

# MBLK12: Algebrai struktúrák (levelező)

(előadásvázlat)

Maróti Miklós, Kátai-Urbán Kamilla

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, és  $\mathbb{R}^{m \times n}$  az  $m \times n$ -es valós mátrixok halmazát,  $\mathbb{Z}_m$  a modulo  $m$  maradékosztályok halmazát.

## 1. MŰVELETI TULAJDONSÁGOK

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

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

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

**4. Tétel.** A  $\mathbb{Z}_m$  halmazon művelet a következőképpen definiált összeadás, kivonás és szorzás:  
$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} - \bar{b} = \overline{a - b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

**5. 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.

**6. Példa.** Ha az előző definícióban szereplő  $\mathcal{F}$  véges halmaz, akkor elemeit felsoroljuk a halmaz jelet elhagyva, például algebrák a következők:  $(\mathbb{Z}; +, \cdot)$ ,  $(\mathbb{Z}; -)$ ,  $(\mathbb{N}; 1, \cdot)$ ,  $(\mathbb{R}^3; +)$ ,  $(\mathbb{R}^{2 \times 2}; \cdot)$ ,  $(\mathbb{Z}; \min, \max)$ ,  $(\mathbb{N}; \text{lnko}, \text{lkkt})$ ,  $(\mathbb{Z}_{12}; +, \cdot)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \neg, \wedge, \vee, \rightarrow)$ ,  $(\mathcal{P}(U); \emptyset, \bar{\phantom{x}}, \cap, \cup, \Delta)$ ,  $(S_n; \cdot)$ ,  $(S_n; \text{id}, \cdot)$ .

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

**8. Példa.** A 6. példában megadott algebrák közül a következők grupoidok:  $(\mathbb{Z}; -)$ ,  $(\mathbb{R}^2; +)$ ,  $(S_n; \cdot)$ .

**9. 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**.

**10. Tétel.** Bármely grupoidban legfeljebb egy egységelem és legfeljebb egy zéruselem van.

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

**12. Példa.** Olyan grupoidokra adunk példát, melyek a 9. definícióban szereplő tulajdonságokkal rendelkeznek.

- (1) Idempotens grupoidok:  $(\mathbb{Z}; \min)$ ,  $(\mathbb{N}; \text{lkkt})$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \vee)$ ,  $(\mathcal{P}(U); \cap)$ .
- (2) Asszociatív grupoidok:  $(\mathbb{N}; \cdot)$ ,  $(\mathbb{R}^3; +)$ ,  $(\mathbb{R}^{2 \times 2}; \cdot)$ ,  $(\mathbb{N}; \text{lnko})$ ,  $(\mathbb{Z}; \max)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$ ,  $(\mathcal{P}(U); \cup)$ ,  $(\mathcal{P}(U); \Delta)$ ,  $(A^A; \cdot)$ ,  $(S_n; \cdot)$ .
- (3) Kommutatív grupoidok:  $(\mathbb{N}; \cdot)$ ,  $(\mathbb{R}^3; +)$ ,  $(\mathbb{N}; \text{lnko})$ ,  $(\mathbb{Z}; \max)$ ,  $(\mathbb{Z}_4; +)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \wedge)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow)$ ,  $(\mathcal{P}(U); \cup)$ ,  $(\mathcal{P}(U); \Delta)$ .
- (4) Zéruselemes grupoidok:

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
$(\mathbb{Z}_3; \cdot)$	$\bar{0}$
$\{\mathbf{i}, \mathbf{h}\}; \wedge$	$\mathbf{h}$
$\{\mathbf{i}, \mathbf{h}\}; \vee$	$\mathbf{i}$
$(\mathcal{P}(U); \cap)$	$\emptyset$
$(\mathcal{P}(U); \cup)$	$U$

(5) Egységelemes grupoidok:

grupoid	egységelem
$(\mathbb{Z}; \cdot)$	1
$(\mathbb{Z}; +)$	0
$(\mathbb{R}^{2 \times 2}; \cdot)$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$(\mathbb{Z}_3; \cdot)$	$\bar{1}$
$(\mathbb{Z}_4; +)$	$\bar{0}$
$\{\mathbf{i}, \mathbf{h}\}; \wedge$	$\mathbf{i}$
$\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow$	$\mathbf{i}$
$(\mathcal{P}(U); \cup)$	$\emptyset$
$(\mathcal{P}(U); \Delta)$	$\emptyset$
$A^A$	$\text{id}_A$
$(S_n; \cdot)$	$\text{id}$

(6) Egységelmeltes grupoidok, ahol minden elemnek van inverze:

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

**13. Példa.** Olyan grupoidokra adunk példát, melyek NEM rendelkeznek a 9. definícióban szereplő tulajdonságokkal.

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

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

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

**15. Példa.** Az 14. 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. A  $\mathcal{P}(U)$  halmazon a  $\cap$  disztributív a  $\cup$ -ra, és fordítva, az  $\cup$  is disztributív a  $\cap$ -ra, továbbá a  $\cap$  disztributív a  $\Delta$ -ra.

- (2) Az  $\mathbb{N}$  halmazon a  $\text{luko}$  abszorptív a  $\text{lkkt}$ -re, és a  $\text{lkkt}$  is abszorptív a  $\text{luko}$ -ra. Az  $\{\mathbf{i}, \mathbf{h}\}$  halmazon a  $\wedge$  abszorptív a  $\vee$ -ra, és fordítva, a  $\vee$  is abszorptív a  $\wedge$ -ra. A  $\mathcal{P}(U)$  halmazon a  $\cap$  abszorptív a  $\cup$ -ra, és fordítva, az  $\cup$  is abszorptív a  $\cap$ -ra.

**16. Példa.** Olyan műveletekre adunk példát, amelyek NEM teljesítik az 14. definícióban megadott tulajdonságokat.

- (1) Az  $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$  halmazon a  $+$  nem disztributív a  $\cdot$ -ra. Az  $\{\mathbf{i}, \mathbf{h}\}$  halmazon az  $\rightarrow$  nem disztributív a  $\vee$ -ra.  
 (2) Az  $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$  halmazon a  $\cdot$  nem abszorptív a  $+$ -ra. A  $\mathcal{P}(U)$  halmazon az  $\cup$  nem abszorptív a  $\Delta$ -ra.

## 2. FÉLCSOPORT, CSOPORT

**17. Definíció.** Az asszociatív grupoidokat **félcsoportnak** nevezzük. Az egységelmest félcsoportokat **monoidnak** nevezzük. Azokat a monoidokat, ahol minden elemnek van inverze **csoporthoz** hívjuk. A kommutatív csoportokat **Abel-csoportoknak** nevezzük.

**18. Példa.** Az  $(\mathbb{N}; +)$  félcsoport, de nem monoid.

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

**20. Példa.** A következők csoportok, de nem (feltétlen) Abel-csoportok:  $(S_n; \cdot)$ , melynek neve a **teljes szimmetrikus csoport**, és az  $(\{M \in \mathbb{R}^{n \times n} : |M| \neq 0\}; \cdot)$ , melynek neve az **általános lineáris csoport**.

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

**22. Tétel.** Az  $(A; \cdot)$  monoidban minden elemnek legfeljebb egy inverze van. Ha az  $a, b$  elemnek van inverze:  $a^{-1}, b^{-1}$ , akkor az  $a^{-1}$  és  $ab$  elemeknek is van inverze, mégpedig

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

**23. Példa.** Az  $(\mathbb{R}^{n \times n}; \cdot)$  monoidban pontosan a nem nulla determinánsú elemeknek van inverze, és éppen ezek az elemek alkotják az általános lineáris csoportot.

**24. 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.

**25. 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:

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

**26. 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  $a^{-1} \cdot a^n = a^n \cdot a^{-1} = a^{n-1}$ .

**27.\* 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  $(ab)^n = a^n b^n$ .

**28. 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  $2 + 2 + 2 = 6$ .

**29. Definíció.** Legyen  $(A; \cdot)$  csoport. Az  $a \in A$  **elem rendje** az a legkisebb pozitív egész  $n \in \mathbb{N}$ , amelyre  $a^n = 1$ . Ha ilyen nincs, akkor  $a$  rendje végtelen. Az elem rendjét  $o(a)$ -val jelöljük.

**30. Példa.** A  $(\mathbb{Z}_6; +)$  csoportban  $o(\bar{4}) = 3$ , mert  $3 \cdot \bar{4} = \bar{0}$ , azaz a harmadik hatvány az egységelem, de a kisebb hatványok nem az egységelemet adják. Az  $(S_5; \cdot)$  csoportban  $o((1\ 2\ 3)(4\ 5)) = 6$ , mert a ciklusok függetlenek, azaz felcserélhetőek, így külön hatványozhatóak.

**31. Tétel.** Legyen  $(A; \cdot)$  csoport,  $a \in A$  véges rendű elem, és  $n, m \in \mathbb{Z}$ -re

- (1)  $a^n = 1$  akkor és csak akkor teljesül, ha  $o(a) \mid n$ ,
- (2)  $a^n = a^m$  akkor és csak akkor teljesül, ha  $n \equiv m \pmod{o(a)}$ .

**32. Megjegyzés.** Vegyük észre, hogy az előző tételnél az (1) speciális esete a (2)-nek  $m = 0$ -ra.

**33.\* Tétel.** Legyen  $(A; \cdot)$  csoport, és  $a, b \in A$  felcserélhető elemek, azaz  $ab = ba$ . Ekkor  $o(ab) = o(a)o(b)$  akkor és csak akkor, ha  $\text{lko}(o(a), o(b)) = 1$ .

### 3. GYŰRŰ, TEST

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

**35. Példa.** Gyűrűk:  $(\mathbb{Z}; +, \cdot)$ ,  $(\mathbb{R}; +, \cdot)$ ,  $(\mathbb{R}^{2 \times 2}; +, \cdot)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow, \vee)$ ,  $(\mathcal{P}(U); \Delta, \cap)$ ,  $(\mathbb{Z}_5; +, \cdot)$ .

**36. Tétel.** Az  $(A; +, \cdot)$  gyűrű esetén a 0 additív egységelem a szorzásra nézve zéruselem. Továbbá tetszőleges  $a, b \in A$  elemekre  $(-a)b = a(-b) = -(ab)$ .

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

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

**39. Példa.** A 35. példában felsorolt gyűrűk közül testek:  $(\mathbb{R}; +, \cdot)$ ,  $(\{\mathbf{i}, \mathbf{h}\}; \leftrightarrow, \vee)$ ,  $(\mathbb{Z}_5; +, \cdot)$ .

### 4. HÁLÓ

**40. Definíció.** Legyen  $(A; \leq)$  részbenrendezett halmaz. Az  $a, b \in A$  elemeknek  $c \in A$  **felső korlátja**, ha  $a \leq c$  és  $b \leq c$ . Az  $a, b$  elemeknek  $d \in A$  **legkisebb felső korlátja**, ha  $d$  felső korlát, és  $a, b$  minden  $c$  felső korlátjára  $d \leq c$ . Duális módon definiálhatjuk a **alsó korlátot** és a **legnagyobb alsó korlátot**.

**41. Példa.** Az alábbi ábrán látható az első részbenrendezésben az 1, 2 elemeknek csak egy felső korlátjuk van, ami a legkisebb is egyben, de nincsen alsó korlátjuk. A második részbenrendezésben a 4, 5 elemeknek két felső korlátjuk van, de nincsen legkisebb felső korlátjuk.



**42. Tétel.** Tetszőleges részbenrendezett halmaz bármely két elemének legfeljebb csak egy legkisebb felső korlátja (legnagyobb alsó korlátja) van.

**43. Definíció.** Az  $(A; \leq)$  részbenrendezett halmaz **hálószerűen rendezett halmaz**, ha tetszőleges  $a, b \in A$  elemeknek van legkisebb felső korlátjuk, melyet  $a \vee b$ -vel jelölünk és az  $a, b$  elemek **egyesítésnek** nevezzük, illetve legnagyobb alsó korlátjuk, melyet  $a \wedge b$ -vel jelölünk és az  $a, b$  elemek **metszetnek** nevezzük.

**44. Példa.** Az előző példában szereplő részbenrendezések nem hálószerűen rendezettek. Az  $(\mathbb{N}_0; |)$  hálószerűen rendezett halmaz, amelyben az egyesítés a legkisebb közös többszörös és a metszet a legnagyobb közös osztó. Az  $(\mathbb{R}; \leq)$  hálószerűen rendezett halmaz, ahol az egyesítés a maximum és a metszet a minimum. A  $(\mathcal{P}(U); \subseteq)$  hálószerűen rendezett halmaz, ahol a halmazelméleti egyesítés és metszet a legkisebb felső korlát és legnagyobb alsó korlát.

**45.\* Tétel.** Legyen  $(A; \leq)$  hálószerűen rendezett halmaz. Ekkor az  $\wedge$  és  $\vee$  műveletek idempotensek, kommutatívok, és asszociatívok, illetve  $\wedge$  abszorptív az  $\vee$ -re és  $\vee$  abszorptív a  $\wedge$ -re.

**46. Definíció.** Az  $(A; \wedge, \vee)$  algebrát **hálónak** nevezzük, ha a kétváltozós  $\wedge$  és  $\vee$  műveletek idempotensek, kommutatívok, és asszociatívok, illetve kölcsönösen abszorptívok egymásra.

**47. Tétel.** Ha adott az  $(A; \wedge, \vee)$  háló, akkor az

$$a \leq b \iff a \wedge b = a$$

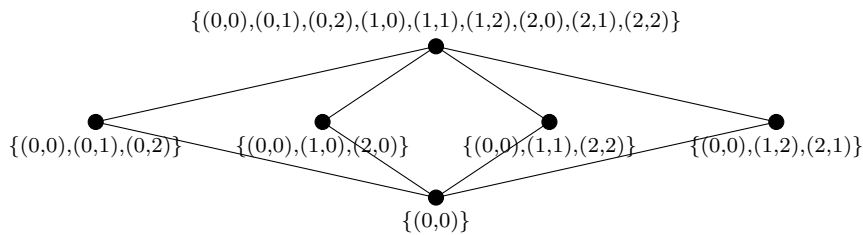
feltétel által definiált  $\leq$  relációval  $(A; \leq)$  hálószerűen rendezett halmaz.

**48.\* Tétel.** Adott alaphalmazon a hálószerűen rendezett halmazok és a hálók természetes módon (az előző két tétel szerint) megfeleltethetők egymásnak.

**49. Példa.** Az  $(\mathbb{N}_0; \text{luko}, \text{lkkt})$ ,  $(\mathbb{R}; \min, \max)$ ,  $(\mathbb{R}; \max, \min)$ ,  $(\mathcal{P}(U); \cap, \cup)$ ,  $(\{\mathbf{h}, \mathbf{i}\}, \wedge, \vee)$  algebrák hálók.

**50. Példa.** Az  $\mathbb{R}^n$  alterei a tartalmazásra nézve hálószerűen rendezett halmazt alkotnak. Ha  $U, V \leq \mathbb{R}^n$  két altér, akkor metszetük  $U \cap V$  és egyesítésük  $U + V = \{u + v : u \in U, v \in V\}$ .

**51.\* Példa.** A  $\mathbb{Z}_3$  test feletti 2-dimenziós  $\mathbb{Z}_3^2$  vektortér altereinek hálója a következő:



$\mathbb{Z}_2^3$  altereinek Hasse-diagrammja már lényegesen bonyolultabb (1 db 0-dimenziós, 7 db 1-dimenziós, 7 db 2-dimenziós és 1 db 3-dimenziós altere van):

