

2018.05.11.

S. Zsemlé

Dimet

gyűrű, test és háló jön.

Gyűrű: $(A; +, \cdot)$, $(A; +)$ legyen Abel-csoport
(asszoc, egységelemes, $\forall$ elemnek inverze, kommutatív)

és $(A; \cdot)$ legyen félcsoport

$\oplus \cdot$ disztributív +-ra.

Példa: $(\mathbb{R}; +, \cdot)$, $(\mathbb{Z}; +, \cdot)$, $(\mathbb{R}^{n \times n}; +, \cdot)$

$A \vee (B \leftrightarrow C) = (A \vee B) \leftrightarrow (A \vee C)$ belátható.

36. tétel: $(A; +, \cdot)$ gyűrű

(1) 0 additív egységelem és multiplikatív zéruselem.

$\downarrow$
 $(\forall a \in A)(a + 0 = 0 + a = a)$ és $(\forall a \in A)(0 \cdot a = a \cdot 0 = 0)$.

Biz: $0 \cdot a = \underline{0 \cdot (a + 0)} = 0 \cdot a + \underline{0 \cdot 0}$
ez nem jó.

$$0 \cdot a = (0 + 0) \cdot a = 0a + 0a$$

$\nearrow + (- (0 \cdot a))$ inverz.

$$(0 \cdot a) + (- (0 \cdot a)) = 0 \cdot a + \underbrace{0 \cdot a + (- (0 \cdot a))}_{0} = 0 \cdot a = 0.$$

$\parallel$
0, inverzrejes itt!

(2) $(-a)b = a(-b) = -(ab)$.

Biz: $0 = 0 \cdot b = (a + (-a)) \cdot b = \underbrace{(ab)}_{\substack{\uparrow \\ \text{ennek} \\ \text{az inverze}}} + (-a) \cdot b = \underbrace{0}_{\substack{\uparrow \\ \text{ez.}}} + (-ab)$

$$0 + (-ab) = a \cdot b + \underbrace{(-a)b + (-ab)}_0$$

$$-(ab) = (-a)b.$$

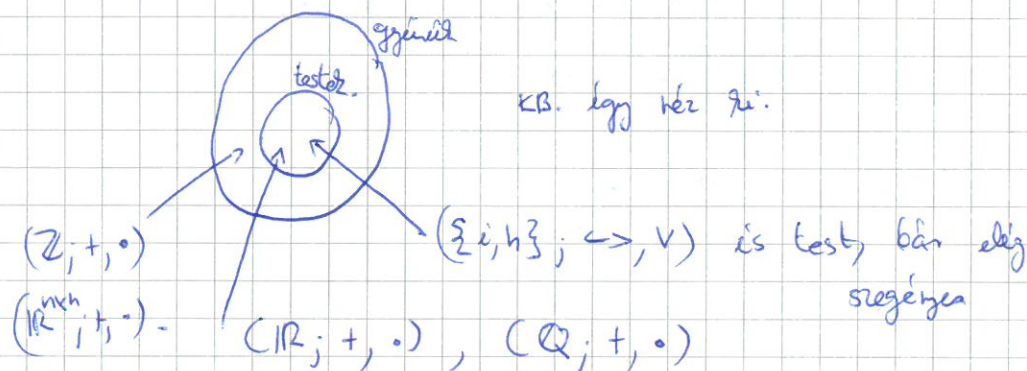
(1)

□

Test: Kétnüveletes struktúra: $(A; +, \cdot)$

⊕ $(A; +)$ Abel-csoport és

$(A \setminus \{0\}; \cdot)$ Abel-csoport és
distributív $+$ -ra.



$(P(u); \Delta, \cap)$ gyűrű, mert $A \cap B = u$.

$(\mathbb{Z}_5; +, \cdot)$ is test.

Inverz: $\bar{0}$ -t vegyük 1 .

$$\bar{2} \cdot \bar{3} = 1$$

$$\bar{4} \cdot \bar{4} = 1$$

OK.

DE! $(\mathbb{Z}_6; +, \cdot)$ már nem test!

$$\bar{2} \cdot \bar{3} = \bar{0}$$

$$2x \equiv 1 \pmod{6}$$

luko $\phi(6, 2) = 2$, $2 \nmid 1$.
nem jó!

38. tétel: $(\mathbb{Z}_n; +, \cdot)$ test $\iff n$ prím.

$(\mathbb{Z}_n; +)$ Abel-csoport.

② $(\mathbb{Z}_n \setminus \{0\}; \cdot)$ - Abel-csoport.

Asszociatív, T , kommutatív.

$$\bar{a} \text{ inv } \bar{b}, \text{ ha } \bar{a} \cdot \bar{b} = \bar{1}$$

$$ab \equiv 1 \pmod{n}$$

megoldható, ha $\text{lnko}(a, n) \mid 1 \Leftrightarrow a$ és n
relatív prímek

$$\forall a \in \mathbb{Z}_n \setminus \{0\} \quad \text{lnko}(a, n) = 1 \Leftrightarrow n \text{ prim. } \square$$

Hálók.

no. definíció. részben rendezett halmaz, Hasse-diagram.

4.2. tétel: $(A; \leq)$ részbenrendezett halmaz, amely 2 elemű
legfeljebb 1 legnagyobb alsó és legfeljebb 1 legkisebb felső
tartalmaz van.

Biz.: Indirekt ut.

$\exists a, b \in A$ két legnagyobb alsó tartalmaz: c, d .

$$c \leq a \quad \text{és} \quad c \leq b$$

$$d \leq a \quad \text{és} \quad d \leq b$$

$$c \geq d \quad \text{és} \quad c \leq d \Rightarrow c = d \quad \swarrow \searrow$$

Hálószerűen rendezett halmaz

$(A; \leq)$ ha $(\forall a, b \in A) (\exists \text{ legnagyobb alsó} \wedge \exists \text{ legkisebb felső tartalmaz})$

Legnagyobb alsó: $a \wedge b$

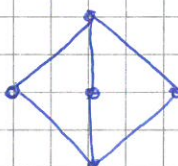
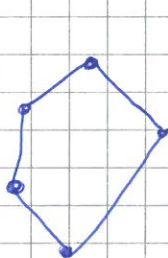
Legkisebb felső: $a \vee b$.

felölismét.

(pl.) 5 pontú:



ilyen
lehetnek



Def: $(A; \wedge, \vee)$ háló, ha $\wedge$ és $\vee$ idempotens, asszoc. és kommut. és oda-vissza abszorblívól is.

(pl.) $(\mathbb{N}_0; \min, \max)$ ilyen.

$(P(U); \cap, \cup)$ is háló.

$(\mathbb{Z}; \min, \max)$

$(\mathbb{N}_0; |)$

$(P(U); \subseteq)$

$(\mathbb{Z}; \leq)$

47. tétel:

$(A; \wedge, \vee)$ háló adott.

$$a \leq b \Leftrightarrow a \wedge b = a.$$

~~háló~~

$(A; \leq)$ részbenrendezett halmaz

Biz: $\leq$ reflexív.

$$(\forall a \in A) (a \leq a)$$



$a \wedge a = a$ mivel hálóban vanunk,

A $\wedge$ művelet idempotens

(2) $\leq$ antiszimmetrik:

$$(\forall a, b \in A) (a \leq b \text{ és } b \leq a \Rightarrow a = b)$$



$$a \wedge b = a$$



$$b \wedge a = b$$

$$a = a \wedge b = b \wedge a = b. \quad \square$$

(3) $\leq$ tranzitív:

$$(\forall a, b, c \in A) (a \leq b, b \leq c \Rightarrow a \leq c) \quad (\text{az } a \wedge c = a)$$



$$a \wedge b = a$$



$$b \wedge c = b$$

$$\underline{a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a}$$

Tehát ez egy résbennrendezett halmaz.

Álló rell: legnagyobb alsó szorlát:

$(A, \leq)$ résbennrendezett halmazban $\wedge$ legnagyobb alsó szorlát.

alsó szorlát:

$$a \wedge b \leq a \text{ és } a \wedge b \leq b$$

$$(a \wedge b) \wedge a = a \wedge b$$

$$a \wedge (b \wedge a)$$

$$a \wedge (a \wedge b)$$

$$\downarrow (a \wedge a) \wedge b$$

$$a \wedge b.$$

$$(a \wedge b) \wedge b =$$

$$= a \wedge (b \wedge b) =$$

$$= a \wedge b.$$

$$a, b \in A \quad \wedge \text{ alsó szorlát, } c \leq a \text{ és } c \leq b.$$

$\wedge$ legnagyobb alsó szorlát: $\forall d$ alsó szorlát $\Rightarrow d \leq \wedge$.
 $d \leq a, d \leq b$

$$\forall d, \quad d \leq a \text{ \& \& } d \leq b \Rightarrow d \leq a \wedge b. \quad \text{hell.}$$

$$\begin{array}{ccc} \updownarrow & \updownarrow & \up \\ d \wedge a = d & d \wedge b = d & (d \wedge (a \wedge b) = d) \end{array}$$

$$(d \wedge (a \wedge b)) = d \wedge (a \wedge b) = (d \wedge a) \wedge b = d \wedge b = d. \quad \square$$

5.7. $\mathbb{Z}_{17}$ -ben

$$(a) \quad \overline{9} + \overline{12} = \overline{9+12} = \overline{21} = \overline{4}.$$

$$(b) \quad \overline{2} \cdot \overline{11} = \overline{22} = \overline{5}.$$

$$(c) \quad \frac{\overline{2}}{\overline{9}} = \frac{\overline{36}}{\overline{9}} = \overline{4}.$$

$$(d) \quad \overline{11}^2 = \overline{-6}^2 = \overline{2}.$$

$$\overline{11}^4 = (\overline{11}^2)^2 = \overline{4}$$

$$\overline{11}^8 = \overline{-1}$$

$$\overline{11}^{16} = \overline{1}$$

$$\overline{11}^{13} = \overline{2}.$$

5.8. 15 nem prím.