

9. Részcsoporthok

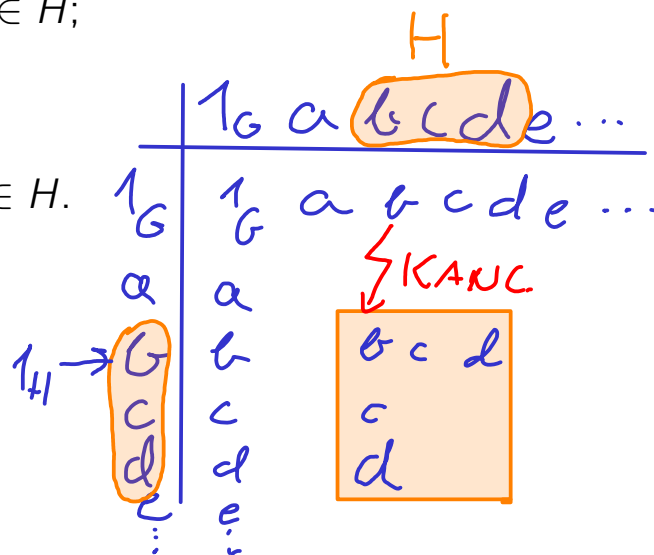
9.1. Definíció. Ha G csoport, és H olyan részgrupoid, ami maga is csoport, akkor azt mondjuk, hogy H **részcsoporthja** G -nek, és ezt így jelöljük: $H \leq G$.

9.2. Tétel. Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoporthja G -nek, ha

1. H zárt a szorzásra: $\forall h_1, h_2 \in H: h_1 \cdot h_2 \in H$;

2. H tartalmazza G egységelemét: $1 \in H$;

3. H zárt az inverzképzésre: $\forall h \in H: h^{-1} \in H$.



9.3. Tétel (Lagrange tétele). Ha G véges csoport és H részcsoporthja G -nek, akkor H elemszáma osztója G elemszámának: $|H| \mid |G|$.

9.4. Példa.

- $(\mathbb{C}; +) \geq (\mathbb{R}; +) \geq (\mathbb{Q}; +) \geq (\mathbb{Z}; +) \geq (\{\text{páros számok}\}; +) \geq (\{0\}; +)$
- $(\mathbb{C} \setminus \{0\}; \cdot) \geq (\mathbb{R} \setminus \{0\}; \cdot) \geq (\mathbb{Q} \setminus \{0\}; \cdot) \geq (\{1\}; \cdot)$
- $(\{1, -1\}; \cdot) \leq (\{1, -1, i, -i\}; \cdot) \leq E_8$
- $(\text{SL}_n(T); \cdot) \leq (\text{GL}_n(T); \cdot)$, ahol
 $\text{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}$ **általános lineáris csoport**
 $\text{SL}_n(T) = \{A \in T^{n \times n} : \det(A) = 1\}$ **speciális lineáris csoport**
- egy alakzat szimmetriacsoportja részcsoporthot alkot az összes egybevágósági transzformációk csoportjában
- $S_4 \geq \{\text{id}, (12)(34), (13)(24), (14)(23)\} = V$ **Klein-csoport**
- az S_n csoportban részcsoporthot alkotnak a páros permutációk

$$\begin{array}{c|cccc} & 1 & -1 & 8 & -8 \\ \hline 1 & 1 & -1 & 8 & -8 \\ -1 & -1 & 1 & -8 & 8 \\ 8 & 8 & -8 & 1 & -1 \\ -8 & -8 & 8 & -1 & 1 \end{array} \cong \mathbb{Z}_4 \times V$$

10. Elem rendje, ciklikus csoportok

10.1. Definíció. Legyen G egy csoport és $a \in G$. Az a elem egész kitevős hatványait a következőképpen értelmezzük:

- $n > 0$ esetén legyen $a^n = \underbrace{a \cdot \dots \cdot a}_n$;
- $n = 0$ esetén legyen $a^n = 1$;
- $n < 0$ esetén legyen $a^n = (a^{-1})^{|n|}$.

10.2. Tétel. Tetszőleges G csoport, $a, b \in G$ elemek és $n, m \in \mathbb{Z}$ kitevők esetén teljesülnek az alábbi azonosságok:

$$(1) \ a^n \cdot a^m = a^{n+m};$$

$$(2) \quad (a^n)^m = a^{nm};$$

(3) ha $ab = ba$, akkor $(ab)^n = a^n b^n$;

$$(4) \quad (ab)^{-1} = b^{-1}a^{-1}.$$

Trivialitás. Az $a \in G$ elemet tartalmazó legszűkebb részcsoport:

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

10.3. Definíció. A G csoportot **ciklikus csoportnak** nevezzük, ha egyetlen elemmel generálható, azaz $\exists a \in G: [a] = G$.

10.4. Példa. $\mathbb{Z}$ és $\mathbb{Z}_n$ ciklikus csoportok:

- 0.4. Példa.** $\mathbb{Z}$ és $\mathbb{Z}_n$ ciklikus csoportok:
- $\mathbb{Z} = [1]$; $1 + \dots + 1 \in [1] \Rightarrow \mathbb{N}_0 \subseteq [1] \xrightarrow{\text{inv.}} \mathbb{Z} \subseteq [1]$
 - $\mathbb{Z}_n = [\bar{1}]$.

10.5. Tétel.

10.6. Megjegyzés. Minden csoportban „hemzsegek” a ciklikus részcsoporthok: bármely G csoportban bármely a elem egy ciklikus részcsoporthot generál.

10.7. Példa. Számítsuk ki a $(\mathbb{C} \setminus \{0\}, \cdot)$ csoportban 2 és i hatványait.

k	...	-4	-3	-2	-1	0	1	2	3	4	5	6	7	...
2^k	...	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{2}$	1	2	4	8	16	32	64	128	...
i^k	...	1	i	-1	$-i$	1	i	-1	$-i$	1	i	-1	$-i$	...

Az első esetben a hatványok mind különbözőek, ezért $(\mathbb{Z}; +) \cong ([2]; \cdot)$

A második esetben négyes periodicitást tapasztalunk, ezért $[i] \cong (\mathbb{Z}_4; +)$

Egy tetszőleges G csoportban egy a elemet hatványozva is ez a két eset lehetséges.

1. eset. A hatványok mind különbözőek.

Ekkor $\varphi: (\mathbb{Z}, +) \rightarrow ([a]; \cdot), k \mapsto a^k$ izomorfizmus,
ezért $([a]; \cdot) \cong (\mathbb{Z}, +)$.

- Injektivitás: feltettük, hogy $k \neq \ell$ esetén $a^k \neq a^\ell$.
- Szürjektivitás: $[a]$ minden eleme előáll a^k alakban.
- Művelettartás: $(k + \ell)\varphi = a^{k+\ell} = a^k \cdot a^\ell = k\varphi \cdot \ell\varphi$.

2. eset. A hatványok között van ismétlődés: $\exists i < j: a^i = a^j \implies a^{j-i} = 1$.

Legyen n a legkisebb **pozitív** kitevő, amelyre $a^n = 1$.

Az $a^0, a^1, a^2, \dots, a^{n-1}$ hatványok páronként különbözőek és minden más hatvány ezek valamelyikével megegyezik:

$k = nq + r$ esetén $a^k = a^{nq+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r$.

Ekkor $\varphi: (\mathbb{Z}_n, +) \rightarrow ([a]; \cdot), \bar{k} \mapsto a^k$ izomorfizmus,
ezért $([a]; \cdot) \cong (\mathbb{Z}_n, +)$.

- Jóldefiniáltság: $k \equiv \ell \pmod{n} \implies a^k = a^\ell$.
- Injektivitás: $k \not\equiv \ell \pmod{n} \implies a^k \neq a^\ell$.
- Szürjektivitás: $[a]$ minden eleme előáll a^k ($k = 0, \dots, n-1$) alakban.
- Művelettartás: $(\bar{k} + \bar{\ell})\varphi = \overline{k+\ell}\varphi = a^{k+\ell} = a^k \cdot a^\ell = \bar{k}\varphi \cdot \bar{\ell}\varphi$.

10.8. Tétel. Egy csoport akkor és csak akkor ciklikus, ha izomorf a következő csoportok valamelyikével:

$$\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \dots, \mathbb{Z}.$$

10.9. Definíció. Az $a \in G$ elem **rendjén** azt a legkisebb n pozitív egész számot értjük, amelyre $a^n = 1$. Ha nincs ilyen n , akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét $o(a)$ jelöli (olvasd: *ordó*):

$$o(a) = \min \{n \in \mathbb{N} : a^n = 1\} \quad (\text{a } \min \emptyset = \infty \text{ megállapodással}).$$

10.10. Definíció. A G csoport **rendjén** elemeinek számát (számosságát) értjük.

10.11. Megjegyzés. Az a elem rendje nem más, mint az általa generált részcsoporthoz rendje: $o(a) = |[a]|$. (Sőt, $[a] \cong \mathbb{Z}_{o(a)}$.)

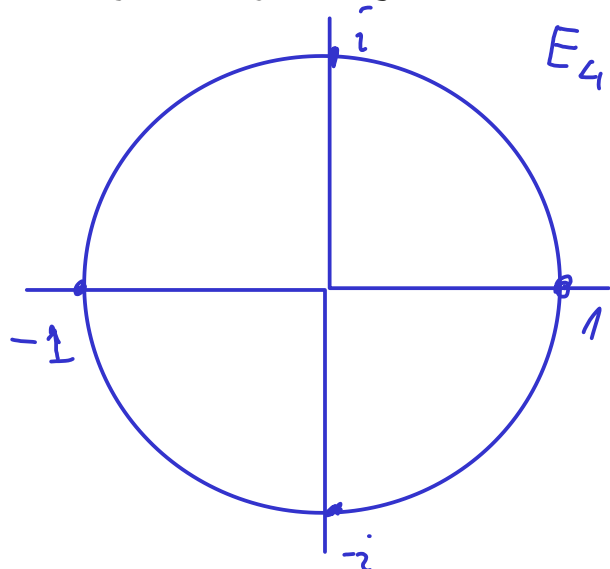
10.12. Példa. Határozzuk meg az $a \in G$ elem rendjét.

- $G = (\mathbb{C} \setminus \{0\}; \cdot)$ $a = 2$: $[2] = \{\dots, \frac{1}{2}, 1, 2, 4, \dots\} \cong \mathbb{Z}$, $o(2) = \infty$
- $G = (\mathbb{C} \setminus \{0\}; \cdot)$ $a = i$: $[i] = \{i, -1, -i, 1\} \cong \mathbb{Z}_4$, $o(i) = 4$
- $G = (\mathbb{C}; +)$ $a = i$: $[i] = \{\dots, -i, 0, i, 2i, \dots\} \cong \mathbb{Z}$, $o(i) = \infty$

10.13. Megjegyzés. Tetszőleges $z \in \mathbb{C} \setminus \{0\}$ komplex szám esetén

$$o(z) = n \iff |[z]| = n \iff \underbrace{[z]}_{n\text{-ed.}} \cong \underbrace{E_n}_{n\text{-ed.}} \cong \mathbb{Z}_n.$$

Az ilyen tulajdonságú számokat nevezzük **primitív n -edik egységgyököknek**.



$$E_4 = \{1, -1, i, -i\} \quad \text{s. 2.}$$

$$[i] = \{1, i, -1, -i\} = E_4 \quad \sigma(i) = 4$$

$$[-i] = \{1, -i, -1, i\} = E_4 \quad \sigma(-i) = 4$$

$$[-1] = \{1, -1\} = E_2 \quad \sigma(-1) = 2$$

$$[1] = \{1\} = E_1 \quad \sigma(1) = 1$$

10.14. Feladat. Határozzuk meg a G csoportban a megadott elem rendjét.

(a) $G = \mathbb{Z}_{10} \ni \bar{2}$ $[2] = \{2, 4, 6, 8, 0\} \cong \mathbb{Z}_5$ $\sigma(2) = 5$

(b) $G = \mathbb{Z}_{10} \ni \bar{3}$ $[3] = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} = \mathbb{Z}_{10}$ $\sigma_{\mathbb{Z}_{10}}(3) = 10$

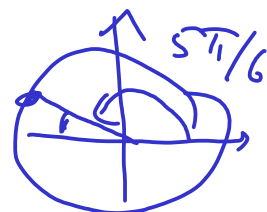
(c) $G = \mathbb{Z}_{10} \ni \bar{4}$ $[4] = \{4, 8, 2, 6, 0\} \cong \mathbb{Z}_5$ $\sigma(4) = 5$
 $[2] =$

(d) $G = \mathbb{Z}_{10}^* \ni \bar{3}$ $[3] = \{3, 9, 7, 1\} \cong \mathbb{Z}_4$ $\sigma_{\mathbb{Z}_{10}^*}(3) = 4$

(e) $G = \mathbb{Z}_{12} \ni \bar{5}$ $[5] = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} = \mathbb{Z}_{12}$ $\sigma_{\mathbb{Z}_{12}}(5) = 12$

(f) $G = \mathbb{Z}_{12}^* \ni \bar{5}$ $[5] = \{5, 1\} = \mathbb{Z}_2$ $\sigma_{\mathbb{Z}_{12}^*}(5) = 2$

(g) $G = \mathbb{C} \setminus \{0\} \ni \overbrace{-\frac{\sqrt{3}}{2} + \frac{1}{2}i}^z = \cos \frac{5\pi}{6} + i \sin \frac{5\pi}{6} = \operatorname{cis} \frac{5\pi}{6}$
 $z^n = \operatorname{cis} \frac{5n\pi}{6} = 1 \Leftrightarrow 12|n$



(h) $G = S_5 \ni (234) = \alpha$
 $\sigma(\alpha) = 3$

(i) $G = S_5 \ni (234)(15) = \beta$ $\sigma(\beta) = 6$
 $\beta^2 = ((234)(15))^2 = (234)^2(15)^2 = \text{id} \in 1, 3, 2 | k$

(j) $G = S_5 \ni (1245)(234) = \gamma$ $\gamma^2 \neq (1245)^2 \cdot (234)^2$
 $\gamma = (1345)(2) \Rightarrow \sigma(\gamma) = 4$

(k) $G = D_{10} \ni a^4$ $[a^4] = \{a^4, a^8, a^2, a^6, a^0 = \text{id}\} \cong \mathbb{Z}_5 \Rightarrow \sigma(a^4) = 5$

(l) $G = D_{10} \ni a^4 t \leftarrow \text{tükr.}$ $(a^4 t)^2 = \text{id} \Rightarrow [a^4 t] = \{a^4 t, \text{id}\} \cong \mathbb{Z}_2$
 $\sigma(a^4 t) = 2$
 $a^4 t \cdot a^4 t = a^4 \cdot a^4 \cdot t \cdot t = \text{id}$

noldali sörvisig $\mathbb{Z}$ -additív nyitott gyűrű.

x egész után $\mathbb{Z}$ - $x \bmod n$

Mi az a legkisebb $x \in \mathbb{N}$, amire $\mathbb{Z}x \equiv 0 \pmod{n}$?

$$x \equiv 0 \pmod{\frac{n}{(n, k)}}$$

$$\frac{n}{(n, k)} \mid x$$

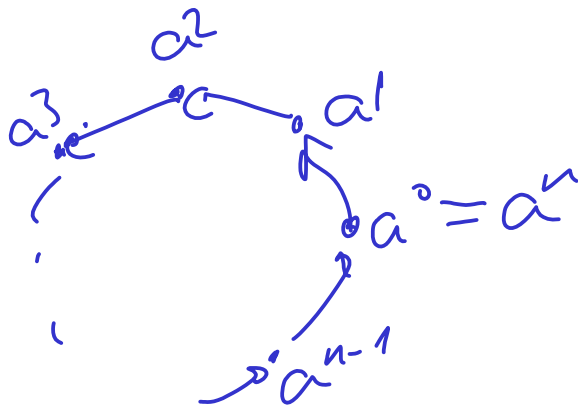
A legkisebb pozit. $x = \frac{n}{(n, k)}$.



Ez a legkisebb
előforduló.
Összehang.
munka jut el.

$$\forall a \in \mathbb{Z}^* \Leftrightarrow (n, k) = 1$$

$$\forall k \in \mathbb{Z}_n^* : [k] = \mathbb{Z}_n^* \Leftrightarrow (n, k) = 1$$



10.15. Tétel (A rend tulajdonságai). Legyen G egy véges csoport és $a \in G$ egy n -edrendű elem.

$$(1) \forall k, \ell \in \mathbb{Z}: a^k = a^\ell \iff k \equiv \ell \pmod{n}$$

$$(2) a^{-1} = a^{n-1} = \overbrace{a \cdot \dots \cdot a}^{n-1}$$

$$(3) \forall k \in \mathbb{Z}: a^k = 1 \iff n \mid k$$

(4) n osztója G elemszámának

$$(5) a^{|G|} = 1$$

$$(6) o(a^k) = \frac{n}{\gcd(n, k)} \quad [a^k] \leq [a] \cong \mathbb{Z}_n \text{ cyclic}$$

Bizonyítás.

$$(1) \text{ldtétel. } [a] \cong \mathbb{Z}_n$$

$$(2) -1 \equiv n-1 \pmod{n} \xrightarrow{(\cdot)} a^{-1} = a^{n-1}$$

$$\forall AG: o(a) = n \Rightarrow a^n = 1 \xrightarrow{(\cdot a^{-1})} a^{n-1} = a^{-1}$$

$$(3) a^k = 1 = a^0 \xrightarrow{(\cdot)} k \equiv 0 \pmod{n} \iff n \mid k$$

$$(4) [a] \leq G \xrightarrow{(\cdot)} |[a]| \mid |G|$$

$$(5) o(a) = n \Rightarrow a^n = 1 \xrightarrow{(\cdot)} a^{|G|} = 1 \quad (|G|/n \in \mathbb{N} \text{ (4)})$$

$$(6) C_{n/k}$$

10.16. Tétel. Minden prímmrendű csoport ciklikus.

Bizonyítás.

$$|G| = p \text{ prím. } (a \in G \Rightarrow \sigma(a) | p \Rightarrow \sigma(a) = 1 \vee \sigma(a) = p$$

$\begin{matrix} \uparrow \\ a=1 \end{matrix}$

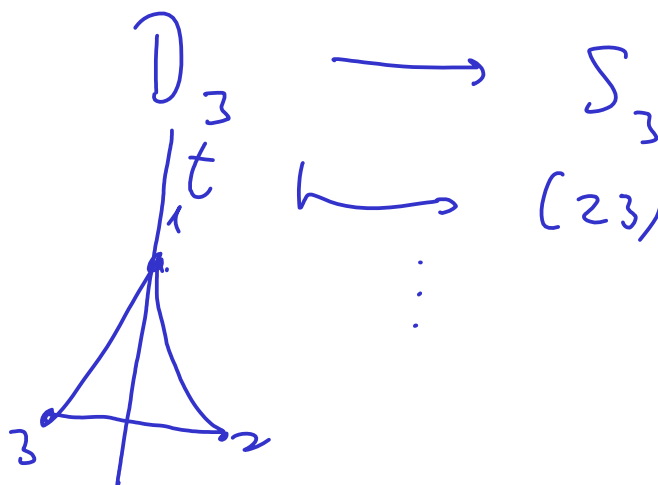
$$\text{Teljesen } \forall a \in G \setminus \{1\} : |[a]| = p \rightarrow [a] = G$$

$\cong \mathbb{Z}_p$

□

10.17. Tétel. A kis elemszámú csoportok (izomorfia erejéig) a következők:

- egyelemű: $\{1\}$;
- kételemű: $\mathbb{Z}_2$;
- háromelemű: $\mathbb{Z}_3$;
- négyelemű: $\mathbb{Z}_4$ és V ;
- ötelemű: $\mathbb{Z}_5$;
- hatelemű: $\mathbb{Z}_6$ és $S_3 \cong D_3$



Bizonyítás.

$$|G| = 4 \quad \forall a \in G : \sigma(a) = 1, 2, 4$$

$$1) \text{ Ha } \exists a \in G : \sigma(a) = 4, \text{ akkor } [a] = G$$

$\cong \mathbb{Z}_4$

$$2) \text{ Ha } \forall a \in G \setminus \{1\} : \sigma(a) = 2 \rightarrow a^2 = 1$$

G:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\cong V$

□

11. Generálás

11.1. Definíció. Legyen G egy csoport és $\emptyset \neq B \subseteq G$. A B részhalmaz által **generált részcsoporthon** a G csoport **legszerűbb** olyan részcsoporthat értjük, ami tartalmazza B -t. Jelölés: $[B]$.

A B halmaz által generált részcsoporthat nem más, mint...

- az összes B -t tartalmazó részcsoporthat metszete;
- azon G -beli elemek halmaza, amelyek megkaphatók B elemeiből kiindulva a szorzás és az inverzképzés véges számú alkalmazásával.

Ha $[B] = G$, akkor azt mondjuk, hogy B **generátorrendszere** G -nek.

11.2. Példa.

- $\mathbb{Z} = [1]$
- $\mathbb{Z}_n = [\bar{1}]$
- $(\mathbb{Q}^+)_1 = [\{\text{prímszámok}\}]$
- $S_n = [\{\text{transzpozíciók}\}]$
- $D_n = [a, t]$

11.3. Feladat. Határozzuk meg a $\mathbb{Z}$ csoportban a $[6, 10]$ részcsoporthat.

Pr: $(\mathbb{Z}, +) \supseteq [6, 10] = \{6, 10, 16, 22, 4, -4, 2, \dots\}$

$2 \in [6, 10] \Rightarrow \underbrace{2 + \dots + 2}_{2k} \in [6, 10] \rightarrow \{2k \mid k \in \mathbb{Z}\} \subseteq [6, 10]$

$6, 10 \text{ prs} \Rightarrow [6, 10] \subseteq [2]$

Ízelet: $[6, 10] = [2] = \{2k \mid k \in \mathbb{Z}\}$

$[6, 10] = \{6x + 10y \mid x, y \in \mathbb{Z}\} = \{c \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} : 6x + 10y = c\}$
 $= \{c \in \mathbb{Z} \mid (6, 10) \mid c\} = \{c \in \mathbb{Z} \mid 2 \mid c\}$

11.4. Feladat. Határozzuk meg a $\mathbb{Z}_{14}$ csoportban a $[\overline{6}, \overline{10}]$ részcsoporthot.

$$[\overline{6}, \overline{10}] = \{\overline{6}x + \overline{10}y : x, y \in \mathbb{Z}\} = \{\overline{2}k : k \in \mathbb{Z}\} = [\overline{2}] = \\ = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{0}\} \cong \mathbb{Z}_7$$

11.5. Feladat. Határozzuk meg a $\mathbb{Z}_{15}$ csoportban a $[\overline{6}, \overline{10}]$ részcsoporthot.

$$[\overline{6}, \overline{10}] = \{\overline{6}x + \overline{10}y : x, y \in \mathbb{Z}\} = \{\overline{2}k : k \in \mathbb{Z}\} = [\overline{2}] = \\ = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{0}\} \cong \mathbb{Z}_{15}$$

11.6. Feladat. Határozzuk meg a $\mathbb{Z}_{28}^*$ csoportban a $[\overline{25}, \overline{27}]$ részcsoporthot.

$$\mathbb{Z}_{28}^* \supseteq [-1, -3] \stackrel{?}{=} \{-1, -3, 1, 3, 9, -9\} = [3]$$

$$\begin{array}{ll} (\pm 1) \cdot (\pm 1) = \pm 1 & (\pm 3) \cdot (\pm 3) = \pm 9 \\ (\pm 1) \cdot (\pm 3) = \pm 3 & (\pm 3) \cdot (\pm 9) = \pm 27 = \pm 1 \\ (\pm 1) \cdot (\pm 9) = \pm 9 & (\pm 9) \cdot (\pm 9) = \pm 81 = \pm 3 \end{array}$$

$$a: 45^\circ \quad a^2: 90^\circ$$

11.7. Feladat. Határozzuk meg a D_8 csoportban az $[a^6, a^3t]$ részcsoporthot.

$$[a^6] = \{a^0, a^4, a^2, a^8 = a^0 = id\} = \{id, a^2, a^4, a^6\} \cong \mathbb{Z}_4$$

$$[a^6, a^3t] \stackrel{?}{=} \{id, a^2, a^4, a^6, a^3t, a^5t, a^7t, a^1t\}$$

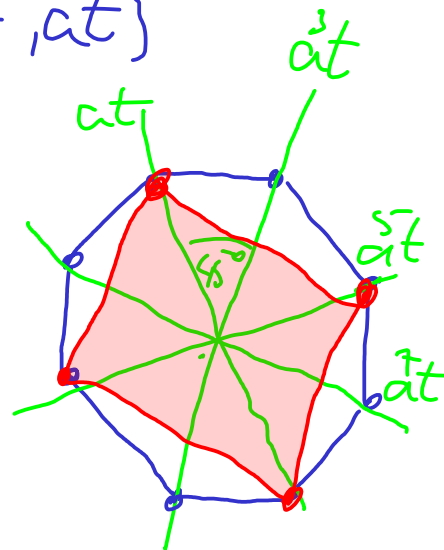
$$= \{a^{2k}, a^{2k+1} \cdot t \mid k \in \mathbb{Z}\} \cong D_4$$

$$a^{2k} \cdot a^{2l} = a^{2(k+l)} \quad \checkmark$$

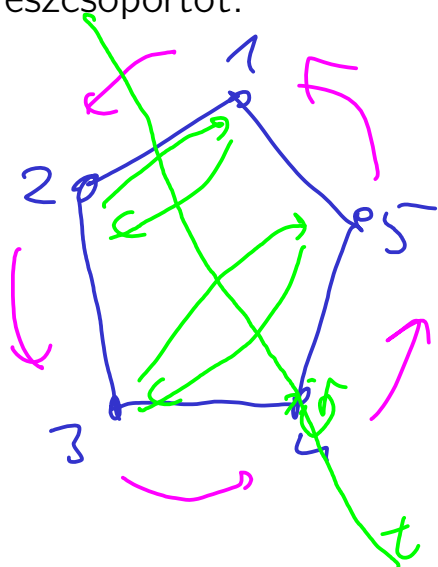
$$a^{2k} \cdot a^{2l+1} t = a^{2(k+l)+1} t \quad \checkmark$$

$$a^{2k+1} t \cdot a^{2l} = a^{2(k-l)+1} t \quad \checkmark$$

$$a^{2k+1} t \cdot a^{2l+1} t = a^{2(k-l)} \quad \checkmark$$



11.8. Feladat. Határozzuk meg az S_5 csoportban az $[(12345), (12)(35)]$ részcsoporthot.



$$[\alpha, \tau] \leq S_5$$

$$\parallel S$$

$$[\alpha, \tau] = D_5$$

$$[\alpha, \tau] = \{id, \alpha, \tau, (15)(24), (10) \}$$

$$10 \text{ elem}$$

1. Az Euler-féle φ függvény

1.1. Definíció. Jelöljük $\varphi(n)$ -nel az n -nél nem nagyobb pozitív egész számok közül azoknak a számát, amelyek n -hez relatív prímek:

$$\varphi(n) = |\{a : 1 \leq a \leq n \text{ és } \text{Inko}(a, n) = 1\}|.$$

Az így kapott függvényt **Euler-féle φ függvénynek** nevezzük. Ha megállapodunk abban, hogy $\mathbb{Z}_1^*$ egyelemű halmaz, akkor tömörebben is megfogalmazhatjuk a definíciót:

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |\mathbb{Z}_n^*|.$$

1.2. Példa. Számítsuk ki közvetlenül a definíció alapján φ néhány értékét:

(a) $\varphi(6) = |\mathbb{Z}_6^*| = |\{1, 2, 3, 4, 5, 6\}| = |\{1, 5\}| = 2$
 $= |\{1, 2, 3, 4, 5\}| = |\{1, 5\}| = 2$ $\mathbb{Z}_6^* = \{1, 5\}$

(b) $\varphi(7) = |\mathbb{Z}_7^*| = |\{1, 2, 3, 4, 5, 6, 7\}| = 6$ $\varphi(p) = p - 1 = |\mathbb{Z}_p^*|$

(c) $\varphi(8) = |\mathbb{Z}_8^*| = |\{1, 2, 3, 4, 5, 6, 7, 8\}| = 4$

(d) $\varphi(1024) = |\mathbb{Z}_{1024}^*| = |\{1, 2, 3, 4, \dots, 1023, 1024\}| = \frac{1024}{2} = 512 = 1024 \cdot (1 - \frac{1}{2})$

p_1 (e) $\varphi(81) = |\mathbb{Z}_{81}^*| = |\{1, 2, 3, 4, 5, 6, \dots, 78, 79, 80, 81\}| = 81 - \frac{81}{3} = 81 \cdot (1 - \frac{1}{3}) = 54$

1.3. Tétel. Tetszőleges p prím és α pozitív egész kitevő esetén

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Bizonyítás. Az $\{1, \dots, p^\alpha\}$ halmaz minden p -edik eleme osztható p -vel (ezek száma $p^{\alpha-1}$), a többiek viszont relatív prímek p^α -hoz (ugye?).

Így tehát $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

1.4. Példa. Számítsuk ki közvetlenül a definíció alapján $\varphi(100)$ értékét.

Mivel $n = 2^2 \cdot 5^2$, egy szám akkor és csak akkor nem relatív prím n -hez, ha osztható 2-vel vagy 5-tel. Ezeket a „rossz” számokat fogjuk „kiszitálni” az $\{1, 2, \dots, 100\}$ halmazból.

$$U = \{1, 2, \dots, 100\}$$

$$|U| = 100$$

$$A_1 = \{a \in U : 2 \mid a\}$$

$$|A_1| = \frac{100}{2} = 50$$

$$A_2 = \{a \in U : 5 \mid a\}$$

$$|A_2| = \frac{100}{5} = 20$$

$$A_1 \cap A_2 = \{a \in U : 10 \mid a\}$$

$$|A_1 \cap A_2| = \frac{100}{2 \cdot 5} = 10$$



$$\begin{aligned} \varphi(100) &= |U| - |A_1| - |A_2| + |A_1 \cap A_2| = 100 - \frac{100}{2} - \frac{100}{5} + \frac{100}{10} = \\ &= 100 \cdot \left(1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{2 \cdot 5}\right) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \end{aligned}$$

1.5. Tétel. Legyen az n pozitív egész szám prímszaktényezős felbontása $n = \prod_{i=1}^k p_i^{\alpha_i}$. Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k \overbrace{(p_i^{\alpha_i} - p_i^{\alpha_i-1})}^{\varphi(p_i^{\alpha_i})} = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1).$$

Bizonyítás. Ha n -nek csak két prímszaktója van, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, akkor az előző példában használt szita-formulát alkalmazhatjuk:

$$U = \{1, \dots, n\}$$

$$|U| = n$$

$$A_1 = \{a \in U : p_1 \mid a\}$$

$$|A_1| = \frac{n}{p_1}$$

$$A_2 = \{a \in U : p_2 \mid a\}$$

$$|A_2| = \frac{n}{p_2}$$

$$A_1 \cap A_2 = \{a \in U : p_1 p_2 \mid a\}$$

$$|A_1 \cap A_2| = \frac{n}{p_1 p_2}$$

$$\varphi(n) = |\overline{A_1 \cup A_2}| = |U| - |A_1| - |A_2| + |A_1 \cap A_2| =$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right)$$

Ha n -nek k darab prímszaktója van, akkor k darab halmazra kell felírni a szita-formulát. A gondolatmenet a fentihez hasonló, csak a formulák nagyobbak. $\square$

1.6. Feladat. Számítsuk ki a tanult képlet alapján φ néhány értékét:

$$(a) \varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$$

$$(b) \varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) = 4 \cdot 6 \cdot 4 = 96$$

$$(c) \varphi(2025) = \varphi(3^4 \cdot 5^2) = (3^4 - 3^3) \cdot (5^2 - 5^1) = 54 \cdot 20 = 1080$$

1.7. Tétel. A primitív n -edik egységgyökök száma $\varphi(n)$ minden n pozitív egész szám esetén.

Bizonyítás. Tudjuk, hogy az n -edik egységgyökök csoportja ciklikus:

$$E_n = \{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\} = [\varepsilon_1], \quad \text{ahol } \varepsilon_k = \varepsilon_1^k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}.$$

Az ε_k egységgyök akkor és csak akkor primitív n -edik egységgyök, ha rendje n . Alkalmazzuk a hatvány rendjére vonatkozó képletet:

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{o(\varepsilon_1)}{\text{lko}(o(\varepsilon_1), k)} = \frac{n}{\text{lko}(n, k)}.$$

Tehát a primitív n -edik egységgyökök halmaza

$$\{\varepsilon_k : 0 \leq k \leq n-1 \text{ és } \text{lko}(k, n) = 1\},$$

ennek a halmaznak pedig éppen $\varphi(n)$ eleme van (ugye?).

□