Algebrai struktúrák

Definíció. Algebrai struktúra: $(A; F)$, ahol A nemüres halmaz, és F az A halmazon értelmezett műveletek egy halmaza.

Példák.

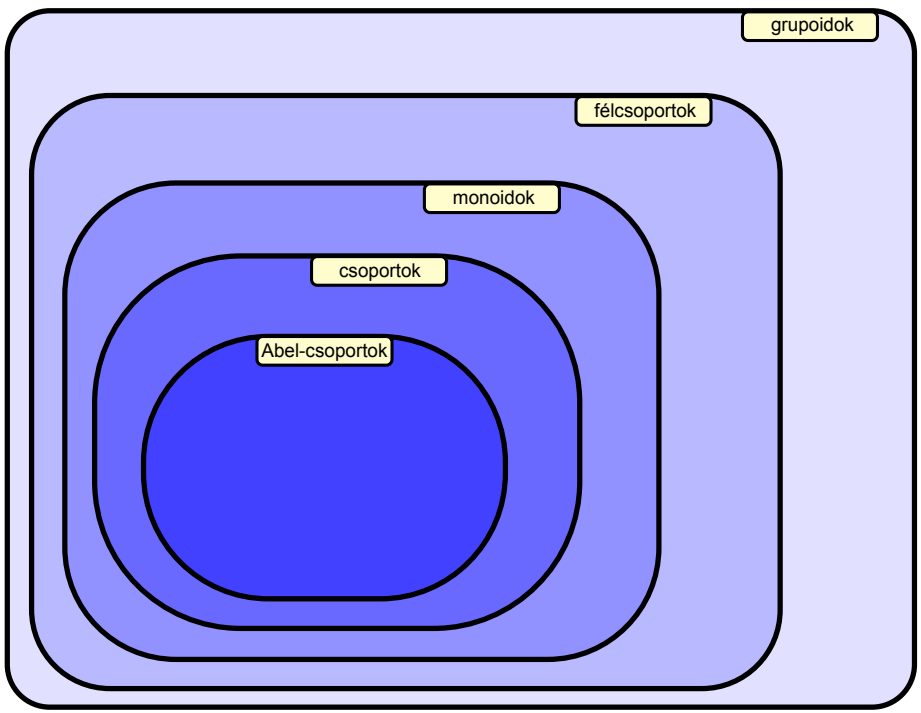
- Az összeadás művelet az egész számok halmazán, ezért $(\mathbb{Z}; +)$ algebrai struktúra.
- Az összeadás és a szorzás művelet az egész számok halmazán, ezért $(\mathbb{Z}; +, \cdot)$ algebrai struktúra.
- A szorzás nem művelet a negatív egész számok halmazán, ezért $(\mathbb{Z}^-; \cdot)$ nem algebrai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

algebrai struktúrák

Félcsoportok és csoportok

Definíció. Legyen A nemüres halmaz.

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



1. feladat

(a) Milyen algebrai struktúra $(\mathbb{N}; +)$?

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

(b) Milyen algebrai struktúra $(\mathbb{Z}; +)$?

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

(c) Milyen algebrai struktúra $(\mathbb{Z}; \cdot)$?

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

1. feladat

(d) Milyen algebrai struktúra $(\mathbb{Z} \setminus \{0\}; \cdot)$?

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

(e) Milyen algebrai struktúra $(\mathbb{Z}_5; +)$?

1. művelet? IGEN $\Longrightarrow$ $(\mathbb{Z}_5; +)$ grupoid
2. asszociatív? IGEN $\Longrightarrow$ $(\mathbb{Z}_5; +)$ félcsoport
3. egységelem? VAN $(\overline{0})$ $\Longrightarrow$ $(\mathbb{Z}_5; +)$ monoid
4. inverz? MINDENKINEK VAN ($\overline{a}$ inverze $\overline{-a}$) $\Longrightarrow$ $(\mathbb{Z}_5; +)$ csoport
5. kommutatív? IGEN $\Longrightarrow$ $(\mathbb{Z}_5; +)$ Abel-csoport

(f) Milyen algebrai struktúra $(\mathbb{Z}_5; \cdot)$?

1. művelet? IGEN $\Longrightarrow$ $(\mathbb{Z}_5; \cdot)$ grupoid
2. asszociatív? IGEN $\Longrightarrow$ $(\mathbb{Z}_5; \cdot)$ félcsoport
3. egységelem? VAN $(\overline{1})$ $\Longrightarrow$ $(\mathbb{Z}_5; \cdot)$ monoid
4. inverz? NINCS MINDENKINEK (pl. $\overline{0}$-nak nincs)

1. feladat

(g) Milyen algebrai struktúra $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$?

1. művelet? IGEN $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$ grupoid
2. asszociatív? IGEN $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$ félcsoport
3. egységelem? VAN $(\overline{1})$ $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$ monoid
4. inverz? MINDENKINEK VAN $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$ csoport
5. kommutatív? IGEN $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; \cdot)$ Abel-csoport

(h) Milyen algebrai struktúra $(\mathbb{Z}_5 \setminus \{\overline{0}\}; +)$?

1. művelet? NEM (pl. $\overline{2} + \overline{3} = \overline{0} \notin \mathbb{Z}_5 \setminus \{\overline{0}\}$) $\Longrightarrow$ $(\mathbb{Z}_5 \setminus \{\overline{0}\}; +)$ nem is grupoid

(i) Milyen algebrai struktúra $(M_2; +)$? (Itt M_2 a 2×2-es valós mátrixok halmaza.)

1. művelet? IGEN $\Longrightarrow$ $(M_2; +)$ grupoid
2. asszociatív? IGEN $\Longrightarrow$ $(M_2; +)$ félcsoport
3. egységelem? VAN $(\mathbf{0} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ $\Longrightarrow$ $(M_2; +)$ monoid
4. inverz? MINDENKINEK VAN (A inverze $-A$) $\Longrightarrow$ $(M_2; +)$ csoport
5. kommutatív? IGEN $\Longrightarrow$ $(M_2; +)$ Abel-csoport

1. feladat

(j) Milyen algebrai struktúra $(M_2; \cdot)$?

1. művelet? IGEN $\implies$ $(M_2; \cdot)$ grupoid
2. asszociatív? IGEN $\implies$ $(M_2; \cdot)$ félcsoport
3. egységelem? VAN $(E = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ $\implies$ $(M_2; \cdot)$ monoid
4. inverz? NINCS MINDENKINEK (pl. $\mathbf{0}$-nak nincs)

(k) Milyen algebrai struktúra $(M_2 \setminus \{\mathbf{0}\}; \cdot)$?

1. művelet? NEM (pl. $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$) $\implies$ $(M_2 \setminus \{\mathbf{0}\}; \cdot)$ nem is grupoid

(l) Milyen algebrai struktúra $\mathrm{GL}_2(\mathbb{R}) := (\{A \in M_2 \mid \det(A) \neq 0\}; \cdot)$?

1. művelet? IGEN (ha $A, B \in \mathrm{GL}_2(\mathbb{R})$, akkor $\det(AB) = \det(A) \cdot \det(B) \neq 0$) $\implies$ $\mathrm{GL}_2(\mathbb{R})$ grupoid
2. asszociatív? IGEN $\implies$ $\mathrm{GL}_2(\mathbb{R})$ félcsoport
3. egységelem? VAN (E) $\implies$ $\mathrm{GL}_2(\mathbb{R})$ monoid
4. inverz? MINDENKINEK VAN (A inverze A^{-1}) $\implies$ $\mathrm{GL}_2(\mathbb{R})$ csoport
5. kommutatív? NEM (pl. $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$)

Gyakorolj!

2. feladat.

(a) Milyen algebrai struktúra $(\mathbb{Q} \setminus \{0\}; +)$?

(b) Milyen algebrai struktúra $(\mathbb{Q} \setminus \{0\}; \cdot)$?

(c) Milyen algebrai struktúra $(\mathbb{Q}^+; +)$?

(d) Milyen algebrai struktúra $(\mathbb{Q}^+; \cdot)$?

(e) Milyen algebrai struktúra $(\mathbb{Z}^-; +)$?

(f) Milyen algebrai struktúra $(\mathbb{Z}_6 \setminus \{\overline{0}\}; \cdot)$?

(g) Milyen algebrai struktúra $(\mathbb{N}; \cdot)$?

3. feladat.

(a) Milyen algebrai struktúra $(\{u, v, w\}; \diamond)$?

$\diamond$	u	v	w
u	v	w	u
v	w	u	v
w	u	v	w

(b) Milyen algebrai struktúra $(\{a, b, c, d\}; \circ)$?

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

3. feladat.

(c) Milyen algebrai struktúra $(\{a, b, c, d\}; *)$?

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

(d) Milyen algebrai struktúra $(\mathcal{P}(\{u, v\}); \cup)$?

(e) Milyen algebrai struktúra $(\{\texttt{igaz}, \texttt{hamis}\}; \rightarrow)$?

(f) Milyen algebrai struktúra $(\{1, -1, i, -i\}; \cdot)$?

Gyakorolj!

4. feladat.

(a) Milyen algebrai struktúra $(\mathbb{Z}; \diamond)$, ahol $a \diamond b = a - b$?

(b) Milyen algebrai struktúra $(\mathbb{Z}; \bullet)$, ahol $a \bullet b = a + b + 23$?

(c) Milyen algebrai struktúra $(\mathbb{Z}; \otimes)$, ahol $a \otimes b = b + 2$?

(d) Milyen algebrai struktúra $(\mathbb{Z}; \oplus)$, ahol $a \oplus b = a$?

(e) Milyen algebrai struktúra $(\mathbb{Q}; \star)$, ahol $a \star b = 12 - 3a - 3b + a \cdot b$?

(f) Milyen algebrai struktúra $(\mathbb{Q} \setminus \{3\}; \star)$, ahol $a \star b = 12 - 3a - 3b + a \cdot b$?

Gyűrűk és testek

Definíció. Legyen A nemüres halmaz, és legyenek $+$ és $\cdot$ kétváltozós műveletek az A halmazon.

- Az $(A; +, \cdot)$ struktúrát **gyűrűnek** nevezzük, ha
  1. $(A; +)$ Abel-csoport, azaz
     - az összeadás asszociatív,
     - van additív egységelem (jelölése: 0),
     - minden elemnek van additív inverze (jelölése: $-a$),
     - az összeadás kommutatív;
  2. $(A; \cdot)$ félcsoport, azaz
     - a szorzás asszociatív;
  3. és a szorzás disztributív az összeadásra, azaz
     - $(a+b)\cdot c = a\cdot c + b\cdot c$ és $c\cdot(a+b) = c\cdot a + c\cdot b$ minden $a, b, c \in A$ esetén.
- Az $(A; +, \cdot)$ struktúrát **testnek** nevezzük, ha
  1. $(A; +, \cdot)$ gyűrű,
  2. $|A| \geq 2$,
  3. a szorzás kommutatív,
  4. van multiplikatív egységelem (jelölése: 1),
  5. minden nemnulla elemnek van multiplikatív inverze (jelölése: a^{-1}).

Példák.

- $(\mathbb{C}; +, \cdot)$ test
- $(\mathbb{R}; +, \cdot)$ test
- $(\mathbb{Q}; +, \cdot)$ test
- $(\mathbb{Z}; +, \cdot)$ gyűrű
- $(\mathbb{N}; +, \cdot)$ nem gyűrű
- $(M_2; +, \cdot)$ gyűrű
- $(\mathcal{P}(\{u, v\}); \triangle, \cap)$ gyűrű
  (additív egységelem: $\emptyset$, multiplikatív egységelem: $\{u, v\}$)
- $(\mathbb{Z}_m; +, \cdot)$ mindig gyűrű, időnként még test is
  (additív egységelem: $\overline{0}$, multiplikatív egységelem: $\overline{1}$)

Maradékosztály-gyűrűk és maradékosztálytestek

Definíció. A $(\mathbb{Z}_m; +, \cdot)$ gyűrűt modulo m **maradékosztály-gyűrűnek** nevezzük

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

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ez nem test, mert $\overline{2}$-nak nincs multiplikatív inverze.

Példa. $\mathbb{Z}_5$ összeadó- és szorzótáblája:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ez test, mert $\overline{0}$ kivételével mindenkinek van multiplikatív inverze:

$$\overline{1}^{-1} = \overline{1}, \quad \overline{2}^{-1} = \overline{3}, \quad \overline{3}^{-1} = \overline{2}, \quad \overline{4}^{-1} = \overline{4}.$$

Példa. Számítsuk ki $\mathbb{Z}_{20}$-ban $\overline{3}$ multiplikatív inverzét.

Jelölje az inverzet $\overline{x}$. Ekkor $\overline{3} \cdot \overline{x} = \overline{1}$, azaz $3x \equiv 1 \pmod{20}$.
Ezt a lineáris kongruenciát könnyen megoldhatjuk:

$$\begin{aligned} 3x &\equiv 1 \pmod{20} \\ 3x &\equiv 21 \pmod{20} \qquad (\text{lnko}\,(3,20) = 1) \\ x &\equiv 7 \pmod{20} \end{aligned}$$

Tehát $\mathbb{Z}_{20}$-ban $\overline{3}^{-1} = \overline{7}$.

Példa. Számítsuk ki $\mathbb{Z}_{20}$-ban a $\dfrac{\overline{4}}{\overline{3}}$ hányadost.

Felhasználhatjuk az előző példa eredményét:

$$\frac{\overline{4}}{\overline{3}} = \overline{4} \cdot \overline{3}^{-1} = \overline{4} \cdot \overline{7} = \overline{28} = \overline{8}.$$

Íme egy másik megoldás, ami nem használja a korábban kiszámolt inverzet:

$$\frac{\overline{4}}{\overline{3}} = \frac{\overline{24}}{\overline{3}} = \frac{\overline{3} \cdot \overline{8}}{\overline{3}} = \overline{8}.$$

Tétel. A $\mathbb{Z}_m$ maradékosztály-gyűrű akkor és csak akkor test, ha m prímszám.