

2025. 09. 08.
algebra 1.

ter: Csoportelmélet, gyűrű (és testelmélet)

Def $A_1 \times A_2 \times \dots \times A_n := \{[a_1, \dots, a_n] : a_i \in A, i \in \underline{n}\}$
Descartes-görget

sík $A^n = \underbrace{A \times \dots \times A}_{n \text{ db}}$

Def Ha A^n hoznak A -ra való egértelmi lehűzését (ezt fogjuk) az A -n értelmezett ~~művelet~~ n valós műveletnek nevezünk. Az A hoz eggyel elemenek húzolását az A -n értelmezett nullváltozós műveletnek nevezünk.

Def Egy \star hozt algebrai struktúrának nevezünk, ha ezen az \star hozon értelmezve van egy művelet

// modern algebra, ami algebrai struktúrákkal foglalkozik

Jel (\star, Ω)

alaphalmaz műveletek hozza

| $(\mathbb{Q}, +), (\mathbb{Q}; +, \cdot), (\mathbb{R}^3, \times)$

S

Def Ált mondjuk, hogy egy $*$ műv. asszoc. egy hozon, ha

$$\forall a, b, c \in S : (a * b) * c = a * (b * c)$$

Def Egy $(S, *)$ alg. str. ált félcsoportnak nevezünk, ha $*$ asszociatív lenne.

// művelets default: binér művelet

Ha $a * \underline{\text{homm.}}$ is, akkor homm. felcsoportról beszélünk.

// homm.: $a * b = b * a$

itt egy
fájlat
+ 2 pontot

Algebra 1.

1

$$(a * a) * a = a * (a * a) \quad \text{(hogyan jönök?)}$$

ez csak jelölés

$$= \begin{cases} a^3 \text{ multiplikatív mód} \\ 3a \text{ additív mód} \end{cases}$$

$$(a * b) * (c * d) = (a * b) * c * d$$

érvényes az általános aszociativitás

Díff Egy $(S, *)$ felcsor e-vel jelölt elemet balneutrális elemnek nevezzük, ha

$$\forall a \in S: e * a = a$$

a joblneutrális a balneutr.-nak a dualise

$$\forall a, b \in S: a * b = b$$

$$\left. \begin{array}{l} (a * b) * c = b * c = c \\ a * (b * c) = a * c = c \end{array} \right\} \rightarrow (a * b) * c = a * (b * c) \rightarrow (S, *)$$

felcsorpart, amelyben \forall elem balneutr.

Díff neutr. elem ami bal- és jobbnutr.

neutr. elem

$$\left((R, +) \right) \rightsquigarrow$$

általában $(S, +)$ nélkül nullelem (additív i.m.)

$$\left((R, \cdot) \right) \rightsquigarrow$$

(S, \cdot) nélkül egységelem (multipl. i.m.)

Péter Ha egy felcsorpartban \exists balneutr. e jobbnutr., akkor van neutrális f is, így $e = f$ és \forall felcsorpartban

\exists balneutr. e jobbnutr. ill. (hetoldali) neutr. van.

$$\text{Biz } \begin{aligned} \textcircled{1} & e * f = f & e \text{ balneutr.} & \left\{ \begin{array}{l} e = f \\ e * f = e \end{array} \right. & f \text{ jobbnutr.} \\ & e * f = e & f \text{ jobbnutr.} & \end{aligned}$$

\textcircled{2} ha $\exists n_1, n_2$ neutr.

$$n_1 = n_2 * n_1 = n_2$$

monoid

Df Egy e neutr.-iú ($S, *$) félcsop a' elemét az a $\in S$ elem balinver-zenek nevezzük, ha $a'*a = e$

|| balinverz dualisa jobbinverz.

Ha a' az a jobb- és balinverze, akkor (hetoldali) inverze,

Jel $\begin{cases} \text{add. -a} \\ \text{mult. } a^{-1} \end{cases}$

Tétel Ha egy ($S, *$) neutr.-os félcsoport a elemének \exists jobb- és balinverze akkor $a' = a''$ és a-nak pontosan egy inverze van.

Biz trivi Δ

(hetoldali)

Df Egy olyan neutrálisos félcsop-ot, melyben \forall elemnek \exists inverze csoporthnak nevezzük.

|| pontosan 1 inverze lehet csak

Ha egy csop. művelete komm. is, hh kommutatív csop.

Tétel Tetszőleges (S, \cdot) félcsop esetén: $\textcircled{1} \leftrightarrow \textcircled{2} \leftrightarrow \textcircled{3} \leftrightarrow \textcircled{4} \leftrightarrow \textcircled{5}$

|| inventibl multiplikatív és $a \cdot b = ab$

$\textcircled{1}$ S csop.

$\textcircled{2}$ S-ben \exists (balneutr.) $\stackrel{e}{\sim}$ balegység és $\forall a \in S, \exists a' \in S: a'a = e$

$\textcircled{3}$ $\textcircled{2}$ -os dualisa

$\textcircled{4}$ Az $ax = b$ egyenletnek \exists mo-sa S-ben $\forall a, b \in S$
esetén

$\textcircled{5}$ Az $ax = b$ egyenletnek van egyértelmű megoldása
 $\forall a, b \in S$ esetén

Biz

algebra 1.

3

Biz

① \rightarrow ② trivi

① \rightarrow ③ trivi

① \rightarrow ④ ha $a, b \in S \rightarrow x = a^{-1}b \rightarrow ax = a(a^{-1}b) = (aa^{-1})b = b$
 $y = ba^{-1} \quad ya = (ba^{-1})a = b$

① \rightarrow ⑤: ① \rightarrow ④ ha $ax = b$ és $a\hat{x} = b \rightarrow ax = a\hat{x} \rightarrow a(ax) = a(a\hat{x}) \Rightarrow$
 $\rightarrow x = \hat{x}$

② \rightarrow ①: ha a' egy a balinverze e -re nézve és a'' az a' balinverze
e-re nézve

$$[a \cdot a' = e \wedge a'a' = (a''a')aa' = a'' \cdot a' = e] \rightarrow a' \text{ invert}$$

$$[a'e = a(a'a) = (a a')a = ea = a] \rightarrow e \text{ egység}$$

③ \rightarrow ①: ② \rightarrow ① dualisa

④ \rightarrow ①: ha $a \in S$ tetszőleges, $\exists y_a \in S: ya = a \rightarrow \forall b \in S \exists x_b \in S:$

$$ax_b = b \rightarrow [y_a \cdot b = y_a(a \times_b) = (y_a a) \times_b = a \times_b = b]$$

$\rightarrow y_a$ baloldali egység

$\forall a \in S: \exists y \in S \quad ya = e \rightarrow y$ a balinverze
e-re nézve \rightarrow

\rightarrow ② \rightarrow ①

⑤ \rightarrow ①: ⑤ \rightarrow ④ \rightarrow ① \square

|| tisz ⑤ feltételek teljesül, de asszoc. nem: kvázioperatorsor

LOOP: egységelemes kvázioperatorsor

Defn Egy S felosztott f elemet idempotencre nevezzük, ha $f^2 = f$.

Tettek + csoporthan pont 1 idempotens elem van és ez az egység.

Biz $\rightarrow e^2 = ee = e$

$\rightarrow f^2 = f \in G, ef = f = f^2 \rightarrow ef^{-1} = f^2 f^{-1} \rightarrow e = f$

Jel \triangleleft a csoporthat jelöli

right angled bend

Feldák csoporthatára

(A) nélküli $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

$\forall q \in Q: 1q = q1 = q$

$(-1)q = q(-1) = -q$

$ij = k, jk = i, hi = j$

$ji = -k, kj = -i, ih = -j$

quaternionok?

$$i^2 = j^2 = k^2 = -1$$

Q csoporthat, mégpedig a quaternionicsoporthat

$(a + ib + jc + kd \rightsquigarrow \text{quaternionálgebra})$

(B) nélküli

D_n az E^3 hongruenciái, melyek egy n szögöt önmagára hézg

$$D_n = \{e, t, f, f^2, \dots, f^{n-1}, tf, \dots, tf^{n-1}\}$$

\downarrow
gimnáziális
 $\frac{n}{2}$ forgatás

$\text{mivel } f^n = e$

$$f^i t = t f^{n-i}$$

is

bizonyítható, hogy D_n csoporthat, ezt a csoporthat n -edfokú diédericsoporthat névezhetjük

$D_2 = \{e, t, f, tf\}$ ("elfajuló" valumi) Klein-csoport
(homom. csoport)

2025. 09. 15.

Def Egy n -elemű hz permutációit (önmagára való bijektív lehelyezését) n -edföli permutációknak nevezünk.

általában nem üreszt értünk hz alatt

multiplikatív szemléletben - vagyunk

Megállapodás, hogy az n -elemű hz n

Jel S_n

$((S_n, \circ))$ a kompozícióra művelets

Jel $\sigma \in S_n \rightarrow \sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$

Műveletek perm-ök között (perm-ök szorzata):

Ja $\sigma_1, \sigma_2 \in S_n$, akkor $\forall k \in \underline{n}: \sigma_1 \sigma_2 = \sigma_1(\sigma_2(k))$

$\sigma: h \rightarrow (h)\sigma$ ezt a jelölést használjuk (tehát jobbról szorzunk)

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\sigma_1 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Tétel (S_n, \circ) csoport

Biz e = id, inverz meghonosítható

Jel S_n : n -edföli szimmetrikus csoport

$$\tilde{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\begin{array}{ll} 1 < 2 & \tilde{\sigma}(1) < \tilde{\sigma}(2) \\ 1 < 3 & \tilde{\sigma}(1) > \tilde{\sigma}(3) \\ 1 < 4 & \tilde{\sigma}(1) < \tilde{\sigma}(4) \\ 2 < 3 & \tilde{\sigma}(2) > \tilde{\sigma}(3) \\ 2 < 4 & \tilde{\sigma}(2) > \tilde{\sigma}(4) \\ 3 < 4 & \tilde{\sigma}(3) < \tilde{\sigma}(4) \end{array}$$

Defn Az $\langle i, j \rangle$ $i < j$ pár a $\tilde{\sigma}$ egy inverziója, ha $\tilde{\sigma}(i) > \tilde{\sigma}(j)$

Defn Egy $\tilde{\sigma}$ nem. páros (nélkül), azaz azt, hogy inverziói száma páros (nélkül).

$$|S_n| = n!$$

Tétel $|S_{n_{\text{páros}}}| = |S_{n_{\text{nélkül}}}| = \frac{n!}{2}$

Biz \square

Jel $S_{n_{\text{páros}}} = A_n$

Tétel Azonos paritású perm-ek szorzata ps, egyébként a szorzat nélkül.

Defn A_n is csoport, n-edföldi alternáló csoport.

Defn Ha $h_1, \dots, h_r \in \mathbb{N}$ páronként különbözök, jelölje (h_1, h_2, \dots, h_r) azt az n-edföldi perm-öt, mely h_1 -hez h_2 -t, h_2 -hez h_3 -at, ..., h_{r-1} -hez h_r -t és h_r -hez h_1 -et rendeli, n többi elemét fixen hagyja, ezt alkuszak nevezik.

Delf Két ciklus diszjunkt, ha $\{k_1, \dots, k_r\} \cap \{l_1, \dots, l_s\} = \emptyset$

$$\begin{array}{|c} S_5\text{-ben } (1\ 2\ 3) \text{ és } (4\ 5) \text{ diszjunkt ciklusok} \\ \hline (1\ 2\ 3) = \begin{pmatrix} h_1 & h_2 & h_3 \\ 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \quad (4\ 5) = \begin{pmatrix} l_1 & l_2 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \end{array}$$

Tétel Diszjunkt ciklusok szorzata nem fügy a tényezők sorrendjétől.

Tétel minden permutáció felírható diszjunkt ciklusok szorzataként, ez a felírás a tényezők sorrendjétől eltekintve egyértelmű.

Biz $b = (1\ 2\ 3\ 4\ 5\ 6) = (3\ 4)(5\ 6)(3\ 4)$

általában \uparrow

Örökkel ha X hz és $X^{-1} = \{x^{-1} | x \in X\}$, ha $X \cap X^{-1} = \emptyset$ jelölje G_X az $X \cup X^{-1}$ hz elemeiből hézagható összes oly véges sorozat hz-át (az üres sorozatot is számítva), amely sorozatokban x és x^{-1} nincs egymás mellett $\notin X \cup X^{-1}$ -re.

$$X = \{x_1, x_2\} \rightarrow X^{-1} = \{x_1^{-1}, x_2^{-1}\}$$

$$x_1 x_2^{-1} x_1 x_2 \in G_{X^{-1}}, \text{ de } x_1 x_2^{-1} x_2 x_1 \notin G_X$$

Művelet G_X -en: Ha $w_1, w_2 \in G_X$, akkor $w_1 \cdot w_2$ az a G_X -beli sorozat, hogy w_1 és w_2 sorozatot appendáljuk, és ebből a sorozatból töröljük a tiltott betűpárokat, ameddig tudjuk

$\underset{\in X}{x}$ -ek betűk, $\underset{\in G}{w}$ -ek szavak, $x x^{-1}$ vagy $x^{-1} x$

$$X = \{x_1, x_2\} \text{ és } w_1 = x_1 x_1^{-1} x_1 x_2, w_2 = x_2 x_1^{-1} x_2^{-1} x_1 \rightarrow$$

$$\rightarrow w_1 \cdot w_2 = x_1 x_2^{-1} x_2 x_2^{-1} x_1^{-1} x_1 = x_1 x_2^{-1} x_2^{-1} x_1$$

Péter G_x az előző sorzárra nézve csoporthoz

Biz $(w_1 w_2) w_3 = w_1 (w_2 w_3)$ hozzácsőzött hossza gy. tely ind. *

Diff G_x az X feletti/ X által generált szabadcsoporthoz nézve

|| $e = \text{üres sorozat}$

|| inverz a "gonosz" tükrökép $(x_1 x_2^{-1} x_3)^{-1} = x_1^{-1} x_2 x_3^{-1}$

Biz *1. eset w_2 hossza = 1

$$(w_1 \cdot x) w_3 = w_1 (x \cdot w_3) \rightarrow 4 \text{ eset}$$

2. eset

$n > 2$ és az ind. felt. igaz + n -nél rövidebb

$w_2 - \text{re}$

ind. felt.

$$(w_1 (w_2)) \cdot w_3 = (w_1 \cdot (\underbrace{\tilde{w}_2 \cdot x})) w_3 \stackrel{1. \text{ eset}}{\downarrow} = ((w_1 \tilde{w}_2) \cdot x) \cdot w_3 \stackrel{1. \text{ eset}}{=} =$$

$$= (w_1 \tilde{w}_2) \cdot (x \cdot w_3) \stackrel{\substack{w_2 \\ \uparrow \\ \text{ind. felt.}}}{=} w_1 (\tilde{w}_2 (x w_3)) \stackrel{1. \text{ eset}}{=} w_1 ((\tilde{w}_2 x) w_3) =$$

$$= w_1 (w_2 w_3)$$

Péter Csoport tetragonális g eleme esetén $(g^{-1})^{-1} = g$

$$\text{Biz } g \cdot (g^{-1})^{-1} = g^{-1} g = e \rightarrow (g^{-1})^{-1} = g \quad \square$$

Diff Hatványozás csoportban: $g^0 := e$

$$g^n := \underbrace{g \cdot g \cdot \dots \cdot g}_{n-\text{szor}} \quad (n \in \mathbb{N})$$

$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{n-\text{szor}} \quad (n \in \mathbb{N})$$

Aly 1. /g

Abb

$$g^{n+m} = g^n g^m$$

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

Abb

$$g \in G(\text{csoport}) \rightarrow \exists m \in \mathbb{Z}: g^m = e \rightarrow (\exists n \in \mathbb{N}_0): g^n = e$$

$$(g \in G(\text{csoport}) \rightarrow \exists m \in \mathbb{Z} \setminus \{0\}: g^m = e \rightarrow (\exists n \in \mathbb{N}^+): g^n = e)$$

$$\left| \begin{array}{l} g^{-5} = e \rightarrow \underbrace{(g^{-5})^{-1}}_{= g^5} = e^{-1} \\ = e \end{array} \right.$$

Def

tíz mondjuk, hogy egy G csoport g elemenek rendje $n \in \mathbb{N}^+$, ha $n = \min \{ g^n = e \}$, ha nincs ilyen n , akkor azt mondjuk, hogy g rendje végtelen. Jel ~~$\Theta(g)$~~ $\Theta(g)$

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix} \in \underbrace{LG_2(\mathbb{Q})}_{\emptyset \notin LG_2(\mathbb{Q})}$$

L lineáris
G csoport
 2×2 -es mtx

$$A^2 = I \rightarrow \Theta(A) = 2$$

$$B^2 = \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$AB = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{bmatrix}, (AB)^2 = \begin{bmatrix} \left(\frac{1}{2}\right)^2 & 0 \\ 0 & 2^2 \end{bmatrix} \neq I \rightarrow \Theta(AB) = \infty$$

egysegelem rendje 1 ($\Theta(e) = 1$)

szorzat rendjéről nem tudunk semmit, előző pl. ban $\Theta(AB) \neq \Theta(A)\Theta(B)$

Rézsorport

Defn Egy G csoport $H \neq \emptyset$ nézhöz től G egy rézsorportjának nevezünk, ha H is csoport a G -n értelmezett műveletre nézve

Tétel Egy G csoport nézhöz a rézsorport $\rightarrow H^2CH \cap H^{-1}CH$
 (ahol $HH = H^2 = \{h_1 h_2 \mid h_1, h_2 \in H\}$
 és $H^{-1} = \{h^{-1} \mid h \in H\}$)

Biz H rézsorport $\rightarrow H^2CH$ (művelet tulajdonsága)

$$\hookrightarrow \exists f \in H \text{ egység } \rightarrow f^2 = f \rightarrow f \text{ idempotens}$$

$\rightarrow f = e$ mivel 1 db idempotens sem van, ez az e

$$h \in H \rightarrow \exists h_H^{-1} \in H : hh_H^{-1} = h_H^{-1}h = e$$

$$\rightarrow h \in G : \exists h_G^{-1} \in G : hh_G^{-1} = h_G^{-1}h = e \rightarrow$$

$$\rightarrow hh_H^{-1} = hh_G^{-1} \rightarrow h_H^{-1} = h_G^{-1} \rightarrow H^{-1}CH$$

$$H \neq \emptyset, H^2CH, H^{-1}CH$$

$$\forall h \in H : h^{-1} \in H \text{ (mert } H^{-1}CH)$$

$$\text{így } \underbrace{hh^{-1}}_e \in H^2CH \rightarrow e \in H \rightarrow$$

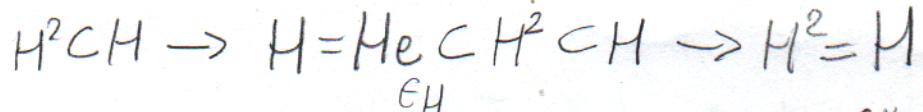
$\rightarrow H$ olyan részfélel, amelyben e egységként

$H^{-1}CH$ miatt H minden elemének van inverze $\rightarrow H$ rézsorport

H rézsorport, akkor $H^2 = H, H^{-1} = H$

$$H^{-1}CH \rightarrow (H^{-1})^{-1} = \{(h^{-1})^{-1} = h \mid h \in H\} = H \quad H = H^{-1}$$

$$(H^{-1})^{-1}CH^{-1} \rightarrow HCH^{-1}$$



~~tető~~ nem sah tartalmazza, hanem egyenlősége is

Tétel $H \neq \emptyset$ részegp. egy G csop. nál $\Leftrightarrow H^{-1}H \subset H$

Biz $H \neq \emptyset$ részegp. $\rightarrow H^{-1}=H$

$$H^{-1}H = H^2 \subset H \rightarrow H^{-1}H \subset H$$

$$H \neq \emptyset \quad H^{-1}H \subset H \rightarrow e \in H \rightarrow H^{-1} = H^{-1}e \subset H^{-1}H \subset H$$

$$\rightarrow H^{-1} \subset H \rightarrow H^{-1} = H$$

$$H^2 = HH = HH^{-1}H \rightarrow H^2 \subset H \rightarrow H \text{ részegp.}$$

Def H egy G csopart részegp. ja. Itt a $\in G$ H szerinti bal (oldali) mellekcsatlakozáson az $aH = \{ah \mid h \in H\}$ részegp. értjük.

Def jobbmellekcsatlakozási a balnak dualisa

Tétel G csop. tetszőleges H részegp. és $a, b \in G$ ($aH \cap bH = \emptyset$)
 $\oplus (aH = bH)$

Biz $aH \cap bH \neq \emptyset \rightarrow \exists x \in G : x \in aH \text{ és } x \in bH \rightarrow$

$$\exists h_1, h_2 \in H : ah_1 = x = bh_2 \leftrightarrow ah_1 = bh_2 \rightarrow$$

$$\rightarrow ah_2h_1^{-1} = bh_2h_1^{-1} \Rightarrow a = b \underbrace{h_2h_1^{-1}}_h = bh \rightarrow aH = bH$$

$$= bH$$

Tétel Egy G csopart tetszőleges H részegp.ja és $a, b \in G$ esetén

$$aH = bH \Leftrightarrow a^{-1}b \in H$$

nem szüksít, hogy $a^{-1}b$ vagy ab^{-1}

2025. 09. 22.

$$a^{-1}b \in H \rightarrow (a^{-1}b)^{-1} \in H$$

$$(ab)^{-1} = b^{-1}a^{-1}$$

$$b^{-1}(a^{-1})^{-1}$$

Biz ha $aH = bH \rightarrow b \in aH$ (mert $b \in bH$) \rightarrow

$$\rightarrow \exists h \in H: b = ah \rightarrow a^{-1}b = \underbrace{a^{-1}ah}_e = h \in H$$

itt lehets
majd

$$\begin{aligned} \hookrightarrow a^{-1}b \in H &\rightarrow \exists h \in H: a^{-1}b = h \rightarrow aa^{-1}b = ah \rightarrow \\ &\rightarrow b = ah \rightarrow bH = (ah)H = a(hH) = aH \quad \square \end{aligned}$$

$$\parallel (ab)^{-1} = b^{-1}a^{-1}$$

$$\parallel (ab)b^{-1}a^{-1} = aee^{-1} = aa^{-1} = e \text{ és } b^{-1}a^{-1}(ab) = e$$

$\parallel Ha = Hb$ változatra is igaz az előző hét áll

Tétel G csoport, H részcsoporthoz, a H szerinti bal- és jobbmellékzónák tállyai halmazai ekvivalensek (megadható bijekció)

$$\text{Biz } \Phi: aH \mapsto Ha^{-1}$$

$$\left\{ \begin{array}{l} \Phi \text{ összehető, hisz } \forall b \in G \quad \Phi: b^{-1}H \mapsto Hb \\ \Phi \text{ injektív, hisz ha } \Phi(aH) = \Phi(bH) \rightarrow Ha^{-1} = Hb^{-1} \rightarrow \end{array} \right.$$

$$\left\{ \begin{array}{l} \Phi \text{ injektív, hisz ha } \Phi(aH) = \Phi(bH) \rightarrow Ha^{-1} = Hb^{-1} \rightarrow \\ \rightarrow a^{-1}b \in H \Leftrightarrow aH = bH \end{array} \right.$$

Néha

számos
felmer

Deff Egy G csoport H részcsoporthoz (bal) jobbmellékzónák száma a H részcsoporthoz G-beli indexének nevezik
és $|G:H|$ módon jelöljük.

vagy 1.

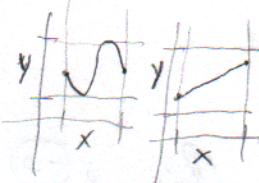
13

Tétel (Lagrange tétel)

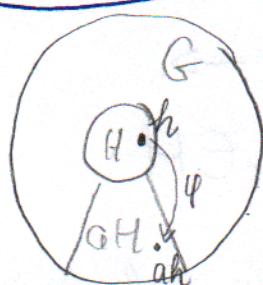
véges G csoport, H részcsoporthoz $|G| = |H| \cdot |G:H|$;

így a H részcsoporthoz rendje aztűja a G csoport rendjének.

$$f: x \rightarrow y$$



Biz



$$\varphi: H \rightarrow aH \quad \varphi: h \mapsto ah$$

φ szürjektív (minden elemet rendeli?)

φ injektív $\varphi(h_1) = \varphi(h_2) \rightarrow ah_1 = ah_2 \rightarrow h_1 = h_2$

$$\text{Így } |H| = |aH| \quad \forall a \in G \text{-re} \rightarrow |G| = |H| \cdot |G:H| \quad \square$$

ilyen formalis aztás

Tétel G csoport, részcsoporthoz rendszereinek metozata is részcsoporthoz rendszereinek metozata is részcsoporthoz.

mi a rendszer?

Biz $H_i, i \in I$ részcsoporthoz G -nek, ha

$$\textcircled{1} \quad \forall i \in I : e \in H_i \rightarrow e \in \bigcap_{i \in I} H_i \rightarrow \bigcap_{i \in I} H_i \neq \emptyset$$

$$\textcircled{2} \quad \forall a, b \in \bigcap_{i \in I} H_i \rightarrow \forall i \in I : a, b \in H_i \rightarrow \forall i \in I : ab \in H_i \\ \rightarrow ab \in \bigcap_{i \in I} H_i$$

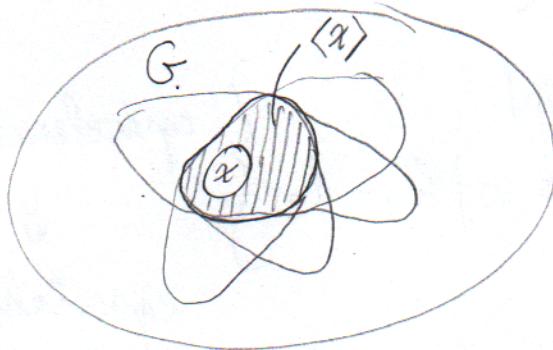
$$\textcircled{3} \quad \forall a \in \bigcap_{i \in I} H_i \rightarrow \forall i \in I : a \in H_i \rightarrow \forall i \in I : a^{-1} \in H_i \rightarrow \\ \rightarrow a^{-1} \in \bigcap_{i \in I} H_i$$

egy hosszú
szöveg

egy alakító
nem létez

Generált részcsoporthoz

Def Egy G csoport $X \neq \emptyset$ részhöz-a által generált, $\langle X \rangle$ módon jelölt részcsoporthoz az X -et tartalmazó összes G -beli részcsoport meghatározását értjük.



Tétel G csoport, $X \subseteq P(G - \emptyset)$

$$\langle X \rangle = \{x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n} \mid n \in \mathbb{N}^+, h_j \in \mathbb{Z}, x_j \in X \ (j \in \mathbb{N})\}$$

ennek X -nak hine
lenni nem?

Biz nom bizonyítjuk

Def Az 1 elem által generált csoportot a ciklikus csoportnak nevezünk.

|| ciklikus részcsoporthoz

Def Egy $(G_1, *)$ csoport egy (G_2, \circ) csoportba való lehűzését homomorfizmusként nevezünk, ha

$$\forall a, b \in G_1 \rightarrow \varphi(a * b) = \varphi(a) \circ \varphi(b)$$

|| műveleti lehűzés

$$|| (G_1, \cdot), (G_2, +): \varphi(ab) = \varphi(a) + \varphi(b)$$

$$|| (G_1, +), (G_2, \cdot): \varphi(a+b) = \varphi(a)\varphi(b)$$

bijektív homomorfizmus = izomorfizmus

Jelölés: G csoport áhlihus $\leftrightarrow G$ izomorf vagy $a(\mathbb{Z}, +)$, vagy $a(\mathbb{Z}_n, +)$ csoportok

\mathbb{Z}_n mod n moduluszály



$$n \geq 2, n \in \mathbb{N}$$

$$h_1 \equiv h_2 \Leftrightarrow n | h_1 - h_2$$

} egyenlőségi reláció
↓

egosztályok

$$\mathbb{Z}_n = \left\{ \begin{bmatrix} 0 \end{bmatrix}_{\equiv}, \begin{bmatrix} 1 \end{bmatrix}_{\equiv}, \dots, \begin{bmatrix} n-1 \end{bmatrix}_{\equiv} \right\}$$

$$[h_1] + [h_2] = [h_1 + h_2]$$

$(\mathbb{Z}_n, +)$ csoport

Biz: $(\mathbb{Z}, +)$ áhlihus ($\mathbb{Z} = \langle 1 \rangle$)

$(\mathbb{Z}_n, +)$ áhlihus ($\mathbb{Z} = \langle [1]_{\equiv} \rangle$)

Ha $G = \langle a \rangle$ egy áhlihus csoport

1. eset) $\text{O}(a)$ végtelen $\forall n_1, n_2 \in \mathbb{Z}^{(n_1 \neq n_2)} a^{n_1} \neq a^{n_2}$
 (mivel $a^{n_1} = a^{n_2} \rightarrow n_1 > n_2, a^{n_1} a^{-n_2} = e \rightarrow a^{\overbrace{n_1 - n_2}^{> 0}} = e \rightarrow \text{O}(a) \neq \infty$)

$$G = \{a^0, a^1, a^{-1}, a^2, a^{-2}, \dots\} \cong \{0, 1, 1, -2, 2, \dots\}$$

hiszen $\exists \varphi: a^k \mapsto k$ izomorfizmus

$$\varphi(a^{k_1} a^{k_2}) = \varphi(a^{k_1 + k_2}) = k_1 + k_2 = \varphi(a^{k_1}) + \varphi(a^{k_2})$$

$$[2. \text{ eset}] \quad \Theta(a) = n \quad (n \in \mathbb{N}_0)$$

$$G = \langle a \rangle = \{a^0, \dots, a^{n-1}\}$$

$a^{h_1} = a^{h_2} \rightarrow a^{h_1-h_2} = e$, mivel $h_1 - h_2$ nem lehet
 n -nél kisebb természetes (ami $\neq 0$), így csak 0 lehet
 (vagy $h_1 = h_2 = n$, vagy $h_1 = n$ és $h_2 = 0$)

$$\begin{aligned} m \in \mathbb{N}^+ \quad a^m &= a^{nt+r} = a^{nt} \cdot a^r = (a^n)^t \cdot a^r = \\ &= e^t a^r = a^r \quad (r \in \underline{0, n-1}) \rightarrow \{a^0, a^1, \dots, a^{n-1}\} \text{ felelősségtelen} \\ &\text{e} = a^0 \text{ egységelem} \end{aligned}$$

$$\parallel a^{h_1} = a^{h_2} \Leftrightarrow a^{h_1-h_2} = e \Leftrightarrow n|h_1-h_2 \Leftrightarrow h_1 \equiv h_2$$

$$a^i \cdot a^{n-i} = a^n = e \quad (a^i)^{-1} = a^{n-i} \rightarrow \{a^0, \dots, a^n\} \text{ csoport}$$

$$\rightarrow G = \{a^0, \dots, a^{n-1}\} \rightarrow G \cong (\mathbb{Z}_n, +)$$

$$\varphi: [k]_{\equiv} \mapsto a^k \text{ izomorfizmus}$$

$$k \in \underline{0, n-1}$$

Áll $\varphi: (G_1, *) \hookrightarrow (G_2, \circ)$ izomorfizmus, ahol $\varphi(e_1) = e_2$

(e_1 a G_1 -nek, e_2 a G_2 -nek neutralis)

$$\forall a \in G_1: \varphi(a^{-1}) = \varphi(a)^{-1}$$

Biz $\varphi(e_1) = \varphi(e_1 * e_1) = \varphi(e_1) \circ \varphi(e_1) \rightarrow \varphi(e_1)$ idempotens, ezért

$$\varphi(e_1) = e_2, \text{kk } \varphi(e_1) = \varphi(a * a^{-1}) = \varphi(a) \circ \varphi(a^{-1}) =$$

$$= e_2 \rightarrow \varphi(a) = \varphi(a)^{-1} \quad \parallel a \varphi(a) - \rightarrow \text{balról jobbra szorozni}$$

Tető ciklikus csoport minden részcsoportja ciklikus (véges/világ)

Biz $G = \langle a \rangle$ ciklikus csoport, H részcsoportja $\rightarrow e \in H$

① $H = \{e\}$, akkor $H = \langle e \rangle$, azaz H ciklikus

② $H \neq \{e\} \rightarrow \exists k \in \mathbb{N}^+ : a^k \in H \rightarrow$ leghisébb ilyen, ez n
($n = \min\{k \in \mathbb{N}^+ : a^k \in H\}$)

Jel $n \in \mathbb{N} \setminus \{0\} \triangleq$
 $\triangleq n_0$

$H = \langle a^n \rangle$, mert:

$$\text{maz: } a^m \in H \rightarrow m = n \cdot t + r \xrightarrow{\epsilon_{0,n-1}}$$

$$a^m = (a^n)^t \cdot a^r \rightarrow \underbrace{(a^n)^t}_{\in H} \in H \quad r < n \rightarrow r=0 \rightarrow m = n \cdot t \rightarrow$$

$\rightarrow a^m = (a^n)^t$ azaz H minden eleme (a^n) valamely hatványa,

így ciklikus \square

\parallel minden ciklikus csoport megszűnlhető

Áll $|\langle a \rangle| = \vartheta(a)$

Áll Véges csoport teljesleges elemek rendje osztja a csoport rendjére

Biz $|G| < \infty$, $a \in G$

$|\langle a \rangle| \mid |G|$ a Lagrange következménye miatt \rightarrow

$\rightarrow \vartheta(a) \mid |G| \quad \square$

Tetel Egy n -edrendű ciklikus csoporthoz az n -edrendű elemek száma $\varphi(n)$ (ahol $\varphi(n)$ az n -nél nem nagyobb n -hez relativ prim egészek számát jelenti)

Besz $|G|=n$ cihb. csop.

G izomorf az n -edik komplex egységegyűjtvékhöz csoporthoz

$$z = r(\cos \varphi + i \sin \varphi)$$

$$\sqrt[n]{z} = \sqrt[n]{r} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right)$$

$$\sqrt[n]{1} = \cos \left(\frac{2\pi k}{n} \right) + i \sin \left(\frac{2\pi k}{n} \right) = \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right)^k$$

Komplex n -edik egységegyűjtvékhöz: $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1} = \langle \varepsilon \rangle$

primitív n -edik egységegyűjtvékhöz

$$\varepsilon^k \text{ primitív} \Leftrightarrow \sigma(\varepsilon^k) = n \Leftrightarrow \gcd(k, n) = 1 \rightarrow$$

$\rightarrow \varphi(n)$ db primitív n -edik egységegyűjtvékhöz száma

A kompl. n -edik egységegyűjtvékhöz ciklikus csoporthoz az n -edrendű elemek pontosan a primitív n -edik egységegyűjtvékhöz, amelyek számáról tudjuk, hogy $\varphi(n)$ -nel egyenlő. □

Tetel G egy n -edrendű ciklikus csoporthoz és $d|n$, G azon elemei, melyek $x^d = e$ egyenlet megoldásai egy d -edrendű ciklikus csoporthoz alkotnak. A G d -edrendű elemeinek száma $\varphi(d)$ és a d -edrendű elemek egymás hatványai.