Csoportok I.

2013 április 12.

1. A csoport definíciói
2. Példák
3. Permutációk
4. Elem rendje, ciklikus csoportok

Ez a rész a tankönyvekben a [Sz] XII/1 és [F] II/1,3 fejezetekben található.

Definíció

Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

1. $*$ **invertálható** művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek legalább egy megoldása van.
2. $*$ **kancellatív** művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek legfeljebb egy megoldása van.

Megjegyzés

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

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

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

Definíció
Legyen $*$ egy kétváltozós művelet a nemüres A halmazon. Tetszőleges $a \in A$ esetén definiáljuk az a-val való balról szorzást és az a-val való jobbról szorzást:

$$\lambda_a \colon A \to A,\ x \mapsto a * x, \qquad \rho_a \colon A \to A,\ x \mapsto x * a.$$

Állítás
Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

1. $*$ *invertálható* $\iff \forall a \in A:\ \lambda_a$ *és* ρ_a *szürjektív.*
2. $*$ *kancellatív* $\iff \forall a \in A:\ \lambda_a$ *és* ρ_a *injektív.*

Biz.
HF □

Következmény
Véges alaphalmaz esetén az invertálhatóság és a kancellativitás egymással ekvivalens.

Biz.
Skatulya-elv. (HF) □

Definíció (I)
Az $\mathbb{A} = (A; *)$ félcsoportot **csoportnak** nevezzük, ha van egységeleme, és minden elemének van inverze.

Definíció (II)
Az $\mathbb{A} = (A; *)$ félcsoportot **csoportnak** nevezzük, ha $*$ invertálható művelet.

Definíció (III)
Az $\mathbb{A} = \left(A; *, e, {}^{-1}\right)$ algebrát **csoportnak** nevezzük, ha $*$ asszociatív kétváltozós művelet, az e (nullváltozós) és $^{-1}$ (egyváltozós) műveletekre pedig teljesülnek az alábbi azonosságok:

$$\forall a \in A:\ a * e = e * a = a;$$
$$\forall a \in A:\ a * a^{-1} = a^{-1} * a = e.$$

Tétel
A csoport három definíciója „lényegében" ekvivalens egymással.

Biz.
(I) $\iff$ (II): [Sz] XII. fejezet, 1.4. Tétel.

(I) $\implies$ (III): Legyen $(A; *)$ csoport az (I) definíció értelmében. Jelölje e az egységelemet, egy tetszőleges $a \in A$ elem inverzét pedig jelöljük a^{-1}-gyel. Ekkor az

$$e \colon A^0 \to A,\ \heartsuit \mapsto e,$$
$$^{-1} \colon A \to A,\ a \mapsto a^{-1}$$

műveletekkel $\left(A; *, e, {}^{-1}\right)$ csoport a (III) definíció értelmében.

(III) $\implies$ (I): Legyen $\left(A; *, e, {}^{-1}\right)$ csoport a (III) definíció értelmében. Ekkor $*$ asszociatív, $e \in A$ egységelem, és minden $a \in A$-ra a^{-1} inverze A-nak, így $(A; *)$ csoport az (I) definíció értelmében. □

Állítás
Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

1. *Ha $(A; *)$ csoport, akkor $*$ kancellatív.*
2. *Ha $*$ asszociatív és kancellatív, akkor $(A; *)$ csoport, feltéve, hogy A véges.*

Biz.
1. [Sz] XII. fejezet, 1.6. Tétel.
$$\begin{aligned} a * x_1 = a * x_2 &\implies a^{-1} * (a * x_1) = a^{-1} * (a * x_2) \\ &\implies (a^{-1} * a) * x_1 = (a^{-1} * a) * x_2 \\ &\implies x_1 = x_2 \end{aligned}$$
2. Ha A véges, akkor a kancellativitásból következik az invertálhatóság, tehát $(A; *)$ csoport a (II) definíció értelmében.

□

Példa
Az $(\mathbb{N}; +)$ félcsoport kancellatív, de nem invertálható (és így nem is csoport).

Jelölés

Ezentúl a csoportműveletet $\cdot$ jelöli, az egységelemet 1, a g elem inverzét pedig g^{-1}. A $(G;\cdot)$ csoportot gyakran csak G-vel jelöljük.

Definíció

Ha $(G;\cdot)$ csoport, $\emptyset \neq H \subseteq G$, és a $(H;\cdot)$ részgrupoid maga is csoport, akkor azt mondjuk, hogy $(H;\cdot)$ **részcsoportja** $(G;\cdot)$-nek.

Állítás

Tetszőleges $(G;\cdot)$ csoport és $\emptyset \neq H \subseteq G$ esetén H akkor és csak akkor részcsoportja $(G;\cdot)$-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:* $1_G \in H$;
3. *H zárt az inverzképzésre:* $\forall h \in H: \ h^{-1} \in H$.

Megjegyzés

Az állítás így is megfogalmazható: H akkor és csak akkor részcsoportja G-nek, ha részalgebrája a $\left(G;\cdot,1_G,^{-1}\right)$ algebrának.

Biz.

Az elegendőség nyilvánvaló. A szükségességhez tegyük fel, hogy $(H;\cdot)$ csoport, és jelölje 1_H az egységelemét. Ekkor tetszőleges $h \in H$ esetén

$$1_H \cdot h = 1_G \cdot h \text{ (miért?), és így } 1_H = 1_G \text{ (miért?).}$$

Tehát $1_G = 1_H \in H$.

Bármely $h \in H$ elemnek van inverze a H csoportban (mondjuk h'), és van inverze a G csoportban is (h^{-1}). Ekkor

$$\begin{aligned} h'(hh^{-1}) &= h' \cdot 1 &&= h'; \\ (h'h)h^{-1} &= 1 \cdot h^{-1} &&= h^{-1}. \end{aligned}$$

Tehát $h^{-1} = h' \in H$. □

Példa

$\mathbb{N}_0$ részalgebrája a $(\mathbb{Z};+)$ csoportnak, de nem részcsoportja (csak részmonoid).

Állítás

A $(G;\cdot)$ csoportban a $B \subseteq G$ részhalmaz által generált részcsoport:

$$[B] = \{b_1^{\varepsilon_1} \cdots b_n^{\varepsilon_n} : n \in \mathbb{N}_0, b_1, \ldots, b_n \in B, \varepsilon_1, \ldots, \varepsilon_n = \pm 1\}.$$

Biz.

[Sz] XII. fejezet, 1.6. Tétel. □

Megjegyzés

Az üres halmaz generátuma a legszűkebb részcsoport: $[\emptyset] = \{1_G\}$.

Állítás

Tetszőleges $\varphi\colon (G;\cdot) \to (H;\cdot)$ csoporthomomorfizmusra

1. $1_G\varphi = 1_H$;
2. $\forall g \in G: \ \left(g^{-1}\right)\varphi = (g\varphi)^{-1}$.

Biz.

[Sz] XII. fejezet, 1.7. Tétel.

Tetszőleges $g \in G$ esetén

1. $1_H \cdot g\varphi = g\varphi = (1_G \cdot g)\varphi = 1_G\varphi \cdot g\varphi \implies 1_H = 1_G\varphi$.
2. $1_H = 1_G\varphi = \left(g \cdot g^{-1}\right)\varphi = g\varphi \cdot g^{-1}\varphi$ és hasonlóan $1_H = g^{-1}\varphi \cdot g\varphi$, tehát $g^{-1}\varphi$ valóban inverze $g\varphi$-nek.

□

Megjegyzés

Az állítás azt fejezi ki, hogy egy $\varphi\colon G \to H$ leképezés akkor és csak akkor homomorfizmus a $(G;\cdot)$ és $(H;\cdot)$ algebrák között, ha homomorfizmus a $\left(G;\cdot,1_G,^{-1}\right)$ és $\left(H;\cdot,1_H,^{-1}\right)$ algebrák között.

Állítás

Ha $\sim$ kongruenciarelációja a G csoportnak, akkor

$$\forall a, b \in G : a \sim b \implies a^{-1} \sim b^{-1}.$$

Biz.

[Sz] XII. fejezet, 4.7. Tétel.

Tegyük fel, hogy $a \sim b$. Ekkor

$$\left.\begin{array}{lcl} a^{-1} & \sim & a^{-1} \\ a & \sim & b \\ b^{-1} & \sim & b^{-1} \end{array}\right\} \implies b^{-1} = a^{-1} \cdot a \cdot b^{-1} \sim a^{-1} \cdot b \cdot b^{-1} = a^{-1}. \quad \square$$

Megjegyzés

Az állítás azt fejezi ki, hogy egy $\sim \subseteq G \times G$ ekvivalenciareláció akkor és csak akkor kongruenciája a $(G; \cdot)$ algebrának, ha kongruenciája a $\left(G; \cdot, 1_G, ^{-1}\right)$ algebrának.

Ez a rész a tankönyvekben a [Sz] V/2 és [F] II/4,6 fejezetekben található.

Példa

Az alábbi H számhalmazok közül melyek alkotnak csoportot a szokásos összeadásra nézve?

- $H = \emptyset$: nem (nem is grupoid)
- $H = \{0\}$: igen (Abel-csoport)
- $H = \mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$: igen (Abel-csoport)
- $H = \mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem (csak félcsoport)
- $H = \{$páros számok$\}$: igen (Abel-csoport)
- $H = \{$páratlan számok$\}$: nem (nem is grupoid)
- $H = \{$irracionális számok$\}$: nem (nem is grupoid)
- $H = \{$véges tizedestörtek$\}$: igen (Abel-csoport)

Példa

Az alábbi H számhalmazok közül melyek alkotnak csoportot a szokásos szorzásra nézve?

- $H = \emptyset$: nem (nem is grupoid)
- $H = \{1\}$: igen (Abel-csoport)
- $H = \mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$: nem (csak monoid)
- $H = \mathbb{C} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$: igen (Abel-csoport)
- $H = \mathbb{Z} \setminus \{0\}$: nem (csak monoid)
- $H = \mathbb{R}^+$, $\mathbb{Q}^+$: igen (Abel-csoport)
- $H = \mathbb{N}$: nem (csak monoid)
- $H = \{$irracionális számok$\}$: nem (nem is grupoid)
- $H = \{$véges tizedestörtek$\} \setminus \{0\}$: nem (csak monoid)

Példa

Csoportot alkot-e az $\mathbb{R}^+ \setminus \{1\}$ halmaz az $x * y := x^{\ln y}$ művelettel?

(0) Grupoid-e egyáltalán, azaz $*$ valóban művelet-e az $\mathbb{R}^+ \setminus \{1\}$ halmazon?

$$x, y \neq 1 \implies x^{\ln y} \neq 1 \text{ (miért?)}$$

(1) Asszociatív-e a $*$ művelet? Tetszőleges $x, y, z \in \mathbb{R}^+ \setminus \{1\}$ esetén

$$\begin{aligned} (x*y)*z &= (x*y)^{\ln z} = \left(x^{\ln y}\right)^{\ln z} = x^{\ln y \cdot \ln z}, \\ x*(y*z) &= x^{\ln(y*z)} = x^{\ln\left(y^{\ln z}\right)} = x^{\ln z \cdot \ln y}. \quad \checkmark \end{aligned}$$

(2) Egységelem? Az e szám! Tetszőleges $x \in \mathbb{R}^+ \setminus \{1\}$ esetén

$$x * e = x^{\ln e} = x^1 = x \qquad \text{és} \qquad e * x = e^{\ln x} = x$$

(3) Vannak-e inverzek? Ha $x, y \in \mathbb{R}^+ \setminus \{1\}$ egymás inverzei, akkor

$$x * y = x^{\ln y} = e \implies x = e^{\frac{1}{\ln y}}. \qquad (y \neq 1)$$

Tehát y inverze csak $e^{\frac{1}{\ln y}}$ lehet. Próbáljuk ki, hogy valóban az-e.

Példa (folyt.)

Tehát x inverze csak $e^{\frac{1}{\ln x}}$ lehet. Próbáljuk ki, hogy valóban az-e.

$$e^{\frac{1}{\ln x}} * x = \left(e^{\frac{1}{\ln x}}\right)^{\ln x} = e^{\frac{1}{\ln x} \cdot \ln x} = e^1 = e$$

$$x * e^{\frac{1}{\ln x}} = x^{\ln\left(e^{\frac{1}{\ln x}}\right)} = x^{\frac{1}{\ln x}} = x^{\frac{\ln e}{\ln x}} = x^{\log_x e} = e$$

A titok nyitja:

$$x * y = x^{\ln y} = \left(e^{\ln x}\right)^{\ln y} = e^{\ln x \cdot \ln y}.$$

Innen látszik, hogy a $*$ művelet kommutatív, azaz $(\mathbb{R}^+ \setminus \{1\}; *)$ Abel-csoport.
A korábbiak is egyszerűbben kijöttek volna, ha már az elején észrevettük volna ezt. (HF végiggondolni)

Példa

Csoportot alkot-e az $\mathbb{R} \times \mathbb{R}$ halmaz az alábbi $*$ művelettel?

$$(a, b) * (c, d) := (ac - bd, ad + bc).$$

Hosszas számolás helyett vegyük észre, hogy ez éppen a komplex számok szorzása!
Tehát $(\mathbb{R} \times \mathbb{R}; *)$ nem csoport,
de $(\mathbb{R} \times \mathbb{R} \setminus \{(0,0)\}; *)$ már Abel-csoport.

Példa

Kvaterniócsoport: $Q = (\{\pm 1, \pm i, \pm j, \pm k\}; \cdot)$ HF

Példa

$(\mathcal{P}(U); \Delta)$ Abel-csoport, de $(\mathcal{P}(U); \cup)$ általában csak monoid (ha $U = \emptyset$, akkor Abel-csoport).

Példa

- $(\mathbb{Z}_{12}; +)$: Abel-csoport
- $(\mathbb{Z}_{12}; \cdot)$: csak monoid
- $(\mathbb{Z}_{12} \setminus \{\overline{0}\}; \cdot)$: csak monoid
- $(\mathbb{Z}_{13} \setminus \{\overline{0}\}; \cdot)$: Abel-csoport
- $(\mathbb{Z}_{12}^*; \cdot)$: Abel-csoport
- $(\mathbb{R}^{n \times n}; \cdot)$: csak monoid
- $\mathrm{GL}_n(\mathbb{R}) = \{M \in \mathbb{R}^{n \times n} : \det(M) \neq 0\}$:
  $n = 1$ esetén Abel-csoport, $n \geq 2$ esetén nemkommutatív csoport
- $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathbb{R}^{n \times n} : \det(M) = 1\}$:
  $n = 1$ esetén Abel-csoport, $n \geq 2$ esetén nemkommutatív csoport
- $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathbb{Z}^{n \times n} : \det(M) \neq 0\}$: (csak monoid)
- $\mathrm{SL}_n(\mathbb{Z}) = \{M \in \mathbb{Z}^{n \times n} : \det(M) = 1\}$:
  $n = 1$ esetén Abel-csoport, $n \geq 2$ esetén nemkommutatív csoport

Példa

A sík összes egybevágósági transzformációi (nemkommutatív) csoportot alkotnak a transzformációk szorzására (egymás utáni végrehajtás).

Egy tetszőleges síkidomot önmagába képező egybevágóságok részcsoportot alkotnak ebben a csoportban (a síkidom szimmetriacsoportja).

Rajzoljunk olyan alakzatot, amelynek szimmetriacsoportja

- egyelemű;
- kételemű;
- háromelemű;
- négyelemű;
- n-elemű;
- megszámlálhatóan végtelen;
- kontinuum számosságú.

Tétel

A sík egybevágóságainak csoportját generálják a tengelyes tükrözések.

Biz.

Az egybevágóságok a következők:

- tengelyes tükrözések;
- forgatások (két tükrözés szorzata, HF);
- eltolások (két tükrözés szorzata, HF);
- csúsztatva tükrözések (három tükrözés szorzata, HF).

□

Definíció

A szabályos n-szög szimmetriacsoportját **n-edfokú diédercsoportnak** nevezzük és D_n-nel jelöljük.

A D_n csoportnak $2n$ eleme van: n forgatás és n tükrözés.
Jelölje f_k sokszög középpontja körüli $\frac{2k\pi}{n}$ szögű forgatást ($0 \leq k \leq n-1$), és legyenek a tükrözések $t_0, t_1, \ldots, t_{n-1}$ (a tengelyeket pozitív körüljárás szerint számozzuk; két „szomszédos" tengely $\frac{\pi}{n}$ szöget zár be egymással). Ekkor $D_n = \{\mathrm{id} = f_0, f_1, \ldots, f_{n-1}, t_0, t_1, \ldots, t_{n-1}\}$.

Állítás

Minden $k \in \{0, 1, \ldots, n-1\}$ esetén

(1) $f_k = f_1^k$;
(2) $t_k = t_0 \cdot f_k = t_0 \cdot f_1^k$.

Biz.

HF □

Következmény

A D_n csoportot generálja $f := f_1$ és $t := t_0$:

$$D_n = [f, t] = \left\{\mathrm{id}, f, f^2, \ldots, f^{n-1}, t, tf, tf^2, \ldots, tf^{n-1}\right\}.$$

Állítás

Ha t és f helyet cserél, akkor f „invertálódik": $ft = tf^{-1}$.
Sőt, minden $k \in \mathbb{Z}$ esetén $f^k t = tf^{-k}$.

Biz.

HF □

Példa

Számoljunk D_{10}-ben! Emlékeztető: $D_{10} = \left\{\mathrm{id}, f, \ldots, f^9, t, tf, \ldots, tf^9\right\}$.

- $f^5 \cdot f^9 = f^{14} = f^4$
- $f^{2013} = f^3$
- $f^{-2013} = f^7$
- $tf^7 \cdot f^9 = tf^{16} = tf^6$
- $f^9 \cdot tf^7 = tf^{-9}f^7 = tf^{-2} = tf^8$
- $tf^9 \cdot tf^7 = ttf^{-9}f^7 = f^{-2} = f^8$
- $\left(tf^7\right)^{-1} = f^{-7}t^{-1} = f^3 t = tf^{-3} = tf^7$ (nem véletlen!)
- $\left(tf^7\right)^{2013} = tf^7$ (ez sem véletlen...)
- $x \cdot tf^4 = tf^5 \iff x = tf^5 \cdot \left(tf^4\right)^{-1} = tf^5 \cdot f^{-4}t = tft = ttf^{-1} = f^9$

Példa

Határozzuk meg a $(\mathbb{C};+)$ csoportban a megadott részhalmaz generátumát.

- $[6,8] = \{\text{páros számok}\}$
- $[6,10,15] = \mathbb{Z}$
- $\left[\frac{1}{2},\frac{1}{3}\right] = \left\{\frac{k}{6} : k \in \mathbb{Z}\right\}$
- $[1,i] = \mathbb{Z}[i]$
- $[\{z \in \mathbb{C} : |z| = 1\}] = \mathbb{C}$

Példa

Határozzuk meg a $(\mathbb{C}^*;\cdot)$ csoportban a megadott részhalmaz generátumát.

- $[\{\text{prímszámok}\}] = \mathbb{Q}^+$
- $\left[\frac{1}{2},\frac{1}{3}\right] = \left\{2^k 3^l : k,l \in \mathbb{Z}\right\}$
- $[1,i] = \{1,-1,i,-i\}$
- $[\{z \in \mathbb{C} : |z| = 1\}] = \{z \in \mathbb{C} : |z| = 1\}$

Példa

Határozzuk meg a B részhalmaz által generált részcsoportot a G csoportban.

- $B = \left\{\overline{4},\overline{10}\right\}$, $G = \mathbb{Z}_{12}$
  $[B] = \left\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\right\} \cong \mathbb{Z}_6$
- $B = \left\{\overline{4},\overline{10}\right\}$, $G = \mathbb{Z}_{13}$
  $[B] = \left\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12}\right\} = \mathbb{Z}_{13}$
- $B = \left\{\overline{5},\overline{7}\right\}$, $G = \mathbb{Z}_{12}^*$
  $[B] = \left\{\overline{1},\overline{5},\overline{7},\overline{11}\right\} = \left\{\overline{1},-\overline{1},\overline{5},-\overline{5}\right\} \cong$ Klein-féle csoport
- $B = \left\{\overline{5}\right\}$, $G = \mathbb{Z}_{13}^*$
  $[B] = \left\{\overline{1},\overline{5},\overline{8},\overline{12}\right\} = \left\{\overline{1},-\overline{1},\overline{5},-\overline{5}\right\} \cong \mathbb{Z}_4$
- $B = \left\{t, tf^6\right\}$, $G = D_{12}$
  $[B] = \left\{f^0, f^6, t, tf^6\right\} \cong$ Klein-féle csoport
- $B = \left\{f^2, tf\right\}$, $G = D_8$
  $[B] = \left\{f^0, f^2, f^4, f^6, tf, tf^3, tf^5, tf^7\right\} \cong D_4$

Ez a rész a tankönyvekben a [Sz] II/6 és [F] II/12 fejezetekben található.

Példa

Adott nemüres A halmaz összes permutációi (vagyis az $A \to A$ bijekciók) csoportot alkotnak a leképezésszorzásra nézve.

Definíció

Az $A = \{1,2,\ldots,n\}$ halmaz összes permutációi alkotta csoportot ***n*-edfokú szimmetrikus csoportnak** nevezzük, és S_n-nel jelöljük.

Egy $\pi \in S_n$ permutációt megadhatunk úgy, hogy $\{1,2,\ldots,n\}$ minden eleme alá odaírjuk a π melletti képét:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\pi & 2\pi & 3\pi & \cdots & n\pi \end{pmatrix}.$$

Vegyük észre, hogy π bijektivitása azt jelenti, hogy a mátrix alsó sorában az $1,2,\ldots,n$ számok egy permutációja van.

Példa

Számítsuk ki S_6-ban a $\pi\rho$, $\rho\pi$, π^{-1} és π^{2013} permutációkat, ahol

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}.$$

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$\rho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 4 & 6 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 3 & 5 & 1 & 2 & 6 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$$

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 4 & 2 \end{pmatrix} \implies \pi^4 = \mathrm{id} \implies \pi^{2013} = \left(\pi^4\right)^{503} \cdot \pi = \pi$$

Definíció

Legyenek $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ különböző elemek, és legyen $\pi \in S_n$ az alábbi permutáció:

$$a_1\pi = a_2,\ a_2\pi = a_3, \ldots, a_{k-1}\pi = a_k,\ a_k\pi = a_1 \text{ és}$$
$$b\pi = b \text{ ha } b \notin \{a_1, \ldots, a_k\}.$$

Ezt a π permutációt röviden így jelöljük: $\pi = (a_1\, a_2 \cdots a_{k-1}\, a_k)$ és **ciklikus permutációnak** vagy röviden **ciklusnak** nevezzük.

Definíció

Két ciklus **idegen**, ha mozgatott elemeik halmaza diszjunkt.

Tétel

Ha π és ρ idegen ciklusok, akkor fölcserélhetőek, azaz $\pi\rho = \rho\pi$.

Biz.

[Sz] II. fejezet, 6.9. Tétel. □

Tétel

Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelmű.

Biz.

[Sz] II. fejezet, 6.11. Tétel. □

Példa

Bontsuk idegen ciklusok szorzatára az alábbi π és ρ permutációkat, majd számítsuk ki 99-edik hatványukat:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}.$$

$$\pi = (13)(2564) \implies \pi^{99} = ((13)(2564))^{99} = (13)^{99}(2564)^{99} =$$
$$= (13)^{2\cdot 49+1} \cdot (2564)^{4\cdot 24+3} = (13)^1 (2564)^3 = (13)(2465) =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$$

$$\rho = (123)(56) \implies \rho^{99} = ((123)(56))^{99} = (123)^{99}(56)^{99} =$$
$$= (123)^{3\cdot 33} \cdot (56)^{2\cdot 49+1} = \mathrm{id} \cdot (56)^1 = (56) =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}$$

Példa

Adjuk meg idegen ciklusok szorzataként az alábbi permutációt:
$(134)(3247)(14527) = (173)(25)(4) = (173)(25)$

Példa

Oldjuk meg S_6-ban az $(123)(2345)\,\pi\,(456) = (134)$ egyenletet.

szorozzunk be balról $(123)^{-1}$-zel:	$(2345)\,\pi\,(456)$	$=$	$(321)(134)$
szorozzunk be balról $(2345)^{-1}$-zel:	$\pi\,(456)$	$=$	$(5432)(321)(134)$
szorozzunk be jobbról $(456)^{-1}$-zel:	π	$=$	$(5432)(321)(134)(654)$
számoljuk ki:	π	$=$	$(165)(24)$

Az első két lépés összevonható:
szorozzunk be balról $[(123)(2345)]^{-1} = (5432)(321)$-gyel.

Tetszőleges csoportban az $axb = c$ egyenlet egyetlen megoldása $x = a^{-1}cb^{-1}$.

Példa

Oldjuk meg S_4-ben a $\pi^2 = (134)$ egyenletet.

Egy S_4-beli permutáció ciklusszerkezete ötféle lehet:

$$\pi = \quad (), \quad (\bullet\,\bullet), \quad (\bullet\,\bullet\,\bullet), \quad (\bullet\,\bullet\,\bullet\,\bullet), \quad (\bullet\,\bullet)(\bullet\,\bullet)$$

$$\pi^2 = \quad (), \quad (), \quad (\bullet\,\bullet\,\bullet), \quad (\bullet\,\bullet)(\bullet\,\bullet), \quad ()$$

Tehát π csak egy hármas ciklus lehet.

Ekkor $\pi^3 = \mathrm{id}$ miatt $\pi^2 = \pi^{-1} = (134)$,
és így $\pi = (143)$ az egyetlen megoldás.

Definíció

A 2 hosszúságú ciklusokat, vagyis az $(i\,j)$ alakú permutációkat **transzpozícióknak** nevezzük.

Tétel

Az S_n csoportot generálják a transzpozíciók, azaz minden S_n-beli permutáció előáll transzpozíciók szorzataként.

Biz.

[Sz] X. fejezet, 6.15. Következmény.

Elég ciklusokra bizonyítani.

$$(a_1\,a_2\,\cdots\,a_{k-1}\,a_k) = (a_1\,a_2)\,(a_1\,a_3)\cdots(a_1\,a_k) \qquad \square$$

Példa

$\pi = (13)\,(2564) = (13)\,(25)\,(26)\,(24)$

vagy

$\pi \cdot (13)\,(25)\,(45)\,(56) = \mathrm{id} \implies \pi = (56)\,(45)\,(25)\,(13)$

Ez a rész a tankönyvekben a [Sz] XII/2 és [F] II/5 fejezetekben található.

Példa

Határozzuk meg a $[2]$ és $[i]$ részcsoportokat a $\mathbb{C}^*$ csoportban.

Általánosan: $[a] = \{a^k : k \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$

k	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8
2^k	$\frac{1}{32}$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{2}$	1	2	4	8	16	32	64	128	256
i^k	$-i$	1	i	-1	$-i$	1	i	-1	$-i$	1	i	-1	$-i$	1

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 $(G;\cdot)$ 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 $([a];\cdot) \cong (\mathbb{Z},+)$.

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

Egy tetszőleges $(G;\cdot)$ csoportban egy a elemet hatványozva két eset lehetséges:

(2) 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 $a^0, a^1, a^2, \ldots, a^{n-1}$ 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: $k \equiv \ell \pmod n \implies a^k = a^\ell$.
- Szürjektivitás: $[a]$ minden eleme előáll a^k $(k = 0,1,\ldots,n-1)$ alakban.
- Injektivitás: $k \not\equiv \ell \pmod n \implies a^k \neq a^\ell$.
- Művelettartás: $(\overline{k}+\overline{\ell})\varphi = \overline{k+\ell}\varphi = a^{k+\ell} \quad = \quad \overline{k}\varphi \cdot \overline{\ell}\varphi = a^k \cdot a^\ell$.

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:

$$o(a) = \min\{n \in \mathbb{N}\colon a^n = 1\}.$$

Definíció

A véges G **csoport rendjén** elemeinek számát értjük.

Definíció

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

Megjegyzés

Az a elem rendje nem más, mint az általa generált részcsoport rendje: $o(a) = |[a]|$ (ha véges).

Tétel

Egy csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \ldots$ csoportok valamelyikével.

Biz.

[Sz] XII. fejezet, 2.8. Tétel (+2.4. Állítás, 2.6. Tétel).

Láttuk, hogy ha $G = [a]$, akkor vagy $G \cong \mathbb{Z}$ (első eset), vagy $G \cong \mathbb{Z}_{o(a)}$ (második eset).

Az világos, hogy ezek a csoportok ciklikusak: $\mathbb{Z} = [1]$, $\mathbb{Z}_n = \left[\overline{1}\right]$. □

Tétel

Ciklikus csoport minden homomorf képe is ciklikus.

Biz.

[Sz] XII. fejezet, 2.13. Tétel.

Legyen $\varphi\colon G \to H$ szürjektív homomorfizmus, és tegyük fel, hogy $[a] = G$. Ekkor

$$H = G\varphi = \{a^k\varphi\colon k \in \mathbb{Z}\} = \left\{(a\varphi)^k : k \in \mathbb{Z}\right\} = [a\varphi].$$

□

Tétel

Ciklikus csoport minden részcsoportja is ciklikus.

Biz.

[Sz] XII. fejezet, 2.10. Tétel.

Legyen $\{1\} \neq H \leq G = [a]$. Legyen n a legkisebb pozitív kitevő, amelyre $a^n \in H$. (Miért létezik ilyen?) Ekkor $[a^n] = H$.

1. $[a^n] \subseteq H$: Világos, hiszen $a^n \in H \implies [a^n] \subseteq H$.
2. $H \subseteq [a^n]$: Legyen $h = a^k \in H$ tetszőleges elem.
   Osszuk el k-t maradékosan n-nel:

$$k = nq + r, \quad 0 \leq r < n - 1.$$

   Ekkor a^r kifejezhető H-beli elemekkel:

$$a^r = a^{nq+r} \cdot a^{-nq} = h \cdot (a^n)^{-q} \in H,$$

   így n minimalitása miatt $r = 0$. Tehát $h = a^{nq} \in [a^n]$.

□

Példa

Határozzuk meg az $a \in G$ elem rendjét, illetve az $[a] \leq G$ részcsoportot.

- $G = \mathbb{C}^*$, $a = 2$: $o(a) = \infty$, $[a] = \left\{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\right\}$
- $G = \mathbb{C}^*$, $a = i$: $o(a) = 4$, $[a] = \{1, -1, i, -i\}$
- $G = \mathbb{C}^*$, $a = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$: $o(a) = 3$, $[a] = \left\{1, -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\right\}$
- $G = \mathbb{C}$, $a = 2$: $o(a) = \infty$, $[a] = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$
- $G = \mathbb{C}$, $a = i$: $o(a) = \infty$, $[a] = \{\ldots, -2i, -i, 0, i, 2i, 3i, \ldots\}$
- $G = \mathbb{Z}_{12}^*$, $a = \overline{5}$: $o(a) = 2$, $[a] = \left\{\overline{1}, \overline{5}\right\}$
- $G = \mathbb{Z}_{13}^*$, $a = \overline{5}$: $o(a) = 4$, $[a] = \left\{\overline{1}, \overline{5}, \overline{8}, \overline{12}\right\}$
- $G = \mathbb{Z}_{12}$, $a = \overline{10}$: $o(a) = 6$, $[a] = \left\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\right\}$
- $G = \mathbb{Z}_{13}$, $a = \overline{10}$: $o(a) = 13$, $[a] = \left\{\overline{0}, \overline{1}, \ldots, \overline{12}\right\}$
- $G = \mathbb{Z}_{35}$, $a = \overline{10}$: $o(a) = 7$, $[a] = \left\{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}, \overline{30}\right\}$

Példa

Határozzuk meg az $a \in G$ elem rendjét, illetve az $[a] \leq G$ részcsoportot.

- $G = D_{12}$, $a = f^{10}$: $o(a) = 6$, $[a] = \left\{\mathrm{id}, f^2, f^4, f^6, f^8, f^{10}\right\}$
- $G = D_{12}$, $a = tf^{10}$: $o(a) = 2$, $[a] = \left\{\mathrm{id}, tf^{10}\right\}$
- $G = S_9$, $a = (368)$: $o(a) = 3$, $[a] = \{\mathrm{id}, (368), (386)\}$
- $G = S_9$, $a = (368)(45)$: $o(a) = 6$,
  $[a] = \{\mathrm{id}, (368), (386), (368)(45), (386)(45)\}$
- $G = S_9$, $a = (368)(46)$: $o(a) = 4$,
  $[a] = \{\mathrm{id}, (3468), (36)(48), (3864)\}$
- $G = S_9$, $a = (12)(345)(6789)$: $o(a) = 12$,
  $[a] = \left\{\mathrm{id}, a, a^2, \ldots, a^{11}\right\}$