

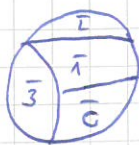
2018.05.04.

7. konzultáció

Diszkrét mat.

Algebrai struktúrák.

Volt: $\mathbb{Z}_n$



$\mathbb{Z}$
mod n - ben.

Így: $1 + 3 = 0$ lesz igaz.

$2 \cdot 3 = 2 \cdot 3 = 2$ lesz igaz. (kongruenciarelaáció)

$2 - 3 = 2 - 3 = 3$ értelmes eredmény.
 $-1 \equiv 3 \pmod{4}$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

$(\mathbb{Z}_n; +)$ művelet.
↑
alaphalmaz
ez egy algebra.

$(\mathbb{Z}; +, \cdot)$ nem művelet: ami kiveszt az alaphalmazból.

groupoid: egyetlen kétváltozós műveleti algebra.

9. elő

$(A; \circ)$ 2 változós művelet.

idempotencia: $(\forall a \in A) (a \circ a = a)$

pl: ÉS, VAGY a logikában.

$(\{1, n\}; \wedge)$, $(\mathcal{P}(U); \cup)$

asszociatív: $(\forall a, b, c \in A) (a \circ (b \circ c) = (a \circ b) \circ c)$

kommutatív, zéruselem létezése, egységelem létezése

$(\forall a \in A) (\exists b \in A) (a \circ b = b \circ a = e)$ egységelem

inverz létezése.

Példa $(\mathbb{Z}_5 \setminus \{\bar{0}\}; \cdot)$ van inverz:

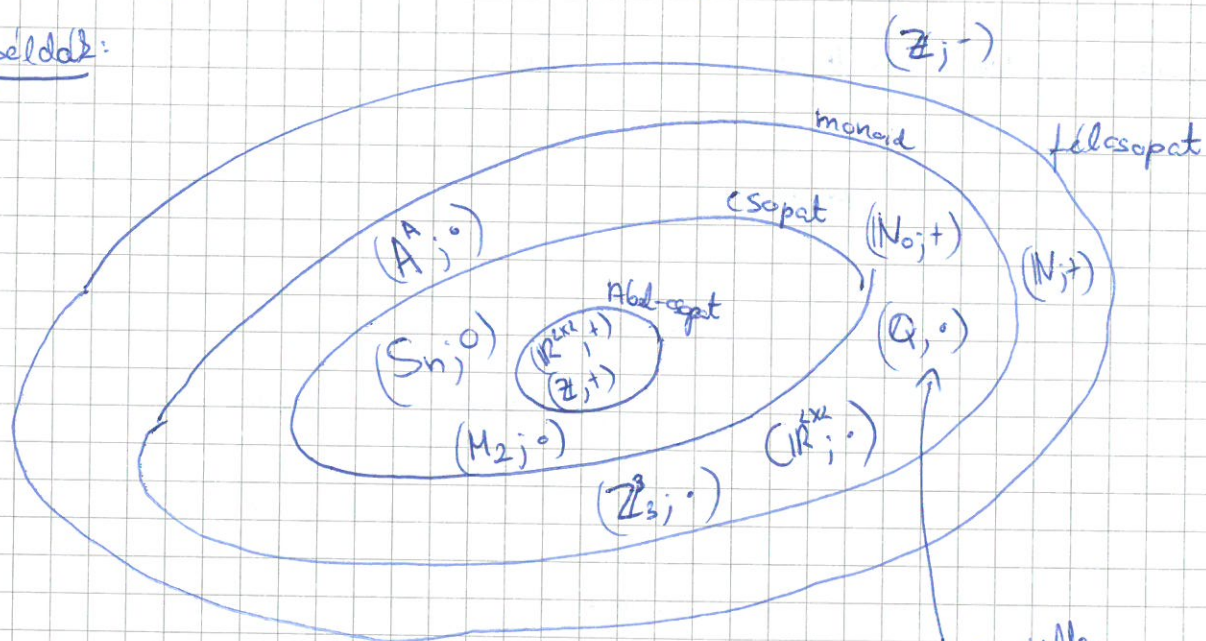
$$\left. \begin{array}{l} \bar{1} \cdot \bar{1} = \bar{1} \\ \bar{2} \cdot \bar{3} = \bar{1} \\ \bar{3} \cdot \bar{2} = \bar{1} \\ \bar{4} \cdot \bar{4} = \bar{1} \end{array} \right\} \checkmark \text{ ok.}$$

gyöggpéldaként.

$(A; \circ)$ grupoid.

- Ha associatív: félcsoport
- associatív és van egyrészlem: monoid
- + még minden elemnek van inverze: csoport
- + még kommutatív is: Abel-csoport

példák:



$$M_2 = \{ A \in \mathbb{R}^{2 \times 2} : |A| \neq 0 \}$$

csúsz

22. tétel:

Biz.: $\forall$ elemnek legfeljebb 1 inverze van. $(A; \cdot)$ monoid. $\hookrightarrow$ egységelem: 1

Ezt látjuk be.

$a \in A$ és indirekt módon tfh $\exists b$ és c , $b \neq c$, a inversei.

$$ab = ba = 1 \text{ és } ac = ca = 1.$$

$$b = 1 \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 1 = c \Rightarrow b = c$$

$\uparrow$ egységelem $\uparrow$ c inverze a-nak $\uparrow$ assoc. $\uparrow$ b inverze a-nak $\uparrow$ egységelem

(1) $(a^{-1})^{-1} = a$ Biz: $a^{-1} \cdot a = a \cdot a^{-1} = 1$
 $\uparrow$ a^{-1} def.

(2) $(ab)^{-1} = b^{-1}a^{-1}$ Biz: $(ab)^{-1} = b^{-1}a^{-1}$
 $(a \cdot b) \cdot (b^{-1}a^{-1}) = a \cdot \underbrace{(bb^{-1})}_1 a^{-1} = \underbrace{a \cdot 1}_a a^{-1} = aa^{-1} = 1$
 $\hookrightarrow$ 1 változás (inverz)

Multiplikatív írásmód: $(A; \cdot)$ $(A; 1, ^{-1}, \cdot)$

Additív írásmód: $(A; +)$ $(A; 0, -, +)$
 $\uparrow$ nulla változás

26. lemma

(1) $a^n \cdot a = a \cdot a^n = a^{n+1}$, $a \in A$ és $n \in \mathbb{Z}$.

$n > 0$: $a^n \cdot a = (\underbrace{a \cdot a \cdot a \cdots a}_{n \text{ db}}) \cdot a = \underbrace{a \cdot a \cdot a \cdots a}_{n+1}$
 $\uparrow$ assoc.

$n = 0$: $a^n \cdot a = 1 \cdot a = a^1 = a^{0+1}$
 $\uparrow$ def. (3)

$$n < 0: \quad a^n \cdot a = \underbrace{(\bar{a}^1 \bar{a}^1 \dots \bar{a}^1)}_{-n \text{ db}} \cdot a = \underbrace{(\bar{a}^1 \bar{a}^1 \dots \bar{a}^1)}_{-n-1 \text{ db}} \cdot \underbrace{(\bar{a}^1 a)}_1 = a^{n+1} \quad \square$$

"
 $-(n+1) \text{ db}$

(2) $\bar{a}^1 \cdot a^n = ?$

$$n > 0: \quad \bar{a}^1 \cdot a^n = \bar{a}^1 \cdot \underbrace{(a \dots a)}_{n \text{ db}} = \underbrace{(\bar{a}^1 \cdot a)}_1 \cdot \underbrace{(a \dots a)}_{n-1 \text{ db}} = a^{n-1}$$

asoc

$n = 0: \quad \checkmark \quad a \quad \text{alap.}$

$$n < 0: \quad \bar{a}^1 a^n = \bar{a}^1 \cdot \underbrace{(\bar{a}^1 \bar{a}^1 \dots \bar{a}^1)}_{-n \text{ db}} = \underbrace{\bar{a}^1 \dots \bar{a}^1}_{-n+1 \text{ db}} = a^{n-1} \quad \square$$

asoc
 "
 $-(n-1)$
 egyezik ki.

elem rendje.

$n \in \mathbb{N}, \quad a^n = 1 \quad \sigma(a) = n$
 $\uparrow$ legkisebb.
 Ha $\nexists n \rightarrow \sigma(a) = \infty$.

$(\mathbb{Z}_6; +)$

$\sigma(0) = 1$

$\underbrace{1 + 1 + \dots + 1}_{6 \text{ db}} = \bar{0}$

$\sigma(\bar{1}) = 6$

$\bar{2} + \bar{2} + \bar{2} = \bar{0} \Rightarrow \sigma(\bar{2}) = 3$

$\bar{3} + \bar{3} = \bar{0} \Rightarrow \sigma(\bar{3}) = 2$

$\bar{4} + \bar{4} + \bar{4} = \bar{0} \Rightarrow \sigma(\bar{4}) = 3$

$\bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \bar{0} \quad \sigma(\bar{5}) = 6$

$\underbrace{\bar{4}}_{3}$

osztói
6-nek!
megj.

31. tétel:

$(A; \cdot)$ csoport. $\sigma(a) < \infty$

(1) $n \in \mathbb{Z}$ és $a^n = 1 \Leftrightarrow \sigma(a) \mid n$.

Biz.: $\Leftarrow$ Tudjuk: $\sigma(a) \mid n \Rightarrow \exists k \in \mathbb{Z}$, hogy $n = k \sigma(a)$

$$a^n = a^{\overset{(\sigma(a)k)}{k \sigma(a)}} = \underbrace{\left(a^{\sigma(a)}\right)^k}_{\text{def: } = 1} = 1.$$

$\Rightarrow a^n = 1$ lesz most a zéróérték. Tíh $\sigma(a) \nmid n$.

Ha n -et másképpen osztjuk $\sigma(a)$ -val:

$$n = k \cdot \sigma(a) + j \quad \text{Tudjuk: } 0 < j < \sigma(a)$$

$$1 = a^n = a^{k \sigma(a) + j} = \underbrace{a^{k \sigma(a)}}_{\substack{\uparrow \\ \text{27. tétel}}} \cdot a^j = \underbrace{\left(a^{\sigma(a)}\right)^k}_1 \cdot a^j = a^j = 1 \quad \begin{array}{l} \swarrow \\ \sigma(a) \text{ a} \\ \text{legkisebb pozitív} \\ \text{zérus: } \boxed{0} \end{array}$$

(2) $a^n = a^m \Leftrightarrow n \equiv m \pmod{\sigma(a)}$

Biz.: $\Leftarrow$ $n \equiv m \pmod{\sigma(a)}$

$$\sigma(a) \mid n - m \Leftrightarrow n = k \sigma(a) + m$$

$$a^n = a^{m + k \sigma(a)} = a^m \cdot \underbrace{\left(a^{\sigma(a)}\right)^k}_1 = a^m$$

$\Rightarrow a^n = a^m \quad \exists k \in \mathbb{Z}$, hogy $n = m + k$.

$$a^n = a^m \cdot a^k = a^m \Rightarrow a^k = 1 \Rightarrow \sigma(a) \mid k \quad \text{len} \\ \text{igaz.}$$

Kaptuk: $n = m + j \cdot \sigma(ca) \Rightarrow n \equiv m \pmod{\sigma(ca)}$. $\square$

Még példa rendre:

$$(S_6; \circ) \quad (1 \ 2 \ 3)^{\boxed{3}} = id$$

$$(1 \ 2 \ 3)(1 \ 2 \ 3) = (1 \ 3 \ 2)$$

$$(1 \ 3 \ 2)(1 \ 2 \ 3) = \cancel{(1)} \cancel{3} \cancel{(2)} = id$$

$$\left((1 \ 2 \ 3)(4 \ 5) \right)^{\boxed{6}} = id$$

$\uparrow \quad \uparrow$
 $3 \quad 2$

lkt rel. átlashosszat lkt-je rel.

IDEGEN CIRKUSOK.

4.9 feladat

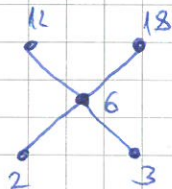
(1) level nélküli fa.



(2) végtelen

egész számok halmaza a
szűkebb egyelő!

(3)



(4)



(5)



1 max $\rightarrow$ legnagyobb
véges
halmaz



(6) végtelen lánc
+ 1 bony.

lineáris reláció

$$\emptyset \subseteq A \times A$$



nem reflexív. (micsoda kezdett)
szimmetrikus, antiszimmetrikus.

5.2.

(6) $(\{-1, 0, 1\}; \sqcup)$, $a \sqcup b = \max(a, b)$.

$\sqcup$	-1	0	1
-1	-1	0	1
0	0	0	1
1	1	1	1

↑
innen
valószínű
előre

Kommutatív: szimmetrikus a főátlóra. ✓

1 a zéruselem, látjuk
sorában is, oszlopában is
1 van.

Zéruselem: kell egy olyan sor és oszlop,
ahol megismétlődik az elemek
sorrendje.
-1 lesz és itt jelenleg.

inverz zérus: -1-nek van inverze, ön maga.

Keresni kell egyezményt a táblázatban, majd szimmetrikus is
megvan.

5.3. típus van a tartalom.

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

nem kommutatív.

↓
nem egyenlő a transzponáltjával.

$$d * c \neq c * d$$

$$d * b = d * c$$

$$d * b \neq c$$

nemancellatív.

nincs zéruselem. (d baloldali, de
nem jobb)

a egyezmény.

$$\left. \begin{array}{l} a \text{ inv. } a. \\ b \text{ inv. } c. \end{array} \right\} \text{enge}$$

7.

Kancellatív más néven egyszerűsítékes.

$$a * x = a * y \Rightarrow x = y.$$

$$x * a = y * a \Rightarrow x = y.$$

Belátható, hogy nem ez, ha ismétlődő elem sorokban vagy oszlopokban.

5.4. feladat (ZH):

(a) $(\mathbb{Q}; \circ)$ $g \circ r = g$

asszociatív: $\forall g, r, u \in \mathbb{Q}, (g \circ r) \circ u \stackrel{!}{=} g \circ (r \circ u)$

$$\underbrace{\underbrace{g \circ r}_g}_{g} = \underbrace{g \circ \underbrace{r \circ u}_r}_g \quad \checkmark$$

Asszociatív.

Nem kommutatív: $g \circ r = g, r \circ g = r,$
ha $r \neq g$.

Zéruselem: $\exists \sigma \in \mathbb{Q} \forall g \in \mathbb{Q} \quad \sigma \circ g = g \circ \sigma = \sigma$

$$\sigma \circ g = \sigma$$

$$g \circ \sigma = g$$

ha $g = \sigma$, bgi van.
nincs zéruselem.

Egységelem: nincs, és inverz sincs

Ez egy falsoposzt. (balzér).

$$(d) (\mathbb{R}; \Delta) \quad x \Delta y = xy - 2(x+y) + 6$$

asszoc.: $\forall x, y, z \in \mathbb{R}, \quad (x \Delta y) \Delta z = x \Delta (y \Delta z)$

$$(xy - 2(x+y) + 6) \Delta z =$$

$$(xy - 2(x+y) + 6)z - 2 \cdot (xy - 2(x+y) + 6 + z) + 6 =$$

$$= xyz - 2xz - 2yz + 6z - 2xy + 4y + 4x - 12 - 2z + 6$$

szimmetrikusnak látszik.

lt a másik irány

kommutatív-e?

$$\forall x, y \in \mathbb{R} \quad x \Delta y = xy - 2(x+y) + 6$$

"

$$y \Delta x = yx - 2(y+x) + 6$$

$\mathbb{R}$ -en $+$ és $\cdot$ kommutatív.

kommutatív felcsop. Eddig.

Zéruselem:

$$\exists \sigma \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad x \Delta \sigma = x \Delta \sigma = \sigma.$$

Zérus.

$$x \Delta \sigma = x\sigma - 2(x+\sigma) + 6 \stackrel{?}{=} 0$$

$$x \cdot \sigma - 2x - 2\sigma + 6 = \sigma$$

$$\sigma(x-2) - 2x + 6 = \sigma$$

$$\sigma(x-2) - \sigma = 2x - 6$$

$$x\sigma - 3\sigma = 2x - 6$$

$$\sigma(x-3) = 2x - 6$$

$$\sigma = \frac{2x-6}{x-3} = \frac{2(x-3)}{x-3} = 2.$$

$x \neq 3!$

ebből
le lehet
olvasni.

$x=3$ külön vizsgálando!

$$3 \Delta \sigma = 3\sigma - 2(3 + \sigma) + 6 =$$

$$= 3\sigma - 6 - 2\sigma + 6 = \sigma. \quad \checkmark \quad \text{jó.} \quad \underline{2 \text{ a zéruselem.}}$$

Egyszélem:

$$\cancel{e \Delta x = ex - 2(e+x) + 6 = a}$$

$$\cancel{ex - 2e - 2x + 6 = a}$$

$$\cancel{ex - 2e - e = 2x - 6}$$

$$\cancel{e(x-3) = 2x-6}$$

$$e = \frac{2(x-3)}{x-3} = 2 \quad x \neq 3.$$

$x=3$:

$$\cancel{e \Delta 3 = e \cdot 3 - 2(e+3) + 6 = e}$$

$$\cancel{3e - 2e - 6 + 6 = e}$$

$$e = e \quad \checkmark$$

OK.

2 egyezlem.

Rossz

kezes ut: $e \Delta x = x$

Rasszoldkeppen.

$e = 3$ jön ki.

A 3 az egyezlem.

Inverz:

$$(\forall x \in \mathbb{R}) (\exists y \in \mathbb{R}) (x \Delta y \stackrel{\text{Komm.}}{=} y \Delta x = e = 3).$$

$$x \Delta y = xy - 2(x+y) + 6 = 3$$

$$\cancel{xy - 2x - 2y + 6 = 3}$$

$$y(x-2) = 2x-3$$

$$y = \frac{2x-3}{x-2}, x \neq 2.$$

(10)

$x = 2$ case:

$$2 \Delta y = 2y - 2(y+2) + 6 = 2y - 2y - 4 + 6 = 2 \neq e.$$

Prices & demand inverse.

$$(\mathbb{R}; \Delta) - \text{monoid}$$
$$(V \setminus \{2\}; \Delta) - \text{Abd-csq.} \quad \square$$

$(P\{N\}; n)$ Monoid.

N egészen

dem sind 24-ben kein Lesi.

5.9.

✓ 7-tes relatív primordiját

$$(\mathbb{Z}_7^*, \cdot) \quad \sigma(\bar{3})$$

$$\overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} = \overline{1} \quad \sigma(\overline{3}) = 6.$$

- Kongruenz
- diag.

isnétla.

1.17. /a

$$72x + 60y = 24$$

$$\text{Link}_0(72, 60) = 12$$

$$72 = 1.60 + 12$$

12/24 ✓ megoldható.

$$60 = 5 \cdot 12 + 0$$

$$12 = 72 - 60$$

असुवि.

11

$$(a') \quad 132x + 72y = 24$$

$$132 = 72 + 60$$

$$72 = 60 + 12$$

$$\text{luko}(132, 72) = 12.$$

$$60 = 5 \cdot 12 + 0$$

$$12 = 72 - 60 = 72 - (132 - 72) =$$

$$= (-1) \cdot 132 + 2 \cdot 72 = 12$$

$$24 = 132 \cdot (-2) + 72 \cdot (4)$$

$$x_0 = -2$$

$$y_0 = 4$$

$$x = -2 + \frac{72}{12} \cdot t$$

$$y = 4 - \frac{132}{12} t \quad t \in \mathbb{Z}.$$

$$(140/9)$$

$$5x \equiv 1 \pmod{6} \Rightarrow x \equiv -1 \pmod{6}$$

$$7x \equiv 9 \pmod{10} \Rightarrow x \equiv 7 \pmod{10}$$

$$\begin{array}{r} 11 \\ 49 \end{array}$$

$$\text{luko}(10, 6) = 2$$

$$7 - (-1) = 8 \quad 2 \mid 8 \checkmark$$

$$x = 7 \cdot 10 + 7 = 30k - 20 + 7 = 30k - 13 \quad \text{negoldhato!}$$

$$10k + 7 \equiv -1 \pmod{6}$$

$$10k \equiv -8 \pmod{6}$$

$$\begin{array}{r} 11 \\ -20 \end{array}$$

$$k \equiv -2 \pmod{3} \Rightarrow k = 3l - 2$$

$$\text{luko}(10, 6) = 2$$

$$x \equiv -13 \pmod{30}$$

logika: predikátum-rekció. lehet.

(2.19)

$$(3) (\forall x)(\forall y) \left((P(x,y) \wedge P(y,x)) \rightarrow E(x,y) \right) \checkmark$$

eljesmi lehet

OK. pozitív.

⊕ befamódizál.

Leépessés: vizsgálni, hogy irányított-e.

Permutáció pl. 3. 20.

Relációk: lehet. Hasse-diagram, refl. szim, tranz. OSLTÁLYOS
LEKÉPEZÉS MAGJA.

3. 20.

$$(2) \left((1 \ 2 \ 4 \ 3)^{-6} \cdot (1 \ 5 \ 4)^{13} \right)^{-4} = (1 \ 4)(2 \ 3)(1 \ 5 \ 4)^5$$

"

$$(1 \ 2 \ 4 \ 3)^2 = (1 \ 2 \ 4 \ 3)(1 \ 2 \ 4 \ 3) = (1 \ 4)(2 \ 3)$$

$$(1 \ 5 \ 4)^{13} = (1 \ 5 \ 4)^1 = (1 \ 5 \ 4)$$

$$(1 \ 4)(2 \ 3)(1 \ 5 \ 4) = \cancel{(1)}(2 \ 3)\cancel{(4)} = (2 \ 3)$$

$$\cancel{(2 \ 3)}^4 = \cancel{(2 \ 3)} \text{ id.} = (2 \ 3)(4 \ 5)$$

$$\left((2 \ 3)(4 \ 5) \right)^4 = (4 \ 5)^4 (2 \ 3)^4 = \text{id}$$

