CSOPORTOK

Waldhauser Tamás

SZTE Bolyai Intézet

Tartalom

Definíció

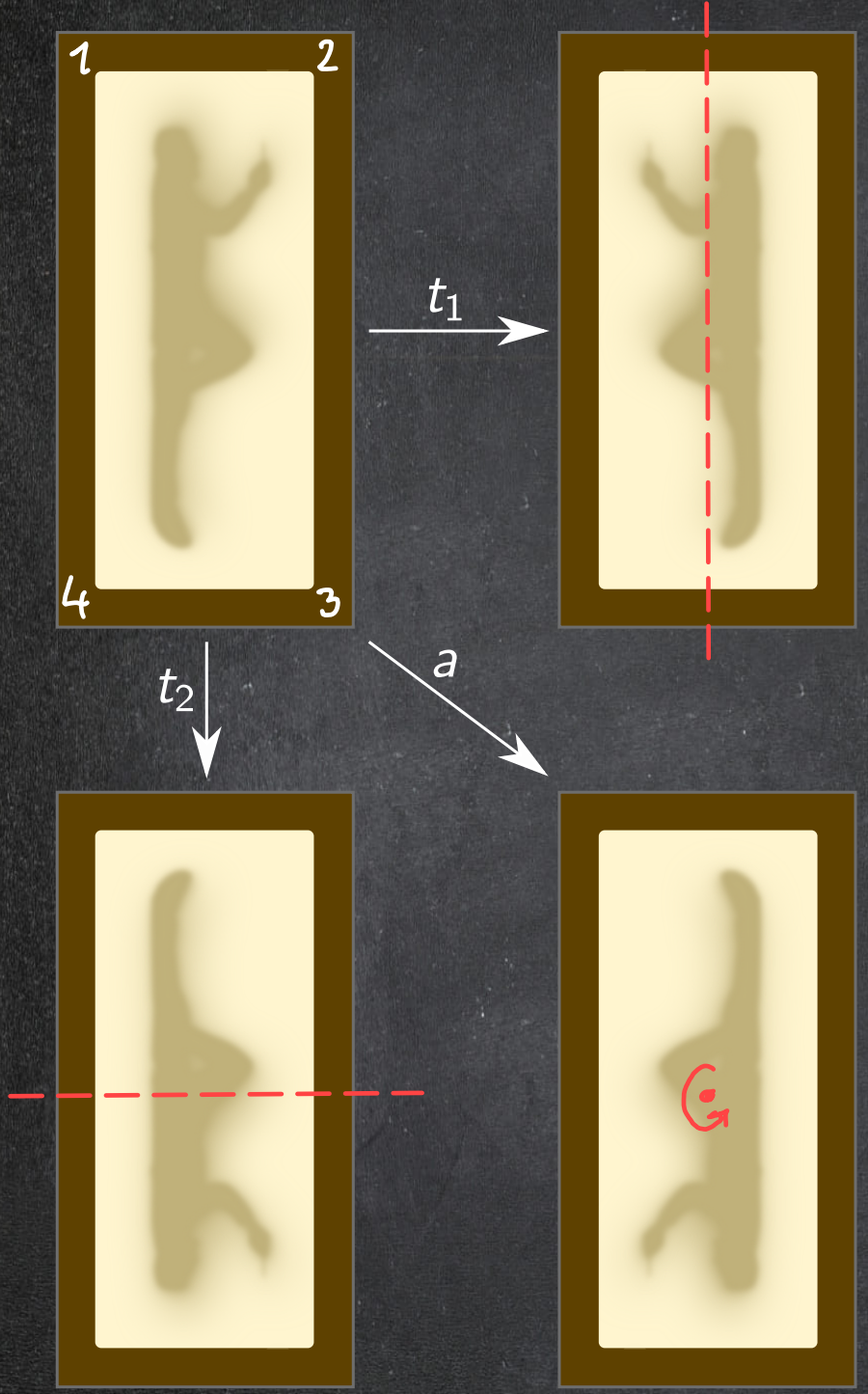
Csoportnak nevezünk egy $(A; *)$ grupoidot, ha

- $*$ asszociatív: $\forall a, b, c \in A\colon\ (a * b) * c = a * (b * c)$;
- létezik egységelem: $\exists e \in A\ \ \forall a \in A\colon\ \ a * e = e * a = a$;
- minden elemnek van inverze: $\forall a \in A\ \ \exists b \in A\colon\ \ a * b = b * a = e$.

	multiplikatív írásmód	additív írásmód
művelet	$a \cdot b = ab$	$a + b$
egységelem	1	0
inverz	a^{-1}	$-a$

Példák

- $(\mathbb{C}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{Z}; +)$, $(\{\text{páros számok}\}; +)$, $\ldots$
- $(\{0\}; +)$
- $(T^{n\times m}; +)$ tetszőleges T testre
- $(\mathbb{Z}_n; +)$ tetszőleges $n \in \mathbb{N}$ esetén
- $(\mathbb{C} \setminus \{0\}; \cdot)$, $(\mathbb{R} \setminus \{0\}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$
- $(\{1\}; \cdot)$, $(\{1, -1\}; \cdot)$, $(\{1, -1, i, -i\}; \cdot) = E_4$
- $(E_n; \cdot)$, ahol $E_n = \{z \in \mathbb{C} : z^n = 1\}$
- $(\mathrm{GL}_n(T); \cdot)$, ahol $\mathrm{GL}_n(T) = \{A \in T^{n\times n} : \det(A) \neq 0\}$
- $(\mathbb{Z}_n^*; \cdot)$ tetszőleges $n \in \mathbb{N}$ esetén
- $(S_n; \cdot)$, ahol $S_n = \{ f : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijekciók} \}$
- szimmetriacsoportok



Klein-csoport

$\cdot$	id	a	t_1	t_2
id	id	a	t_1	t_2
a	a	id	t_2	t_1
t_1	t_1	t_2	id	a
t_2	t_2	t_1	a	id

$\cong V \leq S_4$

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

Tétel

(1) Bármely grupoidban legföljebb egy egységelem létezhet.

(2) Bármely monoidban egy elemnek legföljebb egy inverze lehet.

Biz.:

(1) Tfh. e_1 és e_2 is egységelem.

$$e_1 = e_1 \cdot e_2 = e_2$$

(2) Tfh. a-nak b_1 és b_2 is inverze.

$$\left.\begin{array}{l} (b_1 a)\, b_2 = 1 \cdot b_2 = b_2 \\ b_1 (\underbrace{a b_2}_{1}) = b_1 \cdot 1 = b_1 \end{array}\right\} \Longrightarrow b_1 = b_2$$

$\blacksquare$

$$a^{-1} = f(a)$$

Definíció

Azt mondjuk, hogy az A halmazon értelmezett $\cdot$ kétváltozós művelet. . .

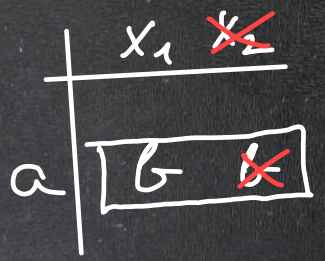
- invertálható, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek legalább egy megoldása van.
- kancellatív, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek legfeljebb egy megoldása van.

Megjegyzés

A kancellativitás így is megfogalmazható: $\forall a, x_1, x_2, y_1, y_2 \in A$:

$$a \cdot x_1 = a \cdot x_2 \implies x_1 = x_2;$$

$$y_1 \cdot a = y_2 \cdot a \implies y_1 = y_2.$$



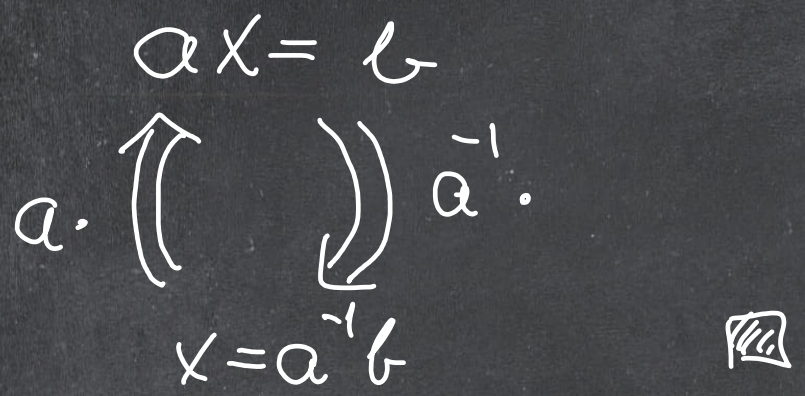
Megjegyzés

Az invertálhatóság azt jelenti, hogy a művelettáblázat minden sorában és minden oszlopában az A halmaz minden eleme legalább egyszer fellép. A kancellativitás pedig azt jelenti, hogy minden sorban és minden oszlopban minden elem legfeljebb egyszer lép fel.

Tétel

Csoport művelete mindig invertálható és kancellatív.

Biz.:



Tétel

Ha az A halmazon értelmezett $\cdot$ kétváltozós művelet asszociatív és invertálható, akkor $(A; \cdot)$ csoport.

Megjegyzés

A fenti tételben véges alaphalmaz esetén kicserélhetjük az invertálhatóságot a kancellativitással, de végtelen alaphalmaz esetén nem.

Az általános asszociativitás tétele

Ha $(A;\cdot)$ félcsoport, akkor minden $n \in \mathbb{N}$ és $a_1, \ldots, a_n \in A$ esetén az $a_1 \cdot \ldots \cdot a_n$ „szorzat" eredménye független a zárójelezéstől.

Definíció

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

- $n > 0$ esetén legyen $a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$
- $n = 0$ esetén legyen $a^n = 1$
- $n < 0$ esetén legyen $a^n = (a^{-1})^{|n|}$

$a^3 = (aa)a = a(aa)$

$na = \underbrace{a + \ldots + a}_{n}$

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) $(a^n)^m = a^{nm}$

$(ab)^n \neq a^n b^n$

$ab \cdots ab \neq a \cdots ab \cdots b$

Tétel

Tetszőleges G csoport és $a, b \in G$ esetén $(ab)^{-1} = b^{-1}a^{-1}$.

Biz.:

$$ab \cdot b^{-1}a^{-1} = a \cdot \underbrace{bb^{-1}}_{1} \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$$

$$b^{-1}a^{-1} \cdot ab = b^{-1} \cdot \underbrace{a^{-1}a}_{1} \cdot b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1$$

Tartalom

A csoport fogalma, példák, alaptulajdonságok

Részcsoportok

Ciklikus csoportok, elem rendje

Mellékosztályok, Lagrange tételének bizonyítása

Normálosztók, faktorcsoportok

Direkt szorzat

Definíció

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

Megjegyzés

A $(G; \cdot)$ algebra részalgebrái nem mind részcsoportok.

Például a $G = (\mathbb{Z}; +)$ csoportban a $H = \mathbb{N}$ részhalmaz zárt az összeadásra, de ez nem részcsoport (csak részfélcsoport).

Tekintsük az inverzképzést egyváltozós műveletnek:

$$G \to G, \ a \mapsto a^{-1},$$

az egységelemet pedig nullváltozós műveletnek.

Ha ezeket is bevesszük az alapműveletek közé, akkor a $(G; \cdot, {}^{-1}, 1)$ algebrát kapjuk, és ennek a részalgebrái már épp a részcsoportok.

Tétel

Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoportja G-nek, ha

(1) H zárt a szorzásra: $\forall h_1, h_2 \in H\colon\ h_1 \cdot h_2 \in H$;

(2) H tartalmazza G egységelemét: $1 \in H$;

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

$G =$

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

$H = \{c, d\}$

	c	d
c	c	d
d	d	c

Lagrange tétele

Ha G véges csoport és H részcsoportja G-nek, akkor H elemszáma osztója G elemszámának: $|H| \mid |G|$.

Példák

Részcsoportot alkot-e a G csoportban a H halmaz?

- $G = \mathbb{Z}$, $H = \mathbb{N}_0$ — nem (nem zárt az inverzképzésre)
- $G = \mathbb{Q}\setminus\{0\}$, $H = \mathbb{Q}^-$ — nem (nem zárt a szorzásra)
- $G = \mathbb{C}\setminus\{0\}$, $H = \{z \in \mathbb{C} : |z| = 1\}$ — igen

  $|z \cdot w| = |z| \cdot |w| = 1 \cdot 1 = 1$

  $|z^{-1}| = |z|^{-1} = 1^{-1} = 1$
- $G = \mathbb{Z}_{21}$, $H = \mathbb{Z}_{21}^*$ — nem (nem zárt az összeadásra)

  $\overline{3}, \overline{4} \in \mathbb{Z}_{21}^*$ de $\overline{3}+\overline{4} = \overline{7} \notin \mathbb{Z}_{21}^*$
- $G = \mathbb{Z}_{21}^*$, $H = \{\overline{1}, \overline{8}, \overline{13}, \overline{20}\}$ — igen ($\cong V$)

	$\overline{1}$	$\overline{8}$	$\overline{13}$	$\overline{20}$
$\overline{1}$	$\overline{1}$	$\overline{8}$	$\overline{13}$	$\overline{20}$
$\overline{8}$	$\overline{8}$	$\overline{1}$	$\overline{20}$	$\overline{13}$
$\overline{13}$	$\overline{13}$	$\overline{20}$	$\overline{1}$	$\overline{8}$
$\overline{20}$	$\overline{20}$	$\overline{13}$	$\overline{8}$	$\overline{1}$

$\cong V$

Definíció

Legyen G egy csoport és $\emptyset \neq B \subseteq G$. A B részhalmaz által generált részcsoporton a G csoport legszűkebb olyan részcsoportját értjük, ami tartalmazza B-t. Jelölés: $[B]$.

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

- az összes B-t tartalmazó részcsoportok 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.

Példák

- $\mathbb{Z} = [1]$ $\quad 1+\cdots+1 = n \in \mathbb{N}, \quad -n = -(1+\cdots+1), \quad 0 = 1+(-1)$
- $\mathbb{Z}_n = [\overline{1}]$
- $\mathbb{Q}^+ = [\{\text{prímszámok}\}]$ $\quad p_1 \cdot \ldots \cdot p_k \in \mathbb{N} \quad \frac{n}{m} = n \cdot m^{-1} \in \mathbb{Q}^+$

Példa

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

Sejtés: $[6,10] \overset{?}{=} \underbrace{\{2r \mid r \in \mathbb{Z}\}}_{S}$

$[6,10] = [2]$

$2 = 6 + 6 - 10 \quad \supseteq$

$6 = 2 + 2 + 2$

$10 = 2 + 2 + 2 + 2 + 2 \quad \subseteq$

① $S \leq \mathbb{Z}$ ✓

$6, 10 \in S$ ✓

S a legkisebb? $\quad 6, 10 \in H \leq \mathbb{Z} \Rightarrow 6 + 6 + (-10) = 2 \in H$

$\Rightarrow [2] \subseteq H$

$[2] = S$

② $[6, 10] = \{6x + 10y \mid x, y \in \mathbb{Z}\}$

$= \{c \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} : 6x + 10y = c\}$

$= \{c \in \mathbb{Z} \mid \underbrace{\text{lnko}(6,10)}_{2} \mid c\} = S$

Példa

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

$$[\overline{6}, \overline{10}] = [\overline{2}] = \{\overline{2k} \mid k \in \mathbb{Z}\} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\}$$

Példa

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

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

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

$$\overline{1} \in [\overline{6}, \overline{10}] \Rightarrow [\overline{1}] \subseteq [\overline{6}, \overline{10}] = \mathbb{Z}_{15}$$

$$\| \\ \mathbb{Z}_{15}$$

Tartalom

A csoport fogalma, példák, alaptulajdonságok

Részcsoportok

Ciklikus csoportok, elem rendje

Mellékosztályok, Lagrange tételének bizonyítása

Normálosztók, faktorcsoportok

Direkt szorzat

Definíció

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

Példák

- $\mathbb{Z} = [1]$
- $\mathbb{Z}_n = [\overline{1}]$

Tétel

Ciklikus csoport minden részcsoportja is ciklikus.

Megjegyzés

Minden csoportban „hemzsegnek” a ciklikus részcsoportok: bármely G csoportban bármely a elem egy ciklikus részcsoportot generál.

Trivialitás

Tetszőleges G csoport és $a \in G$ esetén

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

Példák

A $\mathbb{C} \setminus \{0\}$ csoportban:

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

Az első esetben a hatványok mind különbözőek, ezért $[2] \cong \mathbb{Z}$.

A második esetben négyes periodicitást tapasztalunk, ezért $[i] \cong \mathbb{Z}_4$.

Egy tetszőleges G csoportban egy a elemet hatványozva két eset lehetséges:

(1) A hatványok mind különbözőek.

Ekkor $\varphi\colon (\mathbb{Z},+) \to ([a];\cdot),\ k \mapsto a^k$ 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: $(k+\ell)\varphi = a^{k+\ell} = a^k \cdot a^\ell = k\varphi \cdot \ell\varphi$.

Egy tetszőleges G csoportban egy a elemet hatványozva két eset lehetséges:

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

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

Az $a^0, a^1, a^2, \ldots, a^{n-1}$ hatványok páronként különbözőek (miért?) 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 $\varphi\colon (\mathbb{Z}_n, +) \to ([a]; \cdot),\ \overline{k} \mapsto a^k$ 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 $(k = 0, \ldots, n-1)$ alakban.
- Művelettartás: $(\overline{k} + \overline{\ell})\varphi = \overline{k + \ell}\,\varphi = a^{k+\ell} = a^k \cdot a^\ell = \overline{k}\varphi \cdot \overline{\ell}\varphi$.

Tétel

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

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

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*):

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

Definíció

A G csoport rendjén elemeinek számát (számosságát) értjük.

Megjegyzés

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

Példák

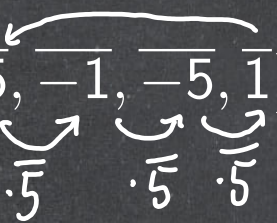
Határozzuk meg az $a \in G$ elem rendjét.

(1) $G = \mathbb{C} \setminus \{0\}$, $a = 2$: $\quad [2] = \{\ldots, \frac{1}{2}, 1, 2, 4, \ldots\} \cong \mathbb{Z}$, $\quad o(2) = \infty$

(2) $G = \mathbb{C} \setminus \{0\}$, $a = i$: $\quad [i] = \{i, -1, -i, 1\} \cong \mathbb{Z}_4$, $\quad o(i) = 4$

(3) $G = \mathbb{C}$, $a = i$: $\quad [i] = \{\ldots, -i, 0, i, 2i, \ldots\} \cong \mathbb{Z}$, $\quad o(i) = \infty$

(4) $G = \mathbb{Z}_{13}^*$, $a = \overline{5}$: $\quad [\overline{5}] = \{\overline{5}, \overline{-1}, \overline{-5}, \overline{1}\} \cong \mathbb{Z}_4$, $\quad o(\overline{5}) = 4$



Megjegyzés

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

$$o(z) = n \iff \big|[z]\big| = n \iff [z] = E_n \cong \mathbb{Z}_n.$$

Az ilyen tulajdonságú számokat nevezzük primitív n-edik egységgyököknek.

A primitív n-edik egységgyökök száma $\varphi(n)$.

Példa

Határozzuk meg $\mathbb{Z}_{20}$-ban az $a = \overline{5},\ b = \overline{6},\ c = \overline{7},\ d = \overline{8}$ elemek rendjét.

$[a] = \{\overline{5}, \overline{10}, \overline{15}, \overline{0}\} \cong \mathbb{Z}_4 \quad \Rightarrow o(a) = 4$

$[b] = \{\overline{6}, \overline{12}, \overline{18}, \overline{4}, \overline{10}, \overline{16}, \overline{2}, \overline{8}, \overline{14}, \overline{0}\} \cong \mathbb{Z}_{10} \Rightarrow o(b) = 10$

$[c] = \{\overline{7}, \overline{14}, \overline{1}, \ldots\} = \mathbb{Z}_{20} \Rightarrow o(c) = 20$

$[d] = \{\overline{8}, \overline{16}, \overline{4}, \overline{12}, \overline{0}\} \cong \mathbb{Z}_5 \Rightarrow o(d) = 5$

A rend tulajdonságai

Legyen G egy véges csoport és $a \in G$ egy n-edrendű elem. Tudjuk, hogy ekkor $G \geq [a] \cong \mathbb{Z}_n$. Ebből következik, hogy...

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

(2) $a^{-1} = a^{n-1}$;

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

(4) n osztója G elemszámának;

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

Következmény (Euler–Fermat-tétel)

Ha a és m relatív prímek, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás.

Alkalmazzuk az (5)-ös tulajdonságot a $G = \mathbb{Z}_m^*$ csoportra ■

Tétel

Minden prímrendű csoport ciklikus.

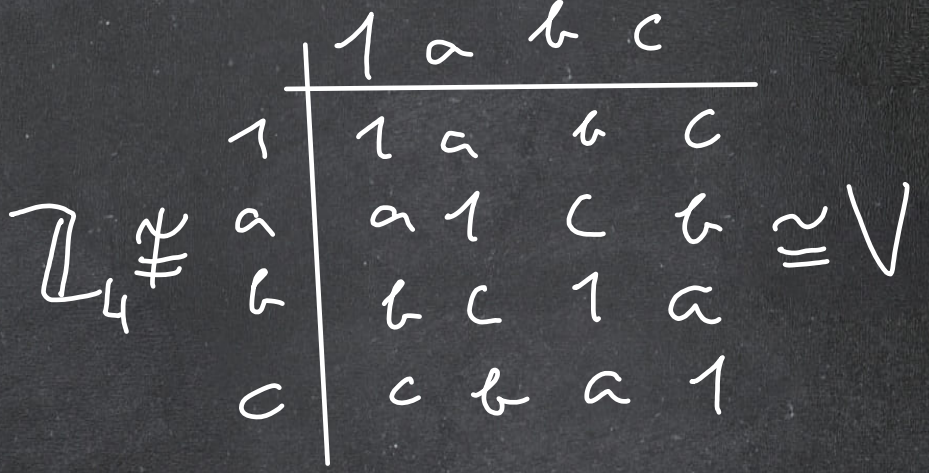
Bizonyítás.

Tfh. $|G| = p$ prímszám. Legyen $a \in G \setminus \{1\}$ tetszőleges elem.
Ekkor $o(a) = p$, és így $[a] = G$. ■

Tétel

A kis elemszámú csoportok (izomorfia erejéig) a következők:

1. egyelemű: $\{1\}$;
2. kételemű: $\mathbb{Z}_2$;
3. háromelemű: $\mathbb{Z}_3$;
4. négyelemű: $\mathbb{Z}_4$, V;
5. ötelemű: $\mathbb{Z}_5$.



Tartalom

A csoport fogalma, példák, alaptulajdonságok

Részcsoportok

Ciklikus csoportok, elem rendje

Mellékosztályok, Lagrange tételének bizonyítása

Normálosztók, faktorcsoportok

Direkt szorzat

Definíció

A G csoport nemüres részhalmazait komplexusoknak nevezzük.
Komplexusok szorzatát és inverzét elemenként értelmezzük:

$$AB = \{ab : a \in A, b \in B\}, \quad A^{-1} = \{a^{-1} : a \in A\} \qquad (\emptyset \neq A, B \subseteq G).$$

Egyelemű komplexusok esetén az alábbi egyszerűsített jelölést használjuk:

$$\{a\}B = aB, \quad B\{a\} = Ba \qquad (a \in G,\ \emptyset \neq B \subseteq G).$$

Tétel

Egy $H \subseteq G$ komplexus akkor és csak akkor részcsoport, ha

$$HH \subseteq H,\ 1 \in H,\ H^{-1} \subseteq H.$$

Megjegyzés

Ha $H \leq G$, akkor nemcsak $HH \subseteq H$, de $H \subseteq HH$ is teljesül, mert $H = \{1\}H \subseteq HH$, tehát $HH = H$. Hasonlóan $H^{-1} = H$ is teljesül.

Definíció

Tetszőleges $H \leq G$ és $a \in G$ esetén az a elem H részcsoport szerinti bal illetve jobb oldali mellékosztályának nevezzük az alábbi halmazokat:

$$aH = \{ah : h \in H\}, \qquad Ha = \{ha : h \in H\}.$$

Példa

Határozzuk meg a $G = \mathbb{Z}_6$ csoportban a $H = \{\overline{0}, \overline{3}\}$ részcsoporthoz tartozó mellékosztályokat.

$$\overline{0} + H = \{\overline{0}, \overline{3}\}, \quad \overline{1} + H = \{\overline{1}, \overline{4}\}, \quad \overline{2} + H = \{\overline{2}, \overline{5}\},$$
$$\overline{3} + H = \{\overline{3}, \overline{0}\}, \quad \overline{4} + H = \{\overline{4}, \overline{1}\}, \quad \overline{5} + H = \{\overline{5}, \overline{2}\}.$$

Példa

Határozzuk meg a $G = \mathbb{Z}$ csoportban a $H = \{3k : k \in \mathbb{Z}\}$ részcsoporthoz tartozó mellékosztályokat.

$$0 + H = \{3k : k \in \mathbb{Z}\},$$

$$1 + H = \{3k + 1 : k \in \mathbb{Z}\},$$

$$2 + H = \{3k + 2 : k \in \mathbb{Z}\}.$$

Tetszőleges a egész szám esetén, $a + H$ nem más, mint a modulo 3 maradékosztálya. Következésképp

$$a + H = b + H \iff a \equiv b \pmod 3 \iff 3 \mid a - b \iff a - b \in H.$$

$$\| \quad a + (-b)$$

Tétel

Legyen $H \leq G$, és definiáljunk a G halmazon egy $\sim$ relációt:

$$a \sim b \iff ab^{-1} \in H.$$

Ekkor $\sim$ ekvivalenciareláció, és egy $a \in G$ elem ekvivalenciaosztálya Ha.

Következmény

Tetszőleges $H \leq G$ esetén a H szerinti jobb oldali mellékosztályok a G halmaz egy osztályozását alkotják. Hasonló érvényes a bal oldali mellékosztályokra is.

Példa

Határozzuk meg a $G = \mathbb{Z}_{13}^*$ csoportban a $H = [\overline{5}] = \{\overline{1}, \overline{5}, \overline{8}, \overline{12}\}$ részcsoporthoz tartozó mellékosztályokat.

$$\begin{aligned}
\overline{1} \cdot H &= \{\overline{1}, \overline{5}, \overline{8}, \overline{12}\} = \overline{5} \cdot H = \overline{8} \cdot H = \overline{12} \cdot H, \\
\overline{2} \cdot H &= \{\overline{2}, \overline{10}, \overline{3}, \overline{11}\} = \overline{10} \cdot H = \overline{3} \cdot H = \overline{11} \cdot H, \\
\overline{4} \cdot H &= \{\overline{4}, \overline{7}, \overline{6}, \overline{9}\} = \overline{7} \cdot H = \overline{6} \cdot H = \overline{9} \cdot H.
\end{aligned}$$

Definíció

A G véges csoport H részcsoportja szerinti bal (vagy jobb) oldali mellékosztályok számát H indexének nevezzük. Jelölés: $[G : H]$.

Lagrange tétele

Tetszőleges G véges csoport és H részcsoport esetén

$$|G| = |H| \cdot [G : H].$$

Következésképp $|H|$ osztója $|G|$-nek.

Bizonyítás.

Bármely $g \in G$ esetén

$$\lambda_g : H \to gH, \ h \mapsto gh$$

bijektív leképezés (miért?), ezért $|gH| = |H|$, azaz a mellékosztályok mind egyforma méretűek (akkorák, mint H).

Tehát a mellékosztályok a G halmazt felbontják $[G : H]$ darab $|H|$-elemű részhalmazra, és így $|G| = |H| \cdot [G : H]$. ■

Tartalom

A csoport fogalma, példák, alaptulajdonságok

Részcsoportok

Ciklikus csoportok, elem rendje

Mellékosztályok, Lagrange tételének bizonyítása

Normálosztók, faktorcsoportok

Direkt szorzat

Definíció

Az $N \leq G$ részcsoportot normálosztónak nevezzük, ha az N szerinti bal és jobb oldali mellékosztályozás megegyezik:

$$\forall a \in G: \quad aN = Na.$$

Jelölés: $N \lhd G$.

Megjegyzés

Abel-csoportban minden részcsoport normálosztó.

Tétel

Ha $N \lhd G$, akkor az N szerinti mellékosztályozás kompatibilis osztályozása a G csoportnak.

Bizonyítás.

Igaz-e, hogy tetszőleges aN és bN mellékosztályokhoz van olyan cN mellékosztály, amelyre $aN \cdot bN \subseteq cN$?

Igen, $c = ab$ jó lesz:

$$aN \cdot bN = a \cdot Nb \cdot N = a \cdot bN \cdot N = ab \cdot NN = ab \cdot N. \qquad \blacksquare$$

Tétel

Ha $N \lhd G$, akkor az N-hez tartozó kongruencia szerinti faktoralgebra csoport, amelyet a G csoport N normálosztó szerinti faktorcsoportjának nevezünk. Jelölés: G/N.

- elemek: aN
- szorzás: $aN \cdot bN = (ab)N$
- egységelem: $1N = N$
- inverz: $(aN)^{-1} = a^{-1}N$

Példa

$G = \mathbb{Z}_{13}^*$ és $N = [\overline{5}] = \{\overline{1}, \overline{5}, \overline{8}, \overline{12}\}$ esetén $G/N = \{\overline{1}N, \overline{2}N, \overline{4}N\}$.

$\cdot$	$\overline{1}N$	$\overline{2}N$	$\overline{4}N$
$\overline{1}N$	$\overline{1}N$	$\overline{2}N$	$\overline{4}N$
$\overline{2}N$	$\overline{2}N$	$\overline{4}N$	$\overline{1}N$
$\overline{4}N$	$\overline{4}N$	$\overline{1}N$	$\overline{2}N$

$$\overline{1}N = \{\overline{1}, \overline{5}, \overline{8}, \overline{12}\}$$
$$\overline{2}N = \{\overline{2}, \overline{10}, \overline{3}, \overline{11}\}$$
$$\overline{4}N = \{\overline{4}, \overline{7}, \overline{6}, \overline{9}\}$$

Legyen $\sim$ kongruenciája a G csoportnak.

$$N = \{a \in G \mid a \sim 1\}$$

$N \leq G$ ⟸

- $1 \in N$
- $a, b \in N \Rightarrow \left.\begin{matrix} a \sim 1 \\ b \sim 1 \end{matrix}\right\} \Rightarrow a \cdot b \sim 1 \cdot 1 \Rightarrow ab \in N$
- $a \in N \Rightarrow \left.\begin{matrix} a \sim 1 \\ a^{-1} \sim a^{-1} \end{matrix}\right\} \Rightarrow 1 \sim a^{-1} \Rightarrow a^{-1} \in N$

$$Na = Nb \iff ab^{-1} \in N \iff ab^{-1} \sim 1 \overset{b \sim b}{\Rightarrow} a \sim b \overset{b^{-1} \sim b^{-1}}{\Leftarrow}$$

$$aN = bN \iff a^{-1}b \in N \iff a^{-1}b \sim 1 \overset{a \sim a}{\Rightarrow} b \sim a \overset{a^{-1} \sim a^{-1}}{\Leftarrow}$$

$N \trianglelefteq G$

$aN = Na$

$\| \quad \overline{a}$

Tétel

Legyen $\sim$ kongruenciája a G csoportnak, és legyen $N = \{a \in G : a \sim 1\}$. Ekkor $N \lhd G$, és a $\sim$ kongruenciához tartozó kompatibilis osztályozás éppen az N szerinti mellékosztályozás.

Következmény

Csoportok esetén kölcsönösen egyértelmű megfeleltetés van a kongruenciák és a normálosztók között.

Tartalom

A csoport fogalma, példák, alaptulajdonságok

Részcsoportok

Ciklikus csoportok, elem rendje

Mellékosztályok, Lagrange tételének bizonyítása

Normálosztók, faktorcsoportok

Direkt szorzat

Definíció

Az G és H csoportok direkt szorzata a $G \times H$ csoport, amelynek műveletét az alábbi módon értelmezzük:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2) \qquad (g_1, g_2 \in G, h_1, h_2 \in H).$$

Tétel

Csoportok direkt szorzata valóban csoport.

Tétel

Ha $\text{Inko}(m, n) = 1$, akkor $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Bizonyítás.

Tfh. $\text{Inko}(m, n) = 1$. Elég belátni, hogy $\mathbb{Z}_m \times \mathbb{Z}_n$ ciklikus, azaz van egy (a, b) generátoreleme. A legesélyesebb jelölt: $(a, b) = (1, 1)$.

Az $(1, 1)$ elem k-adik hatványa (k, k), és ez akkor és csak akkor egyezik meg az egységelemmel, ha $m \mid k$ és $n \mid k$, azaz $\text{Ikkt}(m, n) \mid k$.

Tehát $(1, 1)$ rendje $\text{Ikkt}(m, n) = mn$. ■

Tétel

A $\mathbb{Z}_m \times \mathbb{Z}_n$ csoport akkor és csak akkor ciklikus, ha m és n relatív prímek.

Ha ez a helyzet, akkor $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ az alábbi izomorfizmus mellett:

$$\varphi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad x \bmod mn \mapsto (x \bmod m, x \bmod n).$$

Ez nemcsak csoportizomorfizmus, hanem gyűrűizomorfizmus is.

Következmény

Ha m és n relatív prímek, akkor $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

$$\left.\begin{aligned} x \equiv a \pmod m \\ x \equiv b \pmod n \end{aligned}\right\} \quad x \equiv \dots \pmod{mn}$$

Példa

$\mathbb{Z}_{300} \cong \mathbb{Z}_3 \times \mathbb{Z}_{100} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$

A véges Abel-csoportok alaptétele

Minden véges Abel-csoport prímhatványrendű ciklikus csoportok direkt szorzatára bontható.

Példa

A Klein-csoport direkt felbontása: $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$\cong V$

$\pi_1 : \mathbb{A} \times \mathbb{B} \to \mathbb{A}$
$\pi_2 : \mathbb{A} \times \mathbb{B} \to \mathbb{B}$

Tétel

Ha az $M, N \lhd G$ normálosztókra $MN = G$ és $M \cap N = \{1\}$ teljesül, akkor $G \cong M \times N$.

Fordítva, G minden direkt felbontása egy ilyen normálosztó-párnak felel meg.