

1. Műveletek

Absztrakt algebra

- algebra: az algebrai struktúrák tudománya
- algebrai struktúra: műveletekkel felszerelt nemüres halmaz
- művelet: ?

1.1. Példa. Az összeadás művelet az egész számok halmazán.

$$(3, 8) \rightarrow 11 \quad \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, b) \rightarrow a + b$$

1.2. Definíció. Kétváltozós * **művelet** a nemüres A halmazon:

$$*: A \times A \rightarrow A, (a, b) \rightarrow a * b \quad \text{leképezés.}$$

1.3. Példa.

(a) Művelet-e az osztás a valós számok halmazán?

NEM $2/0$ nem definiált.

(b) Művelet-e a szorzás a negatív egész számok halmazán?

NEM $(-2) \cdot (-3) = 6 \notin \mathbb{Z}^-$

Fontos, hogy:

- $a * b$ értelmezett legyen minden $a, b \in A$ esetén,
- $a * b$ egyértelműen meghatározott legyen minden $a, b \in A$ esetén,
- $a * b$ az A halmazba essen minden $a, b \in A$ esetén.

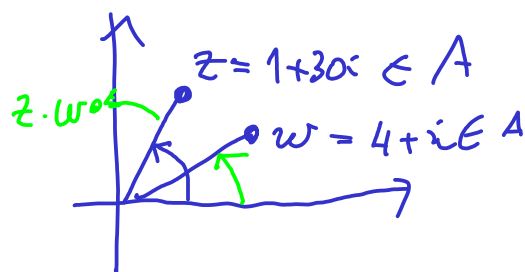
SPOILER!

1.4. Feladat.

- (a) Művelet-e az összeadás a hárommal osztható egész számok halmazán?
IGEN: $3k + 3\ell = 3(k + \ell)$ osztható 3-mal minden $k, \ell \in \mathbb{Z}$ esetén.
- (b) Művelet-e az összeadás a hárommal nem osztható egész számok halmazán?
NEM: pl. $1 + 2 = 3$ nincs benne az alaphalmazban.
- (c) Művelet-e az osztás a pozitív egész számok halmazán?
NEM: pl. $5/7$ nincs benne az alaphalmazban.
- (d) Művelet-e az összeadás az $A = \{a + bi \mid a, b \in \mathbb{R}^+\}$ halmazon?
IGEN: ha $a + bi, c + di \in A$ (azaz $a, b, c, d \in \mathbb{R}^+$), akkor
- $$(a + bi) + (c + di) = (a + c) + (b + d)i \in A,$$
- hiszen $a + c, b + d \in \mathbb{R}^+$.
- (e) Művelet-e $x * y = \sqrt{xy}$ a valós számok halmazán?
NEM: pl. $2 * (-3) = \sqrt{-6}$ nincs benne az alaphalmazban (vagy nem értelmezett).
- (f) Művelet-e $x * y = \sqrt{xy}$ a komplex számok halmazán?
NEM: pl. $(2 - 4i) * (2 + i) = \sqrt{8 - 6i}$ nem egyértelmű, lehet $3 - i$ vagy $-3 + i$.
- (g) Művelet-e a metszés az $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}\}$ halmazon?
IGEN: a megadott hat halmaz közül bármely kettőnek a metszete megegyezik a hat halmaz valamelyikével (macerás esetvizsgálat).

$$A = \{a + bi \mid a, b \in \mathbb{R}^+\}$$

$$\begin{aligned} z \cdot w &= (1 + 3i)(4 + i) = \\ &= 4 + i + 12i - 3 = \\ &= -2 + 13i \notin A \end{aligned}$$



2. Kitérő: maradékosztályok

Emlékeztető. A modulo m kongruencia ekvivalenciareláció az egész számok halmazán. Két szám akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva. Ezért itt az ekvivalenciaosztályokat **modulo m maradékosztályoknak** nevezzük.

2.1. Példa. A modulo 3 maradékosztályok:

$$\bar{0} = \{ \dots, -6, -3, 0, 3, 6, 9, 12, \dots \}$$

$$\bar{1} = \{ \dots, -5, -2, 1, 4, 7, 10, 13, \dots \}$$

$$\bar{2} = \{ \dots, -4, -1, 2, 5, 8, 11, 14, \dots \}$$

2.2. Definíció. Egy a egész szám **modulo m maradékosztálya** a következő halmaz:

$$\bar{a} = \{ b \in \mathbb{Z} : b \equiv a \pmod{m} \} = \{ a + km : k \in \mathbb{Z} \}.$$

A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli:

$$\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \dots, \overline{m-1} \}.$$

2.3. Megjegyzés. A definícióból világos, hogy tetszőleges a, b egész számok esetén

$$\bar{a} = \bar{b} \iff a \equiv b \pmod{m}.$$

2.4. Példa.

$$\mathbb{Z}_3 = \{ \bar{0}, \bar{1}, \bar{2} \} = \{ \overset{\bar{0}}{\bar{1}}, \overset{\bar{2}}{\bar{2}}, \overset{\bar{0}}{\bar{3}}, \overset{\bar{1}}{\bar{4}} \} = \{ \overline{-325}, \overline{1707}, \overline{1777} \}$$

Varázsgömb

Emlékeztető. A kongruenciareláció egy fontos tulajdonsága:

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies \begin{array}{l} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \text{ és} \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}. \end{array}$$

Ugyanez maradékosztályokkal megfogalmazva:

$$\left. \begin{array}{l} \bar{a}_1 = \bar{b}_1 \\ \bar{a}_2 = \bar{b}_2 \end{array} \right\} \implies \begin{array}{l} \overline{a_1 \pm a_2} = \overline{b_1 \pm b_2} \text{ és} \\ \overline{a_1 \cdot a_2} = \overline{b_1 \cdot b_2}. \end{array}$$

2.5. Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást, a kivonást és a szorzást a következőképpen:

$$\bar{a} \oplus \bar{b} := \overline{a + b}, \quad \bar{a} \ominus \bar{b} := \overline{a - b}, \quad \bar{a} \odot \bar{b} := \overline{a \cdot b}.$$

+	...	0	1	2	3	4	...
...	...	...	...	...	...	...	...
0	...	0	1	2	3	4	...
1	...	1	2	3	4	5	...
2	...	2	3	4	5	6	...
3	...	3	4	5	6	7	...
4	...	4	5	6	7	8	...
...	...	...	...	...	...	...	...

+	...	0	1	2	3	4	...
...	...	...	...	...	...	...	...
0	...	0	1	2	3	4	...
1	...	1	2	3	4	5	...
2	...	2	3	4	5	6	...
3	...	3	4	5	6	7	...
4	...	4	5	6	7	8	...
...	...	...	...	...	...	...	...

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}_4$ összeadó- és szorzótáblája:

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1} = \bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2} = \bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

2.6. Feladat. Számoljunk $\mathbb{Z}_{15}$ -ben!

(a) $\bar{8} \oplus \bar{10} = \overline{8+10} = \overline{18} = \bar{3}$

(b) $\bar{8} - \bar{10} = \overline{8-10} = \overline{-2} = \bar{13}$

(c) $\bar{8} \cdot \bar{10} = \overline{80} = \bar{5}$

(d) $\bar{8}/\bar{10} = \overline{8/10} = \bar{x} \Leftrightarrow \bar{10} \cdot \bar{x} = \bar{8} \Leftrightarrow 10x \equiv 8 \pmod{15}$
 mivel $\gcd(10, 15) \nmid 8$

(e) $\bar{6}/\bar{9} = \bar{x} \Leftrightarrow 9x \equiv 6 \pmod{15}$
 $x \equiv 4 \pmod{5}$
 $x \equiv 4, 9, 14 \pmod{15}$
 $\bar{x} = \bar{4}, \bar{9}, \bar{14}$

3. Műveleti tulajdonságok

Legyen $*$ egy művelet az A halmazon.

3.1. Definíció. A $*$ művelet **kommutatív**, ha minden $a, b \in A$ esetén $a*b = b*a$.

3.2. Példa.

- A valós számok szorzása kommutatív.
- A valós számok összeadása kommutatív.
- A pozitív egészek hatványozása nem kommutatív pl. $2^3 \neq 3^2$.

3.3. Definíció. A $*$ művelet **asszociatív**, ha minden $a, b, c \in A$ esetén

$$(a * b) * c = a * (b * c).$$

3.4. Példa.

- A valós számok szorzása asszociatív.
- A valós számok összeadása asszociatív.
- A pozitív egészek hatványozása nem asszociatív, pl. $(2^1)^3 \neq 2^{(1^3)}$.

3.5. Definíció. A $z \in A$ elem **zéruselem**, ha minden $a \in A$ esetén

$$a * z = z = z * a.$$

3.6. Példa.

- A valós számok szorzásánál $z = 0$.
- A valós számok összeadásánál nincs zéruselem.
- A pozitív egészek hatványozásánál nincs zéruselem.

3.7. Definíció. Az $e \in A$ elem **egységelem**, ha minden $a \in A$ esetén

$$a * e = a = e * a.$$

3.8. Példa.

- A valós számok szorzásánál $e = 1$.
- A valós számok összeadásánál $e = 0$.
- A pozitív egészek hatványozásánál nincs egységelem.

3.9. Definíció. Tfh. e egységelem; ekkor a és b egymás **inverzei**, ha

$$a * b = e = b * a.$$

3.10. Példa.

- A valós számok szorzásánál a inverze: $b = \frac{1}{a}$, **ha** $a \neq 0$.
A nullának itt nincs inverze.
- A valós számok összeadásánál a inverze: $b = -a$.
- A pozitív egészek hatványozásánál nincs egységelem, ezért az inverz fogalma nem is értelmezhető.

Absztrakt algebra $A: \sim 10^2$ $B: \sim 10^3$ $C: \sim 10^6$ $D: \text{több}$

Hány kétváltozós műveletet lehet definiálni az $A = \{a, b, c, d\}$ halmazon?

$$\begin{array}{llll} a * a = ? & a * b = ? & a * c = ? & a * d = ? \\ b * a = ? & b * b = ? & b * c = ? & b * d = ? \\ c * a = ? & c * b = ? & c * c = ? & c * d = ? \\ d * a = ? & d * b = ? & d * c = ? & d * d = ? \end{array}$$

Mind a 16 kérdőjel helyére az a, b, c, d elemek bármelyikét írhatjuk, ezért $4^{16} = 4\,294\,967\,296$ lehetőség van.

Íme egy a $4\,294\,967\,296$ művelet közül:

$$\begin{array}{llll} a * a = a & a * b = b & a * c = c & a * d = d \\ b * a = b & b * b = a & \underline{b * c = c} & b * d = d \\ c * a = c & c * b = c & c * c = c & c * d = c \\ d * a = d & d * b = d & d * c = c & d * d = c \end{array}$$

Ezt áttekinthetőbb formában mutatja az alábbi **művelettáblázat**:

*	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	c	c	c
d	d	d	c	c

3.11. Feladat. Vizsgáljuk meg a tanult műveleti tulajdonságok szempontjából:

*	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	c	c	c
d	d	d	c	c

$$\begin{aligned}
 a \cdot a &= a = \dots \cdot a \\
 b \cdot b &= a = \dots \cdot b \\
 c \cdot \dots &\neq a \\
 d \cdot \dots &\neq a
 \end{aligned}$$

SPOILER!

- kommutativitás: teljesül (a táblázat szimmetrikus a főátlóra)
- asszociativitás: teljesül (nem látszik könnyen; később visszatérünk rá)
- zéruselem: c (sorában és oszlopában végig c van)
- egységelem: a (sora és oszlopa megegyezik a „fejléccsel”)
- inverzek: a inverze: a , b inverze: b , c -nek és d -nek nincs inverze.

Varázslat!

$$\begin{array}{c}
 \text{asszoc.} \quad \leftarrow \text{asszoc.} \\
 \begin{array}{c|cccc}
 * & a & b & c & d \\
 \hline
 a & a & b & c & d \\
 b & b & a & c & d \\
 c & c & c & c & c \\
 d & d & d & c & c
 \end{array}
 \cong
 \begin{array}{c|cccc}
 * & 1 & 3 & 0 & 2 \\
 \hline
 1 & 1 & 3 & 0 & 2 \\
 3 & 3 & 1 & 0 & 2 \\
 0 & 0 & 0 & 0 & 0 \\
 2 & 2 & 2 & 0 & 0
 \end{array}
 = (\mathbb{Z}_4; \cdot)
 \end{array}$$

↑
izomorf

SPOILER!

A $*$ művelet a modulo 4 maradékosztályok szorzása „álruhában”.

$$(\{a, b, c, d\}; *) \cong (\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}; \cdot) = (\mathbb{Z}_4; \cdot).$$

Ebből rögtön következik, hogy a $*$ művelet asszociatív.

3.12. Feladat. Vizsgáljuk meg a tanult műveleti tulajdonságok szempontjából:

$\circ$	a	b	c	d
a	c	a	b	b
b	a	b	c	d
c	b	c	b	a
d	b	d	c	a

SPOILER!

- kommutativitás: nem teljesül, pl. $c \circ d = a$ és $d \circ c = c$
- asszociativitás: nem teljesül, pl. $(c \circ c) \circ d = b \circ d = d$ és $c \circ (c \circ d) = c \circ a = b$
- zéruselem: nincs
- egységelem: b (sora és oszlopa megegyezik a „fejléccel”)
- inverzek: a inverzei: c és d , b inverze: b , c inverzei: a és c , d inverze: a

3.13. Feladat. Írjuk fel a $\mathcal{P}(\{u, v\})$ halmazon az egyesítés művelet táblázatát, és vizsgáljuk meg a tanult műveleti tulajdonságok szempontjából.

SPOILER!

$\cup$	$\emptyset$	$\{u\}$	$\{v\}$	$\{u, v\}$
$\emptyset$	$\emptyset$	$\{u\}$	$\{v\}$	$\{u, v\}$
$\{u\}$	$\{u\}$	$\{u\}$	$\{u, v\}$	$\{u, v\}$
$\{v\}$	$\{v\}$	$\{u, v\}$	$\{v\}$	$\{u, v\}$
$\{u, v\}$	$\{u, v\}$	$\{u, v\}$	$\{u, v\}$	$\{u, v\}$

- kommutativitás: teljesül
- asszociativitás: teljesül
- zéruselem: $\{u, v\}$
- egységelem: $\emptyset$
- inverzek: $\emptyset$ inverze $\emptyset$, senki másnak nincs inverze

3.14. Feladat. Vizsgáljuk meg a tanult műveleti tulajdonságok szempontjából az egész számok halmazán értelmezett $a \bullet b = a + b + 23$ műveletet.

SPOILER!

• kommutativitás: **IGÉN**

• asszociativitás: **IGÉN**
 $a \bullet b$

$$(a \bullet b) \bullet c = (a + b + 23) \bullet c = (a + b + 23) + c + 23 = a + b + c + 46$$

$$a \bullet (b \bullet c) = a + (b + c + 23) + 23 = a + b + c + 46$$

• zéruselem: **NINCS**

$$\forall a: a \bullet z = z$$

$$a + z + 23 = z \text{ nem teljesül minden } a\text{-ra}$$

• egységelem: **-23**

$$\forall a: a \bullet e = a$$

$$a + e + 23 = a$$

$$e = -23$$

• inverzek: a inverze: $x = -46 - a$

$$a \bullet x = e = -23$$

$$a + x + 23 = -23$$

$$x = -46 - a$$

4. Kitérő: redukált maradékosztályok

4.1. Definíció. Azt mondjuk, hogy az $\bar{a}, \bar{b} \in \mathbb{Z}_m$ maradékosztályok egymás **multiplikatív inverzei**, ha $\bar{a} \cdot \bar{b} = \bar{1}$. Jelölés: $\bar{b} = \bar{a}^{-1}$.

SPOILER!

$\bar{a}$ inverze $\bar{x}$, ha

$$\bar{a} \cdot \bar{x} = \bar{1}$$

$$ax \equiv 1 \pmod{m}$$

van mo. $\Leftrightarrow \text{lko}(a, m) \mid 1$ a és m rel. príms.

4.2. Tétel. Egy $\bar{a} \in \mathbb{Z}_m$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha $\text{lko}(a, m) = 1$.

Bizonyítás. Az $ax \equiv 1 \pmod{m}$ lineáris kongruenciának akkor és csak akkor van megoldása, ha $\text{lko}(a, m) \mid 1$. $\square$

4.3. Definíció. Az $\bar{a} \in \mathbb{Z}_m$ maradékosztályt **redukált maradékosztálynak**, nevezzük, ha $\text{lko}(a, m) = 1$. A modulo m redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli:

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : \text{lko}(a, m) = 1\}.$$

4.4. Feladat. Soroljuk fel $\mathbb{Z}_{15}^*$ elemeit, és határozzuk meg mindegyik elem inverzét.

$$\mathbb{Z}_{15}^* = \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}$$

$$|\mathbb{Z}_{15}^*| = 8 \quad |\mathbb{Z}_{15}| = 15$$

5. Algebrai struktúrák

5.1. Definíció. **Algebrai struktúrán** olyan $(A; F)$ párt értünk, ahol

- A nemüres halmaz, és
- F az A halmazon értelmezett műveletek egy halmaza.

5.2. Példa.

- Az összeadás művelet az egész számok halmazán, ezért $(\mathbb{Z}; +)$ algebrai struktúra.
- Az összeadás és a szorzás művelet az egész számok halmazán, ezért $(\mathbb{Z}; +, \cdot)$ algebrai struktúra.
- A szorzás nem művelet a negatív egész számok halmazán, ezért $(\mathbb{Z}^-; \cdot)$ nem algebrai struktúra.



algebrai struktúrák



5.3. Definíció. Legyen A nemüres halmaz.

0. Ha $*$ kétváltozós művelet az A halmazon, akkor $(A; *)$ **grupoid**.
1. Ha $(A; *)$ grupoid és $*$ asszociatív, akkor $(A; *)$ **félcsoport**.
2. Ha $(A; *)$ félcsoport és van egységeleme, akkor $(A; *)$ **monoid**.
3. Ha $(A; *)$ monoid és minden elemének van inverze, akkor $(A; *)$ **csoport**.
4. Ha $(A; *)$ csoport és $*$ kommutatív, akkor $(A; *)$ **Abel-csoport**.

5.4. Példa. Milyen algebrai struktúra $(\mathbb{N}; +)$?

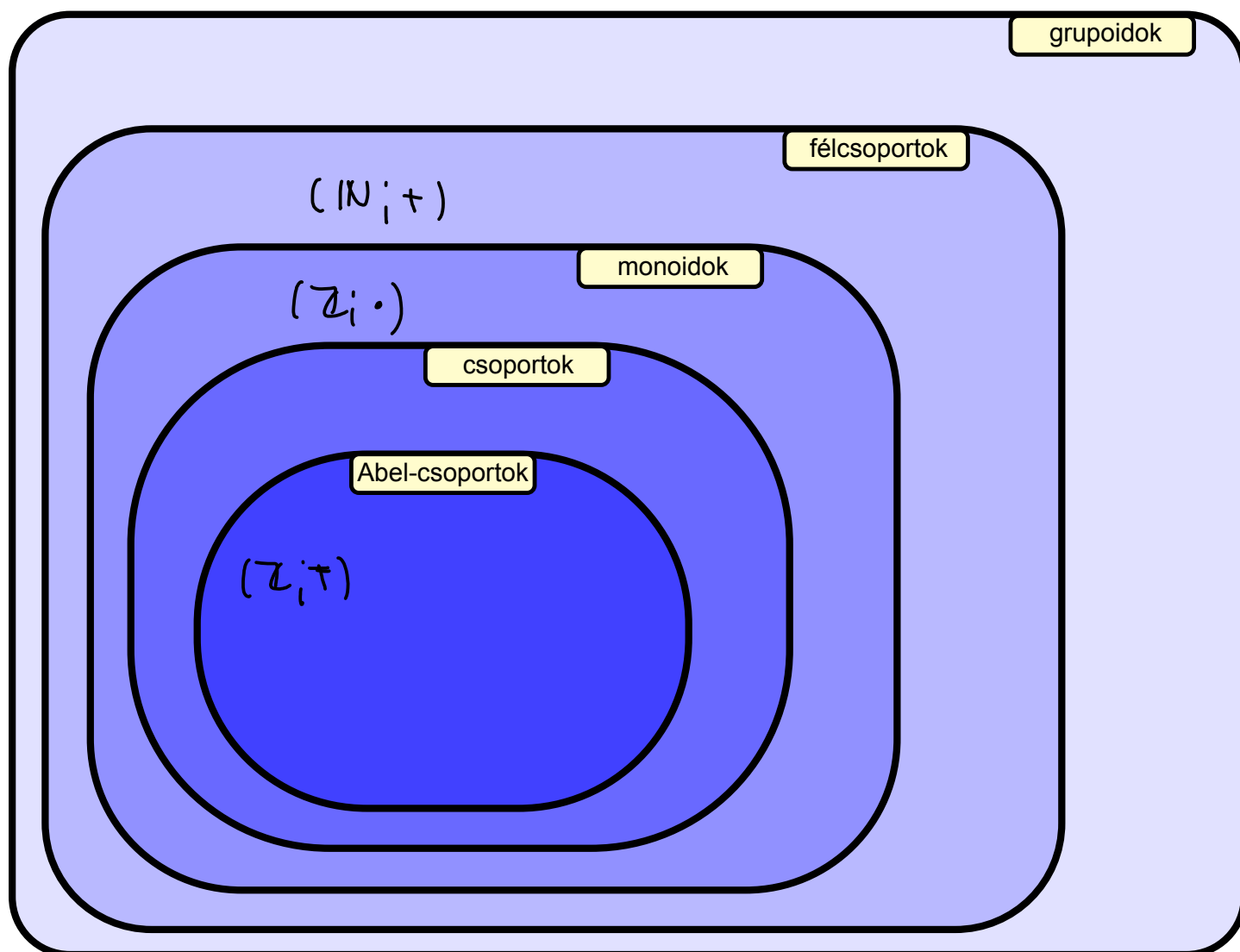
0. művelet? IGEN $\implies (\mathbb{N}; +)$ grupoid
1. asszociatív? IGEN $\implies (\mathbb{N}; +)$ félcsoport
2. egységelem? NINCS

5.5. Példa. Milyen algebrai struktúra $(\mathbb{Z}; +)$?

0. művelet? IGEN $\implies (\mathbb{Z}; +)$ grupoid
1. asszociatív? IGEN $\implies (\mathbb{Z}; +)$ félcsoport
2. egységelem? VAN (0) $\implies (\mathbb{Z}; +)$ monoid
3. inverz? MINDENKINEK VAN (a inverze $-a$) $\implies (\mathbb{Z}; +)$ csoport
4. kommutatív? IGEN $\implies (\mathbb{Z}; +)$ Abel-csoport

5.6. Példa. Milyen algebrai struktúra $(\mathbb{Z}; \cdot)$?

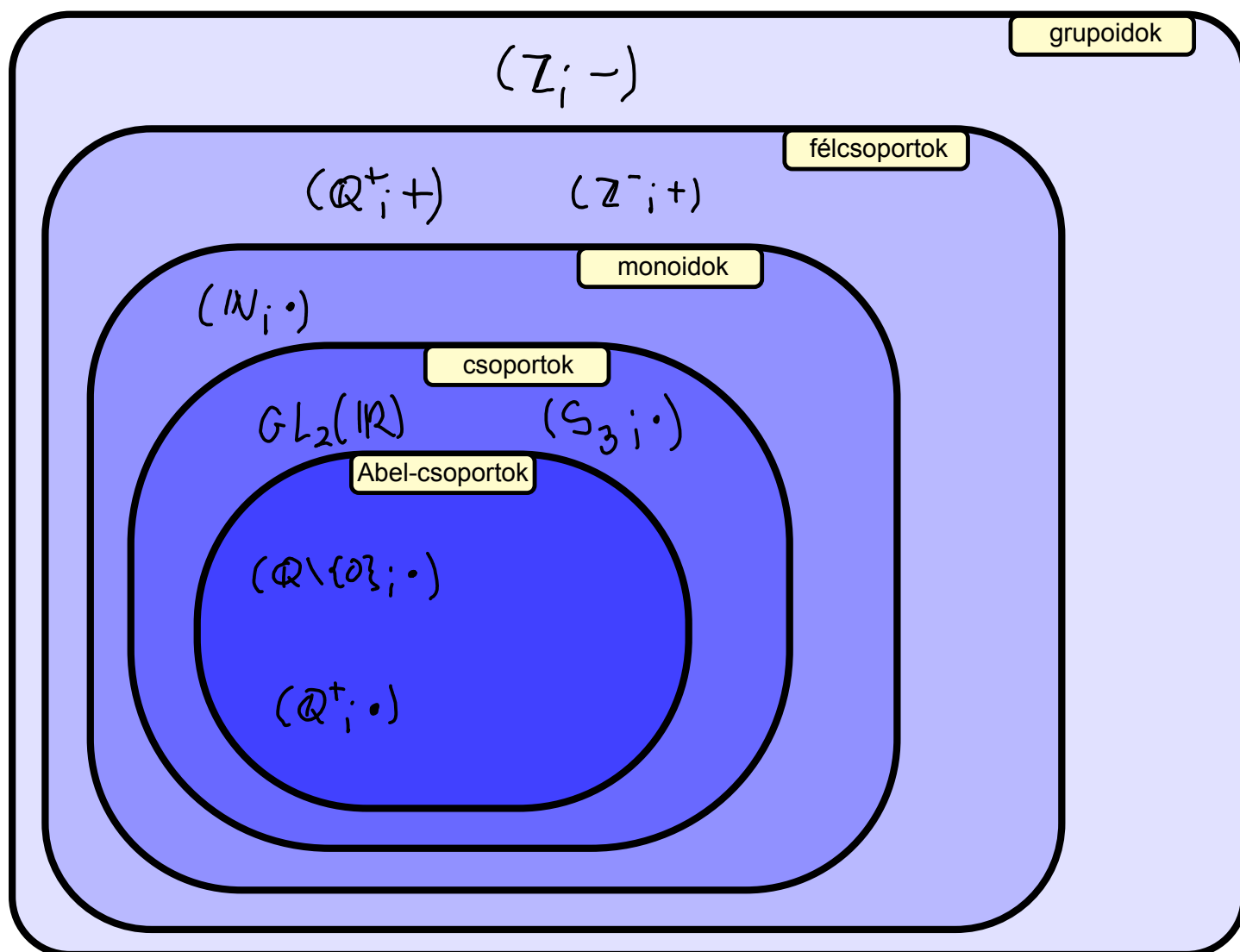
0. művelet? IGEN $\implies (\mathbb{Z}; \cdot)$ grupoid
1. asszociatív? IGEN $\implies (\mathbb{Z}; \cdot)$ félcsoport
2. egységelem? VAN (1) $\implies (\mathbb{Z}; \cdot)$ monoid
3. inverz? NINCS MINDENKINEK (pl. 0-nak nincs)



5.7. Feladat. Milyen algebrai struktúrák az alábbiak?

(M_2 a 2×2 -es valós mátrixok halmazát jelöli.)

- | | | |
|---|---|---|
| (a) $(\mathbb{N}; +)$ | (e) $(\mathbb{Z}_5; +)$ | (i) $(M_2; +)$ |
| (b) $(\mathbb{Z}; +)$ | (f) $(\mathbb{Z}_5; \cdot)$ | (j) $(M_2; \cdot)$ |
| (c) $(\mathbb{Z}; \cdot)$ | (g) $(\mathbb{Z}_5 \setminus \{\bar{0}\}; \cdot)$ | (k) $(M_2 \setminus \{\mathbf{0}\}; \cdot)$ |
| (d) $(\mathbb{Z} \setminus \{0\}; \cdot)$ | (h) $(\mathbb{Z}_5 \setminus \{\bar{0}\}; +)$ | (l) $(\{A \in M_2 : \det(A) \neq 0\}; \cdot)$ |
| | | $\parallel$
$GL_2(\mathbb{R})$ |



5.8. Feladat. Milyen algebrai struktúrák az alábbiak?

$$(\mathbb{Q} \setminus \{0\}; +)$$

$$(\mathbb{Z}_6 \setminus \{\bar{0}\}; \cdot)$$

(a) $(\mathbb{Q} \setminus \{0\}; +)$

(d) $(\mathbb{Q}^+; \cdot)$

(g) $(\mathbb{N}; \cdot)$

(b) $(\mathbb{Q} \setminus \{0\}; \cdot)$

(e) $(\mathbb{Z}^-; +)$

(c) $(\mathbb{Q}^+; +)$

(f) $(\mathbb{Z}_6 \setminus \{\bar{0}\}; \cdot)$

6. Izomorfia

Asszociatív-e ez a művelet?

$a \cdot (b \cdot c)$

$(a \cdot b) \cdot c$

*			
			
			
			

$\approx$

	2	1	0
2	2	2	0
1	2	1	0
0	0	0	0

$= (\mathbb{Z}_3, +)$

SPOILER!

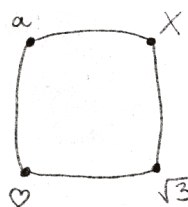
*			
			
			
			

$\approx$

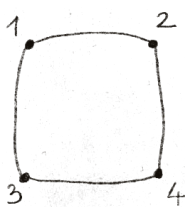
.	$\bar{2}$	$\bar{1}$	$\bar{0}$
$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{1}$	$\bar{2}$	$\bar{1}$	$\bar{0}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

$=$

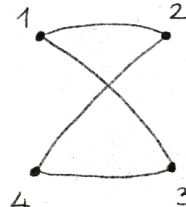
.	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$



$\approx$



$=$



izomorfizmus: $\varphi : \{a, X, \heartsuit, \sqrt{3}\} \rightarrow \{1, 2, 3, 4\}$ bijekció, ami megőrzi a struktúrát:

$$\forall u, v: \{u, v\} \in E(G) \iff \{u\varphi, v\varphi\} \in E(H)$$

izomorfizmus: $\varphi : \{\text{apple}, \text{carrot}, \text{banana}\} \rightarrow \{\bar{0}, \bar{1}, \bar{2}\}$ bijekció, ami megőrzi a struktúrát:

$$\forall u, v, w: u * v = w \iff u\varphi \cdot v\varphi = w\varphi, \text{ azaz}$$

$$\forall u, v: u\varphi \cdot v\varphi = (u * v)\varphi$$

6.1. Definíció. Az $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \circ)$ grupoidok **izomorfak** (jelölés: $\mathbb{A} \cong \mathbb{B}$), ha létezik $\mathbb{A} \rightarrow \mathbb{B}$ **izomorfizmus**, azaz olyan $\varphi: A \rightarrow B$ bijekció, amelyre

$$\forall a_1, a_2 \in A: (a_1 * a_2)\varphi = a_1\varphi \circ a_2\varphi.$$

$$\begin{array}{ccc} \mathbb{A} & \xrightarrow{\varphi} & \mathbb{B} \\ a_1, a_2 & \xrightarrow{\varphi} & a_1\varphi, a_2\varphi \\ \downarrow * & & \downarrow \circ \\ a_1 * a_2 & \xrightarrow{\varphi} & (a_1 * a_2)\varphi = a_1\varphi \circ a_2\varphi \end{array}$$

6.2. Tétel. Izomorfizmusok szorzata és inverze is izomorfizmus.

6.3. Következmény. Az izomorfia ekvivalenciareláció (grupoidok bármely halmazán).

6.4. Feladat. Adjunk meg izomorfizmust az $\mathbb{A} = (\{\text{igaz}, \text{hamis}\}; \leftrightarrow)$ és $\mathbb{B} = (\mathbb{Z}_2; +)$ grupoidok között.

$$\begin{array}{c|cc} \leftrightarrow & \text{i} & \text{h} \\ \hline \text{i} & \text{i} & \text{h} \\ \text{h} & \text{h} & \text{i} \end{array} \quad \cong \quad \begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array}$$

SPOILER!

Az izomorfizmus:

$$\varphi: \{\text{i}, \text{h}\} \rightarrow \{\bar{0}, \bar{1}\}, \quad \text{i} \rightarrow \bar{0}, \text{h} \rightarrow \bar{1}.$$

Ellenőrzés:

$$\begin{aligned} (\text{i} \leftrightarrow \text{i})\varphi &= \bar{0} = \text{i}\varphi + \text{i}\varphi \\ (\text{i} \leftrightarrow \text{h})\varphi &= \bar{1} = \text{i}\varphi + \text{h}\varphi \\ (\text{h} \leftrightarrow \text{i})\varphi &= \bar{1} = \text{h}\varphi + \text{i}\varphi \\ (\text{h} \leftrightarrow \text{h})\varphi &= \bar{0} = \text{h}\varphi + \text{h}\varphi \end{aligned}$$

6.5. Feladat. Adjunk meg izomorfizmust az $\mathbb{A} = (\{1, -1, i, -i\}; \cdot)$ és $\mathbb{B} = (\mathbb{Z}_4; +)$ grupoidok között.

SPOILER!

Egy izomorfizmus:

$$\varphi: 1 \rightarrow \bar{0}, \quad -1 \rightarrow \bar{2}, \quad i \rightarrow \bar{1}, \quad -i \rightarrow \bar{3}$$

$$\beta = \varphi^{-1}: \bar{0} \rightarrow 1, \quad \bar{1} \rightarrow i, \quad \bar{2} \rightarrow -1, \quad \bar{3} \rightarrow -i$$

Tömörebben: $\varphi^{-1}: \mathbb{Z}_4 \rightarrow \{1, -1, i, -i\}, \quad \bar{k} \rightarrow i^k.$

Ez a leképezés azért bijektív, mert $\forall k, \ell \in \mathbb{Z}: i^k = i^\ell \iff k \equiv \ell \pmod{4}.$

A műveletekkel való felcserélhetőség:

$$\beta: \mathbb{Z}_4 \rightarrow E_4, \quad \bar{k} \mapsto i^k$$

$$(\bar{k} + \bar{\ell})\beta = \overline{(k + \ell)}\beta = i^{k+\ell} = i^k \cdot i^\ell = (\bar{k}\beta) \cdot (\bar{\ell}\beta) \quad \checkmark$$

6.6. Feladat. Izomorf-e az $\mathbb{A}$ grupoid $\mathbb{B}$ és $\mathbb{C}$ közül valamelyikkel?

$$\mathbb{A} = (\{\text{igaz}, \text{hamis}\}; \rightarrow), \quad \mathbb{B} = (\{0, 1\}; \circ), \quad \mathbb{C} = (\{0, 1\}; *)$$

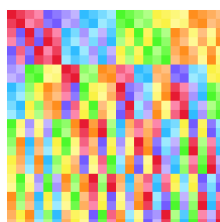
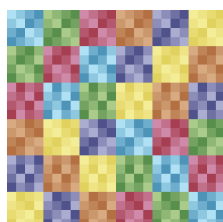
$\circ$	0	1
0	1	1
1	0	1

$*$	0	1
0	0	0
1	0	1

SPOILER!

$\mathbb{A} \cong \mathbb{B}$ a következő izomorfizmus mellett: igaz $\rightarrow$ 1, hamis $\rightarrow$ 0.

$\mathbb{A} \not\cong \mathbb{C}$, mert $\mathbb{C}$ kommutatív, de $\mathbb{A}$ nem.



7. A csoport fogalma, példák, alaptulajdonságok

Emlékeztető. **Csoportnak** nevezünk egy $(A; *)$ grupoidot, ha

- $*$ asszociatív: $\forall a, b, c \in A: (a * b) * c = a * (b * c)$;
- létezik egységelem: $\exists e \in A \quad \forall a \in A: a * e = e * a = a$;
- minden elemnek van inverze: $\forall a \in A \quad \exists b \in A: a * b = b * a = e$.

	multiplikatív írásmód	additív írásmód
művelet	$a \cdot b = ab$	$a + b$
egységelem	1	0
inverz	a^{-1}	$-a$

7.1. Példa.

- $(\mathbb{C}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{Z}; +)$, $(\{\text{páros számok}\}; +)$, ...
- $(\{0\}; +)$
- $(T^{n \times m}; +)$ tetszőleges T testre
- $(\mathbb{Z}_n; +)$ tetszőleges $n \in \mathbb{N}$ esetén
- $(\mathbb{C} \setminus \{0\}; \cdot)$, $(\mathbb{R} \setminus \{0\}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$
- $(\{1\}; \cdot)$, $(\{1, -1\}; \cdot)$, $(\{1, -1, i, -i\}; \cdot)$
- $(E_n; \cdot)$, ahol $E_n = \{z \in \mathbb{C} : z^n = 1\}$
- $(GL_n(T); \cdot)$, ahol $GL_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}$

általános lineáris csoport

- $(\mathbb{Z}_n^*; \cdot)$ tetszőleges $n \in \mathbb{N}$ esetén
- $(S_n; \cdot)$, ahol $S_n = \{f: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ bijekciók} \}$

n -edfokú szimmetrikus csoport

- szimmetriacsoportok

7.2. Példa. A $\{\pm 1, \pm i, \pm j, \pm k\}$ halmaz csoportot alkot az alábbi szorzással. Ezt a csoportot **kvaterniócsoportnak** nevezzük, és Q -val jelöljük.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

7.3. Megjegyzés. A táblázatból elég az

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik \quad \text{és} \quad i^2 = j^2 = k^2 = -1$$

szorzatokat megjegyezni, a többi már magától értetődő.

Az $a + bi + cj + dk$ ($a, b, c, d \in \mathbb{R}$) alakú kifejezéseket **kvaternióknak** nevezzük. Ezeken természetes módon lehet definiálni az összeadás és szorzás műveletét.

7.4. Tétel.

(1) Bármely grupoidban legföljebb egy egységelem létezhet.

(2) Bármely monoidban egy elemnek legföljebb egy inverze lehet.

Bizonyítás.

(1) Ha e_1 és e_2 is egységelem az $(A; *)$ grupoidban, akkor

- $e_1 * e_2 = e_1$ (mert e_2 egységelem), és
- $e_1 * e_2 = e_2$ (mert e_1 egységelem).
- Tehát $e_1 = e_2$.

(2) Ha az a elemnek inverze b és c is, akkor

- $(b * a) * c = e * c = c$, és
- $b * (a * c) = b * e = b$.
- Tehát $b = (b * a) * c = b * (a * c) = c$. □

7.5. Tétel. Tetszőleges $(A; \cdot)$ monoid és $a, b \in A$ elemek esetén...

(1) ha a -nak van inverze, akkor a^{-1} -nek is van, mégpedig $(a^{-1})^{-1} = a$;

(2) ha a -nak és b -nek van inverze, akkor ab -nek is van, mégpedig

$$(ab)^{-1} = b^{-1}a^{-1}.$$

7.6. Tétel (az általános asszociativitás tétele). Ha $(A; \cdot)$ félcsoporth, akkor minden $n \in \mathbb{N}$ és $a_1, \dots, a_n \in A$ esetén az $a_1 \cdot \dots \cdot a_n$ „szorzat” eredménye független a zárójelezéstől.

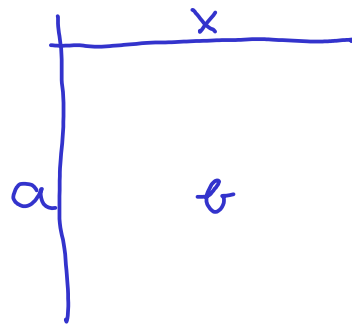
7.7. Definíció. Azt mondjuk, hogy az A halmazon értelmezett $\cdot$ kétváltozós művelet...

- **invertálható**, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek **legalább** egy megoldása van.
- **kancellatív**, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek **legfeljebb** egy megoldása van.

7.8. Megjegyzés. A kancellativitás így is megfogalmazható:

$$\forall a, x_1, x_2, y_1, y_2 \in A: \quad \cancel{a} \cdot x_1 = \cancel{a} \cdot x_2 \implies x_1 = x_2;$$

$$y_1 \cdot \cancel{a} = y_2 \cdot \cancel{a} \implies y_1 = y_2.$$



7.9. Megjegyzés.

- Az invertálhatóság azt jelenti, hogy a művelet táblázat minden sorában és minden oszlopában az A halmaz minden eleme **legalább** egyszer fellép.
- A kancellativitás pedig azt jelenti, hogy minden sorban és minden oszlopban minden elem **legfeljebb** egyszer lép fel.

7.10. Tétel. Csoport művelete mindig invertálható és kancellatív.

Bizonyítás. $\forall (A; \cdot)$ csoport

$$\begin{aligned} a \cdot x &= b && / \bar{a}^{-1} \\ \bar{a}^{-1} \cdot (a \cdot x) &= \bar{a}^{-1} \cdot b \\ (\bar{a}^{-1} \cdot a) \cdot x &= \bar{a}^{-1} \cdot b \\ 1 \cdot x &= \bar{a}^{-1} \cdot b \\ x &= \bar{a}^{-1} \cdot b \end{aligned}$$

legfeljebb 1-szer
KANCELLATIV

$$\begin{aligned} x &= \bar{a}^{-1} \cdot b && / a \\ a \cdot x &= a \cdot (\bar{a}^{-1} \cdot b) \\ a \cdot x &= (a \cdot \bar{a}^{-1}) \cdot b \\ a \cdot x &= 1 \cdot b \\ a \cdot x &= b \end{aligned}$$

legfeljebb 1-szer
INVERTÁLHATÓ $\square$

7.11. Tétel. Ha az A halmazon értelmezett $\cdot$ kétváltozós művelet asszociatív és invertálható, akkor $(A; \cdot)$ csoport.

7.12. Megjegyzés. A fenti tételben véges alaphalmaz esetén kicserélhetjük az invertálhatóságot a kancellativitással, de végtelen alaphalmaz esetén nem.

$(\mathbb{N}; +)$ nem v.p. de kancellatív, azis $x \neq 0$.

$$a + x = b \text{ -ről legf. 1-szer } x = b - a$$

7.13. Feladat. Írjuk fel **a** kételemű és **a** háromelemű csoport művelettáblázatát.

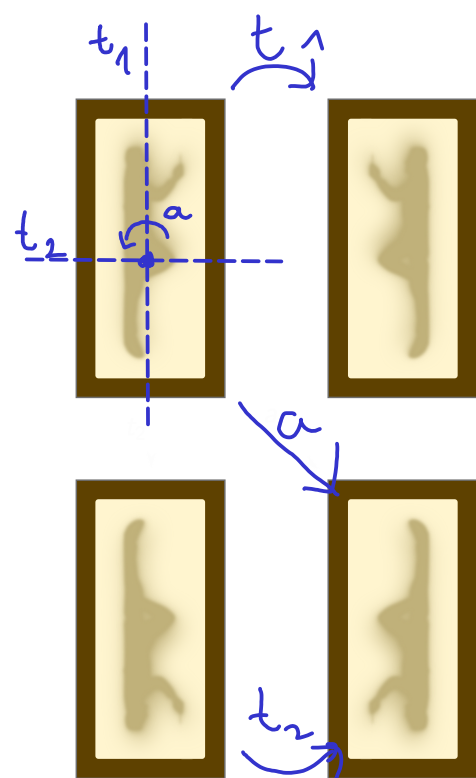
$$G \text{ csoport, } |G|=2 \Rightarrow G \cong \begin{array}{c|cc} & 1 & a \\ \hline 1 & 1 & a \\ a & a & 1 \end{array} \cong \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} = (\mathbb{Z}_2; +)$$

$$G \text{ csoport, } |G|=3 \Rightarrow G \cong \begin{array}{c|ccc} & 1 & a & b \\ \hline 1 & 1 & a & b \\ a & a & b & 1 \\ b & b & 1 & a \end{array} \cong \begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} = (\mathbb{Z}_3; +)$$

$$G \text{ csoport, } |G|=4 \Rightarrow G \cong (\mathbb{Z}_4; +) \text{ vagy } G \cong \begin{array}{c|ccc} & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & 1 & c & b \\ b & b & c & 1 & a \\ c & c & b & a & 1 \end{array}$$

8. Szimmetriacsoportok

Matracfordítás

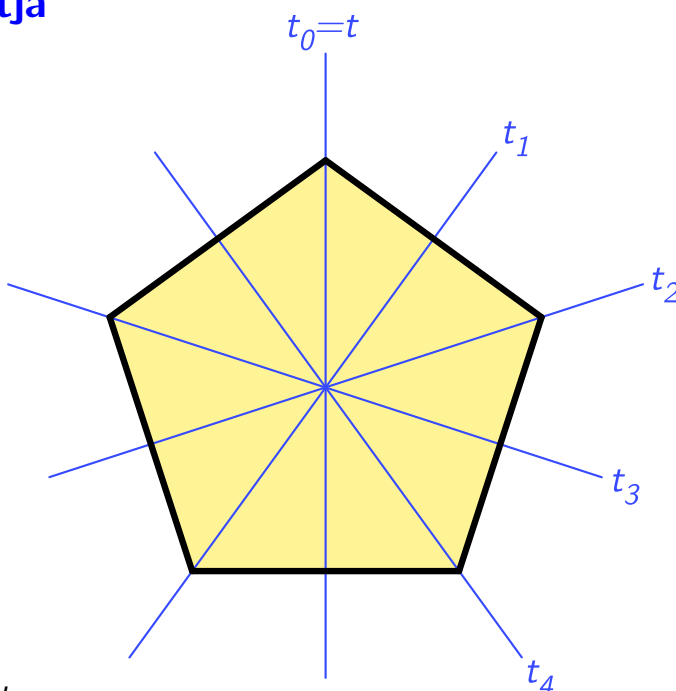
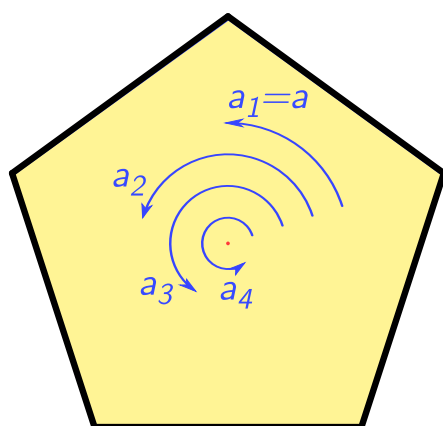


$\cdot$	id	a	t_1	t_2
id	id	a	t_1	t_2
a	a	id	t_2	t_1
t_1	t_1	t_2	id	a
t_2	t_2	t_1	a	id

 $\cong V$

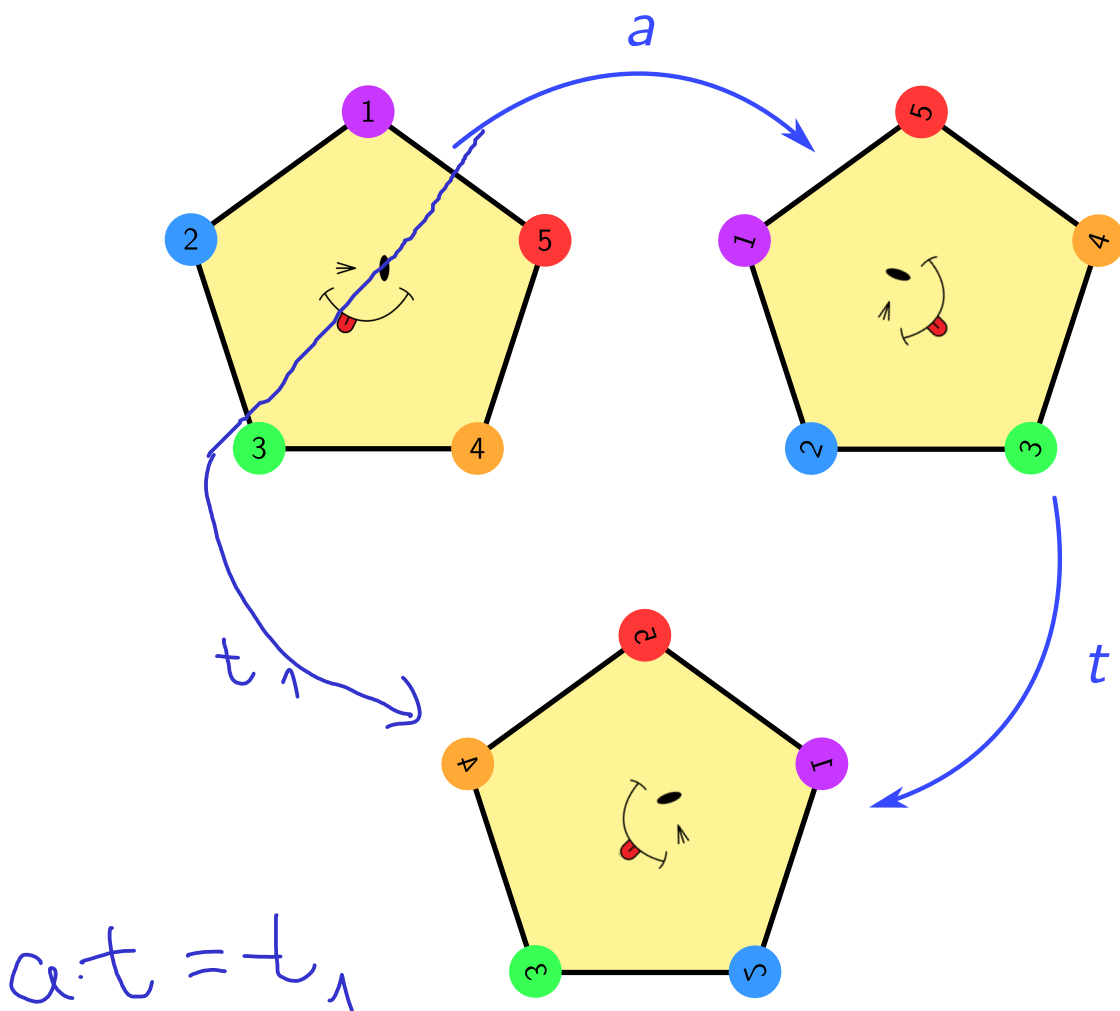
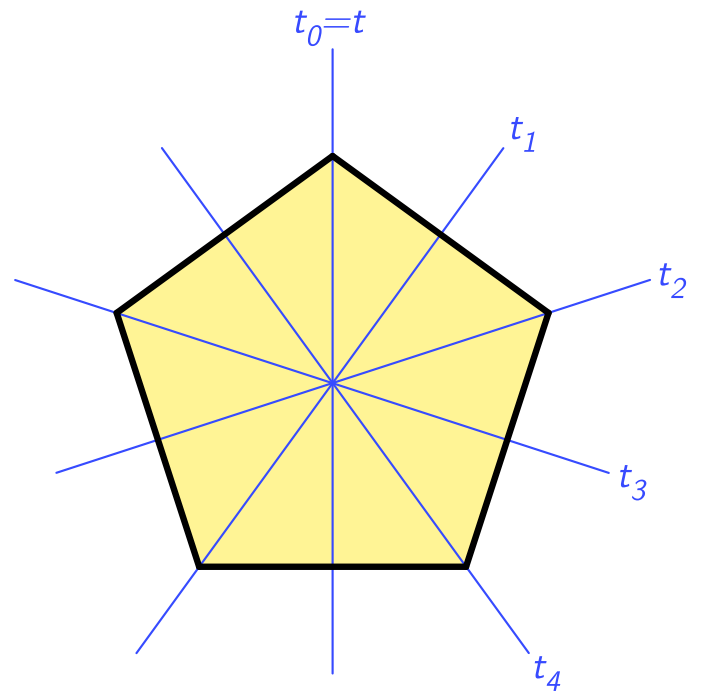
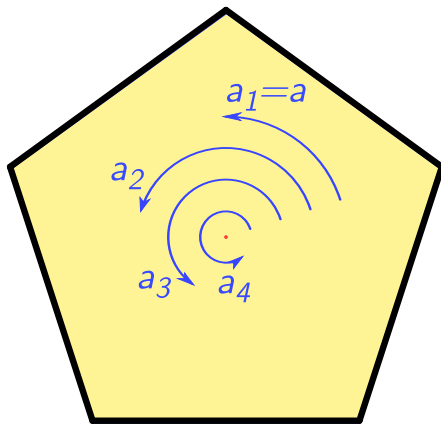
Klein-csoport

A szabályos n -szög szimmetriacsoportja



Jelölje a_k a sokszög középpontja körüli $\frac{2k\pi}{n}$ szögű forgatást ($k = 0, 1, \dots, n-1$). Vegyük észre, hogy $a_k = a_1^k$. A továbbiakban a_1 helyett egyszerűen csak a -t írunk. Így az n -szög **mozgáscsoportja**: $\{\text{id}, a, a^2, \dots, a^{n-1}\} \cong (\mathbb{Z}_n; +)$

Legyenek a szimmetriatengelyekre való tükrözések $t_0, t_1, \dots, t_{n-1}$. A továbbiakban t_0 helyett egyszerűen csak t -t írunk, és szeretnénk a többi tükrözést is t és a segítségével kifejezni.



SPOILER!

Hasonlóan (be)látható, hogy $t_k = a^k t$ minden $k \in \{0, 1, \dots, n-1\}$ esetén.

8.1. Definíció. A szabályos n -szög szimmetriacsoportját **n -edfokú diéder-csoportnak** nevezzük és D_n -nel jelöljük.

8.2. Tétel. A D_n csoportnak $2n$ eleme van:

$$D_n = \{ \text{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t \}, \text{ ahol}$$

- a : a középpont körüli $\frac{2\pi}{n}$ szögű forgatás,
- t : egy szimmetriatengelyre való tükrözés.

Ekkor a^k a középpont körüli $\frac{2k\pi}{n}$ szögű forgatás ($0 \leq k \leq n-1$),

$a, t, at, a^2t, \dots, a^{n-1}t$ transzformációk pedig tengelyes tükrözések (két „szomszédos” tengely $\frac{\pi}{n}$ szöget zár be egymással).

Fennáll továbbá a $ta = a^{-1}t$ összefüggés.

$$ta = a^{-1}t \Leftrightarrow ata = t \Leftrightarrow tata = \text{id}$$

$$(ta)^2 = \text{id}$$

tükr.

$$a^n = \text{id}$$

$$t^2 = \text{id}$$

$$ta = a^{-1}t$$

8.3. Feladat. Számítsuk ki D_{15} -ben az alábbi elemeket. Az eredményt a^k vagy $a^k t$ ($k = 0, 1, \dots, 14$) alakban adjuk meg. $n = 15$

(a) a^{154}

$$154 = 10 \cdot 15 + 4$$

$$a^{154} = \underbrace{(a^{15})^{10}}_{\text{id}} \cdot a^4 = \text{id}^{10} \cdot a^4 = a^4$$

$$154 \equiv 4 \pmod{15}$$

$$a^{154} = a^4$$

(b) $a^7 t \cdot a^{12} t$

$$a^7 t a^{12} t = a^7 a^{-12} \cdot t \cdot t = \underbrace{a^{-5}}_{a^{10} \text{ id}} \cdot t^2 = a^{10}$$

(c) $a^{23} t \cdot a^{18}$

$$a^{23} t a^{18} = a^{23} a^{-18} \cdot t = a^5 t = a^{10} t$$

(d) $(a^{10} t)^3$

$$a^{10} t a^{10} t a^{10} t = \cancel{a^{10}} \cdot \cancel{a^{-10}} / t / t a^{10} t = a^{10} t$$

9. Részcsoportok

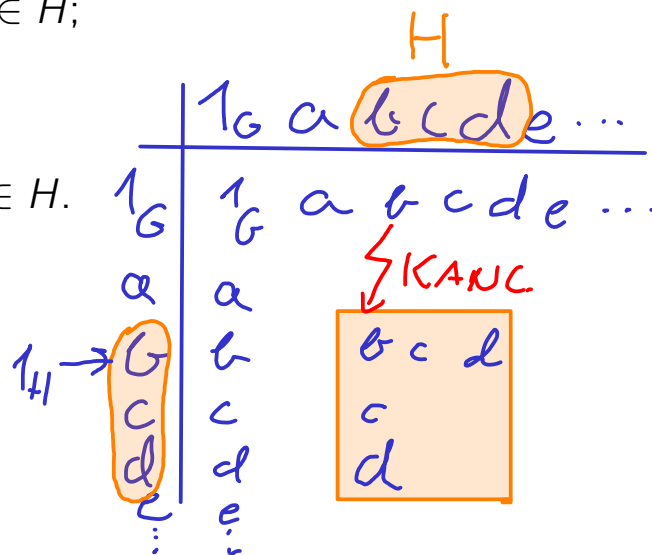
9.1. Definíció. Ha G csoport, és H olyan részgrupoid, ami maga is csoport, akkor azt mondjuk, hogy H **részcsoportja** G -nek, és ezt így jelöljük: $H \leq G$.

9.2. Tétel. Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoportja G -nek, ha

1. H zárt a szorzásra: $\forall h_1, h_2 \in H: h_1 \cdot h_2 \in H$;

2. H tartalmazza G egységelemét: $1 \in H$;

3. H zárt az inverzképzésre: $\forall h \in H: h^{-1} \in H$.



9.3. Tétel (Lagrange tétele). Ha G véges csoport és H részcsoportja G -nek, akkor H elemszáma osztója G elemszámának: $|H| \mid |G|$.

9.4. Példa.

- $(\mathbb{C}; +) \geq (\mathbb{R}; +) \geq (\mathbb{Q}; +) \geq (\mathbb{Z}; +) \geq (\{\text{páros számok}\}; +) \geq (\{0\}; +)$
- $(\mathbb{C} \setminus \{0\}; \cdot) \geq (\mathbb{R} \setminus \{0\}; \cdot) \geq (\mathbb{Q} \setminus \{0\}; \cdot) \geq (\{1\}; \cdot)$
- $(\{1, -1\}; \cdot) \leq (\{1, -1, i, -i\}; \cdot) \leq E_8$
- $(\text{SL}_n(T); \cdot) \leq (\text{GL}_n(T); \cdot)$, ahol
 $\text{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}$ **általános lineáris csoport**
 $\text{SL}_n(T) = \{A \in T^{n \times n} : \det(A) = 1\}$ **speciális lineáris csoport**
- egy alakzat szimmetriacsoportja részcsoportot alkot az összes egybevágósági transzformációk csoportjában
- $S_4 \geq \{\text{id}, (12)(34), (13)(24), (14)(23)\} = V$ **Klein-csoport**
- az S_n csoportban részcsoportot alkotnak a páros permutációk

9.5. Definíció. Az $\{1, 2, \dots, n\}$ halmaz páros permutációinak csoportját **n -edfokú alternáló csoportnak nevezzük.** Jelölés: A_n .

9.6. Tétel. Minden $n \geq 2$ esetén $A_n \leq S_n$ és $|A_n| = \frac{n!}{2}$.

9.7. Feladat. Soroljuk fel az A_3 és A_4 alternáló csoportok elemeit.

$$S_3 = \{ \text{id}, \cancel{(12)}, \cancel{(13)}, \cancel{(23)}, \underbrace{(123)}_{(12)(13)}, \underbrace{(132)}_{(13)(12)} \}$$

$$A_2 = \{id, (123), (132)\}$$

$$S_4: \text{id}, \text{---}, \text{---}, \text{---}, \text{---}$$

$$A_4 = \{ \text{id}, \underbrace{(123), \dots}_{8 \text{ ddr}}, (12)(34), (13)(24), (14)(23) \} \quad V \leq A_4 \leq S_4$$

9.8. Feladat. Részcsoportot alkot-e a G csoportban a H halmaz?

(a) $G = (\mathbb{Z}, +)$ $H = \mathbb{N}_0$ $N \subseteq M$ p.l. $2 \in H$ & $-2 \notin H$

(b) $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ $H = \mathbb{Q}^+ \quad n \in \mathbb{N} \quad -2 \in H \text{ but } (-2) \cdot (-2) \notin H$

(c) $G = \mathbb{C} \setminus \{0\}$; $H = \{z \in \mathbb{C} : |z| = 1\}$ $IGEN$

1. $z, w \in H \Rightarrow |z \cdot w| = |z| \cdot |w| = 1 \cdot 1 = 1 \Rightarrow z \cdot w \in H$

2. $1 (= 1) \Rightarrow 1 \in H$ ✓

3. $z \in H \Rightarrow \left| \frac{1}{z} \right| = \frac{1}{|z|} = \frac{1}{1} = 1 \Rightarrow \frac{1}{z} \in H \checkmark$

(d) $G = (\mathbb{Z}_{21}, +)$ $H = \mathbb{Z}_{21}^*$ $\bar{2}, \bar{5} \in H$, $\text{da } \bar{2} + \bar{5} \notin H$

(e) $G = (\mathbb{Z}_{21}^*, \circ)$ $H = \{ \overline{1}, \overline{8}, \overline{13}, \overline{20} \}$
 $\parallel$
 $-\overline{8}$ $-\overline{1}$

$$\begin{array}{c|cccc} & 1 & -1 & 8 & -8 \\ \hline 1 & 1 & -1 & 8 & -8 \\ -1 & -1 & 1 & -8 & 8 \\ 8 & 8 & -8 & 1 & -1 \\ -8 & -8 & 8 & -1 & 1 \end{array} \approx \cancel{\mathbb{Z}_4} \wr V$$

10. Elem rendje, ciklikus csoportok

10.1. Definíció. Legyen G egy csoport és $a \in G$. Az a elem egész kitevős hatványait a következőképpen értelmezzük:

- $n > 0$ esetén legyen $a^n = \underbrace{a \cdot \dots \cdot a}_n$;

$$"a^n" : \underbrace{a + \dots + a}_n$$

- $n = 0$ esetén legyen $a^n = 1$;

- $n < 0$ esetén legyen $a^n = (a^{-1})^{|n|}$.

10.2. Tétel. Tetszőleges G csoport, $a, b \in G$ elemek és $n, m \in \mathbb{Z}$ kitevők esetén teljesülnek az alábbi azonosságok:

(1) $a^n \cdot a^m = a^{n+m}$;

(2) $(a^n)^m = a^{nm}$;

(3) ha $ab = ba$, akkor $(ab)^n = a^n b^n$;

(4) $(ab)^{-1} = b^{-1} a^{-1}$.

Trivialitás. Az $a \in G$ elemet tartalmazó legszűkebb részcsoporthat:

$$[a] := \{a^k : k \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, \overset{\infty}{1}, \overset{1}{a}, a^2, a^3, \dots\}.$$

10.3. Definíció. A G csoportot **ciklikus csoportnak** nevezzük, ha egyetlen elemmel generálható, azaz $\exists a \in G : [a] = G$.

10.4. Példa. $\mathbb{Z}$ és $\mathbb{Z}_n$ ciklikus csoportok:

- $\mathbb{Z} = [1]$; $1 + \dots + 1 \in [1] \Rightarrow \mathbb{N}_0 \subseteq [1] \xrightarrow{\text{inv.}} \mathbb{Z} \subseteq [1]$

- $\mathbb{Z}_n = [\bar{1}]$.

10.5. Tétel. Ciklikus csoport minden részcsoporthatja is ciklikus.

10.6. Megjegyzés. Minden csoportban „hemzsegek” a ciklikus részcsoporthatok: bármely G csoportban bármely a elem egy ciklikus részcsoporthatot generál.

10.7. Példa. Számítsuk ki a $(\mathbb{C} \setminus \{0\}, \cdot)$ csoportban 2 és i hatványait.

k	...	-4	-3	-2	-1	0	1	2	3	4	5	6	7	...
2^k	...	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{2}$	1	2	4	8	16	32	64	128	...
i^k	...	1	i	-1	$-i$	1	i	-1	$-i$	1	i	-1	$-i$	...

Az első esetben a hatványok mind különbözőek, ezért $(\mathbb{Z}; +) \cong ([2]; \cdot)$

A második esetben négyes periodicitást tapasztalunk, ezért $[i] \cong (\mathbb{Z}_4; +)$

Egy tetszőleges G csoportban egy a elemet hatványozva is ez a két eset lehetséges.

1. eset. A hatványok mind különbözőek.

Ekkor $\varphi: (\mathbb{Z}, +) \rightarrow ([a]; \cdot), k \rightarrow a^k$ izomorfizmus,
ezért $([a]; \cdot) \cong (\mathbb{Z}, +)$.

- Injektivitás: feltettük, hogy $k \neq \ell$ esetén $a^k \neq a^\ell$.
- Szürjektivitás: $[a]$ minden eleme előáll a^k alakban.
- Művelettartás: $(k + \ell)\varphi = a^{k+\ell} = a^k \cdot a^\ell = k\varphi \cdot \ell\varphi$.

2. eset. A hatványok között van ismétlődés: $\exists i < j: a^i = a^j \implies a^{j-i} = 1$.

Legyen n a legkisebb **pozitív** kitevő, amelyre $a^n = 1$.

Az $a^0, a^1, a^2, \dots, a^{n-1}$ hatványok páronként különbözőek és minden más hatvány ezek valamelyikével megegyezik:

$k = nq + r$ esetén $a^k = a^{nq+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r$.

Ekkor $\varphi: (\mathbb{Z}_n, +) \rightarrow ([a]; \cdot), \bar{k} \rightarrow a^k$ izomorfizmus,
ezért $([a]; \cdot) \cong (\mathbb{Z}_n, +)$.

- Jóldefiniáltság: $k \equiv \ell \pmod{n} \implies a^k = a^\ell$.
- Injektivitás: $k \not\equiv \ell \pmod{n} \implies a^k \neq a^\ell$.
- Szürjektivitás: $[a]$ minden eleme előáll a^k ($k = 0, \dots, n-1$) alakban.
- Művelettartás: $(\bar{k} + \bar{\ell})\varphi = \overline{k+\ell}\varphi = a^{k+\ell} = a^k \cdot a^\ell = \bar{k}\varphi \cdot \bar{\ell}\varphi$.

10.8. Tétel. Egy csoport akkor és csak akkor ciklikus, ha izomorf a következő csoportok valamelyikével:

$$\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \dots, \mathbb{Z}.$$

10.9. Definíció. Az $a \in G$ elem **rendjén** azt a legkisebb n pozitív egész számot értjük, amelyre $a^n = 1$. Ha nincs ilyen n , akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét $o(a)$ jelöli (olvasd: *ordó*):

$$o(a) = \min \{n \in \mathbb{N} : a^n = 1\} \quad (\text{a } \min \emptyset = \infty \text{ megállapodással}).$$

10.10. Definíció. A G csoport **rendjén** elemeinek számát (számosságát) értjük.

10.11. Megjegyzés. Az a elem rendje nem más, mint az általa generált részcsoporthat rendje: $o(a) = |[a]|$. (Sőt, $[a] \cong \mathbb{Z}_{o(a)}$.)

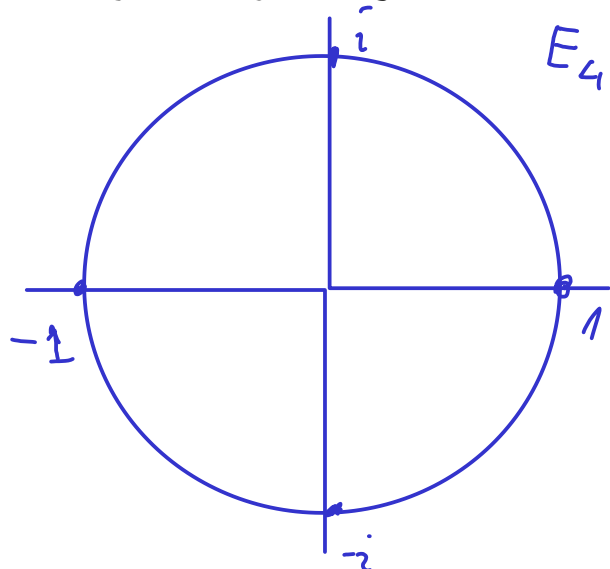
10.12. Példa. Határozzuk meg az $a \in G$ elem rendjét.

- $G = (\mathbb{C} \setminus \{0\}; \cdot)$ $a = 2$: $[2] = \{\dots, \frac{1}{2}, 1, 2, 4, \dots\} \cong \mathbb{Z}$, $o(2) = \infty$
- $G = (\mathbb{C} \setminus \{0\}; \cdot)$ $a = i$: $[i] = \{i, -1, -i, 1\} \cong \mathbb{Z}_4$, $o(i) = 4$
- $G = (\mathbb{C}; +)$ $a = i$: $[i] = \{\dots, -i, 0, i, 2i, \dots\} \cong \mathbb{Z}$, $o(i) = \infty$

10.13. Megjegyzés. Tetszőleges $z \in \mathbb{C} \setminus \{0\}$ komplex szám esetén

$$o(z) = n \iff |[z]| = n \iff \underbrace{[z]}_{n\text{-ed.}} \cong \underbrace{E_n}_{n\text{-ed.}} \cong \mathbb{Z}_n.$$

Az ilyen tulajdonságú számokat nevezzük **primitív n -edik egységgyököknek**.



$$E_4 = \{1, -1, i, -i\} \quad \text{s. 2.}$$

$$[i] = \{1, i, -1, -i\} = E_4 \quad \sigma(i) = 4$$

$$[-i] = \{1, -i, -1, i\} = E_4 \quad \sigma(-i) = 4$$

$$[-1] = \{1, -1\} = E_2 \quad \sigma(-1) = 2$$

$$[1] = \{1\} = E_1 \quad \sigma(1) = 1$$

10.14. Feladat. Határozzuk meg a G csoportban a megadott elem rendjét.

(a) $G = \mathbb{Z}_{10} \ni \bar{2}$ $[2] = \{2, 4, 6, 8, 0\} \cong \mathbb{Z}_5$ $\sigma(2) = 5$

(b) $G = \mathbb{Z}_{10} \ni \bar{3}$ $[3] = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} = \mathbb{Z}_{10}$ $\sigma_{\mathbb{Z}_{10}}(3) = 10$

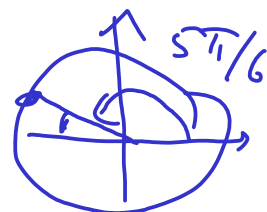
(c) $G = \mathbb{Z}_{10} \ni \bar{4}$ $[4] = \{4, 8, 2, 6, 0\} \cong \mathbb{Z}_5$ $\sigma(4) = 5$
 $[2] =$

(d) $G = \mathbb{Z}_{10}^* \ni \bar{3}$ $[3] = \{3, 9, 7, 1\} \cong \mathbb{Z}_4$ $\sigma_{\mathbb{Z}_{10}^*}(3) = 4$

(e) $G = \mathbb{Z}_{12} \ni \bar{5}$ $[5] = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} = \mathbb{Z}_{12}$ $\sigma_{\mathbb{Z}_{12}}(5) = 12$

(f) $G = \mathbb{Z}_{12}^* \ni \bar{5}$ $[5] = \{5, 1\} = \mathbb{Z}_2$ $\sigma_{\mathbb{Z}_{12}^*}(5) = 2$

(g) $G = \mathbb{C} \setminus \{0\} \ni \overbrace{-\frac{\sqrt{3}}{2} + \frac{1}{2}i}^z = \cos \frac{5\pi}{6} + i \sin \frac{5\pi}{6} = \operatorname{cis} \frac{5\pi}{6}$
 $z^n = \operatorname{cis} \frac{5n\pi}{6} = 1 \Leftrightarrow 12|n$



(h) $G = S_5 \ni (234) = \alpha$
 $\sigma(\alpha) = 3$

(i) $G = S_5 \ni (234)(15) = \beta$ $\sigma(\beta) = 6$
 $\beta^2 = ((234)(15))^2 = (234)^2(15)^2 = \text{id} \Leftrightarrow 3, 2|k$

(j) $G = S_5 \ni (1245)(234) = \gamma$ $\gamma^2 \neq (1245)^2 \cdot (234)^2$
 $\gamma = (1345)(2) \Rightarrow \sigma(\gamma) = 4$

(k) $G = D_{10} \ni a^4$ $[a^4] = \{a^4, a^8, a^2, a^6, a^0 = \text{id}\} \cong \mathbb{Z}_5 \Rightarrow \sigma(a^4) = 5$

(l) $G = D_{10} \ni a^4 t \leftarrow \text{tükr.}$ $(a^4 t)^2 = \text{id} \Rightarrow [a^4 t] = \{a^4 t, \text{id}\} \cong \mathbb{Z}_2$
 $a^4 t \cdot a^4 t = a^4 \cdot a^4 \cdot t \cdot t = \text{id}$
 $\sigma(a^4 t) = 2$

noldali söring $\mathbb{Z}$ -additív végtelen csoport.

x egész utca $\mathbb{Z}$. $x \bmod n$

Mi az a legkisebb $x \in \mathbb{N}$, amire $\mathbb{Z}x \equiv 0 \pmod{n}$?

$$x \equiv 0 \pmod{\frac{n}{(n, k)}}$$

$$\frac{n}{(n, k)} \mid x$$

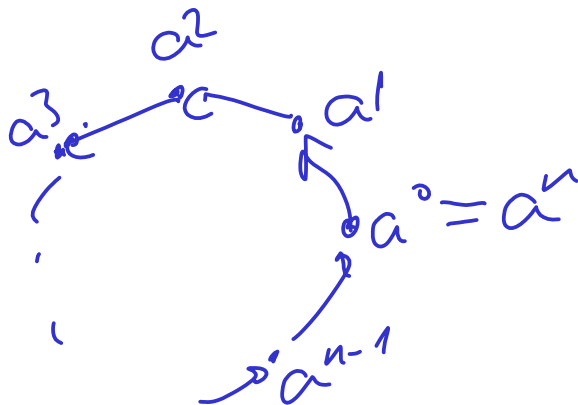
A legkisebb pozit. $x = \frac{n}{(n, k)}$.



Ez a legkisebb
által. div. osztó.
Összehang.
úgy is lehet el.

$$\forall a \in \mathbb{Z}^* \Leftrightarrow (n, a) = 1$$

$$\forall k \in \mathbb{Z}_n: [k] = \mathbb{Z}_n \Leftrightarrow (n, k) = 1$$



10.15. Tétel (A rend tulajdonságai). Legyen G egy véges csoport és $a \in G$ egy n -edrendű elem.

$$(1) \forall k, \ell \in \mathbb{Z}: a^k = a^\ell \iff k \equiv \ell \pmod{n}$$

$$(2) a^{-1} = a^{n-1} = \overbrace{a \cdot \dots \cdot a}^{n-1}$$

$$(3) \forall k \in \mathbb{Z}: a^k = 1 \iff n \mid k$$

(4) n osztója G elemszámának

$$(5) a^{|G|} = 1$$

$$(6) o(a^k) = \frac{n}{\gcd(n, k)} \quad [a^k] \leq [a] \cong \mathbb{Z}_n \text{ cyclic}$$

Bizonyítás.

$$(1) \text{ld tétel. } [a] \cong \mathbb{Z}_n$$

$$(2) -1 \equiv n-1 \pmod{n} \xrightarrow{(\cdot)} a^{-1} = a^{n-1}$$

$$\forall a \in G: o(a) = n \Rightarrow a^n = 1 \xrightarrow{(\cdot a^{-1})} a^{n-1} = a^{-1}$$

$$(3) a^k = 1 = a^0 \xrightarrow{(\cdot)} k \equiv 0 \pmod{n} \iff n \mid k$$

$$(4) [a] \leq G \implies |[a]| \mid |G|$$

$$(5) o(a) = n \implies a^n = 1 \xrightarrow{(\cdot)} a^{|G|} = 1 \quad (|G|/n \in \mathbb{N} \text{ (4)})$$

$$(6) C_{n|k}$$

10.16. Tétel. Minden prímmrendű csoport ciklikus.

Bizonyítás.

$$|G| = p \text{ prím. } (a \in G \Rightarrow \sigma(a) | p \Rightarrow \sigma(a) = 1 \vee \sigma(a) = p$$

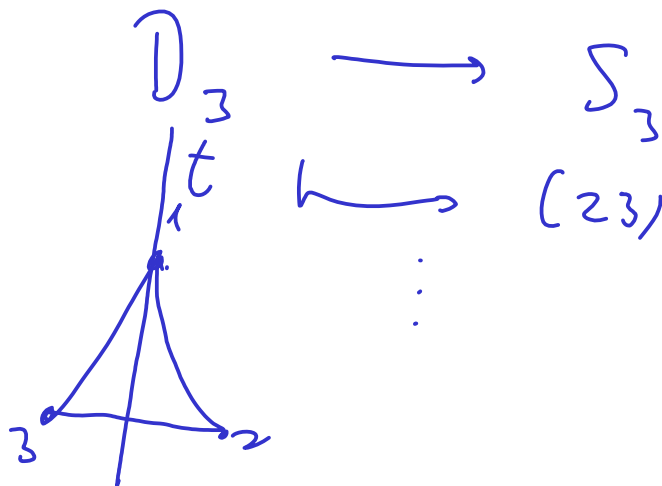
$\uparrow$
 $a=1$

$$\text{Teljesen } \forall a \in G \setminus \{1\} : |[a]| = p \rightarrow [a] = G$$

$\cong \mathbb{Z}_p$

10.17. Tétel. A kis elemszámú csoportok (izomorfia erejéig) a következők:

- egyelemű: $\{1\}$;
- kételemű: $\mathbb{Z}_2$;
- háromelemű: $\mathbb{Z}_3$;
- négyelemű: $\mathbb{Z}_4$ és V ;
- ötelemű: $\mathbb{Z}_5$;
- hatelemű: $\mathbb{Z}_6$ és $S_3 \cong D_3$



Bizonyítás.

$$|G| = 4 \quad \forall a \in G : \sigma(a) = 1, 2, 4$$

$$1) \text{ Ha } \exists a \in G : \sigma(a) = 4, \text{ akkor } [a] = G$$

$\cong \mathbb{Z}_4$

$$2) \text{ Ha } \forall a \in G \setminus \{1\} : \sigma(a) = 2 \rightarrow a^2 = 1$$

$G:$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\cong V$

11. Generálás

11.1. Definíció. Legyen G egy csoport és $\emptyset \neq B \subseteq G$. A B részhalmaz által **generált részcsoporthon** a G csoport **legszerűbb** olyan részcsoporthját értjük, ami tartalmazza B -t. Jelölés: $[B]$.

A B halmaz által generált részcsoporth nem más, mint...

- az összes B -t tartalmazó részcsoporthok metszete;
- azon G -beli elemek halmaza, amelyek megkaphatók B elemeiből kiindulva a szorzás és az inverzképzés véges számú alkalmazásával.

Ha $[B] = G$, akkor azt mondjuk, hogy B **generátorrendszere** G -nek.

11.2. Példa.

- $\mathbb{Z} = [1]$
- $\mathbb{Z}_n = [\bar{1}]$
- $(\mathbb{Q}^+)_1 = [\{\text{prímszámok}\}]$
- $S_n = [\{\text{transzpozíciók}\}]$
- $D_n = [a, t]$

11.3. Feladat. Határozzuk meg a $\mathbb{Z}$ csoportban a $[6, 10]$ részcsoporthot.

pr. $(\mathbb{Z}, +) \supseteq [6, 10] = \{6, 10, 16, 22, 4, -4, 2, \dots\}$

$2 \in [6, 10] \Rightarrow \underbrace{2 + \dots + 2}_{2k} \in [6, 10] \rightarrow \{2k \mid k \in \mathbb{Z}\} \subseteq [6, 10]$

$6, 10 \text{ prs} \Rightarrow [6, 10] \subseteq [2]$

így: $[6, 10] = [2] = \{2k \mid k \in \mathbb{Z}\}$

$[6, 10] = \{6x + 10y \mid x, y \in \mathbb{Z}\} = \{c \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} : 6x + 10y = c\}$
 $= \{c \in \mathbb{Z} \mid (6, 10) \mid c\} = \{c \in \mathbb{Z} \mid 2 \mid c\}$

11.4. Feladat. Határozzuk meg a $\mathbb{Z}_{14}$ csoportban a $[\overline{6}, \overline{10}]$ részcsoporthot.

$$[\overline{6}, \overline{10}] = \{\overline{6}x + \overline{10}y : x, y \in \mathbb{Z}\} = \{\overline{2}k : k \in \mathbb{Z}\} = [\overline{2}] = \\ = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{0}\} \cong \mathbb{Z}_7$$

11.5. Feladat. Határozzuk meg a $\mathbb{Z}_{15}$ csoportban a $[\overline{6}, \overline{10}]$ részcsoporthot.

$$[\overline{6}, \overline{10}] = \{\overline{6}x + \overline{10}y : x, y \in \mathbb{Z}\} = \{\overline{2}k : k \in \mathbb{Z}\} = [\overline{2}] = \\ = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{0}\} \cong \mathbb{Z}_{15}$$

11.6. Feladat. Határozzuk meg a $\mathbb{Z}_{28}^*$ csoportban a $[\overline{25}, \overline{27}]$ részcsoporthot.

$$\mathbb{Z}_{28}^* \supseteq [-1, -3] \stackrel{?}{=} \{-1, -3, 1, 3, 9, -9\} = [3]$$

$$\begin{array}{ll} (\pm 1) \cdot (\pm 1) = \pm 1 & (\pm 3) \cdot (\pm 3) = \pm 9 \\ (\pm 1) \cdot (\pm 3) = \pm 3 & (\pm 3) \cdot (\pm 9) = \pm 27 = \pm 1 \\ (\pm 1) \cdot (\pm 9) = \pm 9 & (\pm 9) \cdot (\pm 9) = \pm 81 = \pm 3 \end{array}$$

11.7. Feladat. Határozzuk meg a D_8 csoportban az $[a^6, a^3t]$ részcsoporthot.

$a: 45^\circ$ $a^2: 90^\circ$

$$[a^6] = \{a^0, a^4, a^2, a^8 = a^0 = id\} = \{id, a^2, a^4, a^6\} \cong \mathbb{Z}_4$$

$$[a^6, a^3t] \stackrel{?}{=} \{id, a^2, a^4, a^6, a^3t, a^5t, a^7t, a^1t\}$$

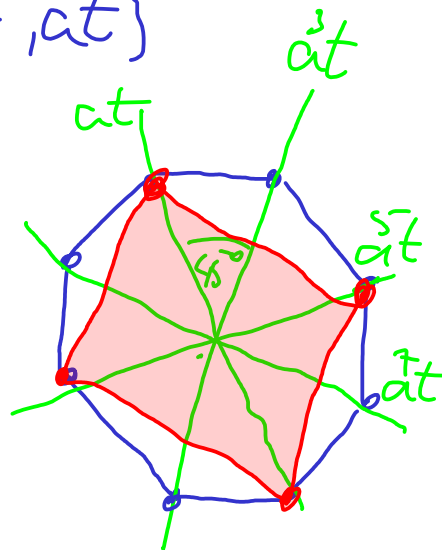
$$= \{a^{2k}, a^{2k+1} \cdot t \mid k \in \mathbb{Z}\} \cong D_4$$

$$a^{2k} \cdot a^{2l} = a^{2(k+l)} \checkmark$$

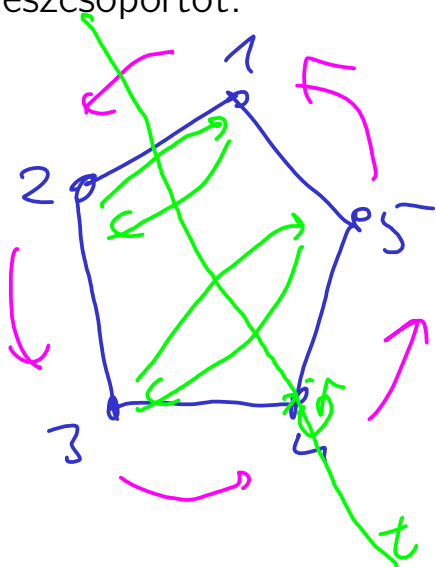
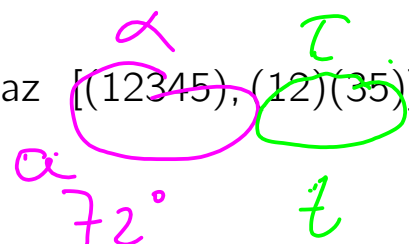
$$a^{2k} \cdot a^{2l+1} t = a^{2(k+l)+1} t \checkmark$$

$$a^{2k+1} t \cdot a^{2l} = a^{2(k-l)+1} t \checkmark$$

$$a^{2k+1} t \cdot a^{2l+1} t = a^{2(k-l)} \cancel{t} = a^{2(k-l)} \checkmark$$



11.8. Feladat. Határozzuk meg az S_5 csoportban az $[(12345), (12)(35)]$ részcsoporthot.



$$[\alpha, \tau] \leq S_5$$

$$\parallel S$$

$$[\alpha, t] = D_5$$

$$[\alpha, t] = \{id, \alpha, \tau, (15)(24), \dots\}$$

10 elem