1. feladat

Határozzuk meg az $(\{a, b, c, d\}; *)$ grupoidban az alábbi részgrupoidokat.

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

Megoldás.

(a) $[c, d] = ?$

$c * d = a,\ d * c = b \implies [c, d] = \{a, b, c, d\}$

(b) $[a, b] = ?$

$a * a = a,\ a * b = b,\ b * a = b,\ b * b = b$, tehát $\{a, b\}$ már zárt $\implies [a, b] = \{a, b\}$

(c) $[d] = ?$

$d * d = a,\ a * d = b$ és $\{a, b, d\}$ már zárt $\implies [d] = \{a, b, d\}$

Részalgebra, generálás

Definíció. Legyen $(A; F)$ egy algebrai struktúra, és legyen $B \subseteq A$ nemüres részhalmaz. Ha B zárt az összes F-beli műveletre, akkor a B halmaz az F-beli műveletekkel (pontosabban azok B-re való megszorításaival) egy $(B; F)$ algebrai struktúrát alkot, amelyet $(A; F)$ részalgebrájának nevezünk.

Példa. Ha csak egyetlen kétváltozós műveletünk van, vagyis egy $(A; *)$ grupoidról van szó, akkor a B halmaz zártsága ezt jelenti:

$$\forall b_1, b_2 \in B: \quad b_1 * b_2 \in B.$$

Például az $(\mathbb{N}; +)$ félcsoportban a páros számok halmaza zárt, és így a páros számok egy részfélcsoportot alkotnak. De a páratlan számok halmaza nem zárt az összeadásra.

Definíció. Tetszőleges $B \subseteq A$ esetén $[B]$ jelöli a legszűkebb B-t tartalmazó zárt halmazt. Ezt a B halmaz által generált részalgebrának, vagy röviden B generátumának nevezzük.

Ha B az egész algebrát generálja, vagyis $[B] = A$, akkor azt mondjuk, hogy B generátorrendszere az $(A; F)$ algebrának.

Állítás. Egy $a \in A$ elem akkor és csak akkor van benne B generátumában, ha a megkapható B elemeiből kiindulva az F-beli műveletek véges sokszori alkalmazásával.

Megjegyzés. A B halmaz akkor és csak akkor zárt, ha $[B] = B$.

2. feladat.

Határozzuk meg az $(\{a, b, c, d\}; *)$ grupoidban az alábbi részgrupoidokat.

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

(a) $[a] = ?$

(b) $[b] = ?$

(c) $[b, c] = ?$

(d) $[a, d] = ?$

(e) $[c, d] = ?$

3. feladat

Határozzuk meg az $(\mathbb{N}; +)$ félcsoportban a $[2, 9]$ részfélcsoportot.

Megoldás.

Az a kérdés, milyen számokat lehet „felépíteni” a 2 és 9 számokból összeadással.

Próbálkozzunk: $[2, 9] = \{2, 9, 11, 4, 13, 20, \ldots\} = ?$

Próbálkozzunk szisztematikusan:

$$\begin{array}{rcccccccc} & 2 & 4 & 6 & 8 & 10 & 12 & 14 & \cdots \\ 9 & 11 & 13 & 15 & 17 & 19 & 21 & 23 & \cdots \\ 18 & 20 & 22 & 24 & 26 & 28 & 30 & 32 & \cdots \\ 27 & 29 & 31 & 33 & 35 & 37 & 39 & 41 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Tehát $[2, 9] = \{2, 4, 6, 8, 9, 10, 11, 12, 13, 14, 15, \ldots\} = \mathbb{N} \setminus \{1, 3, 5, 7\}$.

Gyakorolj!

3. feladat.

Határozzuk meg az $(\mathbb{N}; +)$ félcsoportban az alábbi részfélcsoportokat.

(a) $[2, 9] = ?$

(b) $[2, 5] = ?$

(c) $[3, 5] = ?$

(d) $[4, 10] = ?$

4. feladat

Határozzuk meg az $(\mathbb{N};\cdot)$ félcsoportban a $[2,9]$ részfélcsoportot.

Megoldás.

Az a kérdés, milyen számokat lehet „felépíteni" a 2 és 9 számokból szorzással.

Ha k darab 2-est és ℓ darab 9-est szorzunk, akkor a $2^k \cdot 9^\ell = 2^k \cdot 3^{2\ell}$ számot kapjuk.

Tehát $[2,9] = \{2^k \cdot 3^{2\ell} : k, \ell \in \mathbb{N}_0\}$.

Szavakkal megfogalmazva: egy természetes szám akkor és csak akkor van benne a $[2,9]$ félcsoportban, ha prímfelbontásában csak 2-es és 3-as szerepel, és 3 kitevője páros.

Gyakorolj!

4. feladat.

Határozzuk meg az $(\mathbb{N}; \cdot)$ félcsoportban az alábbi részfélcsoportokat.

(a) $[2, 9] = ?$

(b) $[2, 5] = ?$

(c) $[3, 5] = ?$

(d) $[4, 10] = ?$

Részcsoport

A $(\mathbb{Z}; +)$ csoportban $[2, 9] = \{2, 4, 6, 8, 9, 10, 11, 12, 13, 14, 15, \ldots\}$, ami nem csoport. Ha csoportot szeretnénk, akkor nemcsak az összeadásra, hanem az additív inverz képzésére is „le kell zárni" a halmazt.

Definíció. Legyen $(A; *)$ egy csoport, jelölje e az egységelemet, és jelölje a^{-1} az a elem inverzét. A $B \subseteq A$ halmazt akkor nevezzük részcsoportnak, ha

1. B zárt a $*$ műveletre: $\forall b_1, b_2 \in B: \ b_1 * b_2 \in B$,
2. B zárt az inverzképzésre: $\forall b \in B: \ b^{-1} \in B$,
3. B tartalmazza az egységelemet: $e \in B$.

Definíció. Egy $B \subseteq A$ hamaz által generált részcsoport a legszűkebb B-t tartalmazó részcsoport.

Példa. A $(\mathbb{Z}; +)$ csoportban a páros számok részcsoportot alkotnak, de a pozitív páros számok csak részfélcsoportot.

Állítás. Egy $a \in A$ elem akkor és csak akkor van benne a B által generált részcsoportban, ha a megkapható B elemeiből kiindulva a csoportművelet és az inverzképzés véges sokszor történő alkalmazásával.

5. feladat

(a) Határozzuk meg a $(\mathbb{Z}; +)$ csoportban a $[2, 9]$ részcsoportot.

Megoldás.

Az a kérdés, milyen számokat lehet „felépíteni” a 2 és 9 számokból összeadással és kivonással.

Az 1-es számot ki tudjuk hozni: $9 - 2 - 2 - 2 - 2 = 1$.

Az 1-est saját magával összeadogatva minden pozitív egész kijön, additív inverzzel pedig a negatívak is.

Tehát $[2, 9] = \mathbb{Z}$.

5. feladat

(b) Határozzuk meg a $(\mathbb{Z}; +)$ csoportban a $[6, 10]$ részcsoportot.

Megoldás.

A 2-es számot ki tudjuk hozni: $6 + 6 - 10 = 2 \cdot 6 + (-1) \cdot 10 = 2$.

A 2-esből megkapjuk az összes páros számot.

Páratlan számot pedig nem kapunk, mert 6 és 10 páros, és a páros számok halmaza zárt az összeadásra és az additív inverz képzésére.

Tehát $[6, 10] = \{\text{páros számok}\}$.

Másik megoldás.

Ha x „darab" 6-ost és y „darab" 10-est veszünk, akkor a $6x + 10y$ számot kapjuk.

Tehát $$\begin{aligned}[6, 10] &= \{6x + 10y : x, y \in \mathbb{Z}\} = \\ &= \{c \in \mathbb{Z} : \exists x, y \in \mathbb{Z} \colon 6x + 10y = c\} = \\ &= \{c \in \mathbb{Z} : 2 \mid c\}.\end{aligned}$$

Gyakorolj!

5. feladat.

Határozzuk meg a $(\mathbb{Z}; +)$ csoportban az alábbi részcsoportokat.

(a) $[2, 9] = ?$

(b) $[6, 10] = ?$

(c) $[5, 17] = ?$

(d) $[25, 65] = ?$

(e) $[30, 42, 105] = ?$

6. feladat

(a) Határozzuk meg a $(\mathbb{Z}_{14}; +)$ csoportban a $\left[\overline{6}, \overline{10}\right]$ részcsoportot.

Megoldás.

Ez majdnem ugyanaz, mint az előző feladat, csak minden számra kell tenni egy „vonást". Tehát a páros számok modulo 14 maradékosztályait kapjuk:

$$\left[\overline{6}, \overline{10}\right] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\}.$$

(b) Határozzuk meg a $(\mathbb{Z}_{15}; +)$ csoportban a $\left[\overline{6}, \overline{10}\right]$ részcsoportot.

Megoldás.

Mik a páros számok modulo 15 maradékosztályai?

$$\left[\overline{6}, \overline{10}\right] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}\} = \mathbb{Z}_{15}.$$

Másik megoldás.

Az a kérdés, hogy mely $\overline{b} \in \mathbb{Z}_{15}$ maradékosztályok reprezentálhatóak páros számmal:

$$\begin{aligned}
[6, 10] &= \{\overline{b} \in \mathbb{Z}_{15} : \exists x \in \mathbb{Z} \colon \overline{2x} = \overline{b}\} = \\
&= \{\overline{b} \in \mathbb{Z}_{15} : \exists x \in \mathbb{Z} \colon 2x \equiv b \pmod{15}\} = \\
&= \{\overline{b} \in \mathbb{Z}_{15} : 1 \mid b\} = \mathbb{Z}_{15}.
\end{aligned}$$

Gyakorolj!

6. feladat.

(a) Határozzuk meg a $(\mathbb{Z}_{14}; +)$ csoportban a $\left[\overline{6}, \overline{10}\right]$ részcsoportot.

(b) Határozzuk meg a $(\mathbb{Z}_{15}; +)$ csoportban a $\left[\overline{6}, \overline{10}\right]$ részcsoportot.

(c) Határozzuk meg a $(\mathbb{Z}_{15}; +)$ csoportban a $\left[\overline{25}, \overline{65}\right]$ részcsoportot.

(d) Határozzuk meg a $(\mathbb{Z}_{16}; +)$ csoportban a $\left[\overline{25}, \overline{65}\right]$ részcsoportot.

(e) Határozzuk meg a $(\mathbb{Z}_{21}; +)$ csoportban a $\left[\overline{30}, \overline{42}, \overline{105}\right]$ részcsoportot.

Ciklikus csoportok

Megfigyeltük, hogy

- a $(\mathbb{Z};+)$ csoportban $[2,9]=[1]=\mathbb{Z}$,
- a $(\mathbb{Z};+)$ csoportban $[6,10]=[2]=\{\text{páros számok}\}$,
- a $(\mathbb{Z}_{14};+)$ csoportban $\left[\overline{6},\overline{10}\right]=\left[\overline{2}\right]=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10},\overline{12}\}$,
- a $(\mathbb{Z}_{15};+)$ csoportban $\left[\overline{6},\overline{10}\right]=\left[\overline{2}\right]=\left[\overline{1}\right]=\mathbb{Z}_{15}$.

Definíció. Ha az $(A;*)$ csoportot lehet egyetlen elemmel generálni, azaz van olyan $a\in A$ elem, amelyre $[a]=A$, akkor azt mondjuk, hogy $(A;*)$ ciklikus csoport.

Tétel. Ciklikus csoport minden részcsoportja ciklikus

Példák.

- A $(\mathbb{Z};+)$ csoport ciklikus, mert $\mathbb{Z}=[1]$.
  Ezért minden részcsoportja is ciklikus, pl. $[6,10]=[2]$.
- A $(\mathbb{Z}_m;+)$ csoport minden m modulusra ciklikus, mert $\left[\overline{1}\right]=\mathbb{Z}_m$.
  Ezért minden részcsoportja is ciklikus, pl. $\left[\overline{6},\overline{10}\right]=\left[\overline{2}\right]$.
- Az $(\mathbb{R};+)$ csoport nem ciklikus (miért?).
- Bármilyen $(A;*)$ csoport és bármilyen $a\in A$ elem esetén $[a]$ ciklikus részcsoport.

Ciklikus csoportok

Állítás. Az a elem által generált ciklikus részcsoport:

$$[a] = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\} = \{a^k : k \in \mathbb{Z}\}.$$

Példák. A $(\mathbb{C}\backslash\{0\}; \cdot)$ csoportban

- $[2] = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\} = \{\ldots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \ldots\} \cong (\mathbb{Z}; +)$,
- $[-1] = \{-1, 1\} \cong (\mathbb{Z}_2; +)$,
- $[i] = \{i, -1, -i, 1\} \cong (\mathbb{Z}_4; +)$.

Definíció. Az $(A; *)$ csoportban az $a \in A$ elem rendje az a legkisebb pozitív egész k kitevő, amelyre $a^k = e$. Ha nincs ilyen kitevő, akkor a rendje végtelen. Jelölés: $o(a)$.

Példák. A $(\mathbb{C}\backslash\{0\}; \cdot)$ csoportban

- $o(2) = \infty$,
- $o(-1) = 2$,
- $o(i) = 4$.

Tétel. Ha $o(a) = n$, akkor $[a]$ elemszáma n, sőt, $([a]; *) \cong (\mathbb{Z}_n; +)$.
Ha a végtelen rendű elem, akkor $[a]$ végtelen, sőt, $([a]; *) \cong (\mathbb{Z}; +)$.

7. feladat

Határozzuk meg a $(\mathbb{Z}_{20}; +)$ csoportban az alábbi elemek rendjét.

(a) $o(\overline{5}) = ?$

Megoldás.

$$\left[\overline{5}\right] = \{\overline{5}, \overline{10}, \overline{15}, \overline{0}\} \implies o(\overline{5}) = 4$$

(b) $o(\overline{6}) = ?$

Megoldás.

$$\left[\overline{6}\right] = \{\overline{6}, \overline{12}, \overline{18}, \overline{4}, \overline{10}, \overline{16}, \overline{2}, \overline{8}, \overline{14}, \overline{0}\} \implies o(\overline{6}) = 10$$

(c) $o(\overline{7}) = ?$

Megoldás.

$$\left[\overline{7}\right] = \{\overline{7}, \overline{14}, \overline{1}, \overline{8}, \overline{15}, \overline{2}, \overline{9}, \overline{16}, \overline{3}, \overline{10}, \overline{17}, \overline{4}, \overline{11}, \overline{18}, \overline{5}, \overline{12}, \overline{19}, \overline{6}, \overline{13}, \overline{0}\} \implies o(\overline{7}) = 20$$

(d) $o(\overline{8}) = ?$

Megoldás.

$$\left[\overline{8}\right] = \{\overline{8}, \overline{16}, \overline{4}, \overline{12}, \overline{0}\} \implies o(\overline{8}) = 5$$

(e) $o(\overline{9}) = ?$

Megoldás.

$$\left[\overline{9}\right] = \{\overline{9}, \overline{18}, \overline{7}, \overline{16}, \overline{5}, \overline{14}, \overline{3}, \overline{12}, \overline{1}, \overline{10}, \overline{19}, \overline{8}, \overline{17}, \overline{6}, \overline{15}, \overline{4}, \overline{13}, \overline{2}, \overline{11}, \overline{0}\} \implies o(\overline{9}) = 20$$

Gyakorolj!

7. feladat.

Határozzuk meg a $(\mathbb{Z}_{21}; +)$ csoportban az alábbi elemek rendjét.

(a) $o(\overline{5}) =$

(b) $o(\overline{6}) = ?$

(c) $o(\overline{7}) = ?$

(d) $o(\overline{8}) = ?$

(e) $o(\overline{9}) = ?$

8. feladat.

Határozzuk meg a $(\mathbb{Z}_{30}; +)$ csoportban az alábbi elemek rendjét.

(a) $o(\overline{18}) = ?$

(b) $o(\overline{19}) = ?$

(c) $o(\overline{20}) = ?$

(d) $o(\overline{21}) = ?$

(e) $o(\overline{22}) = ?$

Ráadás

A modulo m maradékosztályok a szorzással nem alkotnak csoportot.

Egy $\overline{a} \in \mathbb{Z}_m$ elemnek akkor és csak akkor van multiplikatív inverze, ha $\operatorname{lnko}(a, m) = 1$.

Az ilyen maradékosztályokat redukált maradékosztályoknak nevezzük.

A redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli.

Nem nehéz ellenőrizni, hogy $(\mathbb{Z}_m^*; \cdot)$ Abel-csoport, amelynek elemszáma $\varphi(m)$.

Amikor kiszámoltuk, hogy milyen nap lesz 2019^{2020} nap múlva, akkor a $\overline{2019} = \overline{3} \in \mathbb{Z}_7^*$. rendjét, illetve az általa generált részcsoporot határoztuk meg:

$$\left[\overline{3}\right] = \{\overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}, \overline{1}\} \implies o(\overline{3}) = 6$$

Az Euler–Fermat-tétel szerint minden $\overline{a} \in \mathbb{Z}_m^*$ maradékosztályra $\overline{a}^{\varphi(m)} = \overline{1}$, amiből az következik, hogy $o(\overline{a}) \mid \varphi(m)$.
Ez speciális esete a következő tételnek:

Lagrange tétele. Egy n-elemű csoportban minden a elemre $a^n = e$, és $o(a) \mid n$.