2025. 09. 08.

Algebra 1.

tov: Csoportelmélet, gyűrű (és testelmélet)

Def $\underbrace{A_1\times A_2\times\ldots\times A_n}_{\text{Descartes-szorzat}} := \{[a_1,\ldots,a_n] : a_i\in A,\ i\in \underline{n}\}$

spec $A^n = \underbrace{A\times\ldots\times A}_{n\text{ db}}$

Def Az A^n hz-nak A-ra való egyértelmű leképezését (~~hz~~ fv-ét) az A-n értelmezett ~~művelet~~ n vált. műveletnek nevezzük. Az A hz egy elemének kijelölését az A-n értelmezett nullváltozós műveletnek nevezzük.

Def Egy A hzt algebrai struktúrának nevezünk, ha ezen az A hzon értelmezve van egy művelet

|| modern algebra, ami algebrai struktúrákkal foglalkozik

Jel (A, Ω)

alaphalmaz, műveletek hza

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

Def Azt mondjuk, hogy egy $*$ műv. asszoc. egy S hzon, ha

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

Def Egy $(S,*)$ alg. str.-át félcsop-nak nevezünk, ha $*$ asszociatív S-en.

|| művelet default: binér művelet

Ha a $*$ komm. is, akk. komm. félcsoportról beszélünk.

|| komm.: $a*b = b*a$

itt egy kalap +2 pontért

|| $(a*a)*a = a*(a*a) =$ hogy jelöljük?

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

ez csak jelölés

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

érvényes az általános asszociativitás

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

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

|| a jobbneutrális a balneutr.-nak a duálisa

| $\forall a, b \in S \quad a*b = b$

| $\left.\begin{array}{l}(a*b)*c = b*c = c \\ a*(b*c) = a*c = c\end{array}\right\} \to (a*b)*c = a*(b*c) \to (S,*)$ félcsoport, amelyben $\forall$ elem balneutr.

Def neutr. elem ami bal- és jobbneutr.

|| $(\mathbb{R},+) \rightsquigarrow$
|| $(\mathbb{R},\cdot) \rightsquigarrow$

általaban $(S,+) \rightsquigarrow$ nullelem (additív i.m.)
$(S,\cdot) \rightsquigarrow$ egységelem (multipl. i.m.)

(neutr. elem)

Tétel Ha egy félcsoportban $\exists$ $\underbrace{\text{balneutr.}}_{e}$ és $\underbrace{\text{jobbneutr.}}_{f}$, akkor van neutrális is és $e=f$ és $\forall$ félcsoportban $\exists!$ baneutr. és jobbneutr., ill (kétoldali) neutr. van.

Biz ① $\left.\begin{array}{ll} e*f = f & e \text{ balneutr.} \\ e*f = e & f \text{ jobbneutr.}\end{array}\right\} e = f$

② ha $\exists\, n_1, n_2$ neutr.

$$n_1 = n_2 * n_1 = n_2$$

|| monoid

2.

Diff Egy e neutr-ú $(S,*)$ félcsop a' elemét az $a \in S$ elem balinverzének nevezzük, ha $a' * a = e$

|| balinverz duálisa jobbinverz.

Ha a' az a jobb- és balinverze, akkor (kétoldali) 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 (a', a'') akkor $a' = a''$ és a-nak pontosan egy inverze van. (kétoldali)

Biz Trivi

Diff Egy olyan neutrálisos félcsop-ot, melyben $\forall$ elemnek $\exists$ inverze csoportnak nevezzük.

|| pontosan 1 inverze lehet csak

Ha egy csop. művelete komm. is, kk komm. csoport.

Tétel Tetszőleges $(S,\cdot)$ félcsop esetén: 1. $\Leftrightarrow$ 2. $\Leftrightarrow$ 3. $\Leftrightarrow$ 4. $\Leftrightarrow$ 5.

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

1. S csop.
2. S-ben $\exists$ (balneutr.) balegység (e) és $\forall a \in S$, $\exists a^{-1} \in S$ (a') : $a^{-1}a = e$ (a')
3. 2.-es duálisa
4. Az $ax = b$, $ya = b$ egyenleteknek $\exists$ mo-sa S-ben $\forall a, b \in S$ esetén
5. Az $ax = b$, $ya = b$ egyenleteknek van egyértelmű megoldása $\forall a, b \in S$ esetén

Biz

Biz. 1. $\to$ 2. trivi

1. $\to$ 3. trivi

1. $\to$ 4. ha $a,b\in S \to x=a^{-1}b \to ax=a(a^{-1}b)=(aa^{-1})b=b$

$y=ba^{-1} \qquad ya=(ba^{-1})a=b$

1. $\to$ 5.: 1 $\to$ 4 ha $ax=b$ és $a\hat{x}=b \to ax=a\hat{x} \to a'(ax)=$

$=a'(a\hat{x}) \to$

$\to x=\hat{x}$

2. $\to$ 1.: ha a' egy a balinverze e-re nézve és a'' az a' balinverze e-re nézve

$\boxed{a\cdot a'=e\,a\,a'=(a''\underbrace{a')a}_{e}a'=a''\cdot a'=e} \to a'$ inverz

$\boxed{a\,e=a(a'a)=(a\,a')a=ea=a} \to e$ egység

3 $\to$ 1: 2 $\to$ 1 duálisa

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

$ax_b=b \to \boxed{y_a\cdot b=y_a(ax_b)=(y_a a)x_b=ax_b=b} \to$

$\to y_a = e$ baloldali egység

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

$\to$ 2. $\to$ 1.

5 $\to$ 1: 5 $\to$ 4 $\to$ 1. $\square$

Az 5. feltétel teljesül, de asszoc. nem: kvázicsoport

LOOP: egységelemes kvázicsoport

Def. Egy S félcsoport f elemét idempotensnek nevezzük, ha $f^2=f$.

Tétel $\forall$ csoportban pont 1 idempotens elem van és ez az egység.

Biz $\boxed{\Leftarrow}$ $e^2 = ee = e$

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

Jel G a csoportot jelöli

‖ right angled bend

Példák csoportokra

(A) példa $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ quaterniók?

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

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

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

$ij = k,\ jk = i,\ ki = j$

$ji = -k,\ kj = -i,\ ik = -j$

Q csoport, mégpedig a quaterniócsoport

($a + ib + jc + kd \rightsquigarrow$ quaternióalgebra)

(B) példa

D_n az E^3 kongruenciái, melyek egy n szöget önmagára képez

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

e: id

f: szimm kp körüli $\frac{2\pi}{n}$ forgatás

f^{n-1}: mivel $f^n = e$

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

bizonyítható, hogy D_n csoport, és ezt a csoportot n-edfokú diédercsoportnak nevezzük

$D_2 = \{e, t, f, tf\}$ („elfajuló" valami) Klein-csoport (komm. csoport)

2025. 09. 15.

általában nem üreshzt értünk hz alatt

Def Egy n-elemű hz permutációit (önmagára való bijektív leképezéseit) <u>n-edfokú permutációknak</u> nevezzük.

multiplikatív szemléletben vagyunk

Megállapodás, hogy az n-elemű hz $\underline{n}$

Jel S_n

$(S_n, \circ)$, itt a kompozíció a művelet

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

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

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

$\sigma: k \to (k)\sigma$ ezt a jelölést használjuk (tehát jobbról szorzunk)

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

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

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

Tétel $(S_n, \circ)$ csoport

Biz $e = id$, inverz megkonstruálható

Jel. S_n: n-edfokú szimmetrikus csoport

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

$1<2 \qquad \sigma(1)<\sigma(2)$

$1<3 \qquad \sigma(1)>\sigma(3)$

$1<4 \qquad \sigma(1)<\sigma(4)$

$2<3 \qquad \sigma(2)>\sigma(3)$

$2<4 \qquad \sigma(2)>\sigma(4)$

$3<4 \qquad \sigma(3)<\sigma(4)$

Deff Az $\langle i,j \rangle$ $i<j$ pár a σ egy inverziója, ha $\sigma(i)>\sigma(j)$

Deff Egy σ perm. páros (ptlan), aszerint, hogy inverziói száma páros (ptlan.)

$\| \; |S_n| = n!$

Tétel $|S_{n\,\text{páros}}| = |S_{n\,\text{ptlan}}| = \dfrac{n!}{2}$

Biz

Jel $S_{n\,\text{páros}} = A_n$

Tétel Azonos paritású perm-ok szorzata ps, egyébként a szorzat ptlan.

Deff A_n is csoport, n-edfokú alternáló csoport.

Deff Ha $k_1, \dots, k_r \in \underline{n}$ páronként különbözők, jelölje $(k_1 k_2 \cdots k_r)$ azt az n-edfokú perm-ot, mely k_1-hez k_2-t, k_2-hoz k_3-at, …, k_{r-1}-hez k_r-t és k_r-hez k_1-et rendeli, $\underline{n}$ többi elemét fixen hagyja, ezt ciklusnak nevezzük.

Ltg. 1 / J

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

S_5-ben $(1\ 2\ 3)$ és $(4\ 5)$ diszjunkt ciklusok

$$\overset{k_1\ k_2\ k_3}{(1\ 2\ 3)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \quad \overset{l_1\ l_2}{(4\ 5)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

Tétel Diszjunkt ciklusok szorzata nem függ a tényezők sorrendjétől.

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

Biz $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = (3\ 4)(5\ 6) = (5\ 6)(3\ 4)$

általában ⇧

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

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

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

Művelet G_X-en: Ha $w_1, w_2 \in G_X$, akk. $w_1 \cdot w_2$ 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, $\underset{\in G}{w}$-k szavak, xx^{-1} vagy $x^{-1}x$

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

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

Tétel G_X az előző szorzásra nézve csoport

Biz $(w_1 w_2) w_3 = w_1 (w_2 w_3)$ középső ~~szó~~ hossza sz. telj ind. *

Def G_X az X feletti / X által generált szabadcsoportnak nevezzük

e = üressorozat
inverz a "gonosz" tükörkép" $(x_1 x_2^{-1} x_3)^{-1} = x_1^{-1} x_2 x_3^{-1}$

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

$n \geq 2$ és az ind. felt. igaz $\forall$ n-nél rövidebb w_2-re

$$(w_1 (w_2) \cdot w_3 = (w_1 \cdot \underbrace{(\tilde{w}_2 \cdot x)}_{w_2}) w_3 \overset{\text{ind. felt.}}{=} ((w_1 \tilde{w}_2) \cdot x) \cdot w_3 \overset{\text{1. eset}}{=}$$

$$= (w_1 \tilde{w}_2) \cdot (x \cdot w_3) \underset{\text{ind. felt.}}{=} w_1 (\tilde{w}_2 (x w_3)) \overset{\text{1. eset}}{=} w_1 ((\tilde{w}_2 x) w_3) =$$

$$= w_1 (w_2 w_3)$$

Tétel Csoport tetszőleges g eleme esetén $(g^{-1})^{-1} = g$

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

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

$$g^n := \overbrace{g \cdot g \cdots g}^{n\text{-szer}} \quad (n \in \mathbb{N})$$

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

Áll $g^{n+m} = g^n g^m$

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

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

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

$$g^{-5} = e \rightarrow \underbrace{(g^{-5})^{-1}}_{= g^5} = e^{-1} = e$$

Def Azt mondjuk, hogy egy G csoport g elemének <u>rendje</u> $n \in \mathbb{N}^+$, ha $n = \min\{g^n = e\}$, ha nincs ilyen n, akkor azt mondjuk, hogy g rendje végtelen. Jel: $o(g)$

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

L lineáris
G csoport
2 2x2-es mtx

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

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

$$AB = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{bmatrix}, \quad (AB)^n = \begin{bmatrix} (\frac{1}{2})^n & \\ & (2)^n \end{bmatrix} \neq I \rightarrow o(AB) = \infty$$

|| egységelem rendje 1 ($o(e) = 1$)

|| szorzat rendjéről nem tudunk semmit, előző pl-ban $\overbrace{o(AB)}^{\infty} \neq \overbrace{o(A)}^{2}\,\overbrace{o(B)}^{2}$

Részcsoport

Def Egy G csoport $H\neq\emptyset$ részhz-t G egy <u>részcsoportjának</u> nevezzük, ha H is csop. a G-n értelmezett műveletre nézve

Tétel Egy G csoport részhz-a részcsoport $\iff H^2\subset H \wedge H^{-1}\subset H$
(ahol $HH=H^2=\{h_1h_2 \mid h_1,h_2\in H\}$
és $H^{-1}=\{h^{-1}\mid h\in H\}$)

Biz H részcsoport $\boxed{\Rightarrow}$ $H^2\subset H$ (művelet tulajdonsága)

$\hookrightarrow \exists f\in H$ egység $\to f^2=f \to f$ idempotens

$\to f=\underbrace{e}_{\in G}$ mivel 1db idempotens elem van, ez az e

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

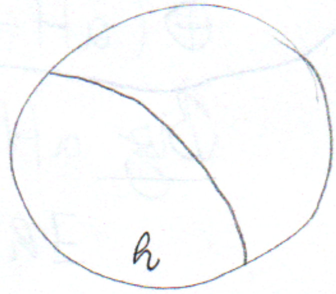
$\to h\in G: \exists h_G^{-1}\in G: hh_G^{-1}=h_G^{-1}h=e \to$

$\to hh_H^{-1}=hh_G^{-1} \to h_H^{-1}=h_G^{-1}$ $\boxed{\Rightarrow}$ $H^{-1}\subset H$

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

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

így $\underbrace{hh^{-1}}_{e}\in H^2\subset H \to e\in H \to$



$\to$ H oly részfélcsop, amelyben e egységelem
$H^{-1}\subset H$ miatt H minden elemének van inverze $\to$ H részcsoport

|| H részcsop, akkor $H^2=H,\ H^{-1}=H$

$H^{-1}\subset H \to (H^{-1})^{-1}=\{(h^{-1})^{-1}=h \mid h\in H\}=H$ } $H=H^{-1}$

$(H^{-1})^{-1}\subset H^{-1} \to H\subset H^{-1}$

$H^2 \subset H \to H = He \subset H^2 \subset H \to H^2 = H$
$\quad\quad\quad\quad\quad\quad\quad\quad {}_{\in H}$

tehát nemcsak tartalmazás, hanem egyenlőség is

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

Biz $H \neq \emptyset$ részcsop $\to H^{-1} = H$

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

$H \neq \emptyset$ $H^{-1}H \subset H \to e \in H \to H^{-1} = H^{-1}\underset{\in H}{e} \subset H^{-1}H \subset H \to$

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

$H^2 = H \cdot H = HH^{-1} \subset H \to H^2 \subset H \to H$ részcsoport

Deff H egy G csoport rcsop-ja. Az $a \in G$ H szerinti bal (oldali) mellékosztályán az $aH = \{ah \mid h \in H\}$ részhzt értjük.

Deff jobbmellékosztály a balnak duálisa

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

Biz $aH \cap bH \neq \emptyset \to \exists x \in G : x \in aH$ és $x \in bH \to$

$\exists h_1, h_2 \in H : ah_1 = x = bh_2 \Leftrightarrow ah_1 = bh_2 \to$

$\to ah_2 h_1^{-1} = bh_2 h_1^{-1} \to a = b\underbrace{h_2 h_1^{-1}}_{h} = bh \to aH = bhH =$

$= bH$

Tétel Egy G csoport tetszőleges H részcsoportja és $\forall a, b \in G$ esetén $aH = bH \Leftrightarrow \underbrace{a^{-1}b}_{} \in H$

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

2025.09.22.

$a^{-1}b \in H \to (a^{-1}b)^{-1} \in H$ $\qquad (ab)^{-1} \overset{?}{=} b^{-1}a^{-1}$

$\qquad\qquad\qquad \overset{\shortparallel}{b^{-1}(a^{-1})^{-1}}$

Biz $\boxed{\Rightarrow}$ ha $aH = bH \to b \in aH$ (mert $b \in bH$) $\to$

$\to \exists h \in H : b = ah \to a^{-1}b = \underbrace{a^{-1}a}_{e}h = h \in H$ $\qquad$ itt lehet majd

$\boxed{\Leftarrow}$ $a^{-1}b \in H \to \exists h \in H : a^{-1}b = h \to aa^{-1}b = ah \to$

$\to b = ah \to bH = (ah)H = a(hH) = aH$ □

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

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

|| $Ha = Hb$ változatra is igaz az előző két áll

Tétel G csoport, H részcsoportja, a H-szerinti bal- és jobbmellékosztályok halmazai ekvivalensek (megadható bijekció)

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

ϕ bijektív:
- ϕ szürjektív, hisz $\forall b \in G$ $\phi : b^{-1}H \mapsto Hb$
- ϕ injektív, hisz ha $\phi(aH) = \phi(bH) \to Ha^{-1} = Hb^{-1} \to$ $\to a^{-1}b \in H \leftrightarrow aH = bH$

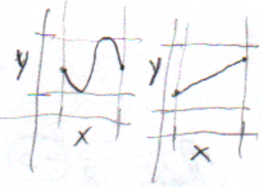
Def Egy G csoport H rcsoport szerinti (bal)jobbmellékosztályok számosságát a H részcsoport G-beli <u>indexének</u> nevezzük és $|G : H|$ módon jelöljük.

Tétel (Lagrange Tétele)

véges G csop., H részcsoportja $|G| = |H| \cdot |G:H|$;

így a H részcsoport rendje osztója a G csoport rendjének.

$f: X \to Y$



Biz

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

φ szürjektív (minden elemet rendel ?)

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

Ít $|H| = |aH|$ $\forall a \in G$-re $\to |G| = |H| \cdot \underbrace{|G:H|}_{\text{ilyen formális osztás}}$ □

Tétel G csop., ~~részcsoport-rendszereinek metszete is részcs.~~

részcsoportjainak metszete is részcsoport $\boxed{\text{mi a rendszer?}}$

Biz H_i, $i \in I$ részcsoportja G-nek, klk

① $\forall i \in I: e \in H_i \to e \in \bigcap_{i \in I} H_i \to \bigcap_{i \in I} H_i \neq \emptyset$

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

$\to ab \in \bigcap H_i$

ez kell

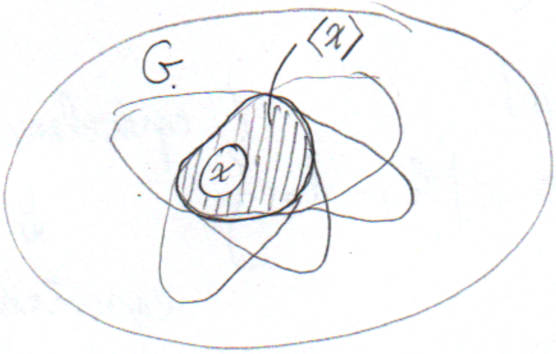
ez a kettő nem elég

③ $\forall a \in \bigcap_{i \in H} H_i \to \forall i \in I: a \in H_i \to \forall i \in I: a^{-1} \in H_i \to$

$\to a^{-1} \in \bigcap_{i \in I} H_i$

Generált részcsoportok

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



Tétel G csop., $X \in \mathcal{P}(G-\emptyset)$ ennek X-nak kéne lenni nem?

$$\langle X \rangle = \{ x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid n \in \mathbb{N}^+, k_j \in \mathbb{Z}, x_j \in \mathbb{Z} \ (j \in \underline{n}) \}$$

Biz nem bizonyítjuk

Def Az 1 elem által generált csoportokat <u>ciklikus csoportoknak</u> nevezzük.

|| ciklikus részcsoport

Def Egy $(G_1, *)$ csoport egy $(G_2, \circ)$ csoportba való φ leképezését <u>homomorfizmusnak</u> nevezünk, ha
$\forall a, b \in G_1 \rightarrow \varphi(a * b) = \varphi(a) \circ \varphi(b)$

|| = művelettartó leképezés

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

|| bijektív homomorfizmus = izomorfizmus

Tétel G csoport ciklikus $\Longleftrightarrow$ G izomorf vagy a $(\mathbb{Z},+)$, vagy a $(\mathbb{Z}_n,+)$ csoporttal

|| $\mathbb{Z}_n$ ~~mod~~ n moduloosztály

$$\left.\begin{array}{l} n \geq 2,\ n \in \mathbb{N} \\ k_1 \equiv k_2 \Longleftrightarrow n \mid k_1 - k_2 \end{array}\right\}$$ ekvivalenciareláció

$\downarrow$

ekvosztályok

osztályok

$$\mathbb{Z}_n = \{[0]_\equiv, [1]_\equiv, \ldots, [n-1]_\equiv\} \qquad [k_1]+[k_2]=[k_1+k_2]$$

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

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

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

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

$\boxed{\text{1. eset}}$ $o(a)$ végtelen $\forall n_1, n_2 \in \mathbb{Z}$ $(n_1 \neq n_2)$ $a^{n_1} \neq a^{n_2}$

(ui. $a^{n_1} = a^{n_2} \rightarrow n_1 > n_2,\ a^{n_1}a^{-n_2} = e \rightarrow a^{\overbrace{n_1-n_2}^{>0}} = e \Rightarrow$

$\rightarrow o(a) \neq \infty$ ↯)

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

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

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

$\boxed{2. \text{eset}}$ $o(a) = n \ (n \in \mathbb{N}_0)$

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

$a^{h_1} = a^{h_2} \to a^{k_1 - k_2} = e$, mivel $k_1 - k_2$ nem lehet n-nél kisebb természetes (ami $\neq 0$), így csak 0 lehet (vagy $k_1 = k_2 = n$, vagy $k_1 = n$ és $k_2 = 0$)

$m \in \mathbb{N}^+$ $a^m = a^{nt+r} = a^{nt} \cdot a^r = (a^n)^t \cdot a^r =$

$= e^t a^r = a^r$ $(r \in \underline{0, n-1})$ $\to \{a^0, a^1, \ldots, a^{n-1}\}$ félcsoport

$e = a^0$ egységelem

$\| \ a^{k_1} = a^{k_2} \Leftrightarrow a^{k_1 - k_2} = e \Leftrightarrow n | k_1 - k_2 \Leftrightarrow k_1 \equiv k_2$

$a^i \cdot a^{n-i} = a^n = e$ $(a^i)^{-1} = a^{n-i} \to \{a^0, \ldots, a^n\}$ csoport

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

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

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

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

__Áll__ $\varphi : (G_1, *) \leftrightarrow (G_2, \circ)$ izomorfizmus, akkor $\varphi(e_1) = e_2$

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

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

__Biz__ $\varphi(e_1) = \varphi(e_1 * e_1) = \varphi(e_1) \circ \varphi(e_1) \to \varphi(e_1)$ idempotens, ezért

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

$= e_2 \to \varphi(a) = \varphi(a)^{-1}$ $\|$ a $\varphi(a)$-t balról kell szorozni

Ald 1

Tétel Ciklikus csoport minden részcsoportja ciklikus (véges/végtelen)

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 $H\supsetneq\{e\}\rightarrow \exists k\in\mathbb{N}^+: a^k\in H\rightarrow$ legkisebb ilyen, ez n

$(n=\min\{k\in\mathbb{N}^+ \mid a^k\in H\})$

Jel $n\,\dot{\cup}\{0\}\triangleq$ $\triangleq n_0$

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

$m\in\mathbb{Z}: a^m\in H\rightarrow m=n\cdot t+\underbrace{r}_{\in 0..n-1}\rightarrow a^m=(a^n)^t\cdot a^r\rightarrow \overbrace{\big(\overbrace{(\underbrace{a^n}_{\in H})^{-1}}^{\in H}\big)^t}^{\in H}\underbrace{a^m}_{\in H}=$

$=\underbrace{((a^n)^{-1})^t(a^n)^t}_{e}a^r\rightarrow a^r\in H \quad r<n\rightarrow r=0\rightarrow m=n\cdot t\rightarrow$

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

|| Minden ciklikus csoport megszámlálható

Áll $|\langle a\rangle|=o(a)$

Áll Véges csoport tetszőleges elemének rendje osztója a csoport rendjének

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

$|\langle a\rangle|\,\big|\,|G|$ a Lagrange következménye miatt $\rightarrow$

$\rightarrow o(a)\,\big|\,|G|$ $\square$

Tétel Egy n-edrendű ciklikus csoportban az n-edrendű elemek száma $\varphi(n)$ (ahol $\varphi(n)$ az n-nél nem nagyobb n-hez relatív prím egészek számát jelenti)

Biz $|G|=n$ cikl. csop.

G izomorf az n-edik komplex egységgyökök csoportjával

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

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

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

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

primitív n-edik egységgyök

ε^k primitív $\Leftrightarrow o(\varepsilon^k)=n) \Leftrightarrow \gcd(k,n)=1 \rightarrow$

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

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

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

2025.09.29.

Biz $G=\{\overset{a^0}{e},a,a^2,\dots,a^{n-1}\}$

$a^k\in G$ mo-sa $x^d=e$ egyenletnek $\Leftrightarrow (a^k)^d=e \Leftrightarrow a^{kd}=e \Leftrightarrow$

$\Leftrightarrow t\in\mathbb{N}^+\,(kd=nt) \Leftrightarrow k=\underbrace{\frac{n}{d}}_{\in\mathbb{N}^+}\cdot t \quad t\in \underline{d}.$

$h=a^{\frac{n}{d}} \to x^d=e$ megoldásai $H=\{e,h,h^2,\dots,h^{d-1}\}$

H egy ciklikus részcsoportot alkot, s $|H|=d$.

$b\in G,\ o(b)=d \to b^d=e \to b\in H$

~~tt~~ G összes d-edrendű eleme H-ban van. Mivel $|H|=d$, ezért a H-ban ~~levő~~ (és így a G-ben) levő d-edrendű elemek száma $\varphi(d)$

Ha $b_1,b_2\in G$ úgy, hogy $o(b_1)=d=o(b_2)$, akkor $b_1,b_2\in H$ és $\langle b_1\rangle=H=\langle b_2\rangle$ ezért $b_1\in\langle b_2\rangle=\{e,b_2,b_2^2,\dots,b_2^{d-1}\}$ és $b_2\in\langle b_1\rangle=\langle e,b_1,b_1^2,\dots,b_1^{d-1}\rangle$ és így b_1 és b_2 egymás hatványai.

Tétel Egy n-edrendű G ciklikus csoportnak annyi részcsoportja van, ahány osztója van n-nek

|| $e|n$, $n|n \to \{e\}$, G triviális részcsoportok

Biz d az n osztója $\xrightarrow[\text{tétel}]{\text{előző}}$ $x^d=e$ egyenlet G-beli megoldásainak H ciklikus részcsoportja d-edrendű.

$d|n$, $h_{1,2}\in H_{1,2}$, $|H_{1,2}|=d$ mivel $\forall$ ciklikus csop. rcsop-ja ciklikus, ezért $\exists$-nek $a_1,a_2\in G$, hogy $H_1=\langle a_1\rangle$, $H_2=\langle a_2\rangle$

$\to o(a_1)=d$ és $o(a_2)=d$ (mert $|H_{1,2}|=d$) $\Rightarrow$

Így $a_1, a_2 \in H$ (ahol H a mo-sai az $x^d = e$ egyenletnek)

$|H| = d$ $\quad O(a_1) = O(a_2) = d$, ezért $\langle a_1 \rangle = d = \langle a_2 \rangle \rightarrow H_1 = H = H_2$

Így n $\forall$ d osztójához $\boxed{!}$ létezik G-beli d-edrendű.

Ha $l \nmid n \rightarrow G$-ben nincs l-edrendű részcsoport (Lagr.-tétel) ∎

Normális részcsoportok

Deff Egy G csoport, N részcsoportját **normális részcsoportnak** (vagy normálosztónak) nevezzük, abban az esetben ha $\forall a \in G \, (aN = Na)$ Jel $N \triangleleft G$

Tétel Egy G csop. N rcsop-ja normális $\Longleftrightarrow \forall a \in G (a^{-1} N a \subset N)$

Biz $N \triangleleft G \rightarrow \forall a \in G \, (aN = Na) \longrightarrow a^{-1}(aN) = a^{-1}(Na)$

$\Rightarrow N = a^{-1} N a \rightarrow a^{-1} N a \subset N$

$\forall a \in G (a^{-1} N a \subset N) \rightarrow a(a^{-1} N a) \subset aN \rightarrow$

$\rightarrow Na \subset aN$

$\forall (a^{-1}) \in G ((a^{-1})^{-1} N a^{-1} \subset N) \rightarrow (a N a^{-1}) a \subset Na \rightarrow$

$\rightarrow aN \subset Na$ $\quad$ Így $aN = Na \rightarrow N \triangleleft G$ ∎

Tétel G csoport $\{N_i\}_{i \in I}$, $\forall i \in I \, (N_i$ normális$) \rightarrow \bigcap_{i \in I} \{N_i\}$ norm.

Biz

Biz $N_i, i \in I$ a G norm. rcsop egy nem üres rendszere, akkor $\bigcap_{i \in I} N_i$ rcsop-ja G-nek

$$\left(g \in \bigcap_{i \in I} N_i,\ a \in G\right) \to \forall i \in I\ (g \in N_i) \to$$
$$\to \forall i \in I\ (a^{-1} g a \in N_i) \to a^{-1} g a \in \bigcap_{i \in I} N_i \to$$
$$\to a^{-1}\left(\bigcap_{i \in I} N_i\right) a \subset \bigcap_{i \in I} N_i \to \left(\bigcap_{i \in I} N_i\right) \triangleleft G$$

Csoport centruma

Diff Egy G csoport centrumán (németben c-nek ejtjük: zentrum) a $Z(G) := \{z \in G \mid \forall a \in G\ (az = za)\}$ rhz-t értjük

$Z(G) \neq \emptyset$, mert $e \in Z(G)$

Tétel G csop $Z(G)$ centruma normális.

Biz $Z(G) \neq \emptyset$

$$z_1, z_2 \in Z(G) \to \forall a \in G\ (a(z_1 z_2) = (z_1 a) z_2 = z_1 (z_2 a))$$
$$\to z_1 z_2 \in Z(G)$$

$$z \in Z(G) \to \forall a \in G\ (z a^{-1} = a^{-1} z) \to (z a^{-1})^{-1} = (a^{-1} z)^{-1} \to$$
$$\to (a^{-1})^{-1} z^{-1} = z^{-1} (a^{-1})^{-1} \to a z^{-1} = z^{-1} a \to z^{-1} \in Z(G)$$

Tehát $Z(G)$ a G rcsop-ja

$\Longrightarrow$

$z \in Z(G)$ és $a \in G \to a^{-1} z a = a^{-1} a z = z \in Z(G)$.

Így $a^{-1} Z(G) a \subset Z(G) \to Z(G) \lhd G$ $\square$

Elem centralizátora

Def Egy G csop. a elemének **centralizátorán** G-nek
a $C(a)=\{g \in G \mid ga=ag\}$ rhz-t értjük

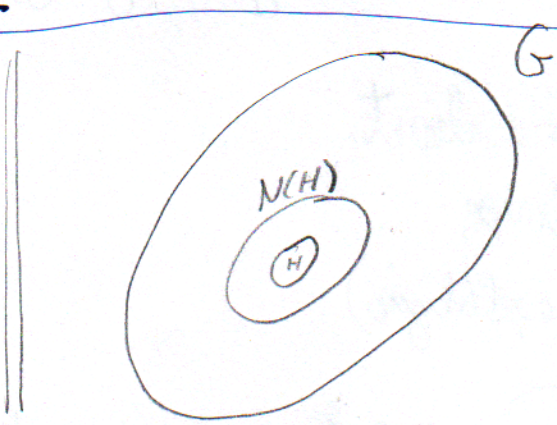
Tétel $a \in G$ csoport $\to$ $C(a)$ rcsop-ja G-nek

Áll $C(a)=G \Leftrightarrow a \in Z(G)$

Részcsoport normalizátora

Def G csop. H rcsop-jának $N(H)$ normalizátora
$N(H)=\{g \in G \mid aH=Ha\}$

Tétel $N(H)$ rcsop-ja G-nek, ha G csop és H rcsop-ja



$H \lhd N(H)$
$N(H)$ a G azon legbővebb H-t tartalmazó részcsoportja, amelyben H normális részcsop.

~~Konj~~

Konjugálás

Def G csop, b eleméről azt mondjuk, hogy egy $a \in G$ elemének **konjugáltja**, ha $\exists g \in G \, (g^{-1}ag = b)$

Jel $a \sim b$ → kicsiben

Áll $\sim$ ekvivalenciareláció (reflexív, szimm., tranz.)

Biz $e^{-1}ae = a \to a \sim a$

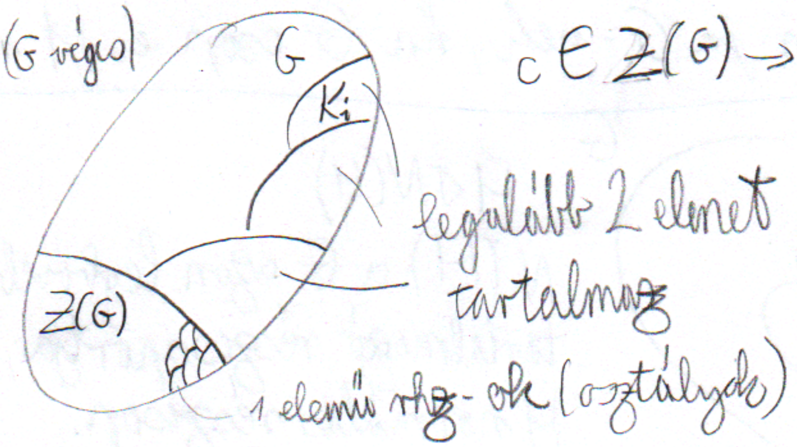
$a \sim b \to \exists g \in G \;\; g^{-1}ag = b \Leftrightarrow a = gbg^{-1} \to$

$\to (g^{-1})^{-1} b g^{-1} = a \to b \sim a$

$a \sim b, \; b \sim c \to \exists g \in G, \exists h \in G \, (g^{-1}ag = b, \; h^{-1}bh = c)$

$\to h^{-1}g^{-1}agh = c \to \underbrace{(gh)^{-1}}_{\in G} agh$ $\blacksquare$

(G véges)



$c \in Z(G) \to \forall g \in G \, ((g^{-1}cg) = g^{-1}gc = c)$

$\boxed{|G| = |Z(G)| + h_1 + \ldots + h_r}$, ahol $h_i \geq 2$ $(h_i = |K_i|)$

osztályegyenlet

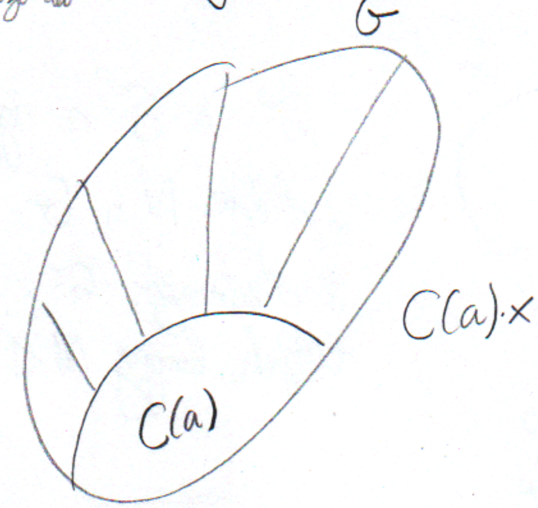
$\forall \sim$ osztályai **konjugáltsági osztályoknak** nevezzük

Tétel Egy G csop. valamely a elemének annyi különböző konjugáltja van, amennyi az a elem $C(a)$ centralizátorának G-beli indexe.

Biz $h, g, a \in G$, $g^{-1}ag = h^{-1}ah \Longleftrightarrow$

$$\Longleftrightarrow ag = gh^{-1}ah \Longleftrightarrow agh^{-1} = gh^{-1}a \overset{\text{df}}{\Longleftrightarrow} (gh^{-1}) \in C(a)$$

$$\underset{\text{egy előző áll}}{\Longleftrightarrow} C(a)g = C(a)h \longrightarrow$$ a különböző konjugáltjainak a száma $= |G : C(a)|$



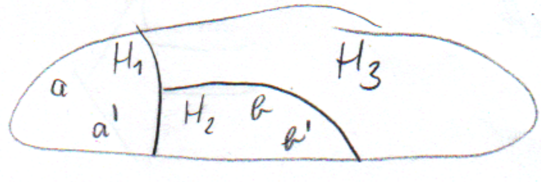
$|G| = |Z(G)| + k_1 + \ldots + k_r$ -ben

$\forall j \in I \quad k_j \geq 2$ és $k_j \,\big|\, |G|$

$k_j = |G : C(a)|, \forall a \in K_j$

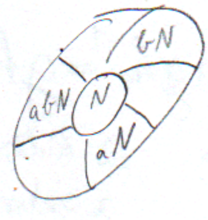
Diff Egy G csoport $G = \bigcup_{i \in I} H_i$ osztályozását ($H_i \cap H_j \neq \emptyset$ $\forall i \neq j$) **kompatibilis osztályozásnak** nevezzük, ha $\forall i, j \in I$ $\exists k \in I$: $H_i H_j \subset H_k$

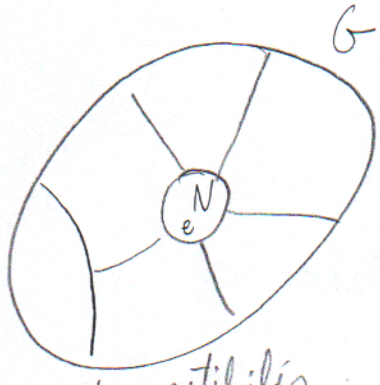
$(ab \in H_3 \rightarrow a'b' \in H_3) \longleftrightarrow H_1 H_2 \subset H_3$



Tétel Egy G csop. N normálisa szti mellékosztályok G egy kompatibilis osztályozását adják. Fordítva G tetszőleges kompatibilis osztályozásának osztályai G valamely norm. rcsop szerinti mellékosztályok

Biz $N \triangleleft G \to (aN)(bN) = a(Nb)N = abN^2 = abN$





kompatibilis osztályozás

σ a G-n egy eq-reláció jelölje N a G-nek e elemét tartalmazó σ-osztályát, megmutatjuk, hogy $N \triangleleft G$

$N \neq \emptyset \ (e \in N)$

$N^2 \subset N$, $N^{-1} \subset N$:

Ha $a, b \in N \to \begin{matrix} a \sim e \\ b \sim e \end{matrix} \to ab \sim ee \to (ab) \in N$

Ha $a \in N \to a \sim e \to aa^{-1} \sim a^{-1} \Leftrightarrow e \sim a^{-1} \to$
$\to a^{-1} \in N$

Ha $a \in N$ és $g \in G \to a \sim e \to g^{-1}ag \sim g^{-1}eg = e \to$
$\to g^{-1}ag \in N$

Így N normálisa G-nek

$\Longrightarrow$

Megmutatjuk, hogy $[a]_\sim = aN \quad \forall a \in G$-re

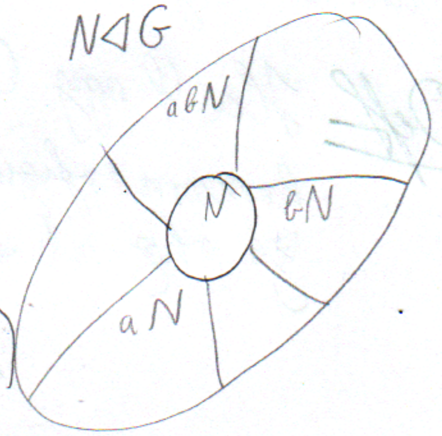
$a \in G \ (a = a \cdot e) \to aN \subset [a]_\sim$

$b \in [a]_\sim \Leftrightarrow b \sim a \to a^{-1}b \sim a^{-1}a = e \to a^{-1}b \in N \Leftrightarrow$

$\Leftrightarrow aN = bN \to (b \in bN \to b \in aN) \to [a]_\sim \subset aN,$

$\#\ [a]_\sim = aN$

Faktorcsoport



Jel G/N a G csoport N normálisai szerinti mellékosztályainak hz-a

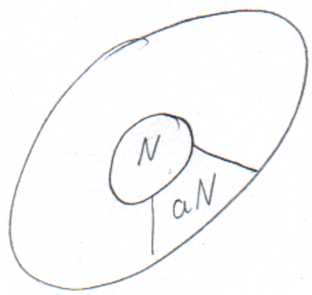
Deff G/N hz-on a szorzás (multipl. műv.)

$$(aN)(bN) := (abN)$$

Tétel A G/N hz az $(aN)(bN) := (abN)$ szorzásra csoportot alkot

Deff A G/N csoportot a G csop. N normálisa szerinti **faktorcsoportjának** nevezzük.

Legyen G véges csoport és $N \triangleleft G$



$$|G| = |N|\,|N:G| = |N|\,|G/N|$$

$$|G| = |N|\,|G/N|$$

Tétel $\varphi: a \mapsto aN$ a G csoportnak a G/N faktorcsoportra való homomorfizmusa G tetszőleges N norm. részcsoportja esetén

<u>Biz</u> $\varphi(ab) = abN = (aN)(bN) = \varphi(a)\varphi(b)$

Az ~~előző~~ fenti tételben szereplő homomorfizmust ún. természetes homomorfizmusnak nevezzük

Def Ha φ egy G_1 csoportnak egy G_2 csoportba való homomorfizmusa, akkor φ **magján** a G_1 következő rhz-át értjük:

$$\{a \in G_1 \mid \varphi(a) = e_2\}$$

ahol e_2 a G_2 egységeleme

Jel $Ker(\varphi)$

Tétel $Ker(\varphi)$ normális részcsoportja G_1-nek, G_1, G_2 tetsz. $\varphi: G_1 \to G_2$ homomorfizmus esetén