

CYCYS

1995. 12. 08.

²
HUBER LÁSZLÓ

VÉGES CIKLIKUS CSOPORTOKNAK
VÉGES CIKLIKUS CSOPORTOKKAL

VALÓ

SZÉTESŐ BŐVÍTÉSEIRŐL

1995

BARÁTOMNAK
ÉS
URANITA TESTVÉREMNEK
SZERETETTEL

Mota

1995. 12. 08.

Köszönettel tartozom Corrádi Keresztélynek és Csörgő Piroskának, akik nélkül érdeklődésem a csoportelmélet iránt bizonytalannal elenyészett volna.

Köszönet illeti Kristóf Miklós barátomat is, aki - túl a gyümölcsöző vitákon - konkrét, "empirikus" segítséggel is szolgált a permutációkkal való reprezentációk és az M-csoportok problémáinál.

Végezetül mély hálával tartozom feleségemnek, Kovács Gabriellának, akinek türelmes buzdítása nélkül ezek a lapok el sem készülhettek volna.

"Istenem, add, hogy ez a mű beteljesedhessen,
eljusson oda, ahova kell, és a lények javát
szolgálja mindhárom világban.

95.12.08. éj

TARTALOM

JELÖLÉSEK		i - iii
I. RÉSZ	A VIZSGÁLT OBJEKTUM. ALAPFOGALMAK ÉS ALAPTÉTELEK	1
II. RÉSZ	REPREZENTÁCIÓK	17
III. RÉSZ	NEVEZETES RÉSZCSOPORTOK. p-CSOPORTOK. NILPOTENCIA.	22
IV. RÉSZ	AZ AUTOMORFIZMUSOKRÓL ÁLTALÁBAN	35
V. RÉSZ	Ch-CSOPORTOK	44
VI. RÉSZ	CSOPORTOK A Ch-N KÍVÜL	64
VII. RÉSZ	NYITOTT KÉRDÉSEK	84
FÜGGELÉK		87
IRODALOM		88

JELÖLÉSEK

i

N	A természetes számok halmaza.
Q	kvaterniócsoport.
Z_m	az m -nél kisebb nemnegatív egészek additív csoportja: $\{0,1,2,\dots, m-1\}$.
R_m	az m -nél kisebb, az m -hez relatív prím pozitív egészek multiplikatív csoportja.
P	a prímszámok halmaza.
P_0	a páratlan prímek halmaza.
PR	olyan számok halmaza, amelyekhez létezik primitív gyök.
D_m	a $2m$ -edrendű diédercsoport.
S_m	az m -edfokú szimmetrikus csoport.
$ G $	a G csoport rendje.
$ g $	a $g \in G$ elem rendje.
$ k _m$	k rendje mod m , azaz a k rendje R_m -ben.
$G^\#$	a G csoportnak az egységelemtől különböző elemeinek halmaza.
(s)	s -edrendű ciklikus csoport, illetőleg: moduló s .
$(s)_c$	c generátorú s -edrendű ciklikus csoport.
(m,n)	az m és n számok Inko -ja (legnagyobb közös osztó).
$[m,n]$	az m és n számok lkkt -je (legkisebb közös többszörös).
$\max(m_1, \dots, m_r)$	az m_1, \dots, m_r egészek legnagyobbika.
$EU(m)$	az EULER-féle függvény: $EU(m) = R_m $
$\pi(m)$	az m prímosztóinak halmaza.
$\text{pr}(m)$	az m -hez tartozó primitív gyökök halmaza.
$k^{-n} \equiv 1(m)$	" k pont az n -ediken" : azt jelenti, hogy $ k _m = n$.
$a b$	a osztója b - nek.
$a \nmid b$	a nem osztója b - nek.
$a \downarrow b$	$a b$ és $a < b$.
$a \rightarrow b$	leképezés a -ról b -re.
$p^\alpha b$	$p^\alpha b$, de $p^{\alpha+1} \nmid b$.
$a \rightleftharpoons b$	a kommutál b -vel.
$\Gamma(G)$	a G csoport generátorainak egy halmaza.
$\Delta_{\Gamma(G)}$	a $\Gamma(G)$ generátorok közötti definiáló relációk halmaza.
$G = \langle \Gamma(G) \Delta_{\Gamma(G)} \rangle$	a G megadása a $\Gamma(G)$ generátorokkal és a $\Delta_{\Gamma(G)}$ relációkkal.
$\text{Hom}(G,H)$	a G csoportot a H -ba leképező homomorfizmusok halmaza.
$\text{Hom}(n,H)$	az (n) ciklust a H -ba leképező homomorfizmusok halmaza.
$\text{Aut } G$	a G teljes automorfizmuscsoportja.
$\text{Inn } G$	a G belső automorfizmusainak halmaza.
$\text{Hol } G$	a G holomorfja.
$\partial(G)$	a G kommutátora.

$\zeta(G)$	a G centruma.
$\zeta_e(G)$	a G elsőcentruma és
$\zeta_h(G)$	hátsócentruma (ld. 21. old..)
$\Phi(G)$	a G Frattini-részcsoportja.
$\Phi_e(G)$	lásd a 23. oldalt..
$\Phi_h(G)$	lásd a 23. oldalt..
$(m k n)$	lásd a 2. oldalt..
$(m k n)_a^b$	lásd a 2. oldalt..
$(m k \cdot n)$	lásd a 10. oldalt..
$(m r, k n)$	lásd a 84. oldalt..
$(m r, k n)_a^b$	lásd a 84. oldalt..
$[k \alpha]$	lásd az 5. oldalt..
CYCYS	1. oldal..
ABEL	a kommutatív csoportok osztálya
NIL	a nilpotens csoportok osztálya
SOL	a feloldható csoportok osztálya
DIV	az osztható csoportok osztálya: legyen $ G =n$, és $n_1 n$. Akkor $\exists H \leq G : H = n_1$.
TODIV	a totálisan osztható csoportok osztálya: $G \in \text{TODIV}$ ha $\forall H \leq G : H \in \text{DIV}$.
MAXPIND	azon csoportok osztálya, amelyekben minden maximális részcsoport prím indexű.
CYCEX	85. oldal.
$\text{MAX}(G)$	a G csoport maximális részcsoportjainak halmaza.
$\text{MGR}(G)$	a G csoport minimális generátorrendszereinek halmaza.
PRET	3. oldal.
PART	7. oldal.
CAT	9. oldal.
SAT	14. oldal.
$G_1 \otimes G_2$	11. oldal.
$\varphi_1 \otimes \varphi_2$	37. oldal.
x -automorfizmus	35. oldal.
c -automorfizmus	37. oldal.
$G_1 \cong G_2$	G_1 izomorf G_2 -vel.
$G_1 \sim G_2$	G_1 izostruktúrális G_2 -vel (lásd a 13. oldalt)..
$H \text{ char } G$	H karakterisztikus G -ben.

\mathcal{B}	47. oldal.
\mathcal{C}	37. oldal.
\mathcal{C}_h	43. oldal.
\mathcal{F}	9. oldal.
\mathcal{F}_c	9. oldal.
\mathcal{X}	14. oldal.
\mathcal{M}	59. oldal.
\mathcal{M}^*	54. oldal.
\mathcal{N}	25. oldal.
\mathcal{P}	25. oldal.
\mathcal{Q}	43. oldal.
\mathcal{R}	31. oldal.
\mathcal{S}	10. oldal.
\mathcal{T}	51. oldal.
\mathcal{X}	35. oldal.
\mathcal{Z}	21. oldal.
$(p)^\alpha$	$(p) \times (p) \times \dots \times (p)$
	$\underbrace{\hspace{10em}}$ α -tényező
$w_p(G)$	83. oldal.
$w(G)$	83. oldal.
H / \sim	a H halmazon a \sim ekvivalenciareláció által létesített osztályozás osztályainak halmaza (a H -nak a \sim szerinti faktorhalmaza).

I. RÉSZ A VIZSGÁLT OBJEKTUM.
ALAPTULAJDONSÁGOK ÉS ALAPTÉTELEK.

1. DEFINÍCIÓ Azoknak a nemizomorf csoportoknak a halmazát, amelyek megkaphatók valamely véges ciklusnak egy véges ciklussal való nemabeli széteső bővítéseként (szemidirekt szorzataként), CYCYS-nek nevezzük. (CYcle – CYcle – Semidirection)

Legyen $A = \langle \Gamma(A) \mid \Delta_{\Gamma(A)} \rangle$ és $B = \langle \Gamma(B) \mid \Delta_{\Gamma(B)} \rangle$ két csoport.
Az A -nak a B -vel való azon széteső bővítése, amelyet a

$$\theta \in \text{Hom}(B, \text{Aut } A)$$

kísér, így prezentálható:

$$G = \langle \Gamma(A) \cup \Gamma(B) \mid \Delta_{\Gamma(A)} \cup \Delta_{\Gamma(B)} \cup \Delta_{\Gamma(AB)} \rangle.$$

ahol

$$\Delta_{\Gamma(AB)} = \{ bab^{-1} = \varphi_b(a), a \in A, b \in B, \varphi_b = \theta(b) \}.$$

Ha $G \in \text{CYCYS}$, akkor

$$A = \langle a \mid a^m = 1 \rangle,$$

$$B = \langle b \mid b^n = 1 \rangle,$$

$$\text{Hom}(B, \text{Aut } A) = \text{Hom}(n, \mathbf{R}_m),$$

és a kísérő homomorfizmus

$$\theta : b \mapsto \varphi_k,$$

ahol

$$\varphi_k : a \mapsto a^k, k \in \mathbf{R}_m,$$

és $\Delta_{\Gamma(AB)}$ az egyetlen

$$bab^{-1} = a^k \quad (1)$$

relációból áll. Így a $G \in \text{CYCYS}$ prezentációja:

$$G = \langle a, b \mid a^m = b^n = 1, bab^{-1} = a^k \rangle. \quad (2)$$

Az (1) relációból

$$b^n ab^{-n} = a^{k^n} = 1 \cdot a \cdot 1 = a = a^1$$

azaz

$$k^n \equiv 1 \pmod{m} \quad (3)$$

más szóval $kl_m \mid n$ következik.

A (2) csoport pont akkor lesz nemabeli, ha

$$k > 1 \quad (4)$$

azaz

$$k \in \mathbf{R}_n^{\#}.$$

2. DEFINÍCIÓ A (2) prezentációra a (3) és a (4) teljesülése esetén a

$$G = (m \mid k \mid n)_a^b$$

szimbólumot vezetjük be, amelyből - ha félreértéstől nem kell tartani - a generátorok feltüntetése el is maradhat.

A CYCYS és az $\{(m \mid k \mid n)\}$ halmaz között nincs bijekció, hiszen (1)-ből következik, hogy

$$\forall t \in \mathbf{R}_n: b^t a b^{-t} = a^{k^t},$$

s így

$$\langle a, b \rangle = \langle a, b^t \rangle,$$

azaz

$$(m \mid k \mid n)_a^b = (m \mid k^t \mid n)_a^{b^t} \quad (5)$$

1. TÉTEL (PRET = PREZENTÁCIÓTÉTEL)

Az $(m \mid k \mid n)$ és $(m \mid l \mid n)$ által szimbolizált CYCYS-csoportok pont akkor izomorfok, ha k és l ugyanazt a részcsoportot generálja R_m -ben:

$$(m \mid k \mid n) \cong (m \mid l \mid n) \Leftrightarrow \langle k \rangle = \langle l \rangle \leq R_m.$$

Bizonyítás: Az (5) miatt elegendő a \Rightarrow implikációt igazolni.
Világos, hogy bármely φ izomorfizmusnál a

$$G = (m \mid k \mid n)_a^b$$

$\varphi(G)$ képét egy

$$\varphi(\langle a \rangle) = \langle c \rangle, \quad \varphi(\langle b \rangle) = \langle d \rangle$$

cikluspár fogja generálni.

Legyen például $\varphi(G) = (m \mid l \mid n)_c^d$,

és $\varphi(a) = c^\gamma, \quad \gamma \in R_m$

$$\varphi(b) = d^\delta, \quad \delta \in R_n.$$

Akkor egyrészt $\varphi(b a b^{-1}) = \varphi(a^k) \Rightarrow d^\delta c^\gamma d^{-\delta} = c^{\gamma \cdot k} \quad (7)$

másrészt a (6) prezentáció szerint

$$d c d^{-1} = c^l,$$

amiből $d^\delta c^\gamma d^{-\delta} = c^{\gamma \cdot l^\delta} \quad (8)$

A (7) és (8)-ból $c^{\gamma \cdot k} = c^{\gamma \cdot l^\delta}$ adódik,

majd $\gamma \in R_m$ miatt $k \equiv l^\delta \pmod{m}$, végül

$\delta \in \mathbf{R}_n$ miatt $\langle k \rangle = \langle 1 \rangle \leq \mathbf{R}_m$ következik.

Q . E . D .

Vezessünk be a $\text{Hom}(n, \mathbf{R}_m)$ halmazon egy \leftrightarrow relációt:

Ha $(n) \cong \langle b \rangle$, akkor

$$\forall \Theta_1, \Theta_2 \in \text{Hom}(n, \mathbf{R}_m) : \Theta_1 \leftrightarrow \Theta_2 \Leftrightarrow \Theta_1(\langle b \rangle) = \Theta_2(\langle b \rangle).$$

Könnyű látni, hogy \leftrightarrow ekvivalenciareláció, és hogy igaz az alábbi :

Az (m) -nek az (n) -nel való összes nem izomorf széteső bővítései

bijektíven megfelelnek a $\text{Hom}(n, \mathbf{R}_m) / \leftrightarrow$ elemeinek,

vagyis a $\text{Hom}(n, \mathbf{R}_m)$ halmazon a \leftrightarrow reláció által létesített

osztályozás osztályainak.

A (3) és (4) -et kielégítő összes $m, k, n \in \mathbf{N}$ számhármassok

$\{(m|k|n)\}$ halmazának két tetszőleges eleme álljon a \cong relációban

egymással pont akkor, ha az általuk reprezentált CYCYS -csoportok

izomorfok. Ekkor világos, hogy a CYCYS és az $\{(m|k|n)\} / \cong$

között bijekció létesíthető.

A következő lemmában néhány igen alapvető, közvetlenül az (1) segítségével

igazolható összefüggéseket sorolunk föl, amelyeket a továbbiakban

lépten-nyomon fölhasználunk.

1. LEMMA Legyen $G = (m | k | n)_a^b$.

$$(I) \quad \langle a \rangle < G, \quad \langle a \rangle \cap \langle b \rangle = 1, \quad G / \langle a \rangle \cong \langle b \rangle.$$

$$(II) \quad \forall g \in G \exists \alpha \in \mathbf{Z}_m \exists \beta \in \mathbf{Z}_n: \quad g = a^\alpha b^\beta.$$

$$(III) \quad |G| = m \cdot n.$$

$$(IV) \quad \forall \alpha_1, \alpha_2 \in \mathbf{Z}_m \quad \forall \beta_1, \beta_2 \in \mathbf{Z}_n:$$

$$(a^{\alpha_1} \cdot b^{\beta_1}) \cdot (a^{\alpha_2} \cdot b^{\beta_2}) = a^{\alpha_1 + \alpha_2 \cdot k^{\beta_1}} \cdot b^{\beta_1 + \beta_2}.$$

$$(V) \quad \forall \alpha \in \mathbf{Z}_m \quad \forall \beta \in \mathbf{Z}_n \quad \forall \gamma \in \mathbf{N}:$$

$$(a^\alpha \cdot b^\beta)^\gamma = a^{\alpha \cdot [k^\beta | \gamma]} \cdot b^{\beta \cdot \gamma}.$$

$$\forall s | m, \quad \forall t | n:$$

$$(VI) \quad \langle a^s, b^t \rangle < G \quad \Leftrightarrow \quad k^t \equiv 1 (s),$$

$$(VII) \quad \langle a^s, b^t \rangle \in \text{ABEL} \quad \Leftrightarrow \quad k^t \equiv 1 \left(\frac{m}{s} \right).$$

Q . E . D .

Az (V) -ben szereplő $[\quad | \quad]$ szimbólum az egész tárgyalás során központi jelentőségű, ezért egy lemmában összefoglaljuk legfontosabb tulajdonságait. A bizonyítás közvetlen számolással lehetséges.

2. LEMMA Legyen $k, \alpha, \beta, \beta_1, \beta_2 \geq 0$ és

$$[k | \alpha] = 1 + k + k^2 + k^3 + \dots + k^{\alpha-1}.$$

Akkor

$$(a) \quad k \neq 1 \text{ esetén } [k \mid \alpha] = \frac{k^{\alpha-1}}{k-1} ,$$

$$(b) \quad [0 \mid \alpha] = 1 ,$$

$$(c) \quad [k \mid 0] = 0 ,$$

$$(d) \quad [1 \mid \alpha] = \alpha ,$$

$$(e) \quad [k \mid 1] = 1 ,$$

$$(f) \quad [k \mid \alpha + \beta] = [k \mid \alpha] + k^\alpha \cdot [k \mid \beta] ,$$

$$(g) \quad \text{Ha } \alpha \geq \beta , \text{ akkor } [k \mid \alpha] - [k \mid \beta] = k^\beta \cdot [k \mid \alpha - \beta] ,$$

$$(h) \quad [k \mid \alpha \cdot \beta] = [k \mid \alpha] \cdot [k^\alpha \mid \beta] ,$$

Ha $k^n = 1$ (m) , akkor

$$(i) \quad [k \mid \alpha \cdot n + \beta] \equiv \alpha \cdot [k \mid n] + [k \mid \beta] \quad (m) ,$$

(j) ha még $\beta_1 \equiv \beta_2$ (n) is, akkor

$$[k^{\beta_1} \mid \alpha] \equiv [k^{\beta_2} \mid \alpha] \quad (m) . \quad \text{Q.E.D.}$$

Az $(m_1 \mid k_1 \mid n_1) \cong (m_2 \mid k_2 \mid n_2)$ reláció fennállásának feltételeit vizsgálva

a PRET csak az $m_1 = m_2$ esetben igazít el. Meglepő módon ez a

reláció akkor is fönnállhat, ha $m_1 \neq m_2$ (s ekkor persze $n_1 \neq n_2$ is).

Némi számolással pl. megmutatható, hogy

$$(4 \mid 3 \mid 30) \cong (12 \mid 7 \mid 10) \cong (20 \mid 11 \mid 6) \cong (60 \mid 31 \mid 2) \quad (9)$$

2. TÉTEL (PART = PARTÍCIÓTÉTEL)

(a) $(s)_c \times (m|k|n)_a^b \cong (m \cdot s|1|n)_d^b$ akkor és csak akkor, ha

$$(m, s) = 1, \quad 1 \equiv 1 (s), \quad \langle k \rangle = \langle 1 \rangle \leq \mathbf{R}_m.$$

Ezt a műveletet úgy nevezzük hogy (konstanssal) szorzás előlről, illetve (konstans) kiemelés(e) előlről.

(b) $(m|k|n)_a^b \times (s)_c \cong (m|k|n \cdot s)_a^d$

pontosan akkor, ha $(n, s) = 1$.

E műveletre úgy hivatkozunk, mint (konstanssal való) szorzásra hátulról, illetve (konstans) kiemelés(é)re hátulról.

(c) $(m_1|k_1|n_1)_{a_1}^{b_1} \times (m_2|k_2|n_2)_{a_2}^{b_2} \cong (m_1 \cdot m_2|k|n_1 \cdot n_2)_a^b$

akkor és csak akkor, ha

$$(m_1, m_2) = (n_1, n_2) = 1,$$

$$\text{és } \langle k \rangle = \langle k_i \rangle \leq \mathbf{R}_{m_i}, \quad i = 1, 2. \quad (10)$$

Bizonyítás (a) Tekinhető az az eset, amikor $k \equiv 1 (m)$.

Ekkor az $a \rightarrow d^s, b \rightarrow b, c \rightarrow d^m$ leképezésről könnyen látható, hogy izomorfizmus.

(b) $a \rightarrow a, b \rightarrow d^s, c \rightarrow d^n$.

99.7.26 du++ folytatás CYC_2

Megjegyzés 2004.9.5 : az 1 (egy) és az l (el) nagyon könnyen összetéveszthető, de aki odafigyel az meg tudja különböztetni, vagy a szövegösszefüggésből vagy logikailag, ti. pl $k \equiv 1 (m)$ esetén csak el lehet az l, mert a $k \equiv 1 (m)$ esetet (k kongruens egy) eleve kizártuk a vizsgálatból!

99.7.26 CYCYS folytatása eredeti kézirat 12. oldalától.

(c) Először vegyük azt az esetet, amikor $k \equiv k_i \pmod{m_i}$, $i = 1, 2$.

Ekkor az $a_1 \rightarrow a^{m_2}$, $a_2 \rightarrow a^{m_1}$, $b_1 \rightarrow b^{n_2}$, $b_2 \rightarrow b^{n_1}$

egy jó leképezés.

A (10) azt jelenti, hogy a jelzett direkt szorzat független a tényezők prezentációjától. Ennek indoklása a következőképpen történhet.

Idézzük föl az alábbi számelméleti tételt:

(SZT) Az $x \equiv a_i \pmod{n_i}$ kongruenciarendszernek pontosan akkor

van megoldása, ha minden i, j párra, ahol $1 \leq i < j \leq r$,

teljesül, hogy $(n_i, n_j) \mid (a_i - a_j)$,

és bármely két megoldás kongruens modulo $[n_1, n_2, \dots, n_r]$.

(Ha az n_i számok ($i = 1, 2, \dots, r$) páronként relatív prímek, akkor ez nem más, mint a kínai maradéktétel.)

Az $(m_1 \cdot m_2 \mid k \mid n_1 \cdot n_2)$ csoportot generálhatjuk így: $a = a_1 \cdot a_2$, $b = b_1 \cdot b_2$.

Térjünk most át az $(m_i \mid k_i \mid n_i)_{a_i}^{b_i}$ -ről az $(m_i \mid k_i^{t_i} \mid n_i)_{a_i}^{b_i^{t_i}}$

csoportokra, ahol $t \in \mathbf{R}_{n_i}$, $i = 1, 2$.

Akkor a $(b_1 \cdot b_2)^x = b_1^x \cdot b_2^x = b_1^{t_1} \cdot b_2^{t_2}$ relációból folyó

$$x \equiv t_i \pmod{n_i}, \quad i = 1, 2$$

kongruenciarendszer $(n_1, n_2) = 1$ miatt mindig megoldható, tehát van olyan

$$x \in \mathbf{R}_{n_1 \cdot n_2}, \quad \text{hogya}$$

$$(m_1 | k_1^{t_1} | n_1)_{a_1} b_1^{t_1-1} \times (m_2 | k_2^{t_2} | n_2)_{a_2} b_2^{t_2-2} \cong (m_1 \cdot m_2 | k^x | n_1 \cdot n_2)_a b^x.$$

Mindez a (10) -et bizonyítja.

Q . E . D .

A (c) -ben szereplő direkt szorzás értelemszerűen akárhány - véges számú - tényezőre is kiterjeszhető.

A PART segítségével most már megérthető a (9) példa:

mind a négy csoport izomorf a

$$(3) \times (4) \times (4 | 3 | 2)$$

csoporttal.

3. DEFINÍCIÓ Azon CYCYS - csoportokat, amelyeknek nincs triviálistól különböző direkt faktora, **felbonthatatlanok**nak nevezzük, és összességüket \mathcal{F} - fel jelöljük (\mathcal{F} - csoportok), \mathcal{F}^c -vel pedig azokat, amelyeknek nincs valódi direkt konstans (ciklikus) tényezőjük.

3. TÉTEL (CAT = CYCYS ALAPTÉTELE)

Minden CYCYSbeli csoport egyértelműen állítható elő prímhatványrendű konstansok (ciklusok) és \mathcal{F} - csoportok direkt szorzataként - eltekintve

a tényezők sorrendjétől és prezentációjától.

BIZONYÍTÁS Az állítás közvetlenül belátható a PART - nak, az ABEL - csoportok alaptételének, valamint REMAK azon tételének segítségével, amely szerint tetszőleges véges csoport két direkt felbontatlan faktorú direkt felbontása izomorf. Q . E . D .

4. DEFINÍCIÓ Azon CYCYS - csoportok halmazát, amelyeknek létezik olyan $(m | k | n)$ prezentációjuk, ahol $n = |k|_m$,

\mathfrak{S} - sel jelöljük. (\mathfrak{S} - csoportok). Ha $n = |k|_m$, akkor használni fogjuk az $(m | k | \dot{n})$, $(m | k | \cdot n)$, $(m | k | (\cdot n) s)$, vagy $(m | k | \dot{n} s)$ jelöléseket is. Az $(m | k | \dot{n})$ az ún. \mathfrak{S} - prezentáció.

A (9) példa (10. o.) mutatja, hogy bizonyos \mathfrak{S} - csoportoknak lehetnek nem - \mathfrak{S} - prezentációik is. A PART (a) és (b) szerint pontosan azok a csoportok ilyenek, amelyek

$$(s) \times (m | k | \cdot n)$$

alakba írhatók, ahol $(m \cdot n, s) = 1$.

Ha $(m | k | n) \notin \mathfrak{S}$, akkor $n = |k|_m \cdot s$, $s > 1$, és most két fontos eset lehetséges:

$$(|k|_m, s) = 1, \text{ de } \pi(s) \subseteq \pi(m), \quad (11)$$

s így $(m|k|n) \cong (m|k||k|_m) \times (s)$, de az (s) konstans előre nem vihető be,

$$\text{vagy} \quad \pi(s) \subseteq \pi(|k|_m), \quad (12)$$

és ekkor az (s) konstans hátulról nem emelhető ki.

Amíg a (11) -nél az $(m|k|n)$ direkt bővítése az $(m|k||k|_m)$ -nek, addig a (12) esetben az $(m|k|n)$ nem bővítése az $(m|k||k|_m)$ -nek, például a $(4|3|4)$ még részcsoporthként sem tartalmaz $(4|3|2) \cong D_4$ csoportot.

5. DEFINÍCIÓ Az $(m|k|\cdot n)$ csoport homológjainak nevezzük az $(m|k|(\cdot n)_s)$ csoportokat, ahol

$$1 < s \quad \text{és} \quad \pi(s) \subseteq \pi(n).$$

6. DEFINÍCIÓ Legyenek az m_i , $i = 1, 2, 3, \dots, r$ számok páronként relatív prímek.

A $G_i = (m_i|k_i|\cdot n_i)$, $i = 1, 2, \dots, r$ csoportok **fúzióján** a

$$G = \bigotimes_{i=1}^r G_i = \left(\prod_{i=1}^r m_i | k | \cdot [n_1, n_2, \dots, n_r] \right)$$

csoportot értjük, ahol $k \equiv k_i(m_i)$, $i = 1, 2, \dots, r$. (13)

Ez a definíció korrekt, mert egyrészt a (13) - nak megfelelő k létezését biztosítja a kínai maradéktétel, másrészt az is egyszerű számelméleti igazság, hogy páronként relatív prím m_i ($i = 1, 2, \dots, r$) számok esetén

$$k \cdot n_i \equiv 1 \pmod{m_i} \Rightarrow k \cdot [n_1, n_2, \dots, n_r] \equiv 1 \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_r} .$$

($k \cdot n_i \equiv 1 \pmod{m_i}$ azt jelenti, hogy $|k_i|_{m_i} = n_i$, ld. JELÖLÉSEK (i).)

(Látnivaló, hogy ha az n_1, n_2, \dots, n_r számok is relatív prímek, akkor - és csak akkor - a fúzió átmege a szokásos direkt szorzatba.)

Tekintsük a fenti $G_i = (m_i |k_i| n_i)_{a_i}^{b_i}$ csoportok direkt szorzatát :

$$G^* = \times_{i=1}^r G_i .$$

Ha most $a = a_1 a_2 \dots a_r$,

és $b = b_1 b_2 \dots b_r$, akkor

$$b a b^{-1} = b_1 a_1 b_1^{-1} b_2 a_2 b_2^{-1} \dots b_r a_r b_r^{-1} = a_1^{k_1} a_2^{k_2} \dots a_r^{k_r} = a ,$$

ahol $k \equiv k_i \pmod{m_i}$, $i = 1, 2, \dots, r$.

Látható tehát, hogy $\langle a, b \rangle = G = \otimes_{i=1}^r G_i \leq G^*$,

Sőt az is kiszámítható (szintén a kínai maradéktétellel), hogy

$$G \triangleleft G^* . \quad (14)$$

Mivel a 6. definícióban az n_i -k ($i = 1, 2, \dots, r$) általában nem lesznek páronként relatív prímek, ezért (13) helyett nem állhat (10), vagyis a fúzió általában nem független a tényezők prezentációjától.

Például

$$(7|2|3) \otimes (9|4|3) = (63|58|3) \cong (63|25|3) = (9|7|3) \otimes (7|4|3),$$

és

$$(7|4|3) \otimes (9|4|3) = (63|4|3) \cong (63|16|3) = (9|7|3) \otimes (7|2|3),$$

ugyanakkor a PRET szerint

$$(63|25|3) \text{ nem izomorf } (63|4|3) \text{ - mal.}$$

7. DEFINÍCIÓ A G_1 és G_2 csoportokat **izostruktúrális**aknak nevezzük,

jelben $G_1 \sim G_2$, ha fúziós felbontásukban azonos számú

tényező van, és e tényezők csak a prezentációjukban különböznek

egymástól. (Az izostrukturalitás nyilván ekvivalenciareláció.)

A közelebbi vizsgálat azt mutatja, hogy izostruktúrális csoportok

részcsoporthálója ugyanolyan, az egymásnak megfelelő hálószemek

vagy izostruktúrálisak, vagy izomorfak. Ezen felül az izostruktúrális

csoportok automorfizmuscsoportjai is izomorfak.

A $(63|4|3)$ és $(63|25|3)$ csoportok esetében például a hálók

megfelelő szemei - a legfelső kivételével - izomorfak egymással.

A fúziót azért kellett \mathfrak{S} - prezentációkra korlátozni, mert különben zavaró többértelműségek lépnének föl.

Tekintsük például a következőket : (2004.9.5 e Eredeti kézirat 21. oldala jön)

$$(3|2|2) \otimes (7|2|6), (3|2|6) \otimes (7|2|3), (3|2|2) \otimes (7|2|3).$$

Formálisan elvégezve a fúziót, mindhárom esetben a

$(21|2|6)$ csoportot kapnánk, holott a PART(c) szerint csakis a

$$(21|2|6) = (3|2|2) \otimes (7|2|3) \text{ felbontás lehet helyes.}$$

8. DEFINÍCIÓ: Az $(m|k|n)$ csoportot magnak nevezzük pont akkor, ha az m egy prím hatványa. A magok halmazát \mathfrak{K} fogja jelölni.

4. TÉTEL: (SAT = az \mathfrak{S} alaptétele):

Bármely \mathfrak{S} csoport fölírható (esetleg prímhatványrendű ciklusokkal szorzott) magok fúziójaként.

Mivel a fúzió a definícióból következőleg kommutatív és asszociatív, ez a felírás

A sorrendtől független, de – miként a fúzió általában – nem független a tényezők prezentációjától.

Bizonyítás: Elegendő a tételbeli fogalmak definícióira, az ABEL – csoportok alaptételére és a PART –ra hivatkozni.

Q. E. D.

Különös sajátosságai a fúzióknak az alábbiak:

(C) Ha $G = G_1 \otimes G_2$ és $H_i \leq G_i$, $i = 1, 2$, akkor

$H_1 \otimes H_2$ általában nem része G -nek.

Például $(5 \mid 3 \mid 4) \otimes (7 \mid 3 \mid 6) = (35 \mid 3 \mid 12)$,

$D_5 \leq (5 \mid 3 \mid 4)$, $D_7 \leq (7 \mid 3 \mid 6)$, de

$D_5 \otimes D_7 = D_{35} \not\leq (35 \mid 3 \mid 12)$.

(D) Diédercsoportok fúziója – már ha egyáltalán elvégezhető – ismét diédercsoport.

E sajátosságok a direkt szorzatéival éppen ellentétesek, hiszen ha (a) – ban

\otimes helyett \times állna, akkor $H_1 \times H_2$ igenis része volna $G_1 \times G_2$ –nek.

Másrészt diédercsoportok direkt szorzata sem nem diédercsoport,

sem nem CYCYS – beli.

3. LEMMA Legyen $(m \mid k \mid n)_a^b = G$. Akkor

(C) $G \in \text{SOL}$,

(D) $G \in \text{DIV}$.

Bizonyítás: Az (i) – re többféle igazolás kínálkozik.

A legkézenfekvőbb arra hivatkozni, hogy a

$$G \triangleright \langle a \rangle \triangleright 1$$

egy olyan normállánc, melynek faktorai abelianok.

A legbonyolultabb viszont az (ii) \Rightarrow (i), azaz a

$$\text{DIV} \subset \text{SOL}$$

tartalmazás igazolása, amelyhez a HALL – tételre van szükség.

Az (ii) – hez elég belátni, hogy ha $s \mid m$ és $t \mid n$, akkor

$$\langle a^s, b^t \rangle \leq G. \quad \text{Q. E. D.}$$

4. LEMMA

(C) Minden $G \in \text{CYCYS}$ előáll egy alkalmas \mathfrak{S} csoport részeként.

(D) Minden $G \in \text{CYCYS}$ része valamely ciklus holomorfiának.

Bizonyítás: (a) Ha $G \in \mathfrak{S}$, akkor nincs mit bizonyítani,

ezért tegyük föl, hogy $G = (m \mid k \mid n \cdot s)$, és $s > 1$.

A DIRICHLET – tétel szerint található olyan p prím, amelyre teljesül, hogy

$$p > m, \quad \text{és} \quad ns \mid p - 1.$$

Tekintsük az

$$(m \mid k \mid n) \otimes (p \mid k_p \mid \cdot(n s)) = (mp \mid 1 \mid \cdot(n s))_b^a$$

fúziót! Világos, hogy $\langle a^p, b \rangle \cong G$.

(b) Az (a) miatt elegendő \mathfrak{S} – csoportokra szorítkozni.

Nyilvánvaló, hogy

$$(m \mid k \mid n) \leq \text{Hol}(m) \cong (m) \cdot \mathbf{R}_m, \quad (15),$$

hiszen $\langle k \rangle \leq \mathbf{R}_m$.

(Később meg fogjuk mutatni, hogy (15) –ben pontosan akkor van egyenlőség,

ha $(m \mid k \mid n)$ speciális tulajdonságú, ld. 84 – 89 oldal.) Q. E. D.

II. RÉSZ. REPREZENTÁCIÓK

(A) A legegyszerűbb a $Z_m \times Z_n$ – ben való ábrázolás.

A szorzási szabály:

$$\forall \alpha_1, \alpha_2 \in Z_m, \quad \forall \beta_1, \beta_2 \in Z_n :$$

$$(\alpha_1, \alpha_2) \cdot (\beta_1, \beta_2) = (\alpha_1 + \alpha_2 \cdot k^{\beta_1}, \beta_1 + \beta_2).$$

Könnyen kiszámolható, hogy az

$$a = (1, 0) \quad , \quad b = (0, 1)$$

generátorokkal valóban az $(m | k | n)_a^b$ csoportot kapjuk.

(C) Egyszerű számolás mutatja, hogy az alábbi, modulo m vett mátrixokkal való reprezentáció az $(m | k | n)_a^b$ csoportokra megfelelő:

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}.$$

(D) Permutációkkal való reprezentációk.

1. LEMMA: A $G = (m | k | n)_a^b$ csoportnak létezik izomorf képe

az S_m – ben .

Bizonyítás: Két általános csoportelméleti tételre támaszkodunk:

(i) Ha $N \triangleleft G$ és $N \cap \partial(G) = 1$, akkor $N \leq \zeta(G)$.

(ii) Ha a véges G csoportban létezik egy olyan k indexű H részcsoport, amelynek összes G – beli konjugáltja csak triviálisan metsződik,

akkor G izomorf módon leképezhető S_k – ba.

Mármost jelölje B a $\langle b \rangle$ összes konjugáltját G – ben . Nyilván $B \triangleleft G$, de

$B \cap \partial(G) = 1$, hiszen már $\langle b \rangle \cap \partial(G) = 1$. (Azt, hogy $\partial(G) \leq \langle a \rangle$, lásd a III.

részben.) Akkor viszont (i) miatt $B \leq \zeta(G)$. Mivel $G \in \mathfrak{S}$, ezért

$\zeta(G) \leq \langle a \rangle$ (ld. III. rész), s így $B \cap \partial(G) = 1$. Mindebből $B = 1$ következik,

s mivel $\langle b \rangle$ indexe G – ben m , az (ii) – vel kapjuk az állítást. Q. E. D.

A permutációkkal való reprezentációk bemutatása előtt állapodjunk meg a permutációk szorzási szabályában. Hasonak az A, B, \dots, Z permutációk az Ω jegyhalmazon, és legyen $i \in \Omega$. Akkor

$$A B \dots Z (i) = A(B(\dots(Z (i)) \dots)) .$$

Szorítkozzunk egyenlőre az \mathfrak{S} – csoportokra, és a jegyhalmaz legyen a

$$Z_m = \{ 0, 1, 2, 3, \dots, m-1 \} .$$

Az $(m | k | n)_a^b$ egy jó reprezentációját kapjuk az S_m – ben a következőképpen:

az a és a b hatása legyen az alábbi:

$$\forall i \in Z_m : a (i) = i + 1 \pmod{m},$$

$$b (i) = k \cdot i \pmod{m} .$$

Az rögtön világos, hogy az a egy m hosszúságú ciklus, azaz

$$|a| = m.$$

A b – nél kicsit más a helyzet, mert a b általában diszjunkt ciklusok szorzataként adódik. Kérdés, hogy milyen hosszúak ezek a ciklusok?

Legyen $i \in \mathbf{Z}_m$, és tegyük fel, hogy

$$b^x(i) = i,$$

azaz $k^x(i) \equiv i \pmod{m}$.

Ebből következik, hogy ha $i \in \mathbf{R}_m$ akkor $x = n$, és ha $i \nmid m$, akkor $x \nmid n$.

(Az az eset, midőn $i \nmid m$, de $(i, m) > 1$, visszavezethető az $i \mid m$ esetre.)

Ez egyszerűen azért van így, mert általában $|k|_{m'} \mid |k|_m$ ha $m' \mid m$.

Más szóval: $m' \mid m \Rightarrow \mathbf{R}_{m'} \leq \mathbf{R}_m$.

Legyen ugyanis $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_r^{\alpha_r}$, ahol a p_i –k páronként különböző

prímek ($i = 1, 2, \dots, r$), és legyen $m' = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \dots p_r^{\beta_r}$, $0 \leq \beta_i \leq \alpha_i$ ($i = 1, 2, \dots, r$)

Akkor triviális, hogy

$$\mathbf{R}_{m'} = \mathbf{R}_{p_1^{\beta_1}} \times \mathbf{R}_{p_1^{\beta_2}} \times \dots \times \mathbf{R}_{p_1^{\beta_r}} \leq \mathbf{R}_{p_1^{\alpha_1}} \times \mathbf{R}_{p_1^{\alpha_2}} \times \dots \times \mathbf{R}_{p_1^{\alpha_r}} = \mathbf{R}_m.$$

Tehát b olyan diszjunkt ciklusok szorzata lesz, amelyeknek hossza osztja az n -t, és feltétlenül lesz közöttük n hosszúságú is. Ezért

$$|b| = n.$$

A $ba = a^k b$ reláció ellenőrzése is nagyon könnyű:

$$\forall i \in \mathbf{Z}_m : b a(i) = b(i+1) = k \cdot (i+1) = k \cdot i + k,$$

$$a^k b(i) = a^k(k \cdot i) = k \cdot i + k,$$

ami teljessé teszi annak igazolását, hogy valóban jó S_m – beli reprezentációt

kaptunk.

Egy gazdaságosabb reprezentációra is van lehetőség, amely a fúzió alapul.

Ezt egy konkrét példán keresztül érthetjük meg a legjobban.

Legyen az ábrázolandó csoport a

$$(3 \mid 2 \mid 2) \otimes (4 \mid 3 \mid 2) \otimes (5 \mid 3 \mid 4) = (60 \mid 23 \mid 4) .$$

Készítsük el a fúziós tényezők reprezentációit az előbb ismertetett módon:

$$(3 \mid 2 \mid 2)_{a_1}^{b_1}: a_1 = (012), b_1 = (12),$$

$$(4 \mid 3 \mid 2)_{a_2}^{b_2}: a_2 = (0123), b_2 = (13),$$

$$(5 \mid 3 \mid 4)_{a_3}^{b_3}: a_3 = (01234), b_3 = (1342) .$$

Kódoljuk át az a_2 és a_3 -at úgy, hogy egymással és az a_1 -gyel is diszjunktak

legyenek: $a_2 = (3456), a_3 = (7 \ 8 \ 9 \ 10 \ 11),$

és megfelelően $b_2 = (46), b_3 = (8 \ 10 \ 11 \ 9) .$

Most legyen $a = a_1 a_2 a_3 = (012)(3456)(7 \ 8 \ 9 \ 10 \ 11),$

$$b = b_1 b_2 b_3 = (12)(46)(8 \ 10 \ 11 \ 9),$$

és egyszerű számolással igazolható, hogy valóban a $(60 \mid 23 \mid 4)_a^b$ csoportot

kaptuk, mégpedig S_{60} helyett az $S_{3+4+5} = S_{12}$ -ben .

Ez a módszer teljes általánosságban alkalmazható, és az az eredménye, hogy

ha $m = m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_r$, ahol az m_i -k páronként relatív prímek, akkor az

$(m \mid k \mid n)$ csoportot az $S_{m_1 + m_2 + \dots + m_r}$ szimmetrikus csoportban sikerül

ábrázolni az $S_{m_1 \cdot m_2 \cdot \dots \cdot m_r} = S_m$ helyett.

Márpedig $m_1 + m_2 + m_3 + \dots + m_r \leq m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_r$,

és itt egyenlőség csakis akkor van, ha az m – nek csak egyetlen prímtényezője van. Eredményünk tehát ez:

2. LEMMA: Legyenek az $m_1, m_2, m_3, \dots, m_r$ számok páronként relatív prímek.

Akkor az $(m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_r \mid k \mid n)$ csoportnak létezik az

$S_{m_1 + m_2 + \dots + m_r}$ szimmetrikus csoportban izomorf képe. Q. E. D.

Az \mathcal{S} – en kívüli csoportok reprezentációja most már könnyű:

Ha az $(m \mid k \mid n \cdot s)_a^{b^*}$, $s > 1$ csoportot akarjuk ábrázolni, akkor

$$a = (0 \ 1 \ 2 \ \dots \ m-1),$$

$$b^* = b \cdot (\beta_1 \ \beta_2 \ \beta_3 \ \dots \ \beta_{ns})$$

ahol b a $(m \mid k \mid n)_a^b$ csoporthoz a szokásos módon megszerkesztett permutáció

és a $(\beta_1 \ \beta_2 \ \beta_3 \ \dots \ \beta_{ns})$ diszjunkt a –val és b –vel is.

A $(60 \mid 23 \mid 8)_a^{b^*}$ esetében például

$$b^* = (12)(46)(8 \ 10 \ 11 \ 9)(12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19).$$



b

III. RÉSZ. NEVEZETES RÉSZCSOPORTOK.

p – CSOPORTOK. NILPOTENCIA

(C) Kommutátor, Centrum, Frattini – részcsoport.

Legyen $G = (m | k | n)_a^b$.

1.LEMMA: $\partial(G) = \langle a^{k-1} \rangle = \langle a^{(m,k-1)} \rangle$.

Bizonyítás: Az I. rész (1) – ből azonnal következik. Q. E. D.

1. DEFINÍCIÓ: A G -t \cong – csoportnak nevezzük pont akkor, ha

$$(m, k - 1) = 1.$$

Ekkor nyilván $\partial(G) = \langle a \rangle$ és $G / \partial(G) = \langle b \rangle$.

COXETER Z – metaciklikusnak nevez egy csoportot, ha mind a kommutátora,

Mind a kommutátor szerinti faktorcsoportja ciklikus.

ZASSENHAUS bebizonyította, hogy minden véges Z – metaciklikus csoport

előállítható \cong – csoportként.

2. LEMMA: $\zeta(G) = \zeta_e(G) \times \zeta_h(G)$, ahol

$\zeta_e(G) = \langle a^{\frac{m}{(m,k-1)}} \rangle$ az ún. első centrum,

$\zeta_h(G) = \langle b^\beta \rangle$ az ún. hátsó centrum, és β kielégíti a $k^\beta = 1$ relációt.

Bizonyítás: közvetlen számolással. Q. E. D.

3. LEMMA: $\zeta(G) = 1 \Leftrightarrow G \in \cong \cap \mathcal{S}$.

Bizonyítás: Az állítás az 1. és 2. lemma következménye. Q. E. D.

Az 1. és 2. lemmákból kiolvasható, hogy

$$2 \leq |\partial(G)| \leq m,$$

$$1 \leq |\zeta_e(G)| \leq \frac{m}{2}, \text{ és}$$

$$|\partial(G)| = 2 \Leftrightarrow |\zeta_e(G)| = \frac{m}{2},$$

$$|\partial(G)| = m \Leftrightarrow |\zeta_e(G)| = 1.$$

Ezek az összefüggések jól mutatják a kommutátor ($\partial(G)$) és az első centrum ($\zeta_e(G)$) közötti sajátos „komplementaritást”.

4. LEMMA: Ha $G_i \in \mathfrak{S} \cap \mathfrak{S}, 1 = 1, 2, \dots, r$, akkor

$$\bigotimes_{i=1}^r G_i \in \mathfrak{S} \cap \mathfrak{S}.$$

Bizonyítás: Egyszerű számelméleti megfontolásokkal az $\mathfrak{S}, \mathfrak{S}$ és a \otimes definíciója alapján. Q. E. D.

5. LEMMA:

(i) Ha m páros, akkor $|\zeta_e(G)| \geq 2$.

(ii) Ha m páros és n páratlan, akkor G – nek van egy olyan centrális faktora, amelynek rendje a 2 valamely pozitív hatványa.

(iii) $a^{[k|n]} \in \zeta_e(G)$.

Bizonyítás: (i) Az m párossága miatt k – nak páratlannak kell lennie, ám ekkor

$$k - 1 \text{ ismét páros, ezért } |\zeta_e(G)| = (m, k - 1) \geq 2.$$

(ii) Legyen $m = 2^\alpha \cdot m_1$, $\alpha \geq 1$, $m_1 > 1$, és $(2, m_1) = 1$. Ha n páratlan, akkor kl_m is az, ezért k csakis R_{m_1} -beli lehet, vagyis $k \equiv 1 \pmod{2^\alpha}$.

De akkor a PRET (a) szerint a (2^α) ciklus kiemelhető G -ből.

(iii) $b a^{[k|n]} = a^{k \cdot [k|n]} b = a^{(k-1) \cdot [k|n]} b = a^{(k-1) \cdot [k|n]} a^{[k|n]} b = a^{[k|n]} b$,

hiszen $(k-1) \cdot [k|n] = k^n - 1 \equiv 0 \pmod{m}$. Q. E. D.

2. DEFINÍCIÓ: A G első – illetve hátsó Frattini – részcsoportján a

$$\Phi_e(G) = \Phi(G) \cap \langle a \rangle, \text{ illetve a}$$

$$\Phi_h(G) = \Phi(G) \cap \langle b \rangle$$

csoportot értjük.

Tekintsük a G egy tetszőleges $a^\alpha b^\beta$ elemét.

Ha $\alpha \in R_m$, akkor $\langle a^\alpha b^\beta, b \rangle \in \text{MGR}(G)$,

Ha pedig $\beta \in R_n$, akkor $\langle a, a^\alpha b^\beta \rangle \in \text{MGR}(G)$.

Ezekben az esetekben tehát $a^\alpha b^\beta \notin \Phi(G)$.

Tegyük föl, hogy $\alpha \notin R_m$ és $\beta \notin R_n$.

Ha $p \in \pi(m)$, és $p \nmid \alpha$, akkor

$$a^\alpha b^\beta \notin \langle a^p, b \rangle \in \text{MAX}(G),$$

ezért $\langle a^p, b, a^\alpha b^\beta \rangle \in \text{MGR}(G)$.

Hasonlóan, ha $q \in \pi(n)$, és $q \nmid \beta$, akkor

$$a^\alpha b^\beta \notin \langle a, b^q \rangle \in \text{MAX}(G),$$

s így $\langle a, b^q, a^\alpha b^\beta \rangle \in \text{MGR}(G).$

Kaptuk, hogy az $a^\alpha b^\beta$ elem egyik esetben sem tartozhat $\Phi(G)$ – hez.

Ezek szerint $\Phi(G) \leq \langle a^{p_1 p_2 \dots p_r}, b^{q_1 q_2 \dots q_s} \rangle,$

ahol $\{p_1, p_2, p_3, \dots, p_r\} = \pi(m),$

$$\{q_1, q_2, q_3, \dots, q_s\} = \pi(n).$$

Mivel $\langle a \rangle \triangleleft G$, ezért

$$\Phi(a) = \langle a^{p_1 p_2 \dots p_r} \rangle \leq \Phi(G),$$

amiből máris következik, hogy

$$\Phi(G) = \langle a^{p_1 p_2 \dots p_r}, b^\gamma \rangle, \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} (\star)$$

ahol $\forall q \in \pi(n): q \mid \gamma.$

A következőket láttuk be:

6. LEMMA: (i) $\Phi(G) = \Phi_e(G) \Phi_h(G),$

(ii) $\Phi_e(G) = \Phi(a).$ Q. E. D.

Általában $\Phi_h(G) \neq \Phi(b)$. Ha például $G = (p \mid k \mid \cdot(p-1)), p \in \mathbf{P}_0$, akkor

Könnyen kiszámolható, hogy $\Phi_h(G) = 1$. Biztosan nagyobb lesz azonban a

$\Phi_h(G)$ 1 – nél, ha G egy s – csoport homológja.

7. LEMMA: Legyen $G = (m \mid k \mid \overset{\bullet}{n} s)_a^b$, ahol

$$\pi(s) \subseteq \pi(n) = \{q_1, q_2, q_3, \dots, q_t\}, s > 1.$$

Akkor $\langle b^n \rangle \leq \Phi(G)$.

Bizonyítás: Mivel $\langle b^n \rangle \triangleleft G$ és $\langle b^n \rangle \leq \Phi(b) = \langle b^{q_1 \dots q_t} \rangle$, alkalmazhatjuk azt

Az általános csoportelméleti tételt, miszerint ha $A \leq G$ és $N \leq \Phi(A)$, akkor

$N \leq \Phi(G)$, mégpedig az $N = \langle b^n \rangle$, $A = \langle b \rangle$ szereposztással. Q. E. D.

8. LEMMA:

(i) $\xi(\bigotimes_{i=1}^r G_i) = \bigotimes_{i=1}^r \xi(G_i)$, ahol ξ a ∂ , ζ_e , Φ_e valamelyike;

(ii) $\Phi(\bigotimes_{i=1}^r G_i) \leq \Phi(\bigotimes_{i=1}^r G_i) = \bigotimes_{i=1}^r \Phi(G_i)$.

Bizonyítás: Az (i) közvetlen számolással belátható a definíciók alapján,

az (ii) pedig az I. rész (14) (19. o.) következménye. Q. E. D.

(D) p – CSOPORTOK. NILPOTENCIA.

3. DEFINÍCIÓ: A CYCYS-beli p – csoportok ($p \in \mathbf{P}$) halmazát \mathcal{P} ,

a nilpotensekét \mathcal{N} fogja jelölni.

9. LEMMA: A $\mathcal{P} \cap \mathcal{N}$ elemei az alábbiak:

$$p \in \mathbf{P}_0 : (p^\alpha \mid p^{\alpha-\beta} + 1 \mid p^\beta), \alpha \geq 2, \alpha > \beta \geq 1 \quad (1a)$$

$$p = 2 : (2^\alpha \mid 2^{\alpha-\beta} + 1 \mid 2^\beta), \alpha \geq 3, \alpha - 1 > \beta \geq 1 \quad (1b)$$

$$(2^\alpha \mid 2^{\alpha-\beta} - 1 \mid 2^\beta), \alpha \geq 3, \alpha - 1 > \beta \geq 1 \quad (1c)$$

$$(2^\alpha \mid 2^\alpha - 1 \mid 2) \cong D 2^\alpha, \alpha \geq 2. \quad (1d)$$

Bizonyítás: A következő számításokban főleg az I. rész 2. lemmabeliekre

támaszkodtunk:

(1a) Az igazolandó, hogy $\mid p^{\alpha-\beta} + 1 \mid p^\alpha = p^\beta$. Ehelyett

a következőt látjuk be:

$$\mid s \cdot p^{\alpha-\beta} + 1 \mid p^\alpha = p^\beta, \text{ ahol } (s, p) = 1.$$

Legyen $0 \leq \gamma < \beta$, akkor

$$\begin{aligned} (s \cdot p^{\alpha-\beta} + 1)^{p^{\beta-\gamma}} - 1 &= s \cdot p^{\alpha-\beta} \cdot [s \cdot p^{\alpha-\beta} + 1 \mid p^{\beta-\gamma}] = \\ &= s \cdot p^{\alpha-\beta} \cdot [s \cdot p^{\alpha-\beta} + 1 \mid p] \cdot [(s \cdot p^{\alpha-\beta} + 1)^p \mid p] \cdot \dots \cdot [(s \cdot p^{\alpha-\beta} + 1)^{p^{\beta-\gamma-1}} \mid p]. \end{aligned}$$

Elemi módon kiszámolható, hogy

$$p \parallel [(s \cdot p^{\alpha-\beta} + 1)^{p^\delta} \mid p], \quad 0 \leq \delta \leq \beta - \gamma - 1,$$

$$\text{és így } (s \cdot p^{\alpha-\beta} + 1)^{p^{\beta-\gamma}} - 1 = A \cdot s \cdot p^{\alpha-\gamma}, \quad p \nmid A,$$

ami pontosan akkor kongruens 0-val modulo p^α , ha $\gamma = 0$.

(1b) $p = 2$ -vel pontosan ugyanaz a számítás menete, mint (1a) -nál.

(1c) Most is azt igazoljuk, hogy

$$\mid s \cdot 2^{\alpha-\beta} + 1 \mid 2^\alpha = 2^\beta, \quad \text{ahol } (2, s) = 1.$$

Legyen ismét $0 \leq \gamma < \beta$.

$$\begin{aligned}
 (s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-\gamma}} - 1 &= s \cdot 2^{\alpha-\beta} \cdot [s \cdot 2^{\alpha-\beta} - 2 \mid 2^{\beta-\gamma}] = \\
 &= (s \cdot 2^{\alpha-\beta} - 2) \cdot [s \cdot 2^{\alpha-\beta} - 1 \mid 2^{\beta-\gamma}] = \\
 &= (s \cdot 2^{\alpha-\beta} - 2) \cdot [s \cdot 2^{\alpha-\beta} - 1 \mid 2] \cdot [(s \cdot 2^{\alpha-\beta} - 1)^2 \mid 2] \cdot \dots \cdot [(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-\gamma-1}} \mid 2]. \\
 &= 2 \cdot (s \cdot 2^{\alpha-\beta-1} - 1) \cdot s \cdot 2^{\alpha-\beta} \cdot [(s \cdot 2^{\alpha-\beta} - 1)^2 \mid 2] \cdot \dots \cdot [(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-\gamma-1}} \mid 2].
 \end{aligned}$$

Könnyű kiszámolni, hogy

$$2 \parallel [(s \cdot 2^{\alpha-\beta} - 1)^{2^\delta} \mid 2], \quad 1 \leq \delta \leq \beta - \gamma - 1,$$

ezért $(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-\gamma}} - 1 = 2 \cdot (s \cdot 2^{\alpha-\beta-1} - 1) \cdot s \cdot 2^{\alpha-\beta} \cdot 2^{\beta-\gamma-1} \cdot A$,

ahol $2 \nmid A$, azaz $(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-\gamma}} - 1 \equiv 2^{\alpha-\beta} \cdot B$, $(B, 2) = 1$.

Ez csakis akkor kongruens 0-val modulo 2^α , ha $\gamma = 0$.

(1d) Az, hogy $|s \cdot 2^\alpha - 1|_{2^\alpha} = 2$, $(2, s) = 1$, egészen triviális.

Q. E. D.

A \mathfrak{p} mármost a 9. lemmabeli p – magokból és azok homológjaiból áll.

10. LEMMA: Valamely adott $p \in \mathbf{P}$ esetén jelölje G_p a \mathfrak{p} egy elemét.

Akkor bármely $G \in \mathcal{N}$ csoport felírható $G = \left(\prod_{i=1}^r G_{p_i} \right) \times (q)$ (2)

alakban, ahol a p_i -k páronként különböző prímek ($i = 1, 2, \dots, r$), valamint
 $(p_1, p_2, p_3, \dots, p_r, q) = 1$.

Bizonyítás: Közvetlenül a nilpotencia definíciója alapján. Q. E. D.

11. LEMMA $\partial(G) \leq \zeta_e(G) \Rightarrow G \in \mathcal{N}$.

Bizonyítás: Legyen $G = (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \mid k \mid n)$, ahol a p_i -k páronként
különböző prímek ($i = 1, 2, \dots, r$). Elemi számolással adódik

hogy $\partial(G) \leq \zeta_e(G) \Leftrightarrow (k-1)^2 \equiv 0 \pmod{p_1^{\alpha_1} \dots p_r^{\alpha_r}}$.

Ebből következik, hogy $p_i^{\varepsilon_i} \mid k-1$, ahol $\varepsilon_i \geq \frac{\alpha_i}{2}$, $i = 1, 2, \dots, r$.

Eszerint $k = s \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \dots \cdot p_r^{\varepsilon_r} + 1$, $(s, p_1 p_2 \dots p_r) = 1$,

ami azt jelenti, hogy G az (1a) vagy (1b) típusú p -magok (vagy homológjaik)
direkt szorzata, esetleg valamilyen konstansokkal bővítve, vagyis G (2) alakú.

Q. E. D.

12. LEMMA Legyen G olyan, mint a 11. lemmában, de legyen még

$\alpha_i \geq 2$, $i = 1, 2, \dots, r$. Akkor

$\Phi_e(G) \leq \zeta_e(G) \Rightarrow G \in \mathcal{N}$.

Bizonyítás: $\Phi_e(G) = \langle a^{p_1 \dots p_r} \rangle \leq \zeta_e(G)$ pontosan akkor, ha

$k-1 \equiv 0 \pmod{p_1^{\alpha_1-1} \dots p_r^{\alpha_r-1}}$.

$$\text{Ámde ekkor } |\partial(G)| = \frac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}}{(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}, k-1)} = d,$$

$$|\Phi_e(G)| = p_1^{\alpha_1-1} \cdot \dots \cdot p_r^{\alpha_r-1} = f, \text{ és } d \mid f, \text{ tehát } \partial(G) \leq \Phi_e(G). \quad \text{Q. E. D.}$$

A $(27 \mid 4 \mid 9)$ csoport példája mutatja, hogy a 11. és 12. lemma feltételei csupán elégségesek, de nem szükségesek a nilpotenciához.

E csoportban ugyanis $\zeta_e(G) < \partial(G) = \Phi_e(G)$.

13. LEMMA Ha $G = (m \mid k \mid n)_a^b \in \mathcal{N}$, akkor $\Phi_h(G) = \Phi(b)$.

Bizonyítás: Felhasználva azt a tételt, miszerint egy direkt szorzat

Frattini – részcsoportha megegyezik a tényezők Frattini – részcsoportha direkt szorzatával, elegendő az állítást $G \in \mathcal{P}$ esetre belátni. Ha azonban

$G \in \mathcal{P}$, akkor alkalmazhatjuk azt a szintén jól ismert tételt, amely szerint

ha G p – csoport, ($p \in \mathbf{P}$), és $H \leq G$, akkor $\Phi(H) \leq \Phi(G)$.

Elég a H –t azonosítani $\langle b \rangle$ – vel. Q. E. D.

(C) További vizsgálatok a Frattini – részcsoportha kapcsolatban:

14. LEMMA Legyen $G = (p^\alpha \mid k \mid \cdot p^\beta q)_a^b$, ($p \in \mathbf{P}$), $q \mid p-1$.

Akkor $\Phi_h(G) = \langle b^{pq} \rangle$.

Bizonyítás: Tudjuk, hogy $\Phi_h(G) = \langle b^\gamma \rangle$, ahol a (\star) szerint (24. o.) $p \mid \gamma$.

Mivel $\Phi(G) = \langle a^p, b^\gamma \rangle \triangleleft G$, ezért $k^\gamma \equiv 1 \pmod{p}$

lásd I. rész 1. LEMMA (VI) (5. o.), amiből $q \mid \gamma$ adódik.

Kaptuk tehát, hogy $pq \mid \gamma$.

Mármost az $\langle a, b^\gamma \rangle$ részcsoport egyrészt normális G -ben, másrészt p -csoport,

így (a 13. LEMMA segítségével) $\Phi(\langle a, b^\gamma \rangle) = \langle a^p, b^\gamma \rangle \leq \Phi(G)$,

amiből $\gamma \mid pq$. Nyertük tehát, hogy $pq \mid \gamma$ és $\gamma \mid pq$, azaz $\gamma = pq$. Q. E. D.

2006.05.05. Eredeti kézirat 51. oldalától:

Legyen adva r számú mag: $G_i = (p_i^{\alpha_i} \mid k \mid \bullet p_i^{\beta_i} q_i)$, (3)

ahol a p_i -k páronként különböző prímek, és $q_i \mid p_i - 1$, $i = 1, 2, \dots, r$.

Ezek fúziójának felírásához legyen $q_i = p_1^{\delta_{1i}} \cdot p_2^{\delta_{2i}} \cdot p_3^{\delta_{3i}} \cdot \dots \cdot p_r^{\delta_{ri}} \cdot \bar{q}_i$,

$(p_1 p_2 \dots p_r, \bar{q}_i) = 1$, $i = 1, 2, \dots, r$.

(Ha fölteszük, hogy $p_1 < p_2 < \dots < p_r$, akkor világos, hogy

$j \geq i$ esetén $\delta_{ji} = 0$.)

Akkor $[q_1, q_2, \dots, q_r] = p_1^{\delta_1} p_2^{\delta_2} \dots p_r^{\delta_r} [\bar{q}_1, \bar{q}_2, \dots, \bar{q}_r]$,

ahol $\delta_i = \max(\delta_{i1}, \delta_{i2}, \dots, \delta_{ir})$, $i = 1, 2, \dots, r$,

és így $[p_1^{\beta_1} q_1, p_2^{\beta_2} q_2, \dots, p_r^{\beta_r} q_r] = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_r^{\varepsilon_r} q$,

ahol $\varepsilon_i = \max(\delta_i, \beta_i)$, $i = 1, 2, \dots, r$, és $q = [\bar{q}_1, \bar{q}_2, \dots, \bar{q}_r]$.

A (3) magok fúziója tehát így írható fel:

$$G = \bigotimes_{i=1}^r G_i = (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \mid k \mid p_1^{\varepsilon_1} p_1^{\varepsilon_1} \dots p_1^{\varepsilon_1} q)_a^b \quad (4)$$

Tudjuk, hogy $\Phi(G) = \langle a^p, b^\gamma \rangle$, ahol most $p = p_1 p_2 \dots p_r$.

$\Phi(G) \triangleleft G$ miatt $k^\gamma \equiv 1 (p)$, és ebből következik, hogy

$$q_i \mid \gamma, i = 1, 2, \dots, r, \text{ tehát } [q_1, q_2, \dots, q_r] \mid \gamma.$$

$$\text{Kaptuk, hogy } p_1^{\delta_1} p_2^{\delta_2} \dots p_r^{\delta_r} q \mid \gamma. \quad (5)$$

4. DEFINÍCIÓ: $(m \mid k \mid n) \in \mathcal{R} \Leftrightarrow (m, n) = 1$.

15. LEMMA:

$$(i) \quad \text{Ha } G_i \in \mathcal{R} \cap \mathcal{S}, i = 1, 2, \dots, r, \text{ akkor } \Phi_h \left(\bigotimes_{i=1}^r G_i \right) = 1.$$

$$(ii) \quad G \in \mathcal{R} \cap \mathcal{S} \text{ esetén } \Phi_h(G) = 1.$$

$$(iii) \quad \text{Ha a (3) magok olyanok, hogy } p_i \nmid q_j, i, j = 1, 2, \dots, r, \quad (6)$$

$$\text{akkor } \Phi \left(\bigotimes_{i=1}^r G_i \right) = \prod_{i=1}^r \Phi(G_i).$$

Bizonyítás: (i) Ha $G_i \in \mathcal{R} \cap \mathcal{S}, i = 1, 2, \dots, r$, akkor (3)-ban $\beta_i = 0$

és (4)-ben $\varepsilon_i = \delta_i$. Innen az (5) adja az állítást.

$$(ii) \quad \text{Ez (i) -ből folyik, de most } \varepsilon_i = \delta_i = 0, i = 1, 2, \dots, r.$$

$$(iii) \quad \text{Ebben az esetben nyilván } \delta_i = 0, \varepsilon_i = \beta_i, i = 1, 2, \dots, r.$$

Könnyű kiszámolni, hogy az $\langle a, b^q \rangle$ részcsoport most nilpotens

(és persze normális), és így a 13. és 14. lemmák fölhasználásával

adódik az állítás.

Q. E. D.

Ha a (6) feltétel nem teljesül, akkor a Φ meghatározása igen bonyodalmas lehet. Legyenek p_1, p_2 prímek, $p_1 < p_2$. Tekintsük a

$$G_1 = (p_1^{\alpha_1} \mid k_1 \mid \bullet p_1^{\beta_1} q_1) ,$$

$$G_2 = (p_2^{\alpha_2} \mid k_2 \mid \bullet p_2^{\beta_2} p_1^{\delta} q_2) \text{ magokat, ahol}$$

$$\beta_1 \geq 0, 1 \leq q_1 \mid p_1 - 1, \beta_2 \geq 0, 1 \leq q_2, \delta \text{ és } p_1^{\delta} q_2 \mid p_2 - 1 .$$

$$\text{A két mag fúziója } G = G_1 \otimes G_2 = (p_1^{\alpha_1} p_2^{\alpha_2} \mid k \mid \bullet p_2^{\beta_2} p_1^{\varepsilon} q)_a^b ,$$

ahol $\varepsilon = \max(\beta_1, \delta)$, $q = [q_1, q_2]$. Mi lesz a $\Phi(G)$?

Az előzőekből annyit mindenesetre tudhatni, hogy $\Phi(G) = \langle a^{p_1 p_2}, b^{\gamma} \rangle$,

ahol $p_1^{\delta} q \mid \gamma$. A továbbiakban két eset lehetséges:

$$(a) \quad \varepsilon = \delta \geq \beta_1 .$$

Tekintsük most a $H = \langle a, b^{p_1^{\delta} q} \rangle$ részcsoportot.

Világos, hogy $H \triangleleft G$, ezért $\Phi(H) \leq \Phi(G)$,

$$\text{másképp } H \text{ nilpotens, hiszen } H = (p_1^{\alpha_1} p_2^{\alpha_2} \mid k^{p_1^{\delta} q} \mid p_2^{\beta_2})_a^{p_1^{\delta} q} ,$$

s így $\Phi(H)$ a 13. lemma szerint számolható: $\Phi(H) = \langle a^{p_1 p_2}, b^{p_2 p_1^{\delta} q} \rangle$

Innen következik, hogy $\gamma \mid p_2 p_1^\delta q$, és kaptuk, hogy $p_1^\delta q \mid \gamma \mid p_2 p_1^\delta q$.

Mármost a $\gamma = p_1^\delta q$ eset nem lehetséges, mert

$$\langle a, b^{p_1^\delta q}, b^{p_2^{\beta_2}} \rangle \in \text{MGR}(G). \text{ Ezért } \gamma = p_2 p_1^\delta q \text{ és } \Phi(G) = \langle a^{p_1 p_2}, b^{p_2 p_1^\delta q} \rangle.$$

(b b) $\varepsilon = \beta_1 > \delta$. Ekkor csoportunk $G = (p_1^{\alpha_1} p_2^{\alpha_2} \mid k \mid p_1^{\beta_1} p_2^{\beta_2} q)_a^b$.

Tekintsük most a $H = \langle a, b^{p_1^{\beta_1} q} \rangle$ részcsoportot.

Ismét $H \triangleleft G$, és ezért $\Phi(H) \leq \Phi(G)$.

Másrészt H most is nilpotens, így a 13. lemma segítségével

$$\Phi(H) = \langle a^{p_1 p_2}, b^{p_2 p_1^{\beta_1} q} \rangle.$$

Mindebből azt nyerjük, hogy $p_1^\delta q \mid \gamma \mid p_2 p_1^{\beta_1} q$,

és most csak az zárható ki, hogy $\gamma = p_1^{\beta_1} q$ legyen, ugyanis

$$\langle a, b^{p_2^{\beta_2}}, b^{p_1^{\beta_1} q} \rangle \in \text{MGR}(G).$$

Közelebbi a γ -ról nem mondható.

IV. RÉSZ. AZ AUTOMORFIZMUSOKRÓL ÁLTALÁBAN

Legyen $G = (m | k | n)_a^b$, és φ a G -nek egy permutációja.

Nyilvánvaló, hogy $\varphi \in \text{Aut } G \Leftrightarrow G = (m | k | n)_{\varphi(a)}^{\varphi(b)}$.

Részletesen ez azt jelenti, hogy

$$|\varphi(a)| = m, \quad (1)$$

$$|\varphi(b)| = n, \quad (2)$$

$$\varphi(b)\varphi(a) = \varphi(a)^k\varphi(b) \quad (3)$$

$$\langle \varphi(a) \rangle \cap \langle \varphi(b) \rangle = 1 \quad (4).$$

Előfordulhatnak a következő esetek is:

$$\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle = 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle = 1, \end{array} \left. \vphantom{\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle = 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle = 1, \end{array}} \right\} (5 a)$$

$$\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle \neq 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle = 1, \end{array} \left. \vphantom{\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle \neq 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle = 1, \end{array}} \right\} (5 b)$$

$$\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle = 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle \neq 1, \end{array} \left. \vphantom{\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle = 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle \neq 1, \end{array}} \right\} (5 c)$$

$$\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle \neq 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle \neq 1, \end{array} \left. \vphantom{\begin{array}{l} \text{és} \\ \langle a \rangle \cap \langle \varphi(b) \rangle \neq 1, \\ \langle \varphi(a) \rangle \cap \langle b \rangle \neq 1, \end{array}} \right\} (5 d)$$

Könnyű meggondolni, hogy az (5 b, c, d) esetekben vagy az $\langle a \rangle$ egy része képződik le a $\langle b \rangle$ - be automorf módon, vagy a $\langle b \rangle$ egy része az $\langle a \rangle$ - ba.

(Az (5 d) – nél mindkét eset fönnáll.) Ez nyilvánvalóan csak úgy lehetséges, ha a mondott részek centrálisak, izomorfok, és mind $\langle a \rangle$ - nak, mind $\langle b \rangle$ - nek direkt faktorai. Az alábbi láttuk be:

1. LEMMA: Az (5 b, c, d) szituációk csak akkor fordulhatnak elő, ha

$$G \cong (s) \times (m | k | n) \times (s), \text{ ahol } (mn, s) = 1 \quad (6)$$

Q . E . D .

1. DEFINÍCIÓ: A (6) alakú csoportok halmazát \mathcal{X} fogja jelölni.

Az olyan automorfizmust, amelyre (5 b), (5 c), vagy (5 d) valamelyike fönnáll, keresztező automorfizmusnak (x – automorfizmusnak) nevezzük.

x – automorfizmusa tehát csak \mathcal{X} csoportnak lehet.

Ha G (6) alakú, akkor $\text{Aut } G = \text{Aut } (m | k | n) \times \text{Aut } (s)^2$.

Ezért egy $G \in \mathcal{X}$ csoport automorfizmuscsoportjának kiszámítása mindig visszavezethető egy olyan csoport automorfizmuscsoportjának meghatározására, amely már nem \mathcal{X} beli. Ezért a továbbiakban mindig föltesszük, hogy $G \notin \mathcal{X}$.

A $G = (m | k | n)_a^b$ bármely φ automorfizmusa

$$\begin{aligned}\varphi(a) &= a^\alpha b^\beta, \\ \varphi(b) &= a^\gamma b^\delta\end{aligned}\tag{7}$$

alakú, ahol az $\alpha, \gamma \in \mathbb{Z}_m, \beta, \delta \in \mathbb{Z}_n$ számoknak az (1), (2), (3) – ből
következőleg ki kell elégíteniük az alábbi relációkat:

Az m a legkisebb pozitív egész, amelyre

$$\alpha [k^\beta | m] \equiv 0 \pmod{m}, \tag{K 11}$$

$$\text{és } \beta m \equiv 0 \pmod{n}, \tag{K 12}$$

Az n a legkisebb pozitív egész, amelyre

$$\gamma [k^\delta | n] \equiv 0 \pmod{m}, \tag{K 21}$$

$$\text{és } \delta n \equiv 0 \pmod{n}, \tag{K 22}$$

valamint

$$\gamma + \alpha k^\delta \equiv \gamma k^{\beta k} + \alpha [k^\beta | k] \pmod{m} \tag{K 31}$$

$$\beta (k - 1) \equiv 0 \pmod{n}, \tag{K 32}$$

Ezt a kissé riasztó kongruenciarendszert KÁNON-nak is nevezzük.

Később látni fogjuk, hogy fontos esetekben ezek a relációk jelentősen
egyszerűsíthetők.

2. DEFINÍCIÓ: A $G = (m | k | n)_a^b$ egy φ automorfizmusát egyszerűnek
nevezzük, ha vagy $a - n$, vagy $b - n$ identikusan hat.

Világos, hogy az identikus automorfizmus egyszerű, és egyszerű automorfizmus nem lehet keresztező.

Egy egyszerű automorfizmus megadásánál nem tüntetjük föl azt a generátort, amelyen identikusan hat. Például $\varphi: a \rightarrow a^\alpha b^\beta, b \rightarrow b$ helyett csak annyit írunk, hogy $\varphi: a \rightarrow a^\alpha b^\beta$.

3. DEFINÍCIÓ: Tekintsük a (7) automorfizmust. Ha a $\varphi_1(a) = a^\alpha b^\beta$ és

$\varphi_2(b) = a^\gamma b^\delta$ maguk is (egyszerű) automorfizmusok, akkor azt mondjuk, hogy a

φ a φ_1 és φ_2 fúziója: $\varphi = \varphi_1 \otimes \varphi_2$.

Amennyiben a (7) – beli φ ilyen értelemben nem bontható föl, akkor φ – t csatolt automorfizmusnak, (c – automorfizmusnak) nevezzük, s az ilyen automorfizmusokkal rendelkező csoportok halmazát \mathcal{C} – vel jelöljük.

Világos, hogy a fúzió különbözik a szokásos, o –rel jelölt kompozíciótól:

$\varphi_1 \otimes \varphi_2 \neq \varphi_1 \circ \varphi_2$. Az is nyilvánvaló, hogy $\varphi_1 \otimes \varphi_2 = \varphi_2 \otimes \varphi_1$, és

$\varphi_1 \otimes (\varphi_2 \otimes \varphi_3) = (\varphi_1 \otimes \varphi_2) \otimes \varphi_3$.

A $A G = (16 | 3 | 4)_a^b$ példája mutatja, hogy \mathcal{C} nem üres.

A G – nek ugyanis van egy $\varphi: a \rightarrow a b^2, b \rightarrow b^3$ automorfizmusa, ámde sem a $\varphi_1: a \rightarrow a b^2$, sem a $\varphi_2: b \rightarrow b^3$ nem automorfizmusa G – nek.

2. LEMMA: Legyen $G = (m | k | n)_a^b$.

(A . 1) A G – nek az $a \rightarrow a^\mu$, $\mu \in \mathbf{R}_m$ egyszerű automorfizmusai egy \mathbf{R}_m - mel izomorf részcsoportot generálnak $\text{Aut } G$ – ben.

(A . 2) Ha a G – ben az $\langle a \rangle$ nem karakterisztikus, akkor G – nek van egy

$$\begin{aligned} \varphi: \quad a &\rightarrow a b^\beta, \quad \beta \downarrow n \\ b &\rightarrow b^\delta, \quad \delta \in \mathbf{R}_n \end{aligned}$$

automorfizmusa.

(B . 1) A G – nek $b \rightarrow b^\delta$ automorfizmusa $\delta \in \mathbf{R}_n^\#$ mellett csak akkor létezik, ha $G \notin \mathfrak{S}$.

(B . 2) Ha G – nek létezik $\omega: b \rightarrow a^\gamma b^\delta$, $\gamma \neq 0$ automorfizmusa, akkor

(a) $\delta \in \mathbf{R}_n, \delta \in \mathbf{R}_n^\# \Leftrightarrow G \notin \mathfrak{S}$;

(b) létezik olyan automorfizmusa is, ahol $\gamma \downarrow m$.

Bizonyítás: (A . 1) triviális.

(A . 2) Ha $\langle a \rangle$ nem karakterisztikus G – ben, akkor mindenesetre léteznie kell

$$\begin{aligned} \text{egy } \psi: \quad a &\rightarrow a^\alpha b^\beta, \quad \beta \neq 0, \\ b &\rightarrow b^\delta, \quad \delta \in \mathbf{R}_n \end{aligned}$$

automorfizmusának, mely $\delta = 1$ esetben egyszerű, és csatolt, ha $\delta \in \mathbf{R}_n^\#$.

Először mutassuk ki, hogy $\alpha \in \mathbf{R}_m$. A ψ hatványait tanulmányozva azt

láthatjuk, hogy $\psi^f(a) = a^{\alpha\alpha'} b^{\beta\beta'}$. Ha speciálisan $|\psi| = f$, akkor

$a^{\alpha\alpha'} b^{\beta\beta'} = a$, tehát $\alpha\alpha' \equiv 1 \pmod{m}$, amiből következik, hogy $\alpha \in \mathbf{R}_m$.

A β –ra térve látható, hogy $\beta = \beta_1 t$, $\beta_1 \downarrow n$, $(t, n) = 1$.

Ilyen fölírás mindig lehetséges.

Ekkor tehát $\psi(a) = a^\alpha (b^t)^{\beta_1}$.

Csakhogy $\langle a, b \rangle = \langle a, b^t \rangle$, azaz $(m | k | n)_a^b = (m | k^t | n)_a^{b^t}$,

ezért föltehetjük, hogy már eleve $\beta \downarrow n$.

Most már a ψ helyett tekinthetjük a $\psi_{\alpha^{-1}} \circ \psi$ automorfizmust, ahol

$$\psi_{\alpha^{-1}} : a \rightarrow a^{\alpha^{-1}}.$$

Ekkor valóban

$$\psi_{\alpha^{-1}} \circ \psi = \varphi : a \rightarrow a b^\beta, \beta \downarrow n$$

$$b \rightarrow b^\delta, \delta \in \mathbf{R}_n.$$

(B.1) A $b^\delta a b^{-\delta} = a^k$ relációból $k^{\delta-1} \equiv 1 (m)$ következik,

s ez $G \in \mathfrak{S}$ esetén csak $\delta = 1$ – gyel teljesülhet.

(B.2) (a) Ha $\delta \notin \mathbf{R}_n$ volna, akkor az $a^\gamma b^\delta$ egy n' ($< n$) –edik hatványából

a b eltűnne, és így $\langle a \rangle \cap \langle a^\gamma b^\delta \rangle \neq 1$ adódna, ami $G \notin \mathfrak{X}$ miatt lehetetlen.

A $\delta \in \mathbf{R}_n^\#$ -ra vonatkozó állítás számolással adódik.

Legyen $\omega : b \rightarrow a^\gamma b^\delta$, $\delta \in \mathbf{R}_n^\#$. Akkor $\omega(ba) = a^\gamma b^\delta a = a^{\gamma+k^\delta} b^\delta$,

$\omega(a^k b) = a^k a^\gamma b = a^{k+\gamma} b$. Az $\omega(ba) = \omega(a^k b)$ relációból $k^{\delta-1} \equiv 1 (m)$

adódik, ami $\delta \in \mathbf{R}_n^\#$ mellett csak $G \notin \mathfrak{S}$ mellett lehetséges.

(b) Írható, hogy $\gamma = \gamma_1 s$, ahol $\gamma_1 \downarrow m$, $(m, s) = 1$.

Ámde $\langle a, b \rangle = \langle a^s, b \rangle$, s így feltehető, hogy már eleve $\gamma \downarrow m$. Q. E. D.

TÉTEL: Ha a $G = (m | k | n)_a^b$ csoportnak a

$$\varphi_1: a \rightarrow a^\alpha b^\beta$$

$$\varphi_2: b \rightarrow a^\gamma b^\delta$$

egyszerű automorfizmusai, akkor ezek fúziója, $\varphi_1 \otimes \varphi_2$ is

automorfizmusa G -nek.

Bizonyítás: Azt kell belátni, hogy a φ_1 -re és a φ_2 -re fölírt kánonból (l. 36. o.)

következik a $\varphi = \varphi_1 \otimes \varphi_2$ -re fölírt kánon.

A φ_1 -nél $\gamma = 0$, $\delta = 1$, így a rá vonatkozó kánon a (K 11), (K 12), (K 32),

$$\text{valamint a } [k^\beta | k] \equiv k(m) \quad (\text{K}_1 31)$$

relációkból áll.

A φ_2 -nél $\alpha = 1$, $\beta = 0$, ezért a rá érvényes relációk a (K 21), (K 22), és a

$$k^\delta \equiv k(m) \quad (\text{K}_2 31)$$

lesznek.

Azt kell tehát csak igazolni, hogy a φ -re fönnáll a (K 31):

$$\gamma + \alpha k^\delta \equiv \gamma k^{\beta k} + \alpha [k^\beta | k] .$$

Fölhasználva a (K₁ 31) és (K₂ 31) – et, megfelelő átrendezés után ebből a

$$\gamma (k^{\beta k} - 1) \equiv 0(m)$$

relációt nyerjük. Vegyük figyelembe, hogy

$$k^{\beta k} - 1 = (k - 1) [k | \beta k] \equiv (k - 1) [k | \beta] [k^\beta | k] \equiv k(k - 1) [k | \beta] \pmod{m}$$

(itt ismét felhasználtuk a (K₁ 31) - et).

A k-val való egyszerűsítés után a bizonyítandó kongruencia ez lesz:

$$\gamma(k - 1) [k | \beta] \equiv 0 \pmod{m} \quad (\oplus)$$

Tegyük föl, hogy $\beta \downarrow n$. Ekkor (K 32) szerint

$$k - 1 = s \frac{n}{\beta} \quad (8)$$

A (K₁ 31) és (K 32) – ből

$$[k^\beta | k] = [k^\beta | k - 1 + 1] = [k^\beta | k - 1] + k^{\beta(k-1)} [k^\beta | 1] \equiv$$

$$\equiv [k^\beta | k - 1] + 1 \equiv k \pmod{m}, \text{ azaz}$$

$$[k^\beta | k - 1] \equiv k - 1 \pmod{m} \quad (9)$$

Írjuk be ide (8) – at a baloldalra:

$$[k^\beta | s \frac{n}{\beta}] \equiv [k^\beta | \frac{n}{\beta}] [k^n | s] \equiv s [k^\beta | \frac{n}{\beta}] \equiv k - 1 \pmod{m} \quad (10)$$

A (K 21) és (K₂ 32) – ből nyerjük, hogy $\gamma[k | n] \equiv 0 \pmod{m}$,

$$\text{S így } \gamma s [k | n] \equiv \gamma s [k | \beta] [k^\beta | \frac{n}{s}] \equiv 0 \pmod{m}.$$

Alkalmazva a (10) – et:

$$\Gamma = \gamma(k - 1) [k | \beta] \equiv 0 \pmod{m},$$

tehát a (⊕) teljesül.

Ha most β helyett egy βt többszöröst veszünk, akkor

$$[k | \beta t] \equiv [k | \beta] [k^\beta | t] \pmod{m}, \text{ és}$$

$$\gamma(k-1) [k | \beta t] = \Gamma [k^\beta | t] \equiv 0 \pmod{m},$$

mert $\Gamma \equiv 0 \pmod{m}$, vagyis a (\oplus) ismét teljesül.

Bizonyítottuk tehát, hogy ha φ_1 és φ_2 - re teljesül a (K 11) – (K 32),

akkor a $\varphi = \varphi_1 \otimes \varphi_2$ - re is.

Végül, mivel $G \notin \mathcal{X}$, ezért $\langle a^\alpha b^\beta \rangle \cap \langle a^\gamma b^\delta \rangle = 1$,

tehát φ valóban automorfizmusa G - nek.

Q. E. D.

3. LEMMA: Legyen $G = (m | k | n)_a^b$. Akkor

$$\text{Inn } G \cong \langle a^{k-1}, b^{n/n_0} \rangle, \text{ ahol } n_0 = |k|_m.$$

Bizonyítás: Következik ez akár abból, hogy $b a b^{-1} = a^k$ és $a^{-1} b a = a^{k-1} b$,

akár abból, hogy $\text{Inn } G \cong G / \zeta(G)$.

Q. E. D.

V. RÉSZ. \mathcal{C}_k – CSOPORTOK

1. DEFINÍCIÓ: A $G = (m | k | n)_a^b$ csoportot \mathcal{C}_k – csoportnak nevezzük, ha $\langle a \rangle \text{ char } G$, vagyis $\langle a \rangle$ karakterisztikus G – ben.

Világos, hogy $G \in \mathcal{C}_k$ esetén a G minden, a IV. rész (7) – ben (36. o.) adott automorfizmusánál $\beta = 0$. Ekkor G automorfizmusai az

$$\begin{pmatrix} \alpha & 0 \\ \gamma & 1 \end{pmatrix}, \quad \alpha \in R_m, \quad \gamma \in Z_m$$

mátrixokkal reprezentálhatók. Az automorfizmusok összetételének megfelel a fenti mátrixok szokásos szorzása, mint azt könnyű kiszámolni.

2. DEFINÍCIÓ: $(m | k | n) \in \mathcal{Q} \Leftrightarrow (k-1, n) = 1$.

1. LEMMA: $\mathcal{Q} \cup \mathcal{R} \cup \mathcal{Z} \subset \mathcal{C}_k$.

Bizonyítás: Legyen $G = (m | k | n)_a^b$. Ha $G \in \mathcal{Q}$, akkor $(k-1, n) = 1$ miatt a (K 32) – ből (36. o.) $\beta \equiv 0 \pmod{n}$ következik.

Ha $G \in \mathcal{R}$, akkor $(m, n) = 1$ miatt a (K 12) – ből (36. o.) következik

ugyanaz. Végül, ha $G \in \mathcal{Z}$, akkor $\partial(G) = \langle a \rangle$. Q. E. D.

2. LEMMA: Ha $(m | k | \dot{n}) \in \mathcal{C}_k$, és $(m, s) = 1$, akkor

$$(s) \times (m | k | \dot{n}) \in \mathcal{C}_k.$$

Bizonyítás: Legyen G_s az $(s)_{a_1}$ és a $G = (m | k | \dot{n})_{a_2}^b$ direkt szorzata.

$$G_s = (s)_{a_1} \times G = (ms | 1 | \dot{n})_{a_1 a_2}^b .$$

$$G_s \in \mathfrak{S} \text{ miatt } \zeta(G_s) = \zeta_e(G_s), \text{ és nyilván } \langle a_1 \rangle \leq \zeta(G_s) .$$

Mivel ciklikus csoportnak minden részcsoportha karakterisztikus, kapjuk, hogy

$$\langle a_1 \rangle \text{ char } \zeta_e(G_s) \text{ char } G_s ,$$

$$\text{amiből } \langle a_1 \rangle \text{ char } G_s .$$

$$\text{Legyen } \varphi \in \text{Aut } G_s . \text{ Akkor } \varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2) ,$$

$$\text{és az előbbiek értelmében } \varphi(a_1) = a_1^{\alpha_1} , \alpha_1 \in \mathbf{R}_s .$$

Ha most $\varphi(a_2) = a_1^\gamma a_2^{\alpha_2} b^\beta$, akkor ennek az elemnek a rendje csak akkor

lehet m , ha $\gamma = 0$. Ám ekkor $\beta = 0$ is, különben az $\langle a_2 \rangle$ az $\langle a_2, b \rangle = G$ -ben

nem volna karakterisztikus. Mindebből az következik, hogy

$$\varphi(\langle a_1, a_2 \rangle) = \langle a_1, a_2 \rangle , \text{ tehát } G_s \in \mathbf{Ch} . \quad \text{Q. E. D.}$$

A VI. rész 1. lemmája (71. o.) mutatja, hogy az iménti állításban

miért volt szükség \mathfrak{S} -csoportokra szorítkozni.

$$\underline{\text{3. LEMMA:}} \quad G_1, G_2 \in \mathbf{Ch} \Rightarrow G_1 \otimes G_2 \in \mathbf{Ch} .$$

Bizonyítás: Legyen $(m_1, m_2) = 1$, és

$$G_1 = (m_1 | k_1 | n_1)_{a_1}^{b_1} \in \mathbf{Ch} , \text{ és } G_2 = (m_2 | k_2 | n_2)_{a_2}^{b_2} \in \mathbf{Ch} .$$

$$\text{Akkor } G_1 \otimes G_2 = (m_1 m_2 | k | n_1 n_2)_{a_1 a_2}^{b_1 b_2} ,$$

ahol $k \equiv k_i (m_i)$, $i = 1, 2$, $n = [n_1, n_2]$.

Tegyük föl, hogy a $G_1 \otimes G_2$ - nek van egy

$$\begin{aligned} \varphi : \quad & a_1 a_2 \rightarrow a_1 a_2 (a_1 a_2)^\beta \\ & b_1 b_2 \rightarrow (b_1 b_2)^\delta \end{aligned}$$

automorfizmusa. tekintsük ennek a φ - nek mondjuk a G_1 - re való

megszorítását. Mivel $G_1 \in \mathbf{Ch}$, ezért a $\varphi(\langle a_1 \rangle) = \langle a_1 \rangle$ relációnak

teljesülnie kell. Ámde $(m_1, m_2) = 1$, s így $\langle a_1 \rangle = \langle a_1^{m_2} \rangle$, és

$$a_1^{m_2} = (a_1 a_2)^{m_2} \quad (*)$$

Ezért $\varphi(a_1^{m_2}) = \varphi((a_1 a_2)^{m_2}) = (a_1 a_2 (b_1 b_2)^\beta)^{m_2} =$

$$= a_1^{[k^\beta | m_2]} b_1^{\beta m_2} a_2^{[k^\beta | m_2]} b_2^{\beta m_2} \in \langle a_1 \rangle.$$

Ebből $[k^\beta | m_2] \equiv 0 (m_2)$ (1 a)

és $\beta m_2 \equiv 0 (n_2)$ (1 b)

következik. (Az, hogy m_2 a legkisebb ilyen szám, abból következik,

hogy a $(*)$ az m_2 -nél kisebb számmal nem teljesül.)

A φ - re fölírt (K 31) és (K 32) (ld. 36. o.):

$$[k^\beta | k] \equiv k^\delta (m_1 m_2) \quad (1 c)$$

$$\beta (k - 1) \equiv 0 (n) \quad (1 d)$$

Vegyük a $k - t \pmod{m_2}$, a β és $\delta - t \pmod{n_2}$, azaz legyen

$$k = k_2 + m_2 x,$$

$$\beta = \beta_2 + n_2 y,$$

$$\delta = \delta_2 + n_2 z,$$

és nézzük meg, mivé lesznek az (1 a – d) relációk.

Az (1 a) – ből:

$$\begin{aligned} [k^\beta | m_2] &\equiv [k_2^{\beta_2 + n_2 y} | m_2] \equiv (k_2^{n_2 y} \equiv 1 (m_2) \text{ miatt}) \equiv \\ &\equiv [k_2^{\beta_2} | m_2] \equiv 0 (m_2) \end{aligned} \quad (1 a a)$$

Az (1 b) – ből:

$$(\beta_2 + n_2 y)m_2 \equiv \beta_2 m_2 \equiv 0 (n_2) \quad (1 b b)$$

Az (1 c) – nél a [|] bal felében közvetlenül áttérhetünk k – ról k₂ – re :

$$[k^\beta | k] \equiv [k_2^{\beta_2 + n_2 y} | k] \equiv k_2^{\delta_2 + n_2 z} (m_2),$$

amiből $k_2^{n_2 y} \equiv k_2^{n_2 z} \equiv 1 (m_2)$ miatt

$$[k_2^{\beta_2} | k] \equiv k_2^{\delta_2} (m_2) .$$

Meg kell még mutatni, hogy

$$[k_2^{\beta_2} | k] \equiv [k_2^{\beta_2} | k_2] (m_2) .$$

$$\text{Íme: } [k_2^{\beta_2} | k] \equiv [k_2^{\beta_2} | k_2 + m_2 x] \equiv [k_2^{\beta_2} | k_2] + k_2^{\beta_2 k_2} [k_2^{\beta_2} | m_2 x] \equiv$$

$$[k_2^{\beta_2} | k_2] + k_2^{\beta_2 k_2} [k_2^{\beta_2} | m_2] [k_2^{\beta_2 m_2} | x] \equiv [k_2^{\beta_2} | k_2] (m_2) ,$$

mivel (1 a a) miatt $[k_2^{\beta_2} | m_2] \equiv 0 \pmod{m_2}$.

Kaptuk tehát, hogy

$$[k_2^{\beta_2} | k_2] \equiv k_2^{\delta_2} \pmod{m_2}. \quad (1 c c)$$

Az (1 d) –ből:

$$\begin{aligned} \beta(k-1) &\equiv (\beta_2 + ny)(k_2 + m_2x - 1) \equiv \\ &\equiv \beta_2(k_2 - 1) \equiv 0 \pmod{n_2}, \end{aligned} \quad (1 d d)$$

hiszen $\beta_2 m_2 \equiv 0 \pmod{n_2}$ az (1 b b) szerint.

Az (1 a a – d d) relációk szerint a G_2 – nek van egy $a_2 \rightarrow a_2 b_2^{\beta_2}, b_2 \rightarrow b_2^{\delta_2}$

automorfizmusa, ellentmondásban azzal, hogy $G_2 \in \mathcal{Ch}$ Q. E. D.

E lemma megfordítása nem igaz. Előfordulhat, hogy $G_1 \in \mathcal{Ch}$, $G_2 \notin \mathcal{Ch}$,

mégis $G_1 \otimes G_2 \in \mathcal{Ch}$.

Például $(7|4|3) \otimes (9|4|3) = (63|4|3) \in \mathcal{Ch}$,

ahol $(7|4|3) \in \mathcal{Ch}$, de $(9|4|3) \notin \mathcal{Ch}$.

3. DEFINÍCIÓ: A $G = (m | k | \dot{n}) \mathcal{B}$ – csoport pontosan akkor, ha

$$[k | n] \equiv 0 \pmod{m}.$$

4. LEMMA:

(i) Ha $(m, s) = 1$, $(m | k | \dot{n}) \in \mathcal{B}$, akkor

$(s) \times (m | k | \dot{n}) \in \mathcal{B}$ pont akkor, ha $s | n$.

(ii) $G_1, G_2 \in \mathcal{B} \Rightarrow G_1 \otimes G_2 \in \mathcal{B}$.

Bizonyítás: egyszerű számolással.

Q. E. D.

Az (ii) megfordítása hamis, például $(9|4|3) \otimes (19|4|3) \in \mathcal{B}$,

de $(9|4|3) \notin \mathcal{B}$.

1. TÉTEL: (\mathcal{B} -TÉTEL): $\mathcal{B} \subset \mathcal{Ch}$.

Bizonyítás: Tegyük föl, hogy $G = (m|k|n)_a^b \in \mathcal{B}$, de $G \notin \mathcal{Ch}$.

Ekkor a G -nek létezik egy

$$\begin{aligned} \varphi: \quad & a \rightarrow a b^\beta, \quad \beta \downarrow n \\ & b \rightarrow b^\delta, \quad \delta \in \mathbf{R}_n \end{aligned}$$

automorfizmusa (ld. 38. o. (A2)).

Írjuk föl a (K31) – et (36. o.) $\alpha = 1, \gamma = 0$ szereposztással:

$$[k^\beta | k] \equiv k^\delta \pmod{m}.$$

Ebből a (K32) – vel (36. o.):

$$[k^\beta | k-1+1] = [k^\beta | k-1] + k^{\beta(k-1)} [k^\beta | 1] \equiv [k^\beta | k-1] + 1 \equiv k^\delta \pmod{m},$$

azaz $[k^\beta | k-1] \equiv k^\delta - 1 \pmod{m}$.

$$\text{Most} \quad k-1 = s \frac{n}{\beta},$$

mivel $\beta \downarrow n$, ezért

$$[k^\beta | k-1] \equiv [k^\beta | s \frac{n}{\beta}] \equiv [k^\beta | \frac{n}{\beta}] [k^n | s] \equiv s [k^\beta | \frac{n}{\beta}] \equiv k^\delta - 1 \pmod{m}. \quad (2)$$

Mivel $G \in \mathcal{B}$, ezért $[k|n] \equiv 0 \pmod{m}$, s így

$$s [k | n] \equiv s [k | \beta] [k^\beta | \frac{n}{\beta}] \equiv 0 \pmod{m} .$$

Használjuk föl itt a (2) – t :

$$[k | \beta] (k^\delta - 1) \equiv 0 \pmod{m} . \quad (3)$$

Mármost (fölhasználva a (K 32) – t, ld. 36. o.):

$$(ab^\beta)^{k-1} = a^{[k^\beta | k-1]} = a^{k^\delta - 1},$$

és a (3) – mal nyerjük, hogy

$$((ab^\beta)^{k-1})^{[k|\beta]} = (a^{k^\delta - 1})^{[k|\beta]} = 1.$$

Ebből következik, hogy

$$(k-1) [k | \beta] = k^\beta - 1 \equiv 0 \pmod{m} ,$$

ellentmondásban azzal, hogy $\beta \downarrow n$ és $G \in \mathfrak{S}$.

Q. E. D.

Az 1. lemma és az 1. tétel szerint

$$\mathfrak{B} \cup \mathfrak{Q} \cup \mathfrak{R} \cup \mathfrak{Z} \subset \mathcal{C}_k .$$

Hogy ez a tartalmazás valódi, azt a (63 | 4 | 3) csoport bizonyítja.

(Egyébként $\mathfrak{Z} \cap \mathfrak{S} \subset \mathfrak{B}$. Ha ugyanis $(m | k | n) \in \mathfrak{Z}$, akkor $(m, k-1) = 1$, és így a $k^n - 1 = (k-1) [k | n] \equiv 0 \pmod{m}$ relációból $[k | n] \equiv 0 \pmod{m}$ következik.) } (\triangleleft)

2. TÉTEL: Legyen $(m | k | \dot{n}) \in \mathcal{C}_h$. Akkor

$$(i) \left(\frac{m}{\gamma} \right) \cdot \mathbf{R}_m \cong \text{Aut}(m|k|\dot{n}) \leq \text{Hol}(m), \text{ ahol } \gamma = \frac{m}{(m, [k|n])};$$

(ii) $\text{Aut}(m|k|\dot{n}) \cong \text{Hol}(m)$ pontosan akkor, ha $(m|k|\dot{n}) \in \mathcal{B}$;

(iii) $\text{Hol}(m) \in \text{CYCYS} \Leftrightarrow m \in \mathbf{PR}$.

Bizonyítás:

(i) A $G = (m|k|n)_a^b \in \mathbf{Cb}$ összes automorfizmusa most

$$\begin{aligned} \varphi : \quad & a \rightarrow a^\alpha, \quad \alpha \in \mathbf{R}_m \\ & b \rightarrow a^\gamma b, \quad \gamma \in \mathbf{Z}_m \end{aligned}$$

alakú, és világos, hogy $\varphi = \varphi_\alpha \otimes \varphi_\beta$, ahol

$$\begin{aligned} \varphi_\alpha : a &\rightarrow a^\alpha, \quad \alpha \in \mathbf{R}_m \\ \varphi_\gamma : b &\rightarrow a^\gamma b, \quad \gamma \in \mathbf{Z}_m \end{aligned}$$

egyszerű automorfizmusok.

Nilvánvaló, hogy $\langle \{\varphi_\alpha \mid \alpha \in \mathbf{R}_m\} \rangle \cong \mathbf{R}_m$.

Írjuk föl φ_γ -ra a (K 21)–et (36. o.):

$$\gamma [k|n] \equiv 0 \pmod{m}.$$

Látható, hogy a szóba jöhető legkisebb γ éppen $\frac{m}{(m, [k|n])}$,

s így
$$\left\langle \varphi_\gamma \cong \left(\frac{m}{\gamma} \right) \right\rangle,$$

és
$$\langle \varphi_\gamma, \{\varphi_\alpha\} \rangle = \text{Aut}G \cong \left(\frac{m}{\gamma} \right) \cdot \mathbf{R}_m.$$

Egyszerű kiszámolni, hogy $\varphi_\alpha \varphi_\gamma \varphi_\alpha^{-1} = \varphi_\gamma^\alpha$

ami éppen azt jelenti, hogy $\text{Aut} G \leq \text{Hol}(m)$.

(Az automorfizmusok szorzási szabálya itt: $\varphi\psi(a) = \varphi(\psi(a))$.)

Továbbá $\varphi_\alpha^{-1} = \varphi_{\alpha^{-1}}$.)

(i i) Világos, hogy (i) – ben egyenlőség akkor és csak akkor van, ha

$\gamma = 1$, azaz $[k | n] \equiv 0 \pmod{m}$, tehát $(m | k | \dot{n}) \in \mathcal{B}$.

(i i i) Ez abból következik, hogy $\text{Hol}(m) \cong \text{Aut } D_m$, és $D_m \in \mathcal{B}$ miatt

$$\text{Aut } D_m \cong (m) \cdot R_m.$$

Az R_m pedig pontosan akkor ciklikus, ha $m \in PR$. Q. E. D.

4. DEFINÍCIÓ: A CYCYSbeli tökéletes csoportok halmazát jelölje \mathcal{T} .

5. LEMMA: $\mathcal{T} = \{ (p^\alpha | k | p^{\alpha-1}(p-1)) \}$, ahol $p \in P_0$, $k \in \text{pr}(p^\alpha)$.

Bizonyítás: Definíció szerint egy csoport akkor és csak akkor tökéletes,

ha $\zeta(G) = 1$, és G minden automorfizmusa belső, tehát

$$\text{Aut } G \cong \text{Inn } G \cong G.$$

Ha $G \in \text{CYCYS}$, akkor $\zeta(G) = 1$ csakis akkor állhat, ha $G \in \mathcal{Z} \cap \mathcal{S}$

(ld. III. rész 3. lemma, 21. o.)

Ezért $G \in \mathcal{B}$ is teljesül (ld. 49. o. (\Leftarrow)).

Ha tehát $G = (m | k | n)_a^b \in \mathcal{T}$, akkor a 2. tétel szerint

$$\text{Aut } G = \langle \varphi, \{\varphi_\alpha\} \rangle,$$

ahol $\varphi: b \rightarrow ab$,
 $\varphi_\alpha: a \rightarrow a^\alpha$, $\alpha \in \mathbf{R}_m$.

A φ nyilván belső automorfizmus, hiszen

$$a^{-1} b a = a^{k-1} b = \varphi^{k-1}(b) ,$$

és a \cong -beliség miatt $\langle \varphi^{k-1} \rangle = \langle \varphi \rangle$.

A φ_α pont akkor lesz belső automorfizmus minden $\alpha \in \mathbf{R}_m$ esetében, ha

$$\langle k \rangle \cong \mathbf{R}_m ,$$

amiből – és a centrumnélküliségből – valóban $m = p^\alpha$, $p \in \mathbf{P}_0$, $k \in \text{pr}(p^\alpha)$ és

$n = \text{EU}(p^\alpha) = p^{\alpha-1}(p-1)$ következik.

Q. E. D.

6. LEMMA: $G \cong \text{Aut } G$ pontosan akkor, ha

(i) $G \in \mathcal{F}$,

(ii) $G = (2p^\alpha | k | p^{\alpha-1}(p-1))_a^b$, $p \in \mathbf{P}_0$, $k \in \text{pr}(2p^\alpha)$,

(iii) $G \cong D_4$.

Bizonyítás: Az (i) – t elintézi az 5. lemma, az (iii) – nél egyszerű számolás

segít, így elég az (ii) – vel foglalkozni.

Az (ii) – beli csoportok a \mathcal{F} – csoportokból állnak elő úgy, hogy azokat

előlről megszorozzuk egy (2) ciklussal. Az 5. lemma szerint $\mathcal{F} \subset \mathcal{B}$, és

a 4. lemma (i) – vel (47. o.) kapjuk, hogy az (ii) – beli G is \mathcal{B} – ben van.

Ám ekkor $\text{Aut } G = \langle \varphi, \varphi_k \rangle$, ahol

$$\varphi: b \rightarrow ab, \quad |\varphi| = 2p^\alpha,$$

$$\varphi_k: a \rightarrow a^k, \quad k \in \text{pr}(2p^\alpha), \quad |\varphi_k| = p^{\alpha-1}(p-1),$$

és egyszerű számolás mutatja, hogy $\varphi \varphi_k \varphi^{-1} = \varphi_k^k$,

tehát valóban $\langle \varphi, \varphi_k \rangle \cong G$.

Q. E. D.

A fentiekből levonható az a következtetés, hogy azokra a $G = (m | k | n)_a^b$ csoportokra, ahol $m \in PR$, $k \in \text{pr}(m)$, fennáll:

$$G \cong \text{Aut } G \cong \text{Hol}(m),$$

és más csoportokra ez nem teljesül.

7. LEMMA: A $G = (m | k | n)_a^b$ csoportban a $\langle b \rangle$ - nek akkor és csak akkor

van m számú különböző automorf képe, ha $[k | n] \equiv 0 (m)$.

Bizonyítás: Tekintsük a

$$\begin{aligned} \varphi: \quad a &\rightarrow a, \\ b &\rightarrow a^\gamma b, \quad \gamma \in \mathbf{Z}_m \end{aligned}$$

leképezést. Ezzel

$$\varphi(ba) = a^\gamma b a = a^{k+\gamma} b,$$

$$\varphi(a^k b) = a^k a^\gamma b = a^{k+\gamma} b,$$

ami azt jelenti, hogy $|a^\gamma b| = n$ esetén φ (egyszerű) automorfizmusa lesz

G - nek. Tekintve, hogy $(a^\gamma b)^n = a^{\gamma[k|n]}$,

az $|a^\gamma b| = n$ összefüggés tetszőleges $\gamma \in \mathbf{Z}_m$ mellett csak akkor állhat fenn,

ha $[k | n] \equiv 0 \pmod{m}$.

Ekkor azonban

$$\langle a^{\gamma_1} b \rangle = \langle a^{\gamma_2} b \rangle \quad (4)$$

csakis $\gamma_1 = \gamma_2$ esetén lehetséges. A (4) –ből ugyanis

$$a^{\gamma_1} b \in \langle a^{\gamma_2} b \rangle$$

következik, azaz egy olyan $x \in \mathbf{Z}_n$ létezése, amellyel

$$a^{\gamma_1} b = (a^{\gamma_2} b)^x = a^{\gamma_2 [k|x]} b^x.$$

Innen $x \equiv 1 \pmod{n}$, de mivel $x \in \mathbf{Z}_n$, ezért $x = 1$, s ezzel $\gamma_1 = \gamma_2$ következik.

Q. E. D.

5. DEFINÍCIÓ: Azokat a $G = (m | k | n)_a^b$ csoportokat, amelyekben a $\langle b \rangle$

különböző automorf képei páronként diszjunktak, \mathcal{M}^* csoportoknak nevezzük.

A definícióból világos, hogy $\mathcal{M}^* \subset \mathcal{S}$.

Ha ugyanis $G \notin \mathcal{S}$, akkor $\zeta_h(G) \neq 1$, és a $\langle b \rangle$ bármely konjugáltjával

összemetsz ebben a nem triviális hátsó centrumban.

8. LEMMA: $(m | k | n)_a^b \in \mathcal{M}^*$ pontosan akkor, ha

$$\forall v \downarrow n: (m, [k | v]) = 1.$$

Bizonyítás: Az 5. definícióval ekvivalens állítás ez:

$(m | k | n)_a^b \in \mathcal{M}^*$ pontosan akkor, ha $\langle b \rangle$ bármely tőle különböző

automorf képével csak triviálisan metsződik, vagyis

$$\forall \gamma \in \mathbf{Z}_m^\# : \langle \mathbf{b} \rangle \cap \langle \mathbf{a}^\gamma \mathbf{b} \rangle = 1. \quad (5)$$

(Ugyanis $\mathcal{M}^* \subset \mathcal{S}$ miatt a \mathbf{b} automorf képei mind $\mathbf{a}^\gamma \mathbf{b}$ alakúak, ahol $\gamma \in \mathbf{Z}_m$)

Az (5) mármost csakis akkor teljesül, ha

$$\forall \gamma \in \mathbf{Z}_m^\# \quad \forall v \downarrow n : \gamma[k|v] \not\equiv 0(m).$$

Innen pedig azonnal kapjuk az

$$\forall v \downarrow n : (m, [k|v]) = 1 \text{ feltételt.} \quad \text{Q. E. D.}$$

6. DEFINÍCIÓ: Ha $\mu \downarrow m$ és $v \downarrow n$, akkor a $G = (m|k|n)_a^b$ csoportnak

az $\langle \mathbf{a}^\mu, \mathbf{b}^v \rangle$ alakú részcsoportjait főrészeknek nevezzük.

Könnyű látni, hogy a főrészek vagy abeliek, vagy CYCYS – beliek.

9. LEMMA: Ha $G \in \mathcal{M}^*$, akkor G minden nemabeli főrésze is \mathcal{M}^* – ban van.

Bizonyítás: Legyen $G = (m|k|n)_a^b$, $\mu \downarrow m$, $v \downarrow n$, és

$$M = \langle \mathbf{a}^\mu, \mathbf{b}^v \rangle \notin \text{ABEL}.$$

$M \in \mathcal{M}^*$ pontosan akkor, ha $\forall v_0 \downarrow \frac{n}{v} : \left(\frac{m}{\mu}, [k^v | v_0] \right) = 1$.

Tegyük föl, hogy valamely v_0 – ra $\left(\frac{m}{\mu}, [k^v | v_0] \right) > 1$.

Akkor nyilván $(m, [k^v | v_0]) > 1$ is fönnáll.

Ugyanakkor $(m, [k | v]) = 1$, mert $G \in \mathcal{M}^*$. Így

$$(m, [k^v | v_0]) = (m, [k | v][k^v | v_0]) = (m, [k | vv_0]) > 1,$$

ami ellentmond annak, hogy $G \in \mathcal{M}^*$.

Q. E. D.

10. LEMMA: Legyen $G = (p^\alpha | k | \cdot p^{\beta r})$, ahol $p \in P, r | p - 1$.

G akkor és csak akkor \mathcal{M}^* – beli, ha

(a) $\beta = 1$ és $r = 1$, vagy

(b) $\beta = 0$.

Bizonyítás: (a) Ez esetben G automatikusan \mathcal{M}^* – ben van, mint minden olyan $(m | k | n)$ csoport, ahol $n \in P$.

(b) Könnyű látni, hogy ekkor $G \in \mathcal{Z}$. Az 5. lemma bizonyításából kiderül,

hogy ha $(m | k | n)_a^b \in \mathcal{Z}$, akkor b minden automorf képe megkapható

konjugálással. Ezért elég bizonyítani, hogy esetünkben a $\langle b \rangle$ bármely, tőle

különböző konjugáltjával diszjunkt:

$$\forall x \in \mathbf{Z}_m^\# : \langle b \rangle \cap \langle a^{-x} b a^x \rangle = 1.$$

Tételezzük föl ennek az ellenkezőjét, azaz tételezzük egy olyan $y \in \mathbf{Z}_n^\#$

szám létezését, amellyel

$$(a^{-x} b a^x)^y = (a^{x(k-1)} b)^y = (a^{x(k-1)[k|y]}) b^y = b^y.$$

Ebből

$$x(k-1)[k|y] \equiv x(k^y - 1) \equiv 0 \pmod{p^\alpha} \quad (6)$$

következik.

Ha $x \in \mathbf{R}_{p^\alpha}$, akkor (6) – ből azt kapjuk, hogy $k^y \equiv 1 \pmod{p^\alpha}$,

tehát $y \equiv 0 \pmod{n}$, ellentmondásban az $y \in \mathbf{Z}_n^\#$ föltevással.

Ha $x \notin \mathbf{R}_{p^\alpha}$, akkor $x = p^\delta x_1$, $1 \leq \delta \leq \alpha - 1$, $(p, x_1) = 1$.

Ekkor (6) – ből nyerjük, hogy $k^y \equiv 1 \pmod{p^{\alpha-\delta}}$.

De ebből megint $y \equiv 0 \pmod{n}$ következik, mert $\mathbf{R}_{p^\alpha} = (p^{\alpha-1}) \times (p-1)$, és

k most a $(p-1)$ ciklusból való, s ezért k rendje r minden $1 \leq \delta \leq \alpha - 1$ esetén is.

Bizonyítottuk tehát, hogy az (a) és (b) esetekben valóban $G \in \mathcal{M}^*$.

Azt kell még megmutatni, hogy más esetekben viszont $G \notin \mathcal{M}^*$.

Ismét két lehetőség van:

(c) $\beta = 1$, $r > 1$,

(d) $\beta \geq 2$.

A (c) – nél elég látni, hogy a $(p \mid k \mid pr)$ főrészt nincs \mathcal{S} – ben, s így

\mathcal{M}^* – ben sem, a (d) – nél pedig a $(p^{\alpha-1} \mid k^r \mid p^\beta)$ főrészt vizsgálata

vezet hasonló eredményre,

(hiszen ha $k^r \mid p^\alpha = p^\beta$, akkor $k^r \mid p^{\alpha-1} = p^{\beta-1}$).

Q. E. D.

3. TÉTEL: Az \mathcal{M}^* – csoportok a következők:

(A) Ha $n \in P$, akkor $(m \mid k \mid n)$ minden további megszorítás nélkül $\in \mathcal{M}^*$.

(B) Tegyük föl, hogy $n \notin P$, és legyenek a p_1, p_2, \dots, p_r számok páronként különböző prímek. Akkor a

$(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \mid k \mid n) \in \mathcal{F}_c$ csoport pont akkor lesz \mathcal{M}^* – ban, ha

$$n \mid (p_1 - 1, p_2 - 1, \dots, p_r - 1) ,$$

és ugyancsak \mathcal{M}^* – beli lesz az

$$(s) \times (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \mid k \mid n)$$

is, ha $(s, p_1 p_2 \dots p_r n) = 1$.

Bizonyítás: (A) triviális.

(B) Mindenekelőtt jegyezzük meg, hogy

$$(n, p_i) = 1, \quad i = 1, 2, \dots, r. \quad (7)$$

Tegyük föl ugyanis, hogy valamely i – re $p_i \mid n_i$, azaz

$$n = p_i^{\beta_i} n_i, \quad \beta_i \neq 0, \quad (p_i, n_i) = 1.$$

Akkor a 10. lemma szerint a $(p_i^{\alpha_i} \mid k \mid p_i^{\beta_i} n_i)$ főrészt

pont akkor lehet \mathcal{M}^* – ban, ha $\beta_i = n_i = 1$.

Ez az $n = p_i$ esetre, tehát (A) –ra vezetne.

Így a (7) – nek fönn kell állnia, és akkor a $(p_i^{\alpha_i} \mid k \mid n)$ főrészt

ismét a 10. lemma szerint – csakis úgy lehet \mathcal{M}^* – beli, ha $n_i \mid p_i - 1$.

Már csak az s – re vonatkozó kirovást kell indokolni.

Az $(s, p_1 p_2 \dots p_r) = 1$ természetesen az előlről való szorozhatóság miatt kell.

Az $(s, n) = 1$ feltétel oka pedig a következő:

Tegyük föl, hogy $(m | k | n) \in \mathcal{M}^*$ és n összetett szám.

Tekintsük az $(s) \times (m | k | n) \cong (ms | l | n)$ (8)

csoportot, ahol a PART szerint $(m, s) = 1, l \equiv 1(s), k \equiv 1(m)$.

Ha (8) \mathcal{M}^* – beli, akkor a 8. lemma szerint $\forall v \downarrow n: (ms, [l | v]) = 1$.

Mármost $k \equiv 1(m)$ miatt $(m, [l | v]) = 1$,

így csak az $(s, [l | v]) = 1$ a vizsgálandó.

Mivel most $l \equiv 1(s)$, ezért $[l | v] \equiv v(s)$, és így

$(s, [l | v]) = 1$ csakis úgy teljesülhet, ha $(s, v) = 1$.

Mivel ennek minden $v \downarrow n$ számra fönn kell állnia,

kapjuk, hogy $(s, n) = 1$.

Q. E. D.

7. DEFINÍCIÓ: Azokat az $(m | k | n)_a^b$ csoportokat, amelyekben a $\langle b \rangle$ – nek

pontosan m számú, páronként diszjunkt automorf képe van,

multiédercsoportoknak nevezzük, és halmazukat \mathcal{M} – mel jelöljük.

Világos, hogy $D_m \in \mathcal{M}$ minden $m \geq 3$ számmal, így a multiédercsoport

fogalma a diédercsoport fogalmának természetes általánosítása.

A definícióból azonnal nyilvánvaló, hogy $\mathcal{M} = \mathcal{M}^* \cap \mathcal{B}$. (9)

(ld. ehhez 7. lemma, 53. o.)

11. LEMMA: Ha $G \in \mathcal{M}$, akkor G minden nemabeli főrésze is \mathcal{M} – beli.

Bizonyítás: Tekintettel a (9) – re csak azt kell belátni, hogy $G \in \mathcal{M}^*$ esetén

a (CYCYSbeli) főrészek \mathcal{B} – ben lesznek.

Tekintsük a $G = (m | k | n)_a^b$ csoportban az $\langle a^\mu, b^\nu \rangle$ főrészt ($\mu \downarrow m, \nu \downarrow n$).

Mivel $G \in \mathcal{B}$, ezért $[k | n] = [k | \nu] \left[k^\nu | \frac{n}{\nu} \right] \equiv 0 (m)$. (10)

Ámde $G \in \mathcal{M}^*$ is, ezért $(m, [k | \nu]) = 1$, s így (10) – ből kapjuk, hogy

$$\left[k^\nu | \frac{n}{\nu} \right] \equiv 0 (m).$$

De akkor $\left[k^\nu | \frac{n}{\nu} \right] \equiv 0 \left(\frac{m}{\mu} \right)$ is igaz, így

$$\langle a^\mu, b^\nu \rangle \cong \left(\frac{m}{\mu} | k^\nu | \frac{n}{\nu} \right) \in \mathcal{B}. \quad \text{Q. E. D.}$$

4. TÉTEL: legyenek a p, p_1, p_2, \dots, p_r számok páronként különböző prímek.

Akkor az \mathcal{M} – csoportok az alábbiak:

(A) $(p) \times (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} | k | p)$, ahol

$$p_i^{\alpha_i} \nmid k - 1, i = 1, 2, \dots, r,$$

$$p \mid (p_1 - 1, p_2 - 1, \dots, p_r - 1);$$

(B) $(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} | k | n)$, ahol

$$p_i^{\alpha_i} \nmid k - 1, i = 1, 2, \dots, r,$$

$$n \mid (p_1 - 1, p_2 - 1, \dots, p_r - 1).$$

Bizonyítás: A (9) – et figyelembe véve elegendő az \mathcal{M}^* – csoportok közül

kikeresni azokat, amelyek \mathcal{B} – ben is benne vannak (segítségül hívva a

4. lemmát is.)

Q. E. D.

A legegyszerűbben úgy találhatunk \mathcal{M} – csoportokat, ha választunk egy

$2 \leq n$ egészet és keresünk olyan $p_i, i = 1, 2, \dots$ prímeket, amelyekre

$$n \mid p_i - 1, i = 1, 2, \dots$$

(A DIRICHLET – tétel szerint végtelen sok ilyen prímet találhatunk.)

Tegyük föl, hogy a p_1, p_2, \dots, p_r alkalmas prímek.

Akkor tetszőleges $\alpha_i \geq 1, i = 1, 2, \dots, r$ számokkal könnyen

megszerkeszthetők a $(p_i^{\alpha_i} \mid k_i \mid n)_{a_i}^{b_i}$ csoportok,

melyek a 4. tétel szerint \mathcal{M} – ben lesznek.

De \mathcal{M} – ben lesz e csoportoknak az összes lehetséges fúziója is,

amelyek így generálhatók: $\langle a, b_1^{t_1} b_2^{t_2} \dots b_r^{t_r} \rangle$, (11)

ahol $a = a_1 a_2 \dots a_r$, és $t_i \in \mathbf{R}_{n_i}, i = 1, 2, \dots, r$.

A (11) összesen $\prod_{i=1}^r \text{EU}(n_i)$ számú csoportot ad, ámde

$\langle a, b_1^{t_1} b_2^{t_2} \dots b_r^{t_r} \rangle \cong \langle a, (b_1^{t_1} b_2^{t_2} \dots b_r^{t_r})^x \rangle$, ha $x \in \mathbf{R}_n$.

Ezért az adott n – hez tartozó nem izomorf, de nyilván izostruktúrális

\mathcal{M} – csoportok száma

(a) összetett n esetén $\prod_{i=1}^r \text{EU}(n_i) / \text{EU}(n)$,

(b) $n \in \mathbf{P}$ esetén a fenti szám kétszerese,

hiszen ha $(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} | k | p) \in \mathcal{M}$, akkor a 4. tétel (A) szerint

$(p) \times (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} | k | n) \in \mathcal{M}$ is .

12. LEMMA: Legyen $p \in \mathbf{P}$, $1 < r | p - 1$, $s \geq 1$. Akkor

$$(p^\alpha | k | (\cdot p^\beta r) s) \in \mathcal{Z} .$$

Bizonyítás: Ha p osztaná $k - 1$ - et, azaz fölírható volna

$$k = t p^\gamma + 1, \quad \gamma \geq 1, \quad (t, p) = 1$$

alakban, akkor a III. rész 9. lemma szerint (25. o.)

$$|k|_{p^\alpha} = p^{\alpha-\beta} \text{ volna.}$$

De most $|k|_{p^\alpha} = p^\beta r$, ahol $r > 1$, így $(p^\alpha, k - 1) = 1$,

és ez a tény független s - től.

Q. E. D.

5. TÉTEL: Az alábbi csoportok $\mathcal{P} \cap \mathcal{Ch}$ - ban vannak:

$$(a) \quad (2^\alpha | 2^{\alpha-1} | 2)_a^b, \quad \alpha \geq 3 ,$$

$$(b) \quad D_{2^\alpha}, \quad \alpha \geq 2 .$$

Bizonyítás: (a) Tekintsük az $a^\gamma b$, $\gamma \in \mathbf{Z}_m$ elemet:

$$(a^\gamma b)^2 = a^{\gamma[2^{\alpha-1}-1]2} = a^{2^{\alpha-1}\alpha}, \text{ s így } |a^\gamma b| \leq 4 .$$

$$(b) \quad D_{2^\alpha} \in \mathcal{M} \subset \mathcal{B} \subset \mathcal{Ch} .$$

Q. E. D.

VI. RÉSZ. CSOPORTOK A \mathcal{C}_k -n KÍVÜL

TÉTEL: Az V. rész 5. tételében felsoroltakon kívül minden más p – csoport a \mathcal{C}_k – n kívül van.

Bizonyítás: A következőkben erősen támaszkodunk az alábbi összefüggésekre:

$$(i) [s p^{\alpha-\beta} + 1 | p^\beta] \equiv p^\beta (p^\alpha), \text{ ahol } p \in P_0, 0 \leq \beta \leq \alpha, (s, p) = 1.$$

$$(ii) [s 2^{\alpha-\beta} + 1 | 2^\beta] \equiv 2^{\alpha-1} + 2^\beta (2^\alpha), \text{ ahol } \alpha > 2, 1 \leq \beta < \alpha-1, (2, s) = 1.$$

$$(iii) [s 2^{\alpha-\beta} - 1 | 2^\beta] \equiv 2^{\alpha-1} (2^\alpha), \text{ ahol } \alpha > 2, 1 \leq \beta < \alpha-1, (2, s) = 1.$$

$$(iv) \text{ Ha } (m | k | n) \cong (m | l | n), \text{ akkor } [k | n] \equiv [l | n] (m).$$

Ezen kongruenciák igazolását lásd a Függelékben.

Rátérünk a tétel bizonyítására.

$$(A) G = (p^\alpha | p^{\alpha-\beta} + 1 | p^{\beta+\delta}) \frac{b}{a}, \text{ ahol } p \in P_0, \alpha \geq 2, \alpha-1 \geq \beta \geq 1, \delta \geq 0.$$

Azt fogjuk vizsgálni, hogy melyik az a legkisebb nemnegatív γ , amellyel

létezik az $\omega: a \rightarrow ab^{p^\gamma}$ egyszerű automorfizmus. Azért keressük a lehető

legkisebb $\gamma - t$, mert annak birtokában kaphatjuk meg a legnagyobb

$\langle \omega \rangle$ ciklust az $\text{Aut } G$ – ben.

$$\text{Fönnáll, hogy } (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}} = a^{\left[(p^{\alpha-\beta}+1)p^\gamma | p^{\beta-\gamma+\delta} \right]}.$$

Tegyük föl először, hogy $\gamma < \beta$.

$$\text{Akkor igaz, hogy } (p^\alpha | (p^{\alpha-\beta} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta}) \cong (p^\alpha | (p^{\alpha-(\beta-\gamma)} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta}).$$

$$\text{Ezért } \left[(p^{\alpha-\beta} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta} \right] \equiv \left[p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma+\delta} \right] \equiv$$

$$\begin{aligned} &\equiv [p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma}] [(p^{\alpha-(\beta-\gamma)} + 1)^{p^{\beta-\gamma}} | p^\delta] \equiv \\ &\equiv p^\delta [p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma}] \equiv p^{\beta-\gamma+\delta} \quad (p^\alpha), \end{aligned}$$

$$\text{tehát } (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}} = a^{p^{\beta-\gamma+\delta}}. \quad (1)$$

Az (1) – ből csak akkor lehet levonni azt a következtetést, hogy

$$|ab^{p^\gamma}| = m, \quad (2)$$

$$\text{ha } \beta - \gamma + \delta \leq \alpha, \quad \text{azaz } \gamma \geq \beta - \alpha + \delta. \quad (3)$$

Tegyük föl, hogy γ kielégíti a (3) – at, s így (2) fennáll.

$$\text{Vizsgáljuk meg, hogy a } \partial(G) = \langle a^{p^{\alpha-\beta}} \rangle \leq \langle ab^{p^\gamma} \rangle \quad (4)$$

reláció milyen feltételek mellett teljesülhet.

$$\text{A (4) másképpen azt jelenti, hogy } a^{p^{\alpha-\beta}} \in \langle a^{p^{\beta-\gamma+\delta}} \rangle,$$

$$\text{amiből nyerjük, hogy } \alpha - \beta \geq \beta - \gamma + \delta, \quad \text{azaz } \gamma \geq 2\beta - \alpha + \delta \quad (5)$$

A továbbiakban tehát föl kell tennünk, hogy γ az (5) – öt is kielégíti.

Annak igazolása van hátra, hogy teljesül – e az alábbi reláció:

$$bab^{p^\gamma}b^{-1} = (ab^{p^\gamma})^{p^{\alpha-\beta+1}}. \quad (6)$$

Ha (5) – ben egyenlőség van, akkor $\alpha - \beta = \beta - \gamma + \delta$,

$$\begin{aligned} \text{s így } bab^{p^\gamma}b^{-1} &= a^{p^{\alpha-\beta+1}}b^{p^\gamma} = a^{p^{\alpha-\beta}}ab^{p^\gamma} = a^{p^{\beta-\gamma+\delta}}ab^{p^\gamma} = \\ &= (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}}ab^{p^\gamma} = (ab^{p^\gamma})^{p^{\alpha-\beta}}ab = (ab^{p^\gamma})^{p^{\alpha-\beta+1}}, \end{aligned}$$

tehát (6) fennáll.

Ha $2\beta - \alpha + \delta$ negatív, akkor $\gamma = 0$, és $\alpha - 2\beta - \delta$ pozitív. Ekkor

$$\text{bab}^{p^\gamma} \text{b}^{-1} = \text{ba} = \text{a}^{p^{\alpha-\beta+1}} \text{b}, \text{ és } (\text{ab}^{p^\gamma})^{p^{\alpha-\beta+1}} = (\text{ab})^{p^{\alpha-\beta+1}} = ((\text{ab})^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}} \text{ab} =$$

$$(\text{a}^{[p^{\alpha-\beta+1} p^{\beta+\delta}]})^{p^{\alpha-2\beta-\delta}} \cdot \text{ab} = (\text{a}^{[p^{\alpha-\beta+1} p^\beta] [(p^{\alpha-\beta+1}) p^\beta p^\delta]})^{p^{\alpha-2\beta-\delta}} \cdot \text{ab} =$$

$$(\text{a}^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}} \cdot \text{ab} = \text{a}^{p^{\alpha-\beta+1}} \text{b}, \text{ tehát (6) ismét teljesül.}$$

Igazoltuk, hogy a $\gamma < \beta$ esetben az $\omega: a \rightarrow \text{ab}^{p^\gamma}$ leképezés valóban automorfizmusa G -nek, ha γ teljesíti az (5)-öt.

Legyen most $\gamma \geq \beta$. Ez nyilván csak akkor lehetséges, ha $\delta > 0$.

$$\text{Ekkor viszont } \zeta_h(G) = \langle \text{b}^{p^\beta} \rangle, \text{ s így } \text{b}^{p^\gamma} \in \zeta_h(G). \text{ Ezért } \text{a} \rightleftharpoons \text{b}^{p^\gamma}.$$

Nézzük meg, mi a feltétele annak, hogy (2) teljesüljön.

$$\text{Mivel } (\text{ab}^{p^\gamma})^{p^\alpha} = \text{a}^{p^\alpha} \text{b}^{p^{\alpha+\gamma}}, \text{ ezért a (2) feltétele, hogy}$$

$$\alpha + \gamma \geq \beta + \delta \text{ legyen, amiből (3) következik.}$$

Mivel $\text{a} \rightleftharpoons \text{b}^{p^\gamma}$, ezért most is fönnáll (1), és a (4)-et vizsgálva ismét az (5)-re jutunk.

$$\text{A (6) relációnál a baloldal } \text{bab}^{p^\gamma} \text{b}^{-1} = \text{a}^{p^{\alpha-\beta+1}} \text{b}^{p^\gamma},$$

$$\text{a jobboldal } (\text{ab}^{p^\gamma})^{p^{\alpha-\beta+1}} = \text{a}^{p^{\alpha-\beta+1}} \text{b}^{p^{\alpha-\beta+\gamma+p^\gamma}}.$$

E két oldal tehát akkor egyezik meg, ha

$$p^{\alpha-\beta+\gamma} + p^\gamma \equiv p^\gamma \pmod{p^{\beta+\delta}}.$$

Ebből $\alpha - \beta + \gamma \geq \beta + \delta$ következik, ami az (5)-tel ekvivalens.

Tehát a (6) most is fennáll, az $\omega: a \rightarrow ab^{p^\gamma}$ leképezés az (5) teljesülése esetén akkor is automorfizmusa G -nek, ha $\gamma \geq \beta$.

$$(B) G = (2^\alpha | 2^{\alpha-\beta} + 1 | 2^\beta)_a^b, \text{ ahol } \alpha \geq 3, \alpha - 2 \geq \beta \geq 1.$$

E csoportnak létezni fog egy

$$\varphi : \begin{aligned} a &\rightarrow ab^{2^\gamma} \\ b &\rightarrow b^\varepsilon \end{aligned}$$

automorfizmusa, ahol γ a legkisebb nemnegatív szám, amelyre

$$\gamma \geq 2\beta - \alpha,$$

és $\varepsilon - t$ az alábbi kongruenciával lehet kiszámítani:

$$(2^{\alpha-\beta} + 1)^\varepsilon \equiv 2^{\alpha-\beta} (2^{\alpha-(\beta-\gamma)} + 1) + 1 \quad (2^\alpha).$$

A bizonyításhoz tekintsük az ab^{2^γ} elemet.

$$\text{Fennáll, hogy } (ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{\left[(2^{\alpha-\beta} + 1)^{2^\gamma} | 2^{\beta-\gamma} \right]}.$$

$$\text{Mivel } (2^\alpha | (2^{\alpha-\beta} + 1)^{2^\gamma} | 2^{\beta-\gamma}) \cong (2^\alpha | (2^{\alpha-(\beta-\gamma)} + 1)^{2^\gamma} | 2^{\beta-\gamma}),$$

$$\text{ezért } \left[(2^{\alpha-\beta} + 1)^{2^\gamma} | 2^{\beta-\gamma} \right] \equiv \left[2^{\alpha-(\beta-\gamma)} + 1 | 2^{\beta-\gamma} \right] \quad (2^\alpha),$$

$$\text{így kapjuk, hogy } (ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{2^{\alpha-1} + 2^{\beta-\gamma}} = a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1} + 1)},$$

amiből az $| ab^{2^\gamma} | = 2^\alpha$ relációra akkor következtethetünk, ha $\alpha \geq \beta - \gamma$,

azaz $\gamma \geq \beta - \alpha$. Ámde ez mindig fennáll, hiszen γ nemnegatív.

Mármost $\partial(G) = \langle a^{2^{\alpha-\beta}} \rangle$, és annak föltétele, hogy $\partial(G) \leq \langle ab^{2^\gamma} \rangle$ legyen, ez:

$$a^{2^{\alpha-\beta}} \in \langle a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)} \rangle = \langle ab^{2^{\beta-\gamma}} \rangle .$$

Ebből nyerjük az $\alpha - \beta \geq \beta - \gamma$, tehát a $\gamma \geq 2\beta - \alpha$ feltételt.

Igazolandó, hogy fönnáll a definiáló reláció:

$$b^\varepsilon ab^{2^\gamma} b^{-\varepsilon} = (ab^{2^\gamma})^{2^{\alpha-\beta}+1} . \quad (**)$$

E reláció baloldala így alakul: $b^\varepsilon ab^{2^\gamma} b^{-\varepsilon} = a^{(2^{\alpha-\beta}+1)\varepsilon} b^{2^\gamma}$.

Ha most $\gamma = 2\beta - \alpha$, azaz $\alpha - \beta = \beta - \gamma$, akkor (**) jobboldala:

$$(ab^{2^\gamma})^{2^{\alpha-\beta}+1} = (ab^{2^\gamma})^{2^{\beta-\gamma}} ab^{2^\gamma} = a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)} ab^{2^\gamma} = a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)+1} b^{2^\gamma} ,$$

és a két oldal pont akkor egyezik meg, ha

$$(2^{\alpha-\beta} + 1)^\varepsilon \equiv 2^{\alpha-\beta} (2^{\alpha-(\beta-\gamma)-1} + 1) + 1 \quad (2^\alpha) .$$

Ha most $\gamma > 2\beta - \alpha$, akkor γ minimalitása miatt $\gamma = 0$ és $\alpha - 2\beta$ pozitív.

Ekkor a (**) jobboldala így alakul:

$$\begin{aligned} (ab)^{2^{\alpha-\beta}+1} &= ((ab)^{2^\beta})^{2^{\alpha-2\beta}} ab = (a^{\lceil 2^{\alpha-\beta} + 1 \rceil 2^\beta})^{2^{\alpha-2\beta}} ab = a^{(2^{\alpha-1}+2^\beta) \cdot 2^{\alpha-2\beta}+1} b = \\ &= a^{2^{2\alpha-2\beta-1}+2^{\alpha-\beta}+1} b = a^{2^{\alpha-\beta}+1} b , \end{aligned}$$

hiszen $2^{2\alpha-2\beta-1} \equiv 0 \pmod{2^\alpha}$ pont azért, mert most $\alpha - 2\beta$ pozitív.

Jelen esetben tehát a (**) az $\varepsilon = 1$ választással kielégül.

Ha a $G = (2^\alpha \mid 2^{\alpha-\beta} + 1 \mid 2^{\beta+\delta}) \frac{b}{a}$ homológot vizsgáljuk, ahol $\delta > 0$, akkor a

fentiekkel teljesen analóg okoskodás a $\gamma \geq 2\beta - \alpha + \delta$ relációt fogja adni,

akárcsak e tétel (A) pontjában.

A homológképzésnél megszűnhet a csatolás. Pl. a $(16 \mid 5 \mid 4)_a^b$ - nek egy

$a \rightarrow ab^2, b \rightarrow b^3$ csatolt automorfizmusa van, ám a $(16 \mid 5 \mid 4)_a^b$ - nek

az $a \rightarrow ab^2$ leképezés egyszerű automorfizmusa.

(C) $G = (2^\alpha \mid 2^{\alpha-\beta} - 1 \mid 2^\beta)_a^b$, ahol $\alpha \geq 4, \alpha - 2 \geq \beta \geq 2$.

E csoportnak létezik egy

$$\omega : \begin{aligned} a &\rightarrow ab^{2^\gamma} \\ b &\rightarrow b^{2^{\gamma-1}} \end{aligned}$$

csatolt automorfizmusa, ahol $\gamma = \beta - 1$, és $|\omega| = 2$.

A bizonyítás stratégiája az eddigiekével azonos:

vizsgáljuk az ab^{2^γ} elemet :

$$(ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{[(2^{\alpha-\beta}-1)^{2^\gamma} 2^{\beta-\gamma}]}.$$

$$\text{Ámde } (2^\alpha \mid (2^{\alpha-\beta} - 1)^{2^\gamma} \mid 2^{\beta-\gamma}) \cong (2^\alpha \mid 2^{\alpha-(\beta-\gamma)} + 1 \mid 2^{\beta-\gamma}). \quad (***)$$

Ez azért van így, mert az $R_{2^\alpha} \cong (2^{\alpha-2}) \times (2)$, $\alpha \geq 3$ csoport szerkezete

olyan, minden (2^ε) $2 \leq \varepsilon \leq \alpha - 2$ ciklusból pontosan kettőt tartalmaz, amelyek

összemetszenek egy $(2^{\varepsilon-1})$ ciklusban. E szerkezet következménye, hogy

$$(2^\alpha \mid (2^{\alpha-\beta} - 1)^{2^\gamma} \mid 2^{\beta-\gamma}) \cong (2^\alpha \mid (2^{\alpha-\beta} + 1)^{2^\gamma} \mid 2^{\beta-\gamma}),$$

amiből a (***) már következik. A (***) következménye pedig ez:

$$\left[(2^{\alpha-\beta} - 1)^{2^\gamma} \mid 2^{\beta-\gamma} \right] \equiv \left[2^{\alpha-(\beta-\gamma)} + 1 \mid 2^{\beta-\gamma} \right] \equiv 2^{\beta-\gamma} (2^{\alpha-(\beta-\gamma)-1} + 1) \quad (2^\alpha).$$

Tehát $(ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)}$, amiből $|ab^{2^\gamma}| = 2^\alpha$ következik.

Most $\partial(G) = \langle a^{2^{\alpha-\beta-2}} \rangle = \langle a^2 \rangle$, és ahhoz, hogy

$$a^2 \in \langle a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)} \rangle = \langle a^{2^{\beta-\gamma}} \rangle \text{ teljesüljön, kell } \beta - \gamma \leq 1, \text{ azaz } \gamma \geq \beta - 1.$$

Ámde $\beta - 1 \geq \gamma$ is fönnáll, így kapjuk, hogy $\gamma = \beta - 1$.

Még azt kell belátni, hogy

$$b^{2^{\beta-1}+1} a b^{2^{\beta-1}} b^{-(2^{\beta-1}+1)} = (ab^{2^{\beta-1}})^{2^{\alpha-\beta-1}}.$$

$$\text{A baloldal: } b^{2^{\beta-1}+1} a b^{2^{\beta-1}} b^{-(2^{\beta-1}+1)} = a^{(2^{\alpha-\beta-1})^{2^{\beta-1}+1}} b^{2^{\beta-1}}, \quad (7)$$

$$\text{A jobboldal: } (ab^{2^{\beta-1}})^{2^{\alpha-\beta-1}} = a^{\left[(2^{\alpha-\beta-1})^{2^{\beta-1}} \mid 2^{\alpha-\beta-1} \right]} b^{2^{\beta-1}}. \quad (8)$$

Bizonyítandó, hogy $(7) = (8)$. Ehhez elég az a kitevőjével foglalkozni, azokat átalakítani, amihez a következő, könnyen (a binomiális együtthatók vizsgálatával) igazolható összefüggést használjuk föl:

$$(2^{\alpha-\beta} - 1)^{2^{\beta-1}} \equiv 2^{\alpha-1} + 1 \quad (2^\alpha).$$

Ezzel az a – nak a (7) – beli kitevője így alakul:

$$\begin{aligned} (2^{\alpha-\beta} - 1)^{2^{\beta-1}+1} &= (2^{\alpha-\beta} - 1)^{2^{\beta-1}} (2^{\alpha-\beta} - 1) \equiv (2^{\alpha-1} + 1)(2^{\alpha-\beta} - 1) \equiv \\ &\equiv 2^{2\alpha-\beta-1} + 2^{\alpha-\beta} - 2^{\alpha-1} - 1 \quad (2^\alpha). \end{aligned} \quad (9)$$

A (8) – beli kitevővel hosszabb a számolás:

$$\begin{aligned}
& \left[(2^{\alpha-\beta} - 1)^{2^{\beta-1}} \mid 2^{\alpha-\beta} - 1 \right] \equiv \left[2^{\alpha-1} + 1 \mid 2^{\alpha-\beta} - 1 \right] \equiv \left[2^{\alpha-1} + 1 \mid 2^{\alpha-\beta} - 2 + 1 \right] \equiv \\
& \equiv \left[2^{\alpha-1} + 1 \mid 2^{\alpha-\beta} - 2 \right] + (2^{\alpha-1} + 1)^{2^{\alpha-\beta}-2} \equiv \left[2^{\alpha-1} + 1 \mid 2^{\alpha-\beta} - 2 \right] + 1 \equiv \\
& \equiv \left[2^{\alpha-1} + 1 \mid 2 \right] \left[(2^{\alpha-1} + 1)^2 \mid 2^{\alpha-\beta-1} - 1 \right] \equiv \left[2^{\alpha-1} + 1 \mid 2 \right] (2^{\alpha-\beta-1} - 1) \equiv \\
& \equiv (2^{\alpha-1} + 2)(2^{\alpha-\beta-1} - 1) \equiv 2^{2\alpha-\beta-2} + 2^{\alpha-\beta} - 2^{\alpha-1} - 1 \quad (2^\alpha). \quad (10)
\end{aligned}$$

A (9) és (10) – et összevetve látjuk, hogy mindössze ennyi igazolandó:

$$2^{2\alpha-\beta-1} \equiv 2^{2\alpha-\beta-2} \quad (2^\alpha).$$

Ámde ez triviális, hiszen e kongruencia mindkét oldala osztható $2^\alpha -$ val – abból kifolyólag, hogy $\alpha - 2 \geq \beta$.

Az $|\omega| = 2$ közvetlen számolással adódik.

$$(D) G = (2^\alpha \mid 2^{\alpha-\beta} - 1 \mid 2^{\beta+\delta}) \frac{b}{a}, \text{ ahol } \alpha \geq 3, \alpha - 2 \geq \beta > 1, \delta \geq 1.$$

G – nek létezik egy $\omega : a \rightarrow ab^{2^{\beta+\delta-1}}$ egyszerű automorfizmusa.

A bizonyításnál ugyanúgy járunk el, mint (A) – nál: az $\omega - t$ $a \rightarrow ab^{2^\gamma}$ alakban keressük, szétválasztva a $\gamma < \beta$ és $\gamma \geq \beta$ eseteket.

$$(E) G = (2^\alpha \mid 2^\alpha - 1 \mid 2^{1+\delta}) \frac{b}{a}, \text{ ahol } \alpha \geq 2, \delta \geq 1.$$

Itt a következő számolás fogja mutatni egy $\omega : a \rightarrow ab^{2^\delta}$ automorfizmus meglétét: vizsgáljuk meg az ab^{2^γ} elemet .

$$(ab^{2^\gamma})^{2^{1-\gamma+\delta}} = a^{\left[(2^{\alpha-1})^{2^\gamma} \mid 2^{1-\gamma+\delta} \right]} = a^{2^{1-\gamma+\delta}}, \text{ ha } \gamma > 0, \text{ és } \gamma = 0 \text{ esetén}$$

$$(ab)^{2^{1+\delta}} = a^{\left[2^{\alpha-1}2^{1+\delta}\right]} = a^{\left[2^{\alpha-1}2\right] \cdot 2^{\delta}} = a^{2^{\alpha} \cdot 2^{\delta}} = 1.$$

Az $(ab^{2^{\gamma}})^{2^{1-\gamma+\delta}} = a^{2^{1-\gamma+\delta}}$ relációból csak akkor következik, hogy $|ab^{2^{\gamma}}| = 2^{\alpha}$,

ha $\alpha \geq 1 - \gamma + \delta$, azaz $\gamma \geq 1 - \alpha + \delta$.

Tegyük fel, hogy ez fönnáll, és nézzük meg, mi a helyzet a kommutátorral.

$$\partial(G) = \langle a^{2^{\alpha-2}} \rangle = \langle a^2 \rangle, \text{ és } \langle a^2 \rangle \leq \langle ab^{2^{\gamma}} \rangle \text{ pontosan akkor, ha } a^2 \in \langle a^{1-\gamma+\delta} \rangle.$$

Ez azonban csakis úgy teljesülhet, ha $2^{1-\gamma+\delta} | 2$, azaz $1 \geq 1 - \gamma + \delta$,

amiből $\gamma \geq \delta$ következik.

Csakhogy $1 + \delta > \gamma$ is fönnáll, ezért végül $\gamma = \delta$.

Mivel most $\zeta_h(G) = \langle b^2 \rangle$, és $\delta \geq 1$, ezért $b^{2^{\delta}} \in \zeta_h(G)$.

Ezért könnyű a $bab^{2^{\delta}}b^{-1} = (ab^{2^{\delta}})^{2^{\alpha-1}}$ reláció ellenőrzése.

$$\text{A baloldal } bab^{2^{\delta}}b^{-1} = a^{2^{\alpha-1}}b^{2^{\delta}},$$

$$\text{a jobboldal } (ab^{2^{\delta}})^{2^{\alpha-1}} = a^{2^{\alpha-1}}b^{2^{\alpha+\delta-2^{\delta}}},$$

és $2^{\alpha+\delta} - 2^{\delta} \equiv 2^{\delta} (2^{1+\delta})$, hiszen $\alpha \geq 2$ miatt $2^{1+\delta} | 2^{\alpha+\delta}$. Q. E. D.

1. LEMMA: Tekintsük az $(m | k | \dot{n} s)$, $s > 1$ csoportot. Ha $(m, s) = 1$,

akkor $(s) \times (m | k | \dot{n} s) \notin \mathcal{Ck}$.

Bizonyítás: Legyen $(s) \times G = (ms | 1 | \dot{n} s)_a^b = G_s$.

Ha most $(n, s) = 1$, akkor $G_s \in \mathcal{X}$, és készen vagyunk, hisz nyilvánvaló,

hogy $\mathcal{X} \cap \mathcal{C}_k = \emptyset$.

Tegyük föl ezért, hogy $\pi(s) \subset \pi(n)$. (11)

(Az $(n, s) \neq 1$ nem elég, mert ettől még előfordulhat, hogy az s -nek egy valódi osztójára, s' -re $(n, s') = 1$, ami megint a $G_s \in \mathcal{X}$ esetre vezetne.)

Tekintsük az ab^n elemet G_s -ben. Egyrészt $(ab^n)^s = a^s b^{ns} = a^s$,

és így $|ab^n| = ms$, másrészt $l \equiv 1 (s)$, ezért $a^{l-1} \in \langle a^s \rangle$, vagyis $\partial(G_s) \leq \langle a^s \rangle$.

Végül $bab^n b^{-1} = a^l b^n$, és $(ab^n)^l = a^l b^{nl}$, ámde ismét $l \equiv 1 (s)$ miatt

$n \equiv ln (ns)$, tehát $bab^n b^{-1} = (ab^n)^l$.

Könnyű látni azt is, hogy $\langle ab^n \rangle \cap \langle b \rangle = 1$.

Mindebből az következik, hogy a G_s -nek létezik egy

$$\varphi : \begin{array}{l} a \rightarrow ab^n \\ b \rightarrow b \end{array}$$

egyszerű automorfizmusa.

Q. E. D.

E lemma kapcsán fölmerülhet a kérdés, hogy az $a^s b^n$ elem miért ne lehetne

az a -nak automorf képe? Hiszen most is $|a^s b^n| = ms$,

és $(a^s b^n)^s = a^{s^2}$, $|a^{s^2}| = m$ miatt $\partial(G_s) \leq \langle a^{s^2} \rangle$.

Tehát az $\langle a^s b^n \rangle$ is egy ms -rendű ciklus, mely tartalmazza a kommutátort.

Ugyanakkor $(a^s b^n)^m = b^{mn}$, és mivel $\langle b^n \rangle \cong (s)$, és $(m, s) = 1$,

ezért $\langle b^{mn} \rangle = \langle b^n \rangle$. Tehát $\langle a^s b^n \rangle \cap \langle b \rangle = \langle b^n \rangle$.

Eszerint az $a^s b^n$ az a – nak csak valamilyen x – automorfizmusnál lehetne a képe, ami megint a $G_s \in \mathcal{X}$ esetre vezetne.

Másrészt azonban, ha (11) fönnáll, akkor a G_s – nek az $\langle a^s b^n \rangle$ szerinti

faktorcsoportha nem lehet ciklikus. E faktorcsoportha ugyanis így generálható:

$$a^{ms} = 1, \quad (12 a)$$

$$b^{ns} = 1, \quad (12 b)$$

$$b a b^{-1} = a^1, \quad (12 c)$$

$$a^s b^n = 1. \quad (12 d)$$

A (12 d) – ből egyrészt $a^{s^2} b^{ns} = a^{s^2} = 1$ következik, ami a (12 a) – val az

$$a^s = 1 \quad (12 e)$$

relációra vezet. Másrészt $a^{ms} b^{mn} = b^{mn} = 1$, ami a (12 b) és $(m, s) = 1$

figyelembe vételével a

$$b^n = 1 \quad (12 f)$$

relációt adja.

A (12 c) – ből $1 \equiv 1 (s)$ miatt lesz

$$b a b^{-1} = a. \quad (12 g)$$

Látnivaló, hogy a (12 e, f, g) relációk egy $(s) \times (n)$ – nel izomorf csoportot határoznak meg, ez azonban éppen a (11) miatt nem lehet ciklikus.

Ciklikus lesz viszont az $(n, s) = 1$ esetben, ami azt jelenti, hogy $G_s \in \mathcal{X}$.

E fejtegetések mellékterméke, hogy $\mathcal{X} \cap \mathcal{C}_k = \emptyset$.

Az 1. lemma lehetővé teszi, hogy bármely \mathcal{S} – csoportból kiindulva

\mathcal{C}_k – ba nem tartozó csoportot készíthessünk. A legegyszerűbb példa:

$G = (6 \mid 5 \mid 4)_a^b$. Ennél $\text{Aut } G = \langle \varphi, \psi, \sigma, \omega \rangle$, ahol

$$\varphi : a \rightarrow a^5, \quad |\varphi| = 2,$$

$$\psi : b \rightarrow ab, \quad |\psi| = 6,$$

$$\sigma : b \rightarrow b^3, \quad |\sigma| = 2,$$

$$\omega : a \rightarrow ab^2, \quad |\omega| = 2.$$

Több – kevesebb számolással kimutatható, hogy $\text{Aut} (6 \mid 5 \mid 4) \cong D_3 \times D_4$.

Nem látszik sokkal bonyolultabbnak a $G = (21 \mid 4 \mid 9)_a^b$ sem, holott itt

$\text{Aut } G = \langle \varphi_3, \varphi_7, \psi_3, \psi_7, \sigma, \omega \rangle$, ahol

$$\varphi_3 : a \rightarrow a^8, \quad |\varphi_3| = 2,$$

$$\varphi_7 : a \rightarrow a^{19}, \quad |\varphi_7| = 6,$$

$$\psi_3 : b \rightarrow a^7b, \quad |\psi_3| = 3,$$

$$\psi_7 : b \rightarrow a^3b, \quad |\psi_7| = 7,$$

$$\sigma : b \rightarrow b^4, \quad |\sigma| = 3,$$

$$\omega : a \rightarrow ab^3, \quad |\omega| = 3.$$

s így $|\text{Aut } G| = 2^2 \cdot 3^4 \cdot 7 = 2268$.

Ez is azt példázza, hogy a \mathcal{C}_k – n kívüli csoportok automorfizmuscsoportjainak meghatározására nincs általános módszer.

2. LEMMA: Ha $(m | k | n) \notin \mathcal{C}_k$, és $(m, s) = 1$, akkor $(s) \times (m | k | n) \notin \mathcal{C}_k$.

Bizonyítás: Ha $(m | k | n)_a^b \notin \mathcal{C}_k$, akkor a 38. o. (A 2) szerint van egy

$$\begin{aligned} \varphi: \quad a &\rightarrow a b^\beta, \quad \beta \downarrow n \\ b &\rightarrow b^\delta, \quad \delta \in \mathbf{R}_n \end{aligned}$$

automorfizmusa. A φ – re fölírt ún. kánon (36. o.):

$$[k^\beta | m] \equiv 0 (m), \quad (\text{KR } 1)$$

$$\beta m \equiv 0 (n), \quad (\text{KR } 2)$$

$$[k^\beta | k - 1] \equiv k^\delta - 1 (m), \quad (\text{KR } 3)$$

$$\beta (k - 1) \equiv 0 (n). \quad (\text{KR } 4)$$

(A \mathcal{J} – tétel (48. o.) bizonyításában láthattuk, hogy $[k^\beta | k] \equiv k^\delta (m)$ és

$\beta (k - 1) \equiv 0 (n)$ relációkból hogyan következik (KR 3).)

Most e lemmában azt kell bizonyítani, hogy ha (KR 1 – 4) – ben áttérünk

m –ről ms –re, k –ről j –re, ahol $(m, s) = 1$, és $j \equiv k (s)$, akkor

a (KR 1 – 4) relációk továbbra is érvényben maradnak. Rögtön látszik, hogy

csak a (KR 3) – at kell közelebbről megvizsgálni. Világos, hogy

$$[j^\beta | j - 1] \equiv j^\delta - 1 (ms)$$

pontosan akkor teljesül, ha

$$[j^\beta | j - 1] \equiv j^\delta - 1 (m), \quad (13)$$

$$\text{és} \quad [j^\beta | j-1] \equiv j^\delta - 1 \quad (s). \quad (14)$$

A (14) $j \equiv 1 \quad (s)$ miatt azonnal fönnáll, így csak a (13) – at kell ellenőrizni.

A $j \equiv k \quad (m)$ miatt (13) – ből lesz

$$[k^\beta | j-1] \equiv k^\delta - 1 \quad (m),$$

de a $j-1$ helyébe nem írható minden további nélkül $k-1$.

Legyen $j = k + mx$. Akkor

$$\begin{aligned} [k^\beta | j-1] &= [k^\beta | k-1 + mx] = [k^\beta | k-1] + k^{\beta(k-1)} [k | mx] = \\ &= (a \text{ (KR 4) miatt}) = [k^\beta | k-1] + [k^\beta | mx] = \\ &= [k^\beta | k-1] + [k^\beta | m] [k^{\beta m} | x] \equiv [k^\beta | k-1] \quad (m), \end{aligned}$$

mert (KR 1) miatt $[k^\beta | m] \equiv 0 \quad (m)$. Q. E. D.

Ha fúzióval akarunk \mathcal{Ch} – n kívüli csoportot előállítani, akkor az V. rész 3.

lemma (44. o.) miatt legalább az egyik fúziós tényezőnek \mathcal{Ch} – n kívül kell

lennie. A $(9|4|3) \otimes (7|4|3) \in \mathcal{Ch}$ példája azonban óvatosságra int, mert

a fúzió lehet \mathcal{Ch} – beli, dacára annak, hogy egy vagy minden tényezője \mathcal{Ch} – n

kívül esik. Tekintsük például ezeket:

$$(5|3|4) \in \mathcal{Ch},$$

$$(7|3|6) \in \mathcal{Ch},$$

$$(9|4|3) \notin \mathcal{Ch},$$

$$(16|5|4) \notin \mathcal{Ch}.$$

Kihasználva a fúzió asszociativitását, a fenti csoportok fúziója

kétféleképpen is felírható:

$$[(7|3|6) \otimes (16|5|4)] \otimes [(5|3|4) \otimes (9|4|3)] \quad (15)$$

$$[(7|3|6) \otimes (9|4|3)] \otimes [(5|3|4) \otimes (16|5|4)] \quad (16)$$

A (15) fölírásnál a szögletes zárójelben álló csoportok nincsenek \mathcal{Ch} – ban,

azonban a (16) – nál \mathcal{Ch} – ban vannak, így az V, rész 3. lemma (44. o.)

szerint ez a négyes fúzió \mathcal{Ch} – beli lesz. Magyarán szólva

$$G_1, G_2 \notin \mathcal{Ch} \nrightarrow G_1 \otimes G_2 \notin \mathcal{Ch} .$$

Legyen

$$G_1 = (p^\alpha | p^{\alpha-\beta} + 1 | p^\beta) , \quad p \in P_0 ,$$

$$G_2 = (q | k | r p^\delta) , \quad (p, qr) = 1 .$$

$$\text{Ekkor } G = G_1 \otimes G_2 = (p^\alpha q | j | r p^\varepsilon)_a^b ,$$

$$\text{ahol } j = s p^{\alpha-\beta} + 1 , \quad (p, s) = 1 \quad (17)$$

$$\varepsilon = \max(\beta, \delta) .$$

A (17) azért helyes, mert $j \equiv p^{\alpha-\beta} + 1 \pmod{p^\alpha}$,

$$\text{tehát} \quad j = u p^\alpha + p^{\alpha-\beta} + 1 ,$$

$$\text{azaz} \quad (u p^\beta + 1) p^{\alpha-\beta} + 1 = j .$$

Milyen feltételek mellett teljesül, hogy $G \notin \mathcal{Ch}$?

A továbbiak előtt jegyezzük meg a következőket:

Általában, ha $a \rightarrow ab^\beta, \beta \neq 0$ egyszerű automorfizmusa az $(m | k | n)_a^b$

csoportnak, akkor (K 31) és (K 32) miatt (36. o.)

$$(ab^\beta)^k = a^{[k^\beta | k]} b^{\beta k} = a^k b^\beta .$$

Akkor egyrészt $(ab^\beta)^{k-1} = ab^\beta (ab^\beta)^{-1} = a^k b^\beta b^{-\beta} a^{-1} = a^{k-1} ,$

másrészt $(ab^\beta)^{k-1} = a^{[k^\beta | k-1]} b^{\beta(k-1)} = a^{[k^\beta | k-1]} .$

(Itt ismét használtuk a (K 32) – t, 36. o.)

Ezekből kapjuk, hogy $[k^\beta | k - 1] \equiv k - 1 \pmod{m} .$ (K 311)

Térjünk vissza a 77. oldali G csoporthoz.

Keressük b – nek azt a legkisebb kitevőjét – méghozzá $t p^\gamma , t \mid r , \varepsilon > \gamma$

alakban, amellyel a $\varphi : a \rightarrow ab^{tp^\gamma}$ egyszerű automorfizmusa lesz G – nek.

A (K 12) – be (36. o.) írjuk be a megfelelő adatokat, akkor kapjuk, hogy

$$t p^{\alpha+\gamma} \equiv 0 \pmod{p^\varepsilon r} .$$

Ebből $t \equiv 0 \pmod{r}$ következik.

Viszont föl volt téve, hogy $t \mid r$, ezért végül kapjuk, hogy $t = r$. (18)

Írjuk föl a (K 311) – et :

$$\left[(sp^{\alpha-\beta} + 1)^{p^\gamma r} \mid sp^{\alpha-\beta} \right] \equiv sp^{\alpha-\beta} \pmod{p^\alpha q} .$$
 (19)

Régebbi vizsgálódásainkból (ld. TÉTEL (A) – ban az (5) $\delta = 0$ – val, 64. o.)

már tudjuk, hogy mod p^α nézve a (19) – et, a $\gamma \geq 2\beta - \alpha$ (20)

relációra jutunk.

Ha most mod q nézzük a (19) – et:

$$\left[(sp^{\alpha-\beta} + 1)^{p^{\gamma r}} \mid sp^{\alpha-\beta} \right] \equiv sp^{\alpha-\beta} \quad (q). \quad (21)$$

Mivel G_2 – re (a 77. oldalon) semmilyen kikötéssel nem éltünk, a (21) akkor lesz biztosan igaz, ha $\gamma \geq \delta$.

(Ekkor ugyanis $(sp^{\alpha-\beta} + 1)^{p^{\gamma r}} \equiv 1 (q)$, s így (21) automatikusan teljesül.)

Mármost $\varepsilon = \max(\beta, \delta) > \gamma \geq \delta$ - ből következik, hogy $\varepsilon = \beta$,

s mivel nyilván $\varepsilon > \gamma$, végül nyerjük, hogy $\beta - 1 \geq \gamma \geq \delta$. (22)

A φ leképezésünk tehát mindenestre olyan lesz, hogy benne b kitevője

(19) miatt $r p^\gamma$ alakú, ahol γ – nak ki kell elégítenie a (20) és (22)

relációkat. (Nem vizsgáltuk az ab^{rp^γ} rendjét, mert (K 311) biztosítja, hogy ez a rend $p^\alpha q$.)

Írjuk föl még (K 32) – t is (36. o.) ; kapjuk belőle, hogy

$$\alpha - \beta + \gamma \geq \varepsilon, \text{ azaz } \gamma \geq \varepsilon - \alpha + \beta \quad (23)$$

A megfelelő γ – nak tehát a (20) , (22) és (23) relációkat ki kell elégítenie.

De ez csak látszólag három reláció, ugyanis most $\varepsilon = \beta$, és így a (23) – ből

$\gamma \geq 2\beta - \alpha$, ami a (20) – szal azonos.

Az elmondottakból most már világos, hogy a

$(7 \mid 4 \mid 3) \otimes (9 \mid 4 \mid 3) = (63 \mid 4 \mid 3)$ miért lesz \mathcal{CA} – beli.

Foglaljuk össze az eddigieket:

3. LEMMA: Legyen

$$G_1 = (p^\alpha | p^{\alpha-\beta} + 1 | p^\beta), \text{ ahol } p \in P_0, \alpha-1 \geq \beta \geq 1,$$

$$G_2 = (q | k | r p^\delta), \quad (p, qr) = 1, \beta-1 \geq \delta \geq 0.$$

Akkor a $G = G_1 \otimes G_2 = (p^\alpha q | s p^{\alpha-\beta} + 1 | p^\beta r)_a^b$, $(s, p) = 1$ csoport

automorfizmuscsoportja tartalmaz egy $\langle \varphi \rangle$ ciklust, ahol $\varphi: a \rightarrow ab^{rp^\gamma}$

egyszerű automorfizmus, és γ az a legkisebb nemnegatív egész, mely

kielégíti a $\gamma \geq 2\beta - \alpha$, és $\beta - 1 \geq \gamma \geq \delta$ relációkat. Q. E. D.

A következő két lemma a 2 – magok fúziójával foglalkozik, és bizonyításuk

a 3. lemmában látottakkal teljesen analóg.

4. LEMMA: Tekintsük a

$$(2^\alpha | 2^{\alpha-\beta} + 1 | 2^\beta), \quad \alpha \geq 3, \alpha-2 \geq \beta \geq 1$$

$$\text{és } (q | k | 2^\delta | r), \quad (2, qr) = 1, \beta-1 \geq \delta \geq 0$$

csoportokat. Ezek fúziójának, a

$$G = (2^\alpha q | s 2^{\alpha-\beta} + 1 | 2^\beta r)_a^b, \quad (2, s) = 1$$

csoportnak lesz egy

$$\omega: \begin{aligned} a &\rightarrow ab^{2^\gamma r} \\ b &\rightarrow b^\varepsilon \end{aligned}$$

automorfizmusa, ahol $\gamma \geq 2\beta - \alpha$ és ε alkalmas $\mathbf{R}_{2^{\beta r}}$ – beli szám. Q. E. D.

5. LEMMA: A

$$(2^\alpha | 2^{\alpha-\beta} - 1 | 2^\beta), \alpha \geq 4, \alpha - 2 \geq \beta \geq 2$$

és $(q | k | 2^\delta r), (2, qr) = 1, \beta - 1 \geq \delta \geq 0$

csoportok fúziójaként előálló

$$G = (2^\alpha q | s 2^{\alpha-\beta} + 1 | 2^\beta r)_a^b, (2, s) = 1$$

csoportnak lesz egy

$$\omega : \begin{aligned} a &\rightarrow ab^{r \cdot 2^{\beta-1}} \\ b &\rightarrow b^{r \cdot 2^{\beta-1} + 1} \end{aligned}$$

c – automorfizmusa, és $|\omega| = 2$.

Q. E. D.

Az e részbeli tételben, illetve a 3., 4., és 5. lemmákban külön nem vizsgáltuk,

hogyan szereplő $(m | k | n)_a^b$ csoportoknál az ab^β elem (az a automorf képe)

által generált ciklus diszjunkt lesz – $\langle b \rangle$ – vel (ami pedig fontos feltétele

annak, hogy ab^β tényleg automorf képe legyen a – nak).

Mivel a fent említett állításokban csak p – csoportok, illetve \mathcal{S} – csoportok

szerepelnek, a következő két lemma segít a fenti probléma megoldásában.

6. LEMMA: Ha $(m | k | n) \in \mathcal{S}$, akkor tetszőleges $b \in \mathbf{Z}_n$ esetén

$$\langle ab^\beta \rangle \cap \langle b \rangle = 1.$$

Bizonyítás: Tegyük föl, hogy $b^x \in \langle ab^\beta \rangle$. Ekkor nyilván $b^x \rightleftharpoons ab^\beta$, ezért

$b^x a b^\beta b^{-x} = a b^\beta$. Másrészt $b^x a b^\beta b^{-x} = a^{k^x} b^\beta$, ahonnan $k^x \equiv 1 \pmod{m}$

következik, ami a csoport \mathcal{S} – belisége miatt csak $x = 0$ – val elégíthető ki.

Q. E. D.

7. LEMMA: Legyen a $G = (m \mid k \mid n)_a^b$ csoportban az m egy prím hatványa,

és tegyük föl, hogy $|ab^\beta| = m$, valamint $\partial(G) \leq \langle ab^\beta \rangle$. Akkor

$$\langle ab^\beta \rangle \cap \langle b \rangle = 1.$$

Bizonyítás: Ha $b^x \in \langle ab^\beta \rangle$ valamely $x \neq 0$ számmal, akkor $\langle b \rangle \cap \partial(G) = 1$

miatt $\langle b^x \rangle \cap \partial(G) = 1$, s mivel $\partial(G) \leq \langle ab^\beta \rangle$, azt kapjuk, hogy egy prímhatvány-

rendű ciklusban diszjunkt valódi részek vannak, ami nyilván lehetetlen.

Q. E. D.

VII. RÉSZ NYITOTT KÉRDÉSEK

1. DEFINÍCIÓ: Legyen G tetszőleges véges csoport, $|G| = n$.

Azt mondjuk, hogy a G – nek a $p \in \pi(n)$ prímre vonatkozó bősége $\alpha -$ jelben $w_p(G) = \alpha -$, ha G – ben van $(p)^\alpha$ részcsoporthoz, de $(p)^{\alpha+1}$ már nincs.

Legyen $w(G) = \max \{ w_p(G) \mid p \in \pi(n) \}$.

Nyilvánvaló, hogy minden G csoportra $w(G) \geq 1$.

1. SEJTÉS: Ha $G \in \text{CYCYS}$, akkor $w(G) \leq 2$.

Ez ekvivalens azzal, hogy ha $G \in \text{CYCYS}$, akkor G bármely részcsoporthoz legföljebb két generátorral prezentálható.

Az I. rész 3. lemmában (15. o.) megállapítottuk, hogy $\text{CYCYS} \subset \text{DIV}$.

2. SEJTÉS: $\text{CYCYS} \subset \text{TODIV}$.

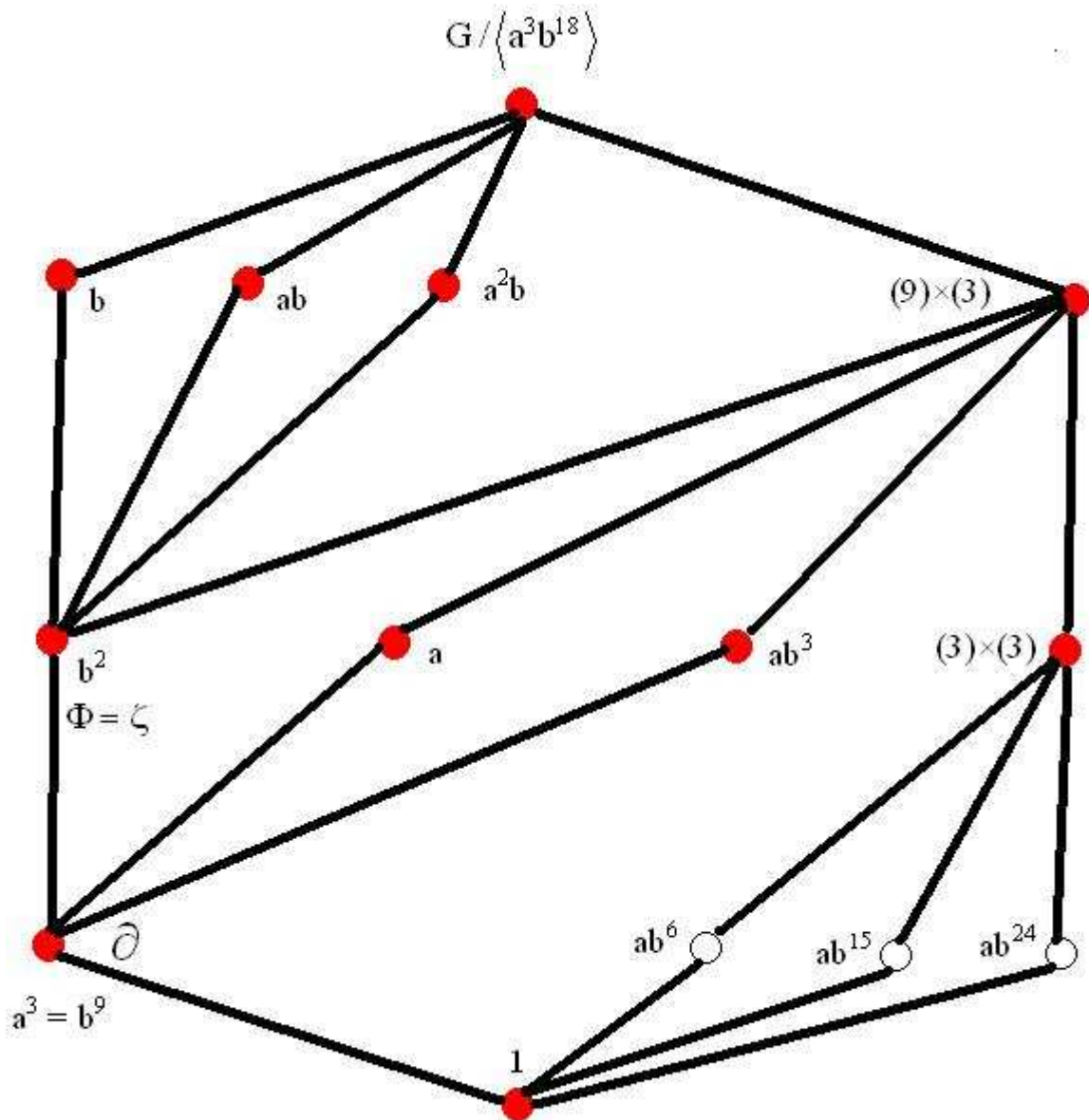
E sejtésre rögvest igent mondhatnánk, ha kiderülne, hogy a $G \in \text{CYCYS}$ minden részcsoporthoz abeli vagy CYCYS beli. Ez azonban sajnos nem igaz.

A legkisebb ellenpélda a $(8 \mid 3 \mid 2)_a^b$, ahol $\langle a^2, ab \rangle \cong Q$.

Hasonlóan nem áll, hogy egy CYCYS beli csoport minden nemabeli faktorcsoporthoz CYCYS beli. Itt a minimális ellenpélda a $G = (4 \mid 3 \mid 4)_a^b$, ahol az $\langle a^2b^2 \rangle$ szerinti faktorcsoporthoz Q – val izomorf.

Egy kevésbé egyszerű ellenpélda a $G = (9 \mid 4 \mid 27)_a^b$,

ahol a $G / \langle a^3b^{18} \rangle$ a következő hálóval rendelkező csoportot adja:



Piros körök jelölik a normálosztókat. E csoport jól láthatóan nem áll elő egyetlen normálosztójának széteső bővítéseként sem.

Az imént vázolt csoport a következő csoportosztályba tartozik:

2. DEFINÍCIÓ: $(m \mid r, k \mid n) \frac{b}{a}$ – vel jelöljük a következő prezentációt:

$$a^m = b^n = 1, \quad (1)$$

$$a^{\frac{m}{r}} = b^{\frac{n}{r}}, \quad (2)$$

$$b a b^{-1} = a^k. \quad (3)$$

E relációk konzisztenciájához az alábbiak szükségesek:

$$r \neq m, \quad r \neq n, \quad (4)$$

$$r \mid (m, n, k-1), \quad (5)$$

$$k^{\frac{n}{r}} \equiv 1 \pmod{m}. \quad (6)$$

A (4) a (2) miatt világos. A (6) a (3) – ből nyerhető:

$$b^{\frac{n}{r}} a b^{-\frac{n}{r}} = a^{k^{\frac{n}{r}}},$$

azaz $a^{\frac{m}{r}} a a^{-\frac{m}{r}} = a^{k^{\frac{n}{r}}}$, ahonnan (6) következik valóban.

Az $r \mid m$ és $r \mid n$ a (2) – ből világos.

Az $r \mid k-1$ – hez gondoljuk meg a következőket:

$$\text{A (3) – ből} \quad b a^{\frac{m}{r}} b^{-1} = a^{\frac{m}{r}k},$$

$$\text{és (2) miatt} \quad b b^{\frac{n}{r}} b^{-1} = b^{\frac{n}{r}k},$$

$$b^{\frac{n}{r}} = b^{\frac{n}{r}k}$$

$$\text{amiből} \quad 1 = b^{\frac{n}{r}(k-1)}, \text{ azaz } \frac{n}{r}(k-1) \equiv 0 \pmod{n}.$$

Innen adódik az $r \mid k-1$.

Az (1), (2), (3) által prezentált csoportok halmazát CYCEX – nek nevezzük.

Rendkívül érdekes, hogy a CYCEX csoportok CYCYSbeli csoportok

faktorcsoporthaikként kaphatók, ugyanakkor $CYCYS \subset CYCEX$,

hiszen elég (2) – ben az $r = 1$ választással élni.

Végezetül még egy talány:

3. SEJTÉS: $CYCYS \subset MAXPIND$.

FÜGGELÉK

A 63. oldalon felsorolt összefüggések bizonyítása:

(i) $[s p^{\alpha-\beta} + 1 \mid p^\beta] \equiv p^\beta \pmod{p^\alpha}$, ahol $p \in P_0$, $0 \leq \beta \leq \alpha$, $(s, p) = 1$.

Bizonyítás: $[s p^{\alpha-\beta} + 1 \mid p^\beta] = \frac{(sp^{\alpha-\beta} + 1)^{p^\beta} - 1}{sp^{\alpha-\beta}} =$

$$= p^\beta + \sum_{k=2}^{p^\beta} \binom{p^\beta}{k} s^{k-1} p^{(k-1)(\alpha-\beta)},$$

ahol a szumma minden tagja osztható p^α – val.

Q. E. D.

(ii) $[s 2^{\alpha-\beta} + 1 \mid 2^\beta] \equiv 2^{\alpha-1} + 2^\beta \pmod{2^\alpha}$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.

Bizonyítás: $[s 2^{\alpha-\beta} + 1 \mid 2^\beta] = \frac{(s \cdot 2^{\alpha-\beta} + 1)^{2^\beta} - 1}{s \cdot 2^{\alpha-\beta}} =$

$$= 2^\beta + \binom{2^\beta}{2} s \cdot 2^{\alpha-\beta} \equiv 2^\beta + 2^{\alpha-1} (2^\beta - 1) s, \text{ de } s = 2^j + 1, j > 0 \text{ esetén}$$

$$2^\beta + 2^{\alpha-1} (2^\beta - 1) (2^j + 1) = 2^\beta + 2^{\alpha-1+\beta} \cdot 2^{\alpha-1+j} - 2^{\alpha-1+j} + 2^{\alpha-1+\beta} - 2^{\alpha-1} \equiv$$

$$\equiv 2^\beta - 2^{\alpha-1} \equiv 2^\beta + 2^{\alpha-1} \pmod{2^\alpha}, \text{ hiszen } -2^{\alpha-1} \equiv 2^{\alpha-1} \pmod{2^\alpha}. \quad \text{Q. E. D.}$$

(iii) $[s 2^{\alpha-\beta} - 1 \mid 2^\beta] \equiv 2^{\alpha-1} \pmod{2^\alpha}$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.

Bizonyítás: $[s \cdot 2^{\alpha-\beta} - 1 \mid 2^\beta] =$

$$= [s \cdot 2^{\alpha-\beta} - 1 \mid 2] \left[(s \cdot 2^{\alpha-\beta} - 1)^2 \mid 2 \right] \dots \left[(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-1}} \mid 2 \right] = s \cdot 2^{\alpha-\beta} \cdot 2^{\beta-1} \cdot A,$$

ahol A páratlan. Végeredményben $[s \cdot 2^{\alpha-\beta} - 1 \mid 2^\beta] \equiv 2^{\alpha-1} B (2^\alpha)$, ahol

$$B = 2j + 1, \text{ és így } 2^{\alpha-1} B = 2^\alpha j + 2^{\alpha-1} \equiv 2^{\alpha-1} (2^\alpha). \quad \text{Q. E. D.}$$

(i v) $(m \mid k \mid n) \cong (m \mid 1 \mid n)$ esetén $[k \mid n] \equiv [1 \mid n] (m)$.

Bizonyítás: egészen triviális.

Q. E. D.

IRODALOM

KUROS: CSOPORTELMÉLET

NIVEN – ZUCKERMAN: BEVEZETÉS A SZÁMELMÉLETBE

HUPPERT: ENDLICHE GRUPPEN I.

COXETER – MOSER: GENERATORS AND RELATIONS

FOR DISCRETE GROUPS

Itt végződik a CYCYS eredeti kézírata.

UTÓIRAT: (Kristóf Miklós)

Huber László 1997 július 2 – án meghalt, 42 éves volt. Kézírata azóta várt hogy végre megjelenhessen. Szerintem a legnagyobb felfedezése az izostruktúrális csoportok volt, ez egy érdekes szimmetria a csoportok világában. Akit a téma jobban érdekel, írjon a címemre: kristofmiklos@freemail.hu.