

MTN212: Műveletek és algebrák

(előadásvázlat, 2022. február 28.)

Kátai-Urbán Kamilla, Maróti Miklós

Jelölje $\mathbb{Z}$ az egész számok halmazát, $\mathbb{N}$ a pozitív egészek halmazát, $\mathbb{N}_0$ a nem negatív egészek halmazát, $\mathbb{Q}$ a racionális számok halmazát, $\mathbb{R}$ a valós számok halmazát, $\mathbb{R}_0^+$ a nem negatív valós számok halmazát, $\mathbb{R}^{m \times n}$ az $m \times n$ -es valós mátrixok halmazát.

Legyen m természetes szám. Ekkor $\mathbb{Z}_m$ jelölje a $\overline{0}, \overline{1}, \dots, \overline{m-1}$ elemek halmazát. Ezen a halmazon a következőképpen definiáljuk az összeadást és a szorzást.

1. Definíció. Tetszőleges $\overline{a}, \overline{b} \in \mathbb{Z}_m$ esetén $\overline{a} + \overline{b} = \overline{c} \in \mathbb{Z}_m$, ahol c az a nemnegatív egész maradék, amit akkor kapunk, ha az $a + b$ egész számot maradékosan osztjuk az m számmal. A szorzást a $\mathbb{Z}_m$ halmazon az összeadáshoz hasonlóan definiáljuk.

2. Példa. A $\mathbb{Z}_6$ halmazon $\overline{2} + \overline{5} = \overline{1}$ és $\overline{2} \cdot \overline{5} = \overline{4}$.

1. MŰVELETI TULAJDONSÁGOK

3. Jelölés. Legyen A egy tetszőleges halmaz, jelölje A^n az n -tényezős $A \times A \times \dots \times A$ Descartes-szorzatot.

4. Definíció. Legyen A tetszőleges nemüres halmaz, és $n \in \mathbb{N}_0$. Az A -n értelmezett **n -változós művelet** egy $A^n \rightarrow A$ leképezést értünk, n -et a művelet változószámának (aritásának) nevezzük.

5. Megjegyzés. Az előző definíció $n = 0$ esetén egy elem kijelölését jelenti az A halmazból.

6. Definíció. Legyen A tetszőleges nemüres halmaz, $\mathcal{F}$ pedig jelölje az A -n értelmezett műveletek egy halmazát, ekkor az $(A; \mathcal{F})$ párt **algebrának** nevezzük.

7. Példa. Ha az előző definícióban szereplő $\mathcal{F}$ véges halmaz, akkor elemeit felsoroljuk a halmaz jelet elhagyva, például algebrák a következők: $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Z}; -)$, $(\mathbb{N}; 1, \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2 \times 2}; \cdot)$, $(\mathbb{Z}; \min, \max)$, $(\mathbb{N}; \text{lko}, \text{lkkt})$, $(\mathbb{Z}_{12}; +, \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \neg, \wedge, \vee, \rightarrow)$.

8. Definíció. Azokat az algebrákat, amelyeknek egy kétváltozós művelete van **grupoidnak** nevezzük.

9. Példa. A 7. példában megadott algebrák közül a következők grupoidok: $(\mathbb{Z}; -)$, $(\mathbb{R}^2; +)$.

10. Definíció. (Grupoid műveleti tulajdonságai)

- (1) Az $(A; \circ)$ grupoid **idempotens**, ha $(\forall a \in A)(a \circ a = a)$.
- (2) Az $(A; \circ)$ grupoid **asszociatív**, ha $(\forall a, b, c \in A)(a \circ (b \circ c) = (a \circ b) \circ c)$.
- (3) Az $(A; \circ)$ grupoid **kommutatív**, ha $(\forall a, b \in A)(a \circ b = b \circ a)$.
- (4) Az $(A; \circ)$ grupoidban van **zéruselem**, ha $(\exists o \in A)(\forall a \in A)(a \circ o = o \circ a = o)$.
- (5) Az $(A; \circ)$ grupoidban van **egységelem**, ha $(\exists e \in A)(\forall a \in A)(a \circ e = e \circ a = a)$.
- (6) Ha az $(A; \circ)$ grupoidban e egységelem, és $(\forall a \in A)(\exists b \in A)(a \circ b = b \circ a = e)$, akkor minden elemnek van **inverze**.

11. Házi feladat. (márc. 1.) Az $A = \{a, b, c\}$ halmazon adja meg a $\circ$ műveletet művelet táblázat segítségével úgy, hogy idempotens legyen, ne legyen kommutatív, és b legyen egységelem. Igazolja is a tulajdonságokat!

12. Tétel. Bármely grupoidban legfeljebb egy egységelem és legfeljebb egy zéruselem van.

13. Házi feladat. (márc. 1.) Igazolja, hogy tetszőleges grupoidban legfeljebb egy zéruselem van.

14. Definíció. Ha a grupoidnak van egységeleme, **egységelemes**, ha van zéruseleme, **zéruselemes** grupoidnak nevezzük.

15. Példa. Olyan grupoidokra adunk példát, melyek a 10. definícióban szereplő tulajdonságokkal rendelkeznek.

- (1) Idempotens grupoidok: $(\mathbb{Z}; \min)$, $(\mathbb{N}; \text{lkkt})$, $(\{\mathbf{i}, \mathbf{h}\}; \vee)$.

- (2) Asszociatív grupoidok: $(\mathbb{N}; \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2 \times 2}; \cdot)$, $(\mathbb{N}; \text{lnko})$, $(\mathbb{Z}; \max)$, $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$, $(A^A; \cdot)$.
(3) Kommutatív grupoidok: $(\mathbb{N}; \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{N}; \text{lnko})$, $(\mathbb{Z}; \max)$, $(\mathbb{Z}_4; +)$, $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$.
(4) Zéruselemes grupoidok: $(\mathbb{Z}; \cdot)$ zéruseleme a 0, $(\mathbb{R}^{2 \times 2}; \cdot)$ zéruseleme a 2×2 -es zérómátrix, $(\mathbb{N}; \text{lnko})$ zéruseleme az 1, $(\mathbb{Z}_4; \cdot)$ zéruseleme a $\bar{0}$, $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$ zéruseleme a $\mathbf{h}$.

grupoid	zéruselem
$(\mathbb{Z}; \cdot)$	0
$(\mathbb{R}^{2 \times 2}; \cdot)$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
$(\mathbb{N}; \text{lnko})$	1
$(\mathbb{Z}_3; \cdot)$	$\bar{0}$
$(\{\mathbf{i}, \mathbf{h}\}; \wedge)$	$\mathbf{h}$
$(\{\mathbf{i}, \mathbf{h}\}; \vee)$	$\mathbf{i}$

- (5) Egységelemes grupoidok: $(\mathbb{Z}; \cdot)$ egységeleme az 1, $(\mathbb{Z}; +)$ egységeleme a 0, $(\mathbb{R}^{2 \times 2}; \cdot)$ egységeleme a 2×2 -es egység mátrix, $(\mathbb{Z}_4; \cdot)$ egységeleme az $\bar{1}$, $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$ egységeleme az $\mathbf{i}$.

grupoid	egységelem
$(\mathbb{Z}; \cdot)$	1
$(\mathbb{Z}; +)$	0
$(\mathbb{R}^{2 \times 2}; \cdot)$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$(\mathbb{Z}_3; \cdot)$	$\bar{1}$
$(\mathbb{Z}_4; +)$	$\bar{0}$
$(\{\mathbf{i}, \mathbf{h}\}; \wedge)$	$\mathbf{i}$
$(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$	$\mathbf{i}$
$(A^A; \cdot)$	id_A

- (6) Egységelmekes grupoidok, ahol minden elemnek van inverze: $(\mathbb{Z}; +)$ -ban az a inverze $-a$, $(\mathbb{R}^3; +)$ -ban a v inverze $-v$, $(\mathbb{Q} \setminus \{0\}; \cdot)$ -ban a inverze $1/a$, $(\mathbb{Z}_4; +)$ -ban a $\bar{0}$ és a $\bar{2}$ inverze önmaga, a $\bar{3}$ és $\bar{1}$ egymás inverzei, $(\mathbb{Z}_3 \setminus \{\bar{0}\}; \cdot)$ -ban minden elem inverze önmaga.

grupoid	a inverze
$(\mathbb{Z}; +)$	$-a$
$(\mathbb{R}^3; +)$	$-a$
$(\mathbb{Q} \setminus \{0\}; \cdot)$	$\frac{1}{a}$
$(\mathbb{Z}_3 \setminus \{\bar{0}\}; \cdot)$	a
$(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$	a

16. Példa. Olyan grupoidokra adunk példát, melyek NEM rendelkeznek a 10. definícióban szereplő tulajdonságokkal.

- (1) Nem idempotens grupoidok: $(\mathbb{Z}; +)$, $(\mathbb{Z}; -)$, $(\mathbb{Q}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2 \times 2}; \cdot)$, $(\mathbb{Z}_4; +)$, $(\{\mathbf{i}, \mathbf{h}\}; \rightarrow)$.
(2) Nem asszociatív grupoidok: $(\mathbb{Z}; -)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \rightarrow)$.
(3) Nem kommutatív grupoidok: $(\mathbb{Z}; -)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\mathbb{R}^{2 \times 2}; \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \rightarrow)$, $(A^A; \cdot)$.
(4) Grupoidok, ahol nincs zéruselem: $(\mathbb{Z}; -)$, $(\mathbb{Z}; +)$, $(\mathbb{N}; \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{Z}_4; +)$, $(\{\mathbf{i}, \mathbf{h}\}; \rightarrow)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$.
(5) Grupoidok, ahol nincs egységelem: $(\mathbb{N}; +)$, $(\mathbb{Z}; -)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \rightarrow)$.
(6) Egységelemes grupoidok, ahol nincs minden elemnek inverze: $(\mathbb{N}_0; +)$, $(\mathbb{Z}; \cdot)$, $(\mathbb{Q}; \cdot)$, $(\mathbb{R}^{2 \times 2}; \cdot)$, $(\mathbb{Z}_3; \cdot)$, $(\mathbb{Z}_4; \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$, $(\{\mathbf{i}, \mathbf{h}\}; \vee)$, $(A^A; \cdot)$.

17. Definíció. Legyen $\circ$ és $\star$ két kétváltozós művelet az A halmazon.

- (1) A **disztributív** a $\star$ -ra nézve, ha $(\forall a, b, c \in A)((a \circ (b \star c) = (a \circ b) \star (a \circ c)) \wedge ((b \star c) \circ a = (b \circ a) \star (c \circ a)))$.
(2) A **abszorptív** a $\star$ -ra nézve, ha $(\forall a, b \in A)((a \circ (a \star b) = a) \wedge ((a \star b) \circ a = a))$.

18. Példa. Az előző definícióban szereplő fogalmakra adunk példát.

- (1) Az $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ halmazon a $\cdot$ disztributív a $+$ -ra. Az $\mathbb{N}$ halmazon a lnko disztributív a lkkt -re, és a lkkt is disztributív a lnko -ra. Az $\{\mathbf{i}, \mathbf{h}\}$ halmazon a $\wedge$ disztributív a $\vee$ -ra, és fordítva, a $\vee$ is disztributív a $\wedge$ -ra.
(2) Az $\mathbb{N}$ halmazon a lnko abszorptív a lkkt -re, és a lkkt is abszorptív a lnko -ra. Az $\{\mathbf{i}, \mathbf{h}\}$ halmazon a $\wedge$ abszorptív a $\vee$ -ra, és fordítva, a $\vee$ is abszorptív a $\wedge$ -ra.

2. FÉLCSOPORT, CSOPORT

19. Definíció. Az asszociatív grupoidokat **félcsoporthnak** nevezzük. Az egységelmek félcsoporthokat **monoidnak** nevezzük. Azokat a monoidokat, ahol minden elemnek van inverze **csoportoknak** hívjuk. A kommutatív csoportokat **Abel-csoportoknak** nevezzük.

20. Példa. Az $(\mathbb{N}; +)$ félcsoporth, de nem monoid.

21. Példa. A következők monoidok, de nem csoportok: $(\mathbb{N}; \cdot)$, $(\mathbb{N}_0; +)$, $(\mathbb{R}; \cdot)$, $(\mathbb{R}^{n \times n}; \cdot)$, $(\mathbb{Z}_n; \cdot)$.

22. Példa. Az $(\{M \in \mathbb{R}^{n \times n} : M\text{-nek létezik inverze}\}; \cdot)$ csoport, melynek neve az **általános lineáris csoport**, nem (feltétlen) Abel-csoport.

23. Példa. A következők Abel-csoportok: $(\mathbb{Z}; +)$, $(\mathbb{Z}_n; +)$, $(\mathbb{R} \setminus \{0\}; \cdot)$, $(\mathbb{R}^{n \times m}; +)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$.

24. Tétel. Tetszőleges monoidban minden elemnek legfeljebb egy inverze van.

25. Tétel. Legyen $(A; \cdot)$ monoid. Ha az $a, b \in A$ elemnek van inverze: a^{-1}, b^{-1} , akkor az a^{-1} és ab elemeknek is van inverze, mégpedig

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

26. Megjegyzés. Tudjuk, hogy csoportban az egységelem és az elemek inverze egyértelműen meghatározott, de nem mindig egyértelmű, hogy ezeket hogyan is jelöljük. Ha ez meg szeretnénk adni, akkor a $(A; \cdot)$ helyett $(A; \cdot, {}^{-1}, 1)$ -et írunk, ahol a második művelet az 1-változós inverzképzés, és 1 az egységelem (0-változós művelet). A csoportok **multiplikatív írásmódja** alatt a $(A; \cdot, {}^{-1}, 1)$ műveleti szimbólumokat értjük. Az **additív írásmód** alatt a $(A; +, -, 0)$ műveleti szimbólumokat értjük, és általában csak akkor használjuk, ha a csoport kommutatív.

27. Definíció. Legyen $(A; \cdot, {}^{-1}, 1)$ tetszőleges csoport. Az $a \in A$ elem **n -edik hatványát** ($n \in \mathbb{Z}$) a következőképpen definiáljuk:

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n \text{ db}}, & \text{ha } n > 0, \\ 1, & \text{ha } n = 0, \\ \underbrace{a^{-1} \cdots a^{-1}}_{-n \text{ db}}, & \text{ha } n < 0. \end{cases}$$

Ha az $(A; +, -, 0)$ csoport additív írásmódban van megadva, akkor a hatványozást $n \cdot a$ -val jelöljük, de ugyan úgy definiáljuk mint a multiplikatív írásmódnál:

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ db}}, & \text{ha } n > 0, \\ 0, & \text{ha } n = 0, \\ \underbrace{(-a) + \cdots + (-a)}_{-n \text{ db}}, & \text{ha } n < 0. \end{cases}$$

28. Lemma. Legyen $(A; \cdot, {}^{-1}, 1)$ tetszőleges csoport, $a \in A$ és $n \in \mathbb{Z}$. Ekkor $a^n \cdot a = a \cdot a^n = a^{n+1}$ és $a^{-1} \cdot a^n = a^n \cdot a^{-1} = a^{n-1}$.

29.* Tétel. Legyen $(A; \cdot)$ tetszőleges csoport. Bármely $m, n \in \mathbb{Z}$ -re és $a, b \in A$ -ra

- (1) $a^m a^n = a^{m+n}$,
- (2) $(a^m)^n = a^{mn}$,
- (3) ha $ab = ba$, akkor $(ab)^n = a^n b^n$.

30. Példa. Az $(\mathbb{R} \setminus \{0\}; \cdot)$ csoportban az $a = 2$ elem harmadik hatványa 8, mert $2 \cdot 2 \cdot 2 = 8$. Az $(\mathbb{R}; +)$ csoportban az $a = 2$ elem harmadik hatványa viszont 6, mert $2 + 2 + 2 = 6$.

3. GYŰRŰ, TEST

31. Definíció. Az $(A; +, \cdot)$ algebrát **gyűrűnek** nevezzük, ha $(A; +)$ Abel-csoport, $(A; \cdot)$ félcsoport, és $a \cdot$ disztributív az $+$ -ra. Az $(A; +)$ Abel-csoportot a **gyűrű additív csoportjának**, az $(A; \cdot)$ félcsoportot a **gyűrű multiplikatív félcsoportjának** nevezzük.

32. Példa. Gyűrűk: $(\mathbb{Z}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$, $(\mathbb{R}^{2 \times 2}; +, \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow, \vee)$, $(\mathbb{Z}_5; +, \cdot)$.

33. Tétel. Az $(A; +, \cdot)$ gyűrű esetén

- (1) a 0 additív egységelem a szorzásra nézve zéruselem,
- (2) tetszőleges $a, b \in A$ elemekre $(-a)b = a(-b) = -(ab)$.

34. Definíció. Az $(A; +, \cdot)$ gyűrűt **egységelemesnek** nevezzük, ha $(A; \cdot)$ monoidot alkot, azaz van a szorzásra nézve egységeleme.

35. Példa. A $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Z}_n; +, \cdot)$, $(\mathbb{R}^{n \times n}; +, \cdot)$ gyűrűk mind egységelemesek, a $(\{\text{páros számok}\}, +, \cdot)$ gyűrű nem egységelemes. Egységelemes gyűrűkben van értelme megkérdezni, hogy mely elemeknek van multiplikatív inverze.

36. Definíció. Az $(A; +, \cdot)$ gyűrűt **testnek** nevezzük, ha az $(A \setminus \{0\}; \cdot)$ Abel-csoportot alkot, amelyet a **test multiplikatív csoportjának** nevezzük.

37.* Tétel. A $(\mathbb{Z}_n; +, \cdot)$ gyűrű pontosan akkor test, ha n prím.

38. Példa. A 32. példában felsorolt gyűrűk közül testek: $(\mathbb{R}; +, \cdot)$, $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow, \vee)$, $(\mathbb{Z}_5; +, \cdot)$.