Algebrai struktúrák

1. A Példatár 4.2.1., 4.2.3., 4.2.4. feladataiból

Eml.:

$(G;\circ)$ **félcsoport**, ha :	$(G;\circ)$ **csoport**, ha :
G zárt a $\circ$ műveletre	G zárt a $\circ$ műveletre
$\circ$ kétváltozós	$\circ$ kétváltozós
$\circ$ asszociatív	$\circ$ asszociatív
	létezik egységelem
	minden elemnek létezik inverze

megj.: a $\circ$ művelet neve: "kompozíció". (Vigyázat: a művelet konkrét esetben tetszőleges kétváltozós st. művelet lehet!)

4.2.1. Félcsoport-e? Amennyiben igen, van-e egység- ill. zéruselem?

(a) $(\mathcal{P}(H);\Delta)$, ahol $\mathcal{P}(H)$ a H halmaz hatványhalmaza és Δ a szimmetrikus differencia;
Mo.:
a szimmetrikus differencia kétváltozós művelet
műveleti zártság: $X, Y \in \mathcal{P}(H) \;\Rightarrow\; X \,\Delta\, Y \in \mathcal{P}(H)$ (hiszen $X, Y \subseteq H \Rightarrow X \,\Delta\, Y \subseteq H$)
asszociativitás: $\forall\, X, Y, Z \in \mathcal{P}(H) \quad X \,\Delta\, (Y \,\Delta\, Z) = (X \,\Delta\, Y) \,\Delta\, Z$ (pl. Venn-diagrammal!)
Kaptuk: $(\mathcal{P}(H);\Delta)$ félcsoport.

egységelem: $\emptyset$ egységelem, mert $\forall\, X \in \mathcal{P}(H) \quad X \,\Delta\, \emptyset = \emptyset \,\Delta\, X = X$
zéruselem: nincs
(megj.: minden elemnek létezik inverze: minden elem inverze önmaga, mert $X \,\Delta\, X = \emptyset$.
Ezért $(\mathcal{P}(H);\Delta)$ csoport.)

(b) $(V\,;\,\cdot)$ ahol V a háromdimenziós vektorok halmaza, $\cdot$ a skaláris szorzás;
Mo.:
Az alaphalmaz nem zárt a műveletre: $v_1, v_2 \in V \not\Rightarrow v_1 \cdot v_2 \in V$; sőt: $v_1, v_2 \in V \Rightarrow v_1 \cdot v_2 \notin V$
$(V\,;\,\cdot)$ nem algebrai struktúra, ezért nem is félcsoport.

(c) $(V\,;\,\times)$ ahol V a háromdimenziós vektorok halmaza, $\times$ a vektoriális szorzás;
Mo.:
A vektoriális szorzás nem asszociatív művelet: általában $v_1 \times (v_2 \times v_3) \neq (v_1 \times v_2) \times v_3$
$(V\,;\,\times)$ nem félcsoport.

4.2.3. Bizonyítsa be, hogy az $\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$ alakú mátrixok ($n \in \mathbb{N}$) a szorzásra nézve félcsoportot alkotnak és ez a félcsoport izomorf az $(\mathbb{N}\,;+)$ félcsoporttal.
Mo.:
Jelöljük M-mel az $\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$ alakú mátrixok halmazát.

Először belátjuk, hogy $(\mathrm{M}\,,\,\cdot)$ félcsoport:

műveleti zártság: $\begin{bmatrix}1 & m\\0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & n\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & m+n\\0 & 1\end{bmatrix}$, továbbá $m, n \in \mathbb{N} \Rightarrow m + n \in \mathbb{N}$, vagyis az alaphalmaz zárt a műveletre.
asszociativitás: a mátrixszorzás általában asszociatív, tehát itt is.
Kaptuk: $(\mathrm{M}\,,\,\cdot)$ félcsoport.

Az izomorfia bizonyítása előtt tekintsük át M elemeit:
$$\mathrm{M} = \left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 2\\0 & 1\end{bmatrix}, \ldots, \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}, \ldots\right\}.$$

Hasonlóan: $\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$.
Megadunk egy φ művelettartó bijekciót a két megszámlálhatóan végtelen számosságú halmaz között. A fenti sorbarendezésekkel adódik egy triviális bijekció a két halmaz között, kérdés, művelettartó-e:
Tekintsük a $\varphi : \mathrm{M} \to \mathbb{N}$ leképezést, amelyre $\varphi\left(\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}\right) = n$. Ez nyilvánvalóan bijekció a két halmaz között.

Továbbá:
$$\varphi\left(\begin{bmatrix}1 & m\\0 & 1\end{bmatrix}\cdot\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}\right)=\varphi\left(\begin{bmatrix}1 & m+n\\0 & 1\end{bmatrix}\right)=m+n=\varphi\left(\begin{bmatrix}1 & m\\0 & 1\end{bmatrix}\right)+\varphi\left(\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}\right),$$
tehát φ művelettartó.
Ezzel beláttuk, hogy: $(\mathrm{M}\,,\,\cdot)\cong(\mathbb{N}\,;\,+)$.

megj.: a művelettartás mint tulajdonság könnyen jegyezhető alakban: "kompozíció képe a képek kompozíciója". A példában az első félcsoport kompozíciója a mátrixszorzás, a másik félcsoporté a (számok) összeadása.

4.2.4. Az alábbiak közül melyek alkotnak csoportot?

(a) A valós számok halmaza, ha a művelet a szorzás.
Mo.:
a szorzás kétváltozós művelet
műveleti zártság: $x, y\in\mathbb{R}\Rightarrow x\cdot y\in\mathbb{R}$
asszociativitás: $\forall x,y,z\in\mathbb{R}\quad x\cdot(y\cdot z)=(x\cdot y)\cdot z$ (axióma)
egységelem: az 1 egységelem, mert $\forall x\in\mathbb{R}\ \ 1\cdot x=x\cdot 1=x$
inverz: minden nem-nulla szám inverze a szám reciproka: $\forall x\in\mathbb{R}\setminus\{0\}\quad x^{-1}=\frac{1}{x}$, de a 0-nak nincs inverze.
Ez utóbbi miatt: $(\mathbb{R}\,;\,\cdot)$ nem csoport.

(b) A pozitív valós számok halmaza, ha a művelet a szorzás.
HF.: $(\mathbb{R}^+\,;\,\cdot)$ csoport.

(c) A pozitív valós számok halmaza, ha a művelet az osztás.
Mo.:
Az osztás művelete nem asszociatív: általában $x:(y:z)\neq(x:y):z$,
mert $x:(y:z)=\frac{xz}{y}$ és $(x:y):z=\frac{x}{yz}$.
Továbbá nincs egységelem: $\nexists e\in\mathbb{R}\quad\forall x\in\mathbb{R}\quad e:x=x:e=x$
Kaptuk: $(\mathbb{R}^+\,;\,:)$ nem csoport.

(d) Az $A=\{1,2,3,4,5,6,7\}$ halmaz, ha a művelet a mod8 szorzás.
A mod8 szorzás műveleti jele: $\otimes_8$

Néhány példa a számolásra:
$2\otimes_8 3=6$
$2\otimes_8 4=0$
$3\otimes_8 4=4$
$5\otimes_8 6=6$
$3\otimes_8 5=7$
stb.

Látható, hogy a művelet kivezet az alaphalmazból, mert pl. $2\otimes_8 4=0\notin A$.
Kaptuk: $(A\,;\,\otimes_8)$ nem csoport.

(e) A $B=\{1,3,5,7\}$ halmaz a mod8 szorzásra nézve.
HF.: $(B\,;\,\otimes_8)$ csoport.

2. Legyen $A=\{a,b,c,d\}$. Tekintsük a $\varphi: A\to A$ leképezések $T(A)$ halmazát a kompozíció művelettel: $(T(A);\circ)$.

(a) Az egyes leképezéseket értéktáblájukkal jelölve (ld. tankönyv 94-95. old.), gyakoroljuk a kompozíció műveletét a $(T(A);\circ)$ transzformáció-félcsoportban.

$$T(A)=\left\{\begin{pmatrix}a & b & c & d\\a & b & c & d\end{pmatrix},\begin{pmatrix}a & b & c & d\\a & b & d & c\end{pmatrix},\dots,\begin{pmatrix}a & b & c & d\\a & a & c & a\end{pmatrix},\dots,\begin{pmatrix}a & b & c & d\\b & b & b & b\end{pmatrix},\dots\right\}$$

$T(A)$ neve: A **teljes transzformáció-félcsoportja** (részfélcsoportjai: A **transzformáció-félcsoportjai**)

$|T(A)| =$ ahány 4-hosszú a,b,c,d sorozat van, ha ismétlődés megengedett $=V^i_{4,4}=4^4=256$

$\begin{pmatrix}a & b & c & d\\d & b & a & d\end{pmatrix}$ egy leképezés az $a\mapsto d$, $b\mapsto b$, $c\mapsto a$, $d\mapsto d$ hozzárendelési szabállyal.

Két leképezés kompozíciója képezésekor ügyelnünk kell, melyik a belső ill. melyik a külső függvény:

$$\underbrace{\begin{pmatrix}a & b & c & d\\a & c & d & d\end{pmatrix}}_{\text{külső}}\circ\underbrace{\begin{pmatrix}a & b & c & d\\d & c & a & c\end{pmatrix}}_{\text{belső}}=\begin{pmatrix}a & b & c & d\\d & d & a & d\end{pmatrix}$$

Itt a kompozíció a következő hozzárendelési szabállyal tekintendő:

$$\begin{aligned} &a \mapsto d \mapsto d \\ &b \mapsto c \mapsto d \\ &c \mapsto a \mapsto a \\ &d \mapsto c \mapsto d \end{aligned}$$

Hasonlóan:

$$\begin{pmatrix} a & b & c & d \\ d & b & a & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & b & d & a \end{pmatrix}$$

(b) Igazoljuk, hogy $(T(A);\circ)$ félcsoport. Csoport-e?

Mo.:
A $\circ$ kétváltozós művelet.
műveleti zártság: triviálisan teljesül
asszociativitás: leképezések kompozíciója általában asszociatív
HF.: Lássuk be, hogy pl.

$$\left[\begin{pmatrix} a & b & c & d \\ a & a & d & d \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ b & c & b & a \end{pmatrix}\right] \circ \begin{pmatrix} a & b & c & d \\ d & b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & a & d & d \end{pmatrix} \circ \left[\begin{pmatrix} a & b & c & d \\ b & c & b & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ d & b & c & a \end{pmatrix}\right]$$

Kaptuk: $\boldsymbol{(T(A);\circ)}$ **félcsoport**.

Továbbá:
egységelem: $\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$ egységelem (identikus leképezés)
Ezzel tetszőleges $T(A)$-beli $\begin{pmatrix} a & b & c & d \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ elemre:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$$

Itt $i_1\ i_2\ i_3\ i_4$ az $a\ b\ c\ d$ elemek egy permutációja.

HF.: Lássuk be, hogy pl.:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & c & d & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & c & d & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & c & d & a \end{pmatrix}$$

inverz: pl. az $\begin{pmatrix} a & b & c & d \\ a & a & c & c \end{pmatrix}$ elemnek nincs inverze:

$$\underbrace{\begin{pmatrix} a & b & c & d \\ a & a & c & c \end{pmatrix}}_{\text{elem}} \circ \underbrace{\begin{pmatrix} a & b & c & d \\ a & ? & c & ? \end{pmatrix}}_{\text{inverze}} = \underbrace{\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}}_{\text{egység}}$$

A belső függvény nem tud úgy elemet rendelni b-hez ill. d-hez, hogy a b ill. d elemek kompozíció általi képe b ill. d legyen.

megj.: csak a bijektív elemeknek van inverze.

Kaptuk: $(T(A);\circ)$ nem csoport.

(c) Részfélcsoport-e $(\{\alpha,\beta\};\circ)$, ha

$$\alpha = \begin{pmatrix} a & b & c & d \\ a & a & b & b \end{pmatrix} \qquad \beta = \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix}.$$

Mo.:

eml.: *részfélcsoport*: "részhalmaz és félcsoport ugyanazzal a művelettel"

$\{\alpha,\beta\}$ egy kételemű részhalmaza $T(A)$-nak. Azt kell még belátnunk, hogy $(\{\alpha,\beta\};\circ)$ félcsoport.
műveleti zártság: tételesen ellenőrizzük az összes lehetséges elempárral:

$$\begin{pmatrix} a & b & c & d \\ a & a & b & b \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & a & b & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \quad \Rightarrow \quad \alpha\circ\alpha = \beta \in \{\alpha,\beta\}$$

$$\begin{pmatrix} a & b & c & d \\ a & a & b & b \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \quad \Rightarrow \quad \alpha \circ \beta = \beta \in \{\alpha, \beta\}$$

$$\begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \quad \Rightarrow \quad \beta \circ \beta = \beta \in \{\alpha, \beta\}$$

$$\begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & a & b & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & a & a & a \end{pmatrix} \quad \Rightarrow \quad \beta \circ \alpha = \beta \in \{\alpha, \beta\}$$

asszociativitás: öröklődik $(T(A); \circ)$-ból.

Kaptuk: Az $\boldsymbol{(\{\alpha, \beta\}\,;\circ)}$ algebrai struktúra a $\boldsymbol{(T(A);\circ)}$ teljes-transzfomáció-félcsoportnak egy **részfélcsoportja**. (Azaz: $T(A)$ egy transzformáció-félcsoportja)

(d) Legyenek $S(A)$ elemei $T(A)$ bijektív elemei. Részfélcsoport-e $(S(A); \circ)$? Csoport-e?
Mo.:
$T(A)$ bijektív elemei A permutációi:

$$S(A) = \left\{ \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix}, \ldots, \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \right\}$$

A táblázatok alsó sorában az $a\ b\ c\ d$ elemek egy-egy permutációja áll.

$$|S(A)| = P_4 = 4! = 24$$

$$S(A) \subseteq T(A)$$

műveleti zártság: bijektív leképezések kompozíciója bijektív (spec.: permutációk egymásutánja permutáció)
asszociativitás: öröklődik $(T(A); \circ)$-ból.
Eddig: $(S(A); \circ)$ félcsoport; részfélcsoport $(T(A); \circ)$-ban.
Továbbá:
egységelem: $\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$ egységelem (identikus leképezés)
inverz: $S(A)$ minden elemének van inverze: $\begin{pmatrix} a & b & c & d \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ inverze $\begin{pmatrix} i_1 & i_2 & i_3 & i_4 \\ a & b & c & d \end{pmatrix}$

(megj.: az inverz leképezés általános alakjában a felső sorban az $a\ b\ c\ d$ elemek nem a megszokott ábécérendben állnak (kivéve, ha az egységelem inverzéről van szó). Az egyértelműséget ez nem befolyásolja.)

Pl.: az $\begin{pmatrix} a & b & c & d \\ c & b & d & a \end{pmatrix}$ elem inverze $\begin{pmatrix} c & b & d & a \\ a & b & c & d \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$.

Kaptuk: $\boldsymbol{(S(A);\circ)}$ **csoport**. Név: A **szimmetrikus csoportja**

megj.: $(S(A); \circ)$ nem részcsoportja $(T(A); \circ)$-nak, mert ez utóbbi nem csoport.

$S(A)$ részcsoportjai: A **permutációcsoportjai**

(e) megj.: A permutációk ún. táblázatos írásmódjának alternatívája az ún. **ciklikus írásmód**.
def.: **ciklus** olyan $(i_1 i_2 \ldots i_k)$ permutáció, amelyben a hozzárendelési szabály a következő:

$$i_1 \mapsto i_2 \mapsto \ldots \mapsto i_k \mapsto i_1$$

pl.:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} = (1243)(5)$$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$ tehát egy 4-hosszú és egy 1-hosszú ciklus szorzataként írható fel.

Megj.: a "szorzat" szó itt szimbolikusan értendő, nem műveletként.

Egy ciklus első eleme a balzárójel utáni elem, utolsó eleme a jobbzárójel előtti elem; minden elem képe a ciklusban utána álló elem, ciklus utolsó elemének képe a ciklus első eleme.

Tétel: Minden permutáció felírható diszjunkt ciklusok szorzataként (a ciklusok sorrendjétől eltekintve egyértelműen).

Pl.:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (12)(345) = (345)(12)$$

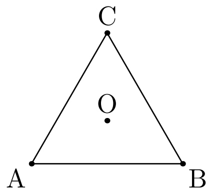
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = (12534)$$

Permutációk kompozíciója ciklikus írásmódban:
itt is: arra kell csak vigyáznunk, hogy először a belső, majd a külső függvény hozzárendelési szabályát kövessük. Pl.:

$$\underbrace{(124)(3)(5)}_{\text{külső}} \circ \underbrace{(1)(234)(5)}_{\text{belső}} = (123)(4)(5)$$

3. Írja le ciklikus írásmóddal **a szabályos háromszög forgáscsoportjának** elemeit!

A szóban forgó csoport elemei: egy szabályos háromszöget önmagába vivő síktranszformációk, azaz a szabályos háromszög forgásegybevágóságai a síkon. A művelet: kompozíció (síktranszformációk kompozíciója). Szokásos jelöléssel: $(F_3; \circ)$. A megoldásban kihasználjuk, hogy egy egybevágóság a háromszög csúcspontjait a háromszög csúcspontjaiba viszi bijektív módon, azaz egy egybevágóság egyértelműen leírható a háromszög csúcspontjai permutációjaként.



$$F_3 = \{e, f, f^2\}$$

Mo.:

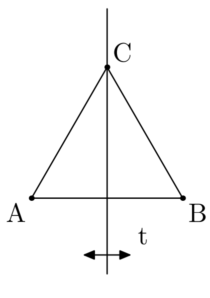
$$\begin{array}{ccccccc} e & = & \text{O középpontú 0°-os forgatás} & = & \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} & = & (A)(B)(C) \\ f & = & \text{O középpontú 120°-os forgatás} & = & \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} & = & (ABC) \\ f^2 & = & \text{O középpontú 240°-os forgatás} & = & \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} & = & (ACB) \end{array}$$

A forgatás pozitív forgásirányban értendő (óramutató járásával ellenkezőleg).

megj.: $f^3 = e$, $e^{-1} = e$, $f^{-1} = f^2$, $(f^2)^{-1} = f$, $f^2 \circ f^2 = f$ stb.

4. Írja le ciklikus írásmóddal a szabályos háromszög szimmetriáit!
(Név: **a szabályos háromszög diéder-csoportja**)
Igaz-e ebben a csoportban az $(ABC) \circ (A)(BC) = (AB)(C)$ egyenlőség?

$$D_3 = \{e, f, f^2, t, ft, f^2t\}$$



Mo.:

Itt e , f , f^2 mint előbb, továbbá:

$t =$ az AB szakasz felezőmerőlegesére való tengelyes tükrözés =

$= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = (AB)(C)$

$ft =$ az AB szakasz felezőmerőlegesére való tengelyes tükrözés és O kp-ú 120°-os forgatás egymásutánja =

$= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = (AC)(B)$

$f^2t =$ az AB szakasz felezőmerőlegesére való tengelyes tükrözés és O kp-ú 240°-os forgatás egymásutánja =

$= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = (A)(BC)$

megj.: $|D_3| = 6 = 3! =$ az A B C elemek összes permutációinak a száma.

(Kölcsönösen egyértelmű a megfelelés D_3 elemei és az A B C elemek összes permutációi között.)

megj.: $t^2 = f^3 = e$, $tf = t \circ f = f^2t$, $tf^2 = t \circ f^2 = ft$,
$t^{-1} = t$, $(ft)^{-1} = ft$, $(f^2t)^{-1} = f^2t$
$t \circ ft = t \circ tf^2 = e \circ f^2 = f^2$,
$f \circ tf = f \circ f^2t = f^3t = e \circ t = t$ stb.

Igaz-e ebben a csoportban az $(ABC) \circ (A)(BC) = (AB)(C)$ egyenlőség?

I. mo.: áttérünk táblázatos alakra:
b.o.: $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$

j.o.: $\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$

A bal- és jobboldali elem megegyezik, tehát igaz az állítás.

II. mo.: elmagyarázzuk a hozzárendelési szabályt:
b.o.: $A \mapsto A \mapsto B$, $B \mapsto C \mapsto A$, $C \mapsto B \mapsto C$
j.o.: $A \mapsto B$, $B \mapsto A$, $C \mapsto C$
A bal- és jobboldali elem hozzárendelési szabálya megegyezik, tehát igaz az állítás.

III. mo.: a diédercsoport elemeiben gondolkodva:
b.o.: $f \circ f^2t = f^3t = et = t$
j.o.: t (ld. fent)
A bal- és jobboldali elem megegyezik, tehát igaz az állítás.

5. Mutassa meg, hogy $(\mathbb{Z}_3; \oplus_3)$ és a szabályos háromszögek forgáscsoportja izomorf egymással! Mutassa meg, hogy mindegyik izomorf a Π_3 permutációcsoporttal!

I. mo.

1. áll.: $(\mathbb{Z}_3; \oplus_3) \cong (F_3; \circ)$
biz.: $\mathbb{Z}_3 = \{0, 1, 2\}$, $\oplus_3$ a mod3 összeadás. Tekintsük át szisztematikusan a műveleti eredményeket a két csoportban:

$(\mathbb{Z}_3; \oplus_3)$	$(F_3; \circ)$
$0 \oplus_3 0 = 0$	$e \circ e = e$
$0 \oplus_3 1 = 1$	$e \circ f = f$
$0 \oplus_3 2 = 2$	$e \circ f^2 = f^2$
$1 \oplus_3 0 = 1$	$f \circ e = f$
$1 \oplus_3 1 = 2$	$f \circ f = f^2$
$1 \oplus_3 2 = 0$	$f \circ f^2 = e$
$2 \oplus_3 0 = 2$	$f^2 \circ e = f^2$
$2 \oplus_3 1 = 0$	$f^2 \circ f = e$
$2 \oplus_3 2 = 1$	$f^2 \circ f^2 = f$

Mindkét csoportban az összes lehetséges elempárral elvégeztük a műveletet.

Ezek után megadunk egy művelettartó bijekciót a két halmaz között:

$$\varphi : \mathbb{Z}_3 \to F_3 \qquad \text{ahol} \qquad \begin{array}{l} \varphi(0) = e \\ \varphi(1) = f \\ \varphi(2) = f^2 \end{array}$$

φ nyilvánvalóan bijekció a két halmaz között,
a művelettartás pedig a fenti táblázatban pontról pontra ellenőrizhető:
tetszőleges $a, b \in \mathbb{Z}_3$ esetén $\varphi\,(a \oplus_3 b) = \varphi(a) \circ \varphi(b)$ (vagyis, hogy "kompozíció képe a képek kompozíciója")

pl.:

$$\left.\begin{array}{l} \varphi(1 \oplus_3 2) = \varphi(1) \circ \varphi(2), \text{mert} \\ \text{b.o.: } \varphi(1 \oplus_3 2) = \varphi(0) = e \\ \text{j.o.: } \varphi(1) \circ \varphi(2) = f \circ f^2 = e \end{array}\right\} \qquad \text{Ezt demonstrálja az előbbi 9 soros táblázat 6. sora.}$$

Az öszes többi a, b elempárra hasonlóan kiolvasható a táblázatból az összefüggés.
Kaptuk: $(\mathbb{Z}_3; \oplus_3) \cong (F_3; \circ)$

megj.: $(\mathbb{Z}_3; \oplus_3)$ csoportban $0^{-1} = 0$, $1^{-1} = 2$, $2^{-1} = 1$.

2. áll.: Mindkét csoport izomorf a Π_3 permutációcsoporttal.
biz.: $(\Pi_3; \circ)$ permutációcsoport részcsoport az $(S_3; \circ)$ szimmetrikus csoportban.
(Itt az S_3 halmaz korábbi jelölésekkel $S(A)$-nak gondolandó, ahol A egy háromelemű halmaz. Mivel az, hogy konkrétan mik ennek az A halmaznak az elemei, strukturális szempontból teljesen mindegy, ezért elhagyhatjuk az A-ra történő utalást, és elég csupán alsó indexben jelölnünk, hogy háromelemű halmaz szimmetrikus csoportjáról van szó. A feladatban mindazonáltal célszerű konkrét elemekkel dolgozni, ezért legyen pl.: $A = \{1, 2, 3\}$.)
általában: $\Pi_n = \left\{(123\ldots n)^k \mid k = 0, 1, 2, \ldots, n-1\right\} = \left\{\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 3 & 4 & \ldots & 1 \end{pmatrix}^k \mid k = 0, 1, 2, \ldots, n-1\right\}$
most:

$$\Pi_3 = \left\{(123)^k \mid k = 0, 1, 2\right\} = \{(1)(2)(3), (123), (132)\} =$$

$$= \left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^k \mid k = 0, 1, 2\right\} = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$$

Mivel az izomorfia tranzitív tulajdonság, ezért elég pl. azt belátni, hogy $(F_3; \circ) \cong (\Pi_3; \circ)$
Ellenőrizhető, hogy az alábbi egy művelettartó bijekció a két halmaz között:

$$\varphi : \mathbb{F}_3 \to \Pi_3 \qquad \text{ahol} \qquad \begin{array}{l} \varphi(e) = (1)(2)(3) \\ \varphi(f) = (123) \\ \varphi(f^2) = (132) \end{array}$$

II. mo.

A három csoport páronkénti izomorfiája abból is következik, hogy mindhárom csoport harmadrendű ciklikus csoport:

$$|F_3| = |\mathbb{Z}_3| = |\Pi_3| = 3$$

és

$$F_3 = \left\{f^k \mid k \in \mathbb{Z}\right\} = \left\{f^0, f^1, f^2\right\}$$

$$\mathbb{Z}_3 = \left\{1^k \mid k \in \mathbb{Z}\right\} = \left\{1^0, 1^1, 1^2\right\}$$

$$\Pi_3 = \left\{(123)^k \mid k \in \mathbb{Z}\right\} = \left\{(123)^0, (123)^1, (123)^2\right\}$$

Ebből:

$$(F_3; \circ) \cong (\mathbb{Z}_3; \oplus_3) \cong (\Pi_3; \circ)$$

6. Mutassa meg, hogy az 5. komplex egységgyökök a szorzással csoportot alkotnak!
Igazolja, hogy ez a csoport izomorf az ötödrendű forgáscsoporttal!

Az 5. komplex egységgyökök: $\sqrt[5]{1}$ értékei.

$$\sqrt[5]{1} = \sqrt[5]{\cos 0° + j\sin 0°} = \begin{cases} \cos 0° + j\sin 0° & =: \ \epsilon \\ \cos 72° + j\sin 72° & =: \ \gamma \\ \cos 144° + j\sin 144° & =: \ \gamma^2 \\ \cos 216° + j\sin 216° & =: \ \gamma^3 \\ \cos 288° + j\sin 288° & =: \ \gamma^4 \end{cases}$$

Geometriailag: egy origó középpontú, 1-sugarú szabályos 5-szög öt csúcspontja, amelyek közül az egyik csúcspont a sík $(1,0)$ koordinátájú pontjába esik. Az alaphalmazt jelöljük: $\sqrt[5]{\mathbf{1}}$ -tel.
Mo.:
1. áll.: $\left(\sqrt[5]{\mathbf{1}};\cdot\right)$ csoport.
biz.:
műveleti zártság: a halmaz két tetszőleges elemének szorzata 1-hosszú, irányszöge pedig a 72° egész számú többszöröse: minden ilyen komplex szám $\sqrt[5]{\mathbf{1}}$-beli.
asszociativitás: komplex számok szorzása általában asszociatív
egységelem: ϵ
inverz

$$\begin{aligned} &\epsilon^{-1} = \epsilon \\ &\gamma^{-1} = \gamma^4 \\ &(\gamma^2)^{-1} = \gamma^3 \\ &(\gamma^3)^{-1} = \gamma^2 \\ &(\gamma^4)^{-1} = \gamma \end{aligned}$$

Ezzel beláttuk, hogy $\left(\sqrt[5]{\mathbf{1}};\cdot\right)$ csoport.

2. áll.: $\left(\sqrt[5]{\mathbf{1}};\cdot\right) \cong (F_5;\circ)$
biz.: teljesül az izomorfia, mert mindkét csoport ötödrendű ciklikus csoport:

$$\left|\sqrt[5]{\mathbf{1}}\right| = |F_5| = 5$$

és

$$\sqrt[5]{\mathbf{1}} = \left\{\gamma^k \mid k \in \mathbb{Z}\right\} = \left\{\gamma^0, \gamma^1, \gamma^2, \gamma^3, \gamma^4\right\} \qquad F_5 = \left\{f^k \mid k \in \mathbb{Z}\right\} = \left\{f^0, f^1, f^2, f^3, f^4\right\}$$

megj.: az ötödrendű forgáscsoport a szabályos ötszög forgáscsoportja.

7. Példatár 4.3.4. , 4.3.6. feladataiból

Eml.:

$(R;\oplus,\otimes)$ **gyűrű, ha**
$(R;\oplus)$ kommutatív csoport
$(R;\otimes)$ félcsoport
teljesül a kétoldali disztributivitás :
$\forall a,b,c \in R$
$a\otimes(b\oplus c) = (a\otimes b)\oplus(a\otimes c)$
és
$(b\oplus c)\otimes a = (b\otimes a)\oplus(c\otimes a)$

spec: ha a $\otimes$ műveletnek is van egységeleme: **egységelemes gyűrű**
spec: ha a $\otimes$ művelet kommutatív: **kommutatív gyűrű**

Test: olyan egységelemes, kommutatív gyűrű, amelyben az additív egységelemen kívül minden elemnek van multiplikatív inverze.

megj.: az $\oplus$ és $\otimes$ műveletek szerepe nem szimmetrikus, ezért pl. a disztributivitási szabályokban sem felcserélhetők egymással! (Tehát ez egy más típusú disztributivitás, mint pl. disztibutív hálók esetében, ahol a $\wedge$ és $\vee$ műveletek szerepe szimmetrikus volt!)

megj.: az $\oplus$ ill. $\otimes$ műveletek neve: "összeadás" , "szorzás". (Vigyázat: a két művelet konkrét esetben tetszőleges kétváltozós stb. művelet lehet!)

megj.: az *additív* jelző az $\oplus$ művelettel való kapcsolatot, a *multiplikatív* jelző az $\otimes$ művelettel való kapcsolatot fejezi ki. Pl.: additív egységelem: értsd: az $\oplus$ művelet egységeleme.

4.3.4. Gyűrű-e? Test-e?

$(D;+,\cdot)$, ahol
$D=\left\{x \mid x=a+b\sqrt{n} \quad a,b\in\mathbb{Q}\,;\ n \text{ olyan rögzített pozitív egész, amelyhez nem létezik } q\in\mathbb{Q}\,,\ \text{hogy } n=q^2\right\}$,
a műveletek a szokásosak.

Mo.:

$+$
műveleti zártság: $(a+b\sqrt{n})+(c+d\sqrt{n})=(a+c)+(b+d)\sqrt{n}$ és itt $a+c\in\mathbb{Q}$, $b+d\in\mathbb{Q}$
asszociativitás: valós számok összeadása asszociatív
egységelem: $0+0\sqrt{n}$ és itt $0\in\mathbb{Q}$
inverz: az $a+b\sqrt{n}$ elem inverze: $(-a)+(-b)\sqrt{n}$ és itt $-a,-b\in\mathbb{Q}$
kommutativitás: valós számok összeadása kommutatív
Tehát **$(D;+)$ kommutatív csoport**

$\cdot$
műveleti zártság: $(a+b\sqrt{n})\cdot(c+d\sqrt{n})=(ac+bdn)+(ad+bc)\sqrt{n}$ és itt $ac+bdn\in\mathbb{Q}$, $ad+bc\in\mathbb{Q}$
asszociativitás: valós számok szorzása asszociatív
Tehát **$(D;\cdot)$ félcsoport**

disztributivitás: D elemei valós számok, és valós számokra teljesül a kétoldali disztributivitás
szimbolikusan:
$(a+b\sqrt{n})\cdot[(c+d\sqrt{n})+(e+f\sqrt{n})]=(a+b\sqrt{n})\cdot(c+d\sqrt{n})+(a+b\sqrt{n})\cdot(e+f\sqrt{n})$
ill.
$[(c+d\sqrt{n})+(e+f\sqrt{n})]\cdot(a+b\sqrt{n})=(c+d\sqrt{n})\cdot(a+b\sqrt{n})+(e+f\sqrt{n})\cdot(a+b\sqrt{n})$
Tehát **$(D;+,\cdot)$ gyűrű**

Továbbá:
a $\cdot$ műveletnek van *egységeleme* (multiplikatív egység): $1+0\sqrt{n}$,
tehát **$(D;+,\cdot)$ egységelemes gyűrű**;

a $\cdot$ művelet *kommutatív*: $(a+b\sqrt{n})\cdot(c+d\sqrt{n})=(c+d\sqrt{n})\cdot(a+b\sqrt{n})$, mert

$(a+b\sqrt{n})\cdot(c+d\sqrt{n})=(ac+bdn)+(ad+bc)\sqrt{n}$

$(c+d\sqrt{n})\cdot(a+b\sqrt{n})=(ca+dbn)+(cb+db)\sqrt{n}=(ac+bdn)+(ad+bc)\sqrt{n}$

tehát **$(D;+,\cdot)$ kommutatív gyűrű**, és így

$(D;+,\cdot)$ egyégelemes, kommutatív gyűrű.

multiplikatív inverz: mivel az 1 $(=1+0\sqrt{n})$ a multiplikatív egységelem, ezért egy szám multiplikatív inverze a szám reciproka: $a+b\sqrt{n}$ inverze $\frac{1}{a+b\sqrt{n}}$.

Ez akkor nem értelmes, ha $a+b\sqrt{n}=0+0\sqrt{n}$, viszont ez éppen az additív egységelem, aminek a test-definíció szerint nem is kell hogy legyen multiplikatív inverze. Kérdés tehát: az $\frac{1}{a+b\sqrt{n}}$ szám D-beli-e?

$$\frac{1}{a+b\sqrt{n}}=\frac{a-b\sqrt{n}}{(a+b\sqrt{n})(a-b\sqrt{n})}=\frac{a-b\sqrt{n}}{a^2-b^2n}=\left(\frac{a}{a^2-b^2n}\right)+\left(-\frac{b}{a^2-b^2n}\right)\sqrt{n}$$

és itt

$$\frac{a}{a^2-b^2n}\ ,\ -\frac{b}{a^2-b^2n}\ \in\mathbb{Q}$$

Ez a kifejezés akkor nem értelmes (akkor nem létezik inverz), ha $a^2-b^2n=0$, azaz ha

(a) $\frac{a^2}{b^2}=n$ azaz $\left(\frac{a}{b}\right)^2=n$: viszont ezt az esetet D definíciója kizárta;

vagy ha

(b) $a = b = 0$, de ezt az esetet már az előbb kizártuk.

Kaptuk: $\boldsymbol{(D; +, \cdot)}$ **test**

4.3.6.

(a) $(M; +, \cdot)$, ahol M az $n \times n$-es mátrixok halmaza a valós számtest felett[1]. Műveletek a mátrixösszeadás és -szorzás.
Mo.:
$(M; +, \cdot)$ egységelemes gyűrű. HF

(b) $(M; +, \cdot)$, ahol M az $n \times n$-es mátrixok halmaza az $\mathbb{Z}_2$ számtest felett. Műveletek a mod2 mátrixösszeadás és -szorzás.
$\mathbb{Z}_2 = \{0, 1\}$
Példák a műveletekkel való számolásra $n = 3$ esetben:

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Mo.:
$(M; +, \cdot)$ egységelemes gyűrű. HF

(c) $(M; +, \cdot)$, ahol $M = \left\{ \mathbf{M} \mid \mathbf{M} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a, b \in \mathbb{R} \right\}$, műveletek a mátrixösszeadás és -szorzás.
Mo.:
$(M; +, \cdot)$ gyűrű. HF

(d) $(M; +, \cdot)$, ahol $M = \left\{ \mathbf{M} \mid \mathbf{M} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a, b \in \mathbb{R} \right\}$, műveletek a mátrixösszeadás és -szorzás.
Mo.:

M elemei: "főátlóban ugyanaz, mellékátlóban egymás ellentettjei"

$+$
műveleti zártság: $\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ -(b_1 + b_2) & a_1 + a_2 \end{bmatrix} \quad (\in M)$
asszociativitás: a mátrixösszeadás általában asszociatív
egységelem: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (\in M)$
inverz: $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ inverze $\begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \quad (\in M)$
kommutativitás: a mátrixösszeadás általában kommutatív

$\cdot$
műveleti zártság: $\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix} \quad (\in M)$
asszociativitás: a mátrixszorzás általában asszociatív

disztributivitás: mátrixokra általában igaz

Eddig: $\boldsymbol{(M; +, \cdot)}$ **gyűrű**.

Továbbá:
a $\cdot$ műveletnek van *egységeleme* (multiplikatív egység): $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (\in M)$

tehát $\boldsymbol{(M; +, \cdot)}$ **egységelemes gyűrű**;

[1] Azaz a mátrix elemei valós számok.

a $\cdot$ művelet *kommutatív*: $\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}$, mert

$$\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}$$

és

$$\begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2a_1 - b_2b_1 & a_2b_1 + a_1b_2 \\ -(a_2b_1 + a_1b_2) & a_2a_1 - b_2b_1 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}$$

tehát $\boldsymbol{(M; +, \cdot)}$ **kommutatív gyűrű**;

multiplikatív inverz: egy elem csoprtbeli inverze (ha létezik), megegyezik az elem szokásos inverzmátrixsszával.

det $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a^2 + b^2 \neq 0$ ha $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Tehát az additív egységelemen kívül minden elemnek van multiplikatív inverze.

Kérdés: az inverz minden esetben M-beli-e?

áll.: $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ multiplikatív inverze: $\begin{bmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix} \in M$

biz.: $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1} = \dfrac{\text{adj} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}}{\det \begin{bmatrix} a & b \\ -b & a \end{bmatrix}} = \frac{1}{a^2+b^2} \cdot \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}$

Ez csak akkor nem értelmes, ha $a^2 + b^2 = 0$, de ezt az esetet már az előbb kizártuk.

Kaptuk: $\boldsymbol{(M; +, \cdot)}$ **test**.