 az egyetlen eleme, vagyis $\ker f = \{1\}$. Fordítva, ha $\ker f = \{1\}$, akkor

$$f(x) = f(y) \Leftrightarrow f(x) \circ f(y)^{-1} = 1' \Leftrightarrow f(x) \circ f(y^{-1}) = 1' \Leftrightarrow f(x * y^{-1}) = 1' \Leftrightarrow x * y^{-1} = 1 \Leftrightarrow x = y,$$

vagyis f injektív. □

(d) ha $H \leq G$ és $H' \leq G'$ akkor és csakis akkor, ha $f(H) \leq G'$ és $f^{-1}(H') \leq G$.

Megoldás. Legyen H a G egy részcsoportja. Ekkor $1 \in H$, így $f(1) = 1' \in f(H)$, vagyis $f(H) \neq \emptyset$. Továbbá, tetszőleges $x, y \in f(H)$ esetén léteznek $g, h \in G$ úgy, hogy $x = f(g)$ és $y = f(h)$, így

$$x \circ y^{-1} = f(g) \circ f(h)^{-1} = f(g) \circ f(h^{-1}) = f(g * h^{-1}) \in f(G)$$

az (a) alpont alapján és mivel G részcsoport. Ezzel beláttuk, hogy $f(G)$ részcsoportja a G' csoportnak.

Ha H' egy részcsoportja a G' csoportnak, akkor az $f^{-1}(H') = \{h \in H \mid f(h) \in H'\}$ halmaz nem üres, mert $1' \in H'$ és az $f(1) = 1'$ alapján $1 \in f^{-1}(H')$. Ezenkívül, ha $g, h \in f^{-1}(H')$, vagyis $f(g), f(h) \in H'$, akkor

$$f(g * h^{-1}) = f(g) \circ f(h^{-1}) = f(g) \circ f(h)^{-1} \in H',$$

vagyis $g * h^{-1} \in f^{-1}(H)$, az (a) alpont alapján és mivel H' részcsoport. Ezzel beláttuk, hogy $f^{-1}(H')$ a G részcsoportja. □

További feladatok

16. Legyen $a \in \mathbb{R}^*$. Igazoljuk, hogy $f_a : (\mathbb{R}, +) \to (\mathbb{R}, +)$, $f_a(x) = a \cdot x$ egy csoportizomorfizmus és adjuk meg az inverzét!

Megoldás. Legyen $a \in \mathbb{R}^*$ rögzített. Minden $x, y \in \mathbb{R}$ esetén $f_a(x+y) = a \cdot (x+y) = a \cdot x + a \cdot y = f_a(x) + f_a(y)$, tehát $f_a : \mathbb{R} \to \mathbb{R}$, $f_a(x) = a \cdot x$ egy csoportmorfizmus az $(\mathbb{R}, +)$ csoportról önmagára.

Az f_a inverze $f_{\frac{1}{a}}$, mivel minden $x \in \mathbb{R}$ esetén

$$\left(f_a \circ f_{\frac{1}{a}}\right)(x) = f_a\left(f_{\frac{1}{a}}\right)(x) = f_a\left(\frac{1}{a} \cdot x\right) = a \cdot \left(\frac{1}{a} \cdot x\right) = x,$$

$$\left(f_{\frac{1}{a}} \circ f_a\right)(x) = f_{\frac{1}{a}}\left(f_a\right)(x) = f_{\frac{1}{a}}\left(a \cdot x\right) = \frac{1}{a} \cdot (a \cdot x) = x.$$

□

17. Igazoljuk, hogy

(a) $f : (\mathbb{C}, +) \to (\mathbb{C}, +)$, $f(z) = \bar{z}$;

(b) $f : (\mathbb{C}^*, \cdot) \to (\mathbb{C}^*, \cdot)$, $f(z) = \bar{z}$;

(c) $f : (H, \cdot) \to (H, \cdot)$, $f(z) = \bar{z}$, ahol $H = \{z \in \mathbb{C} \mid |z| = 1\}$

csoportizomorfizmusok és adjuk meg az inverzüket.

Megoldás.

(a) Az $f : \mathbb{C} \to \mathbb{C}$, $f(z) = z$ csoportmorfizmus a $(\mathbb{C}, +)$ csoportról önmagára, mert minden $z = a + ib, w = c + id \in \mathbb{C}$ esetén

$$\begin{aligned} f(z + w) &= f((a + ib) + (c + id)) = \overline{(a + id) + (c + id)} = (a - ib) + (c - id) \\ &= \overline{a + ib} + \overline{c + id} = f(a + ib) + f(c + id) \\ &= f(z) + f(w). \end{aligned}$$

Az f inverze $f^{-1}(z) = f(z) = \overline{z}$, mivel minden $z = a + bi \in \mathbb{C}$ esetén

$$\begin{aligned} (f \circ f)(z) &= (f \circ f)(a + ib) = f(f(a + ib)) = f(\overline{a + ib}) \\ &= \overline{\overline{a + ib}} = \overline{a - ib} = a + ib \\ &= z. \end{aligned}$$

Tehát f egy bijektív csoportmorfizmus, így csoportizomorfizmus.

(b) Az $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(z) = \overline{z}$ függvény jól értelmezett, mert ha $z \neq 0$, akkor $\overline{z} \neq 0$. Az f egy csoportmorfizmus, mert minden $z = a + ib, w = c + id \in \mathbb{C}^*$ esetén

$$\begin{aligned} f(z \cdot w) &= \overline{z \cdot w} = \overline{(a + ib)(c + id)} = \overline{(ac - bd) + i(ad + bc)} \\ &= (ac - bd) - i(ad + bc) = (a - ib)(c - id) = \overline{a + ib} \cdot \overline{c + id} \\ &= \overline{z} \cdot \overline{w} = f(z) \cdot f(w) \end{aligned}$$

Az f inverze az előző alponthoz hasonlóan $f^{-1}(z) = f(z) = \overline{z}$. Tehát f egy bijektív csoportmorfizmus, vagyis csoportizomorfizmus.

(c) Az $f : H \to H$, $f(z) = \overline{z}$ függvény jól értelmezett, mert $|z| = |\overline{z}|$, ezért ha $z \in H$, vagyis $|z| = 1$, akkor $|\overline{z}| = 1$, vagyis $f(z) = \overline{z} \in H$. Az előző alponthoz hasonlóan f egy csoportmorfizmus, továbbá bijektív, mert $f^{-1}(z) = f(z) = \overline{z}$, minden $z \in H$ esetén. Tehát f egy csoportizomorfizmus.

□

18. Igazoljuk, hogy $exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, $exp(x) = e^x$ egy csoportizomorfizmus, ahol $\mathbb{R}_{>0} = (0, +\infty)$. Határozzuk meg az exp csoportizomorfizmus az inverzét! Írjuk fel, hogy mit jelent, hogy az inverz is csoportmorfizmus!

Megoldás. Minden $x, y \in \mathbb{R}$ esetén

$$exp(x + y) = e^{x+y} = e^x e^y = exp(x) \cdot exp(y),$$

ezért exp egy csoportmorfizmus. Az exp függvény bijektív, mert $exp^{-1}(x) = \ln x$, minden $x \in (0, +\infty)$. Bijektív csoportmorfizmus inverze is csoportmorfizmus, ezért $\ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ is csoportmorfizmus, vagyis minden $x, y \in \mathbb{R}_{>0} = (0, +\infty)$ esetén $\ln(x \cdot y) = \ln x + \ln y$. □

19. Legyen $H = \{z \in \mathbb{C} \mid |z| = 1\}$. Igazoljuk, hogy $\varphi : (\mathbb{R}, +) \to (H, \cdot)$, $\varphi(x) = \cos x + i \sin x$ egy csoportmorfizmus és határozzuk meg a magját.

Megoldás. Minden $x, y \in \mathbb{R}$ esetén

$$f(x+y) = \cos(x+y) + i\sin(x+y) = (\cos x + i\sin x)(\cos y + i\sin y) = f(x)\cdot f(y),$$

ezért f egy csoportmorfizmus. Az f csoportmorfizmus magja

$$\begin{aligned}\ker f &= \{x \in \mathbb{R} | f(x) = 1\} = \{x \in \mathbb{R} | \cos x + i\sin x = 1\}\\ &= \{x \in \mathbb{R} \,|\, \cos x = 1 \text{ és } \sin x = 0\} = \{2k\pi \,|\, k \in \mathbb{Z}\}.\end{aligned}$$

□

20. Igazoljuk, hogy $f : (\mathbb{Z}, +) \to (U_n, \cdot)$, $f(k) = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$ egy csoportmorfizmus. Határozzuk meg a magját!

Megoldás. Minden $k, h \in \mathbb{Z}$ esetén

$$\begin{aligned}f(k+h) &= \cos\left(\frac{2(k+h)\pi}{n}\right) + i\sin\left(\frac{2(k+h)\pi}{n}\right)\\ &= \cos\left(\frac{2k\pi}{n} + \frac{2h\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n} + \frac{2h\pi}{n}\right)\\ &= \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)\cdot\left(\cos\frac{2h\pi}{n} + i\sin\frac{2h\pi}{n}\right)\\ &= f(k)\cdot f(h),\end{aligned}$$

tehát f csoportmorfizmus. Az f csoportmorfizmus magja

$$\begin{aligned}\ker f &= \{k \in \mathbb{Z} \,|\, f(k) = 1\} = \left\{k \in \mathbb{Z} \,\middle|\, \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = 1\right\}\\ &= \left\{k \in \mathbb{Z} \,\middle|\, \frac{2k\pi}{n} \in 2\pi\mathbb{Z}\right\} = \{k \in \mathbb{Z} \,|\, k \in n\mathbb{Z}\} = n\mathbb{Z}.\end{aligned}$$

□

21. Legyen $(G, +)$ egy csoport és $H \leq G$ egy részcsoportja. Igazoljuk, hogy

$$x\rho y \;\Leftrightarrow\; x - y \in H, \qquad x, y \in G,$$

egy ekvivalenciareláció a G-n. Ebben az esetben a $G/\rho = \{\rho(g) \,|\, g \in G\}$ faktorhalmazt G/H-val jelöljük. Ha $(G, +)$ kommutatív csoport, akkor igazoljuk, hogy $(G/H, \oplus)$ is egy csoport a $\rho(g_1) \oplus \rho(g_2) = \rho(g_1 + g_2)$, minden $\rho(g_1), \rho(g_2) \in G/\rho$ művelettel.