

Huber László

**Véges ciklikus csoportoknak
véges ciklikus csoportokkal való
széteső bővítéseiről**

1995

**Barátomnak és Uranita
testvéremnek szeretettel**

**Mota
1995. 12. 08.**

TARTALOM

Köszönetnyilvánítás

Jelölések

**I. rész: A vizsgált objektum
Alaptulajdonságok és alaptételek**

II. rész: Reprezentációk

III. rész: Nevezetes részcsoporthok

IV. rész: Az automorfizmusokról általában

V. rész: Ch – csoportok

VI. rész: Csoportok a $Ch - n$ kívül

VII. rész: Nyitott kérdések

Függelék

Irodalom

Utóirat

Köszönetnyilvánítás

Köszönettel tartozom Corrádi Keresztélynek és Csörgő Piroskának, akik nélkül érdeklődésem a csoportelmélet iránt bizonynyal 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

Jelölések

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 lko-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.
$pr(m)$	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-részcssoportja.
$\Phi_e(G)$	lásd a 23. oldalt..
$\Phi_h(G)$	lásd a 23. oldalt..
$(m \mid k \mid n)$	lásd a 2. oldalt..
$(m \mid k \mid n)_a^b$	lásd a 2. oldalt..
$(m \mid k \mid \cdot n)$	lásd a 10. oldalt..
$(m \mid r, k \mid n)$	lásd a 84. oldalt..
$(m \mid r, k \mid n)_a^b$	lásd a 84. oldalt..
$[k \mid \alpha]$	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 $n_1 \mid n$. 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 részcssoport prím indexű.
CYCEX	85. oldal.
$\text{MAX}(G)$	a G csoport maximális részcssoportjainak 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 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.
$\mathcal{K}$	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.
$(p)^\alpha$	$(p) \times (p) \times \dots \times (p)$
α -tényező	$\underbrace{\hspace{10em}}$
$w_p(G)$	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

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

[2]

$$\text{és } \Delta_{\Gamma(AB)} \text{ az egyetlen } bab^{-1} = a^k \tag{1}$$

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

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

$$\text{Az (1) relációból } b^n ab^{-n} = a^{k^n} = 1 \cdot a \cdot 1 = a = a^1$$

azaz

$$k^n \equiv 1 \pmod{m} \tag{3}$$

más szóval $|k|_m \mid n$ következik.

A (2) csoport pont akkor lesz nemabeli, ha

$$k > 1 \tag{4}$$

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

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

s így

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

[3]

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 $\mathbf{R}_m$ -ben:

$$(m \mid k \mid n) \cong (m \mid l \mid n) \iff \langle k \rangle = \langle l \rangle \leq \mathbf{R}_m.$$

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 $\varphi(a) = c^\gamma$, $\gamma \in \mathbf{R}_m$

$$\varphi(b) = d^\delta, \quad \delta \in \mathbf{R}_n.$$

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

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

amiből

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

A (7) és (8) -ból

$$c^{\gamma \cdot k} = c^{\gamma \cdot l^\delta} \quad \text{adódik,}$$

majd $\gamma \in \mathbf{R}_m$ miatt

$$k \equiv l^\delta \quad (m), \quad \text{végül}$$

$\delta \in \mathbf{R}_n$ 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:

$\text{Ha } (n) \equiv \langle b \rangle$, akkor

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

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

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

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

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

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

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

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

$$(a^\alpha \cdot b^\beta)^\gamma = a^{\alpha \cdot \gamma} \cdot b^{\beta \cdot \gamma}.$$

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

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

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

Q . E . D .

Az (V) -ben szereplő $[\mid]$ 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

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

[6]

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

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

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

Némi számolással pl. megmutatható, hogy

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

2. TÉTEL (PART = PARTÍCIÓTÉTEL)

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

$$(m, s) = 1, \quad 1 \equiv 1(s), \quad \langle k \rangle = \langle 1 \rangle \leq R_m.$$

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

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

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

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

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

akkor és csak akkor, ha

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

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

Bizonyítás (a) Tekinthető 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 $k \equiv k_i(m_i), i = 1, 2$.

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

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 $x \equiv a_i (n_i)$ kongruenciarendszernek pontosan akkor van megoldása, ha minden i, j párra, ahol $1 \leq i \leq j \leq r$,

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 $(m_i \mid k_i \mid n_i)_{a_i} b_i^{t_i}$ -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

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

[9]

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

$$x \in \mathbf{R}_{n_1 \cdot n_2}, \quad \text{hogy} \\ (m_1 \mid k_1^{t_1} \mid n_1)_{a_1} b_1^{t_1} \times (m_2 \mid k_2^{t_2} \mid n_2)_{a_2} b_2^{t_2} \equiv (m_1 \cdot m_2 \mid k^x \mid n_1 \cdot n_2)_a b^x.$$

Mindez a (10) -et bizonyítja.

Q . E . D .

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

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

mind a négy csoport izomorf a

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

csoporttal.

3. DEFINÍCIÓ Azon CYCYS - csoportokat, amelyeknek nincs triviálistól

különböző direkt faktora, **felbonthatatlanoknak** 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 felbont-

hatatlan 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 $(m | k | \hat{n})$, $(m | k | \cdot n)$, $(m | k | (\cdot n) s)$, vagy $(m | k | \hat{n} s)$

jelöléseket is. Az $(m | k | \hat{n})$ 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)

[12]

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

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

$(k^{n_i} \equiv 1 (m_i))$ 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 átmegy a szokásos direkt szorzatba.)

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

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

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

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

[13]

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.

[14]

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 $(m|k|\cdot n)$ csoportot magnak nevezzük pont akkor, ha

az m egy prím hatványa. A magok halmazát $\mathfrak{M}$ 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.

(folytatás: CYC3 2004.9.5 e)

[15]

Különös sajátosságai a fúzióknak az alábbiak:

(a) 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

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

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

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

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

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

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

(b) Minden $G \in \text{CYCYS}$ része valamely ciklus holomorfjának.

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

ezért tegyük föl, hogy $G = (m \mid k \mid \dot{n} \cdot s)$, 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

$$(m \mid k \mid \dot{n}) \otimes (p \mid k_p \mid \sqcup(n s)) = (mp \mid 1 \mid \sqcup(n s))_b^a$$

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

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

Nyilvánvaló, hogy

$$(m \mid k \mid \dot{n}) \leq \text{Hol}(m) \cong (m) \cdot R_m, \quad (15),$$

hiszen $\langle k \rangle \leq R_m$.

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

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

II. rész Reprezentációk

(A) A legegyszerűbb a $\mathbf{Z}_m \times \mathbf{Z}_n$ – ben való ábrázolás.

A szorzási szabály:

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

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

Könnyen kiszámolható, hogy az

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

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

(B) Egyszerű számolás mutatja, hogy az alábbi, modulo m vett

mátrixokkal való reprezentáció az $(m | k | n)_a^b$ csoportokra megfelelő:

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

(C) Permutációkkal való reprezentációk.

1. LEMMA: A $G = (m | k | n)_a^b$ csoportnak létezik izomorf képe az $\mathbf{S}_m$ – 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 részcsoporthoz, amelynek összes G – beli konjugáltja csak triviálisan metsződik,

[18]

akkor G izomorf módon leképezhető $\mathbf{S}_k$ – ba.

Mármint 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 $\mathcal{S}$ – csoportokra, és a jegyhalmaz legyen a

$$\mathbf{Z}_m = \{ 0, 1, 2, 3, \dots m-1 \} .$$

Az $(m | k | n)_a^b$ egy jó reprezentációját kapjuk az $\mathcal{S}_m$ – ben a következőképpen:

az a és b hatása legyen az alábbi:

$$\forall i \in \mathbf{Z}_m : a(i) = i + 1 \bmod m,$$

$$b(i) = k \cdot i \bmod m .$$

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

$$|a| = m.$$

[19]

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 $k \mid m' \mid k \mid m$ 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:

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

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

ami teljessé teszi annak igazolását, hogy valóban jó $\mathcal{S}_m$ – belí reprezentációt

[20]

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 ismertett 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 $\mathcal{S}_{60}$ helyett az $\mathcal{S}_{3+4+5} = \mathcal{S}_{12}$ –ben .

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

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

$(m \mid k \mid \dot{n})$ csoportot az $\mathcal{S}_{m_1 + m_2 + \dots + m_r}$ 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 $(m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_r \mid k \mid \dot{n})$ 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 $(m \mid k \mid \dot{n} \cdot s)_a^{b^*}$, $s > 1$ 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 $(m \mid k \mid \dot{n})_a^b$ 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

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



III. rész

Nevezetes részcsoporthok

(A) p – CSOPORTOK. NILPOTENCIA Kommutátor, Centrum, Frattini – részcsoporth.

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 $G \rightarrow \mathfrak{S}$ – 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 faktorcsoporthja ciklikus.

ZASSENHAUS bebizonyította, hogy minden véges Z – metaciklikus csoport előállítható $\mathfrak{S}$ – csoportként.

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

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

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

Bizonyítás: közvetlen számolással. Q. E. D.

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

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

[22]

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 $G_i \in \mathcal{Z} \cap \mathcal{S}$, $i = 1, 2, \dots, r$, akkor

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

Bizonyítás: Egyszerű számelméleti megfontolásokkal az $\mathcal{S}$, $\mathcal{Z}$ 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 $k-1$ ismét páros, ezért $|\zeta_e(G)| = (m, k-1) \geq 2$.

[23]

(ii) Legyen $m = 2^\alpha \cdot m_1$, $\alpha \geq 1$, $m_1 > 1$, és $(2, m_1) = 1$. Ha n páratlan, akkor $|k|_m$ is az, ezért k csakis $\mathbf{R}_{m_1}$ – beli lehet, vagyis $k \equiv 1 \pmod{2^\alpha}$.

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

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

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

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

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

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

csoporthot értjük.

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

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

Ha pedig $\beta \in \mathbf{R}_n$, 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 $\alpha \notin \mathbf{R}_m$ és $\beta \notin \mathbf{R}_n$.

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

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

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

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

[24]

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

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

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

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

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

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

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

$$\left. \begin{aligned} \Phi(G) &= \langle a^{p_1 p_2 \dots p_r}, b^\gamma \rangle, \\ \text{ahol } \forall q \in \pi(n): q \mid \gamma. \end{aligned} \right\} (\star)$$

A következőket láttuk be:

$$\underline{\text{6. LEMMA:}} \quad (\text{i}) \quad \Phi(G) = \Phi_e(G) \Phi_h(G),$$

$$(\text{ii}) \quad \Phi_e(G) = \Phi(a). \quad \text{Q. E. D.}$$

Általában $\Phi_h(G) \neq \Phi(b)$. Ha például $G = (p \mid k \mid (p-1))$, $p \in P_0$, akkor Könnyen kiszámolható, hogy $\Phi_h(G) = 1$. Biztosan nagyobb lesz azonban a

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

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

(B) p – CSOPORTOK. NILPOTENCIA.

3. DEFINÍCIÓ: A CYCYS-beli p – csoportok ($p \in \mathbf{P}$) halmazát $\mathbf{p}$,
a nilpotenseket $\mathbf{N}$ fogja jelölni.

9. LEMMA: A $\mathbf{p} \cap \mathbf{N}$ elemei az alábbiak:

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

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

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

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

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

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

a következőt látjuk be:

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

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

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

[27]

Legyen ismét $0 \leq \gamma < \beta$.

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

Könnyű kiszámolni, hogy

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

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

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

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 $G = \left(\bigtimes_{i=1}^r G_{p_i} \right) \times (q)$ (2)

[28]

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 – részcsoportja megegyezik a tényezők Frattini – részcsoportjainak 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, ($p \in \mathcal{P}$), 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 – részcsoporttal kapcsolatban:

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

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:

[31]

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

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

$\Phi(G) \triangleleft G$ miatt $k^y \equiv 1 \pmod{p}$, és ebből következik, hogy $q_i \mid y$, $i = 1, 2, \dots, r$, tehát $[q_1, q_2, \dots, q_r] \mid y$.

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

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

15. LEMMA:

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

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

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

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

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.

(i i) Ez (i) –ből folyik, de most $\varepsilon_i = \delta_i = 0$, $i = 1, 2, \dots, r$.

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

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

[32]

(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

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

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

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

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

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

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

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

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

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

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

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

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

[33]

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.

[34]

IV. rész

Az automorfizmusokról általában

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

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

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:

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

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

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

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

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 fennáll.) Ez nyilvánvalóan csak úgy lehetséges, ha a mondott részek centrálisak, izomorfok, és mind $\langle a \rangle$ - nak, mind $\langle b \rangle$ - nek direkt faktori. Az alábbi láttuk be:

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

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

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 fennáll, keresztező automorfizmusnak (x – automorfizmusnak) nevezzük.

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

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

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 fölteszük, hogy $G \notin \mathcal{X}$.

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

$$\varphi(a) = a^\alpha b^\beta, \quad (7)$$

$$\varphi(b) = a^\gamma b^\delta$$

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

Az m a legkisebb pozitív egész, amelyre

$$\alpha [k^\beta \mid m] \equiv 0 \pmod{m}, \quad (\text{K } 11)$$

$$\text{és } \beta m \equiv 0 \pmod{n}, \quad (\text{K } 12)$$

Az n a legkisebb pozitív egész, amelyre

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

$$\text{és } \delta n \equiv 0 \pmod{n}, \quad (K 22)$$

valamint

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

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

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.

[37]

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 $G = (16 | 3 | 4)_a^b$ 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 $a \rightarrow a^\mu$, $\mu \in R_m$ egyszerű automorfizmusai egy

R_m - mel izomorf részcsoporthot generálnak $\text{Aut } G$ – ben.

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

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

automorfizmusa.

(B . 1) A G – nek $b \rightarrow b^\delta$ automorfizmusa $\delta \in R_n$ mellett csak akkor létezhet, ha $G \notin \mathcal{S}$.

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

(a) $\delta \in R_n$, $\delta \in R_n \Leftrightarrow G \notin \mathcal{S}$;

(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 egy ψ :

$$a \rightarrow a^\alpha b^\beta, \beta \neq 0,$$

$$b \rightarrow b^\delta, \delta \in R_n$$

automorfizmusának, mely $\delta = 1$ esetben egyszerű, és csatolt, ha $\delta \in R_n$.

Először mutassuk ki, hogy $\alpha \in R_m$. 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 $\alpha \in R_m$.

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

Ilyen fölírás mindig lehetséges.

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

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

$$\Psi_{\alpha^{-1}} \circ \Psi = \varphi: \quad a \rightarrow a b^\beta, \beta \downarrow n$$

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

(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 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.

[40]

(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 automorfizmus 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),

$$\text{valamint a } [k^\beta | k] \equiv k (m) \quad (K_1 31)$$

relációkból áll.

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

$$k^\delta \equiv k (m) \quad (K_2 31)$$

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

[41]

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

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

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

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

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

$$\begin{aligned} [k^{\beta} \mid k] &= [k^{\beta} \mid k - 1 + 1] = [k^{\beta} \mid k - 1] + k^{\beta(k-1)} [k^{\beta} \mid 1] \equiv \\ &\equiv [k^{\beta} \mid k - 1] + 1 \equiv k \pmod{m}, \text{ azaz} \\ [k^{\beta} \mid k - 1] &\equiv k - 1 \pmod{m} \end{aligned} \quad (9)$$

Írjuk be ide (8) – at a baloldalra:

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

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

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

Alkalmazva a (10) – et:

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

tehát a $(\oplus)$ teljesül.

Ha most β helyett egy β t többszöröst veszünk, akkor

[42]

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

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

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 $G \notin \mathfrak{X}$, 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 $G = (m \mid k \mid n)_a^b$. 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.

[43]

V. rész Ch – csoportok

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

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

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

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

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

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

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

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

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

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

[44]

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

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

Mivel ciklikus csoportnak minden részcsoportha karakterisztikus, kapjuk, hogy

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

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

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

és az előbbieket értelmében $\varphi(a_1) = a_1^{\alpha_1}$, $\alpha_1 \in R_s$.

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 $\mathcal{S}$ -csoportokra szorítkozni.

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

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

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

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

[45]

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

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

$$a_1 a_2 \rightarrow a_1 a_2 (a_1 a_2)^\beta$$

φ :

$$b_1 b_2 \rightarrow (b_1 b_2)^\delta$$

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

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

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

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

$$\text{Ebből} \quad [k^\beta | m_2] \equiv 0 \pmod{m_2} \quad (1 \text{ a})$$

$$\text{és} \quad \beta m_2 \equiv 0 \pmod{n_2} \quad (1 \text{ b})$$

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 $k - t \bmod m_2$, a β és $\delta - t \bmod n_2$, azaz legyen

[46]

$$k = k_2 + m_2 x,$$

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

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

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 k_2 – 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 $\left[k_2^{\beta_2} \mid m_2 \right] \equiv 0 \pmod{m_2}$.

Kaptuk tehát, hogy

$$\left[k_2^{\beta_2} \mid k_2 \right] \equiv k_2^{\delta_2} \pmod{m_2}. \quad (1 \text{ c c})$$

Az (1 d) –ből:

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

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 $G_2 \in \mathbf{Ch}$ Q. E. D.

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

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

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

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

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

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

4. LEMMA:

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

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

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

Bizonyítás: egyszerű számolással.

Q. E. D.

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

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

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

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

Ekkor a G – nek létezik egy

$$a \rightarrow a b^\beta, \beta \downarrow n$$

φ :

$$b \rightarrow b^\delta, \delta \in R_n$$

automorfizmusa (ld. 38. o. (A 2)).

Írjuk föl a (K 31) – et (36. o.) $\alpha = 1, \gamma = 0$ szereposztással:

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

Ebből a (K 32) – vel (36. o.) :

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

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

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

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

[49]

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

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 $G \in \mathcal{S}$.

Q. E. D.

Az 1. lemma és az 1. tétel szerint

$$\mathcal{B} \cup \mathcal{Q} \cup \mathcal{R} \cup \mathcal{Z} \subset \mathcal{A}.$$

Hogy ez a tartalmazás valódi, azt a $(63 \mid 4 \mid 3)$ csoport bizonyítja.

(Egyébként $\mathfrak{Z} \cap \mathfrak{S} \subset \mathfrak{B}$. Ha ugyanis $(m \mid k \mid n) \in \mathfrak{Z}$, akkor

$(m, k-1) = 1$, és így a $k^n - 1 = (k-1) [k \mid n] \equiv 0 \pmod{m}$ relációból $[k \mid n] \equiv 0 \pmod{m}$ következik.) ($\triangleleft$)

2. TÉTEL: Legyen $(m \mid k \mid \dot{n}) \in \mathfrak{Ch}$. Akkor

[50]

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

(i i) $\text{Aut}(m \mid k \mid \dot{n}) \cong \text{Hol}(m)$ pontosan akkor, ha $(m \mid k \mid \dot{n}) \in \mathfrak{B}$;

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

Bizonyítás:

(i) A $G = (m \mid k \mid n)_a^b \in \mathfrak{Ch}$ összes automorfizmusa most

$$a \rightarrow a^\alpha, \quad \alpha \in R_m$$

$\varphi :$

$$b \rightarrow a^\gamma b, \quad \gamma \in Z_m$$

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

$$\varphi_\alpha : a \rightarrow a^\alpha, \quad \alpha \in R_m$$

$$\varphi_\gamma : b \rightarrow a^\gamma b, \quad \gamma \in Z_m$$

egyszerű automorfizmusok.

Nyilvánvaló, hogy $\langle \{\varphi_\alpha \mid \alpha \in R_m\} \rangle \cong R_m$.

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

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

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

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

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

[51]

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 $[k | n] \equiv 0 (m)$, 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. ($\triangleleft$)).

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

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

[52]

ahol $\varphi : b \rightarrow ab$,

$$\varphi_\alpha : a \rightarrow a^\alpha, \alpha \in R_m .$$

A φ nyilván belső automorfizmus, hiszen

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

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

A φ_α pont akkor lesz belső automorfizmus minden $\alpha \in R_m$ esetében, ha

$$\langle k \rangle \cong R_m,$$

amiből – és a centrumnélküliségből – valóban $m = p^\alpha$, $p \in P_0$, $k \in \text{pr}(p^\alpha)$ 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) $G \in \mathcal{T}$,

(i i) $G = (2p^\alpha \mid k \mid p^{\alpha-1}(p-1))_a^b$, $p \in P_0$, $k \in \text{pr}(2p^\alpha)$,

(i i i) $G \cong D_4$.

Bizonyítás: Az (i) – t elintézi az 5. lemma, az (i i i) – nél egyszerű számolás segít, így elég az (i i) – vel foglalkozni.

Az (i i) – beli csoportok a $\mathcal{T}$ – csoportokból állnak elő úgy, hogy azokat előlről megszorozzuk egy (2) ciklussal. Az 5. lemma szerint $\mathcal{T} \subset \mathcal{B}$, és

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

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

[53]

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

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

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 $G = (m \mid k \mid \dot{n})_a^b$ csoportokra, ahol $m \in PR$, $k \in \text{pr}(m)$, fönnáll:

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

és más csoportokra ez nem teljesül.

7. LEMMA: A $G = (m \mid k \mid n)_a^b$ csoportban a $\langle b \rangle$ – nek akkor és csak akkor van m számú különböző automorf képe, ha $[k \mid n] \equiv 0 \pmod{m}$.

Bizonyítás: Tekintsük a

$$a \rightarrow a,$$

$$b \rightarrow a^\gamma b, \gamma \in \mathbf{Z}_m$$

leképezést. Ezzel

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

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,

[54]

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

[55]

automorf képeivel csak triviálisan metsződik, vagyis

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

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

Az (5) mármost csakis akkor teljesül, ha

$$\forall \gamma \in \mathbf{Z}_m \forall v \downarrow n: \gamma[k|v] \not\equiv 0 \pmod{m}.$$

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 $\langle a^\mu, b^v \rangle$ 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

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

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

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

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

[56]

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 $p \in \mathbf{P}$, $r|p-1$.

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 $(m \mid k \mid n)$ csoport, ahol $n \in P$.

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

hogy ha $(m \mid k \mid \dot{n})_a^b \in \mathcal{S}$, akkor b minden automorf képe megkapható konjugálással. Ezért elég bizonyítani, hogy esetünkben a $\langle b \rangle$ bármely, tőle különböző konjugáltjával diszjunkt:

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

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

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

[57]

következik.

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

tehát $y \equiv 0 \pmod{n}$, ellentmondásban az $y \in \mathbb{Z}_n$ föltevessel.

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

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

De ebből megint $y \equiv 0 \pmod{n}$ következik, mert $\mathbb{R}_{p^\alpha} = (p^{\alpha-1}) \times (p-1)$, 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 $(p \mid k \mid pr)$ főrész nincs $\mathcal{S}$ –ben, s így

$\mathcal{M}^*$ –ben sem, a (d) –nél pedig a $(p^{\alpha-1} \mid k^r \mid p^\beta)$ főrész vizsgálata vezet hasonló eredményre, (hiszen ha $|k^r|_{p^\alpha} = p^\beta$, akkor $|k^r|_{p^{\alpha-1}} = p^{\beta-1}$). Q. E. D.

[58]

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

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

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

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

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

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

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

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

Bizonyítás: (A) triviális.

(B) Mindenekelőtt jegyezzük meg, hogy

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

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

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

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 $n_i \mid p_i - 1$.

[59]

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 $(m \mid k \mid n) \in \mathcal{M}^*$ és n összetett szám.

$$\text{Tekintsük az } (s) \times (m \mid k \mid n) \cong (ms \mid l \mid n) \quad (8)$$

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 $\forall v \downarrow n : (ms, [l \mid v]) = 1$.

Mármint $k \equiv 1 (m)$ miatt $(m, [l \mid v]) = 1$,

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

Mivel most $l \equiv 1 \pmod{s}$, ezért $[1 | v] \equiv v \pmod{s}$, és így
 $(s, [1 | v]) = 1$ csakis úgy teljesülhet, ha $(s, v) = 1$.

Mivel ennek minden $v \downarrow n$ számra fenn 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.)

[60]

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

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 $\langle a^\mu, b^v \rangle$ főrészt ($\mu \downarrow m, v \downarrow n$).

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

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

$$\left[k^v | \frac{n}{v} \right] \equiv 0 \pmod{m}.$$

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

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

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

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

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

$p_i^{\alpha_i} \nmid k-1, i = 1, 2, \dots, r,$

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

[61]

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

$$n | p_i - 1, i = 1, 2, \dots$$

(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 $(p_i^{\alpha_i} | k_i | n)_{a_i}^{b_i}$ 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

$$\langle a, b_1^{t_1} b_2^{t_2} \dots b_r^{t_r} \rangle \cong \langle a, (b_1^{t_1} b_2^{t_2} \dots b_r^{t_r})^x \rangle, \text{ ha } x \in \mathbf{R}_n.$$

Ezért az adott n – hez tartozó nem izomorf, de nyilván izostruktúrális

$\mathcal{M}$ – csoportok száma

[62]

(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

$$(p) \times (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} | k | n) \in \mathcal{M} \text{ is.}$$

12. LEMMA: Legyen $p \in \mathcal{P}$, $1 < r | p - 1$, $s \geq 1$. Akkor

$$(p^\alpha | k | (p^\beta r)s) \in \mathcal{Z}.$$

Bizonyítás: Ha p osztaná $k - 1$ -et, azaz fölírható volna

$$k = t p^\gamma + 1, \gamma \geq 1, (t, p) = 1$$

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 $\mathcal{P} \cap \mathcal{C}$ -ban vannak:

$$(a) \quad (2^\alpha | 2^{\alpha-1} | 2)_a^b, \alpha \geq 3,$$

$$(b) \quad D_{2^\alpha}, \alpha \geq 2.$$

Bizonyítás: (a) Tekintsük az $a^\gamma b$, $\gamma \in \mathbb{Z}_m$ elemet:

$$(a^\gamma b)^2 = a^{\gamma[2^{\alpha-1}-1|2]} = a^{2^{\alpha-1}\alpha}, \text{ s így } |a^\gamma b| \leq 4.$$

$$(b) \quad D_{2^\alpha} \in \mathcal{M} \subset \mathcal{B} \subset \mathcal{C}.$$

Q. E. D.

[63]

VI. rész

Csoportok a $\mathcal{Ch} - n$ kívül

TÉTEL: Az V. rész 5. tételében felsoroltakon kívül minden más p – csoport a $\mathcal{Ch} - n$ kívül van.

Bizonyítás: A következőkben erősen támaszkodunk az alábbi összefüggésekre:

- (i) $[s p^{\alpha-\beta} + 1 | p^\beta] \equiv p^\beta (p^\alpha)$, ahol $p \in P_0$, $0 \leq \beta \leq \alpha$, $(s, p) = 1$.
- (i i) $[s 2^{\alpha-\beta} + 1 | 2^\beta] \equiv 2^{\alpha-1} + 2^\beta (2^\alpha)$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.
- (i i i) $[s 2^{\alpha-\beta} - 1 | 2^\beta] \equiv 2^{\alpha-1} (2^\alpha)$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.
- (i v) Ha $(m | k | n) \cong (m | l | n)$, 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.

$$\text{Fönnáll, hogy } (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}} = a^{[(p^{\alpha-\beta}+1)p^\gamma | p^{\beta-\gamma+\delta}]}.$$

Tegyük föl először, hogy $\gamma < \beta$.

$$\text{Akkor igaz, hogy } (p^\alpha | (p^{\alpha-\beta} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta}) \equiv (p^\alpha | (p^{\alpha-(\beta-\gamma)} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta}).$$

$$\text{Ezért } [(p^{\alpha-\beta} + 1)^{p^\gamma} | p^{\beta-\gamma+\delta}] \equiv [p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma+\delta}] \equiv$$

[64]

$$\begin{aligned} &\equiv [p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma}] [(p^{\alpha-(\beta-\gamma)} + 1)^{p^{\beta-\gamma}} | p^\delta] \equiv \\ &\equiv p^\delta [p^{\alpha-(\beta-\gamma)} + 1 | p^{\beta-\gamma}] \equiv p^{\beta-\gamma+\delta} (p^\alpha), \end{aligned}$$

$$\text{tehát } (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}} = a^{p^{\beta-\gamma+\delta}}. \quad (1)$$

Az (1) – ből csak akkor lehet levonni azt a következtetést, hogy

$$|ab^{p^\gamma}| = m, \quad (2)$$

$$\text{ha } \beta - \gamma + \delta \leq \alpha, \text{ azaz } \gamma \geq \beta - \alpha + \delta. \quad (3)$$

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.

$$\text{A (4) másképpen azt jelenti, hogy } a^{p^{\alpha-\beta}} \in \langle a^{p^{\beta-\gamma+\delta}} \rangle,$$

$$\text{amiből nyerjük, hogy } \alpha - \beta \geq \beta - \gamma + \delta, \text{ azaz } \gamma \geq 2\beta - \alpha + \delta \quad (5)$$

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.

[65]

Ha $2\beta - \alpha + \delta$ negatív, akkor $\gamma = 0$, és $\alpha - 2\beta - \delta$ pozitív. Ekkor

$$\begin{aligned} bab^{p^\gamma}b^{-1} &= ba = a^{p^{\alpha-\beta+1}}b, \text{ és } (ab^{p^\gamma})^{p^{\alpha-\beta+1}} = (ab)^{p^{\alpha-\beta+1}} = ((ab)^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}}ab = \\ &= (a^{[p^{\alpha-\beta+1}|p^{\beta+\delta}]})^{p^{\alpha-2\beta-\delta}} \cdot ab = (a^{[p^{\alpha-\beta+1}|p^\beta]})^{[(p^{\alpha-\beta+1})p^\beta|p^\delta]} \cdot ab = \\ &= (a^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}} \cdot ab = a^{p^{\alpha-\beta+1}}b, \text{ tehát (6) ismét teljesül.} \end{aligned}$$

Igazoltuk, hogy a $\gamma < \beta$ esetben az $\omega: a \rightarrow ab^{p^\gamma}$ leképezés valóban automorfizmusa G – nek, ha γ teljesíti az (5) – öt.

Legyen most $\gamma \geq \beta$. Ez nyilván csak akkor lehetséges, ha $\delta > 0$.

$$\text{Ekkor viszont } \zeta_h(G) = \langle b^{p^\beta} \rangle, \text{ s így } b^{p^\gamma} \in \zeta_h(G). \text{ Ezért } a \rightleftharpoons b^{p^\gamma}.$$

Nézzük meg, mi a feltétele annak, hogy (2) teljesüljön.

Mivel $(ab^{p^\gamma})^{p^\alpha} = a^{p^\alpha}b^{p^{\alpha+\gamma}}$, ezért a (2) feltétele, hogy

$\alpha + \gamma \geq \beta + \delta$ legyen, amiből (3) következik.

Mivel $a \equiv b^{p^\gamma}$, ezért most is fennáll (1), és a (4) – et vizsgálva ismét az (5) – re jutunk.

A (6) relációnál a baloldali $bab^{p^\gamma}b^{-1} = a^{p^{\alpha-\beta+1}}b^{p^\gamma}$,

a jobboldali $(ab^{p^\gamma})^{p^{\alpha-\beta+1}} = a^{p^{\alpha-\beta+1}}b^{p^{\alpha-\beta+\gamma+p^\gamma}}$.

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.

[66]

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) $G = (2^\alpha \mid 2^{\alpha-\beta} + 1 \mid 2^\beta)_a^b$, ahol $\alpha \geq 3$, $\alpha - 2 \geq \beta \geq 1$.

E csoportnak létezni fog egy

$$a \rightarrow ab^{2^\gamma}$$

$\varphi:$

$$b \rightarrow b^\varepsilon$$

automorfizmusa, ahol γ a legkisebb nemnegatív szám, amelyre

$$\gamma \geq 2\beta - \alpha,$$

és $\varepsilon - t$ az alábbi kongruenciával lehet kiszámítani:

$$(2^{\alpha-\beta} + 1)^\varepsilon \equiv 2^{\alpha-\beta} (2^{\alpha-(\beta-\gamma)} + 1) + 1 \pmod{2^\alpha}.$$

A bizonyításhoz tekintsük az ab^{2^γ} elemet.

Fennáll, hogy $(ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{\left[(2^{\alpha-\beta+1})^{2^\gamma} \mid 2^{\beta-\gamma}\right]}$.

Mivel $(2^\alpha \mid (2^{\alpha-\beta} + 1)^{2^\gamma} \mid 2^{\beta-\gamma}) \cong (2^\alpha \mid (2^{\alpha-(\beta-\gamma)} + 1)^{2^\gamma} \mid 2^{\beta-\gamma})$,

ezért $\left[(2^{\alpha-\beta} + 1)^{2^\gamma} \mid 2^{\beta-\gamma}\right] \equiv \left[2^{\alpha-(\beta-\gamma)} + 1 \mid 2^{\beta-\gamma}\right] \pmod{2^\alpha}$,

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 $(16 \mid 5 \mid 4) \frac{b}{a}$ - nek egy

$a \rightarrow ab^2, b \rightarrow b^3$ csatolt automorfizmusa van, ám a $(16 \mid 5 \mid 4) \frac{b}{a}$ - nek az $a \rightarrow ab^2$ leképezés egyszerű automorfizmusa.

(C) $G = (2^\alpha \mid 2^{\alpha-\beta} - 1 \mid 2^\beta) \frac{b}{a}$, ahol $\alpha \geq 4, \alpha - 2 \geq \beta \geq 2$.

E csoportnak létezik egy

$$a \rightarrow ab^{2^\gamma}$$

ω :

$$b \rightarrow b^{2^{\gamma-1}}$$

csatolt automorfizmusa, ahol $\gamma = \beta - 1$, és $|\omega| = 2$.

A bizonyítás stratégiája az eddigiekével azonos:

vizsgáljuk az ab^{2^γ} elemet :

$$(ab^{2^\gamma})^{2^{\beta-\gamma}} = a^{[(2^{\alpha-\beta}-1)2^\gamma | 2^{\beta-\gamma}]}$$

$$\text{Ámde } (2^\alpha | (2^{\alpha-\beta}-1)2^\gamma | 2^{\beta-\gamma}) \cong (2^\alpha | 2^{\alpha-(\beta-\gamma)} + 1 | 2^{\beta-\gamma}). \quad (***)$$

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

$$(2^\alpha | (2^{\alpha-\beta}-1)2^\gamma | 2^{\beta-\gamma}) \cong (2^\alpha | (2^{\alpha-\beta}+1)2^\gamma | 2^{\beta-\gamma}),$$

amiből a (***) már következik. A (***) következménye pedig ez:

[69]

$$[(2^{\alpha-\beta}-1)2^\gamma | 2^{\beta-\gamma}] \equiv [2^{\alpha-(\beta-\gamma)} + 1 | 2^{\beta-\gamma}] \equiv 2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1} + 1) \quad (2^\alpha).$$

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 fennáll, így kapjuk, hogy $\gamma = \beta - 1$.

Még azt kell belátni, hogy

$$b^{2^{\beta-1}+1}ab^{2^{\beta-1}}b^{-(2^{\beta-1}+1)} = (ab^{2^{\beta-1}})^{2^{\alpha-\beta-1}}.$$

$$\text{A baloldal: } b^{2^{\beta-1}+1}ab^{2^{\beta-1}}b^{-(2^{\beta-1}+1)} = a^{(2^{\alpha-\beta}-1)2^{\beta-1}+1}b^{2^{\beta-1}}, \quad (7)$$

$$\text{A jobboldal: } (ab^{2^{\beta-1}})^{2^{\alpha-\beta-1}} = a^{[(2^{\alpha-\beta}-1)2^{\beta-1} | 2^{\alpha-\beta-1}]}b^{2^{\beta-1}}. \quad (8)$$

Bizonyítandó, hogy (7) = (8). Ehhez elég az a kitevőjével foglalkozni,

azokat átalakítani, amihez a következő, könnyen (a binomiális együtthatók vizsgálatával) igazolható összefüggést használjuk föl:

$$(2^{\alpha-\beta}-1)^{2^{\beta-1}} \equiv 2^{\alpha-1} + 1 \pmod{2^\alpha}.$$

Ezzel az a – nak a $(7) -$ beli kitevője így alakul:

$$\begin{aligned} (2^{\alpha-\beta}-1)^{2^{\beta-1}+1} &= (2^{\alpha-\beta}-1)^{2^{\beta-1}} (2^{\alpha-\beta}-1) \equiv (2^{\alpha-1}+1)(2^{\alpha-\beta}-1) \equiv \\ &\equiv 2^{2\alpha-\beta-1} + 2^{\alpha-\beta} - 2^{\alpha-1} - 1 \pmod{2^\alpha}. \end{aligned} \quad (9)$$

A $(8) -$ beli kitevővel hosszabb a számolás:

[70]

$$\begin{aligned} \left[(2^{\alpha-\beta}-1)^{2^{\beta-1}} \mid 2^{\alpha-\beta}-1 \right] &\equiv \left[2^{\alpha-1}+1 \mid 2^{\alpha-\beta}-1 \right] \equiv \left[2^{\alpha-1}+1 \mid 2^{\alpha-\beta}-2+1 \right] \equiv \\ &\equiv \left[2^{\alpha-1}+1 \mid 2^{\alpha-\beta}-2 \right] + (2^{\alpha-1}+1)^{2^{\alpha-\beta}-2} \equiv \left[2^{\alpha-1}+1 \mid 2^{\alpha-\beta}-2 \right] + 1 \equiv \\ &\equiv \left[2^{\alpha-1}+1 \mid 2 \right] \left[(2^{\alpha-1}+1)^2 \mid 2^{\alpha-\beta-1}-1 \right] \equiv \left[2^{\alpha-1}+1 \mid 2 \right] (2^{\alpha-\beta-1}-1) \equiv \\ &\equiv (2^{\alpha-1}+2)(2^{\alpha-\beta-1}-1) \equiv 2^{2\alpha-\beta-2} + 2^{\alpha-\beta} - 2^{\alpha-1} - 1 \pmod{2^\alpha}. \end{aligned} \quad (10)$$

A (9) és $(10) -$ et összevetve látjuk, hogy mindössze ennyi igazolandó:

$$2^{2\alpha-\beta-1} \equiv 2^{2\alpha-\beta-2} \pmod{2^\alpha}.$$

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.

$$(ab^{2^\gamma})^{2^{1-\gamma+\delta}} = a^{\left[(2^\alpha-1)^{2^\gamma} 2^{1-\gamma+\delta} \right]} = a^{2^{1-\gamma+\delta}}, \text{ ha } \gamma > 0, \text{ és } \gamma = 0 \text{ esetén}$$

$$(ab)^{2^{1+\delta}} = a^{\left[2^{\alpha-1}2^{1+\delta}\right]} = a^{\left[2^{\alpha-1}2\right]2^{\delta}} = a^{2^{\alpha} \cdot 2^{\delta}} = 1.$$

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 $2^{1-\gamma+\delta} \mid 2$, azaz $1 \geq 1 - \gamma + \delta$,

amiből $\gamma \geq \delta$ következik.

Csak hogy $1 + \delta > \gamma$ 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.

A baloldal $bab^{2^{\delta}}b^{-1} = a^{2^{\alpha-1}}b^{2^{\delta}}$,

a jobboldal $(ab^{2^{\delta}})^{2^{\alpha-1}} = a^{2^{\alpha-1}}b^{2^{\alpha+\delta-2^{\delta}}}$,

és $2^{\alpha+\delta} - 2^{\delta} \equiv 2^{\delta} \pmod{2^{1+\delta}}$, hiszen $\alpha \geq 2$ miatt $2^{1+\delta} \mid 2^{\alpha+\delta}$. Q. E. D.

1. LEMMA: Tekintsük az $(m \mid k \mid \dot{n} s)$, $s > 1$ csoportot. Ha $(m, s) = 1$,

akkor $(s) \times (m \mid k \mid \dot{n} s) \notin \mathcal{A}$.

Bizonyítás: Legyen $(s) \times G = (ms \mid 1 \mid \dot{n} s)_a^b = G_s$.

Ha most $(n, s) = 1$, akkor $G_s \in \mathcal{X}$, és készen vagyunk, hisz nyilvánvaló,

hogy $\mathcal{X} \cap \mathcal{A} = \emptyset$.

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 osztója, $s' - re (n, s') = 1$, 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 $1 \equiv 1 \pmod{s}$, ezért $a^{1-1} \in \langle a^s \rangle$, vagyis $\partial(G_s) \leq \langle a^s \rangle$.

Végül $bab^n b^{-1} = a^1 b^n$, és $(ab^n)^1 = a^1 b^{n1}$, ámde ismét $1 \equiv 1 \text{ (s)}$ miatt

$n \equiv 1n \text{ (ns)}$, tehát $bab^n b^{-1} = (ab^n)^1$.

Könnyű látni azt is, hogy $\langle ab^n \rangle \cap \langle b \rangle = 1$.

Mindebből az következik, hogy a G_s -nek létezik egy

$$a \rightarrow ab^n$$

φ :

$$b \rightarrow b$$

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 $(m, s) = 1$,

[73]

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 $G_s \in \mathcal{A}$ esetre vezetne.

Másrészt azonban, ha (11) fennáll, akkor a G_s – nek az $\langle a^s b^n \rangle$ szerinti faktorcsoportha nem lehet ciklikus. E faktorcsoportha ugyanis így generálható:

$$a^{ms} = 1, \quad (12 \text{ a})$$

$$b^{ns} = 1, \quad (12 \text{ b})$$

$$b a b^{-1} = a^1, \quad (12 \text{ c})$$

$$a^s b^n = 1. \quad (12 \text{ d})$$

A (12 d) – ből egyrészt $a^{s^2} b^{ns} = a^{s^2} = 1$ következik, ami a (12 a) – val az

$$a^s = 1 \quad (12 \text{ e})$$

relációra vezet. Másrészt $a^{ms} b^{mn} = b^{mn} = 1$, ami a (12 b) és $(m, s) = 1$

figyelembe vételével a

$$b^n = 1 \quad (12 \text{ f})$$

relációt adja.

A (12 c) – ből $l \equiv 1$ (s) miatt lesz

$$b a b^{-1} = a \quad . \quad (12 g)$$

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 $G_s \in \mathcal{X}$.

[74]

E fejtegetések mellékterméke, hogy $\mathcal{X} \cap \mathcal{C} = \emptyset$.

Az 1. lemma lehetővé teszi, hogy bármely $\mathcal{S}$ – csoportból kiindulva

$\mathcal{C}$ – 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

$$\varphi_3 : a \rightarrow a^8, \quad |\varphi_3| = 2,$$

$$\varphi_7 : a \rightarrow a^{19}, \quad |\varphi_7| = 6,$$

$$\psi_3 : b \rightarrow a^7 b, \quad |\psi_3| = 3,$$

$$\psi_7 : b \rightarrow a^3 b, \quad |\psi_7| = 7,$$

$$\sigma : b \rightarrow b^4, \quad |\sigma| = 3,$$

$$\omega : a \rightarrow ab^3, \quad |\omega| = 3.$$

s így $|\text{Aut } G| = 2^2 \cdot 3^4 \cdot 7 = 2268$.

Ez is azt példázza, hogy a $\mathcal{C}_n$ – n kívüli csoportok automorfizmuscsoportjainak meghatározására nincs általános módszer.

2. LEMMA: Ha $(m | k | n) \notin \mathcal{C}_n$, és $(m, s) = 1$, akkor $(s) \times (m | k | n) \notin \mathcal{C}_n$.

Bizonyítás: Ha $(m | k | n) \notin \mathcal{C}_n$, akkor a 38. o. (A 2) szerint van egy

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

automorfizmusa. A φ – re fölírt ún. kánon (36. o.) :

$$[k^\beta | m] \equiv 0 \pmod{m}, \quad (\text{KR } 1)$$

$$\beta m \equiv 0 \pmod{n}, \quad (\text{KR } 2)$$

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

$$\beta(k - 1) \equiv 0 \pmod{n}. \quad (\text{KR } 4)$$

(A $\mathcal{B}$ – tétel (48. o.) bizonyításában láthattuk, hogy $[k^\beta | k] \equiv k^\delta \pmod{m}$ és

$\beta(k - 1) \equiv 0 \pmod{n}$ 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 $j \equiv k(s) \pmod{m}$, akkor

a (KR 1 – 4) relációk továbbra is érvényben maradnak. Rögtön látszik, hogy csak a (KR 3) – at kell közelebbről megvizsgálni. Világos, hogy

$$[j^\beta | j - 1] \equiv j^\delta - 1 \pmod{ms}$$

pontosan akkor teljesül, ha

$$[j^\beta | j - 1] \equiv j^\delta - 1 \pmod{m}, \quad (13)$$

$$\text{és} \quad [j^\beta | j - 1] \equiv j^\delta - 1 \pmod{s}. \quad (14)$$

A (14) $j \equiv 1 \pmod{s}$ miatt azonnal fennáll, így csak a (13) – at kell ellenőrizni.

A $j \equiv k \pmod{m}$ miatt (13) –ból lesz

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

de a $j - 1$ helyébe nem írható minden további nélkül $k - 1$.

Legyen $j = k + mx$. Akkor

$$\begin{aligned} [k^\beta | j - 1] &= [k^\beta | k - 1 + mx] = [k^\beta | k - 1] + k^{\beta(k-1)} [k | mx] = \\ &= (\text{a (KR 4) miatt}) = [k^\beta | k - 1] + [k^\beta | mx] = \\ &= [k^\beta | k - 1] + [k^\beta | m] [k^{\beta m} | x] \equiv [k^\beta | k - 1] \pmod{m}, \end{aligned}$$

mert (KR 1) miatt $[k^\beta | m] \equiv 0 \pmod{m}$.

Q. E. D.

Ha fúzióval akarunk $\mathcal{C}_h$ – n kívüli csoportot előállítani, akkor az V. rész 3.

lemma (44. o.) miatt legalább az egyik fúziós tényezőnek $\mathcal{C}_h$ – n kívül kell lennie. A $(9 | 4 | 3) \otimes (7 | 4 | 3) \in \mathcal{C}_h$ példája azonban óvatosságra int, mert

a fúzió lehet $\mathcal{C}_h$ – belüli, dacára annak, hogy egy vagy minden tényezője $\mathcal{C}_h$ – n kívül esik. Tekintsük például ezeket:

$$(5 | 3 | 4) \in \mathcal{C}_h,$$

$$(7 | 3 | 6) \in \mathcal{C}_h,$$

$$(9 | 4 | 3) \notin \mathcal{C}_h,$$

$$(16 | 5 | 4) \notin \mathcal{C}_h.$$

Kihasználva a fúzió asszociativitását, a fenti csoportok fúziója

[77]

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 $\mathcal{C}_h$ – ban,

azonban a (16) – nál $\mathcal{C}_h$ – ban vannak, így az V, rész 3. lemma (44. o.)

szerint ez a négyes fúzió $\mathcal{C}_h$ – belüli lesz. Magyarán szólva

$$G_1, G_2 \notin \mathcal{C}_h \nrightarrow G_1 \otimes G_2 \notin \mathcal{C}_h.$$

Legyen

$$G_1 = (p^\alpha | p^{\alpha-\beta} + 1 | p^\beta), p \in P_0,$$

$$G_2 = (q | k | r p^\delta), (p, qr) = 1.$$

$$\text{Ekkor } G = G_1 \otimes G_2 = (p^\alpha q | j | r p^\varepsilon)_a^b,$$

$$\text{ahol } j = s p^{\alpha-\beta} + 1, (p, s) = 1 \quad (17)$$

$$\varepsilon = \max(\beta, \delta).$$

A (17) azért helyes, mert $j \equiv p^{\alpha-\beta} + 1 \pmod{p^\alpha}$,

$$\text{tehát } j = u p^\alpha + p^{\alpha-\beta} + 1,$$

$$\text{azaz } (u p^\beta + 1) p^{\alpha-\beta} + 1 = j.$$

Milyen feltételek mellett teljesül, hogy $G \notin \mathcal{C}_h$?

A továbbiak előtt jegyezzük meg a következőket:

Általában, ha $a \rightarrow ab^\beta, \beta \neq 0$ egyszerű automorfizmusa az $(m | k | n) \frac{b}{a}$ csoportnak, akkor (K 31) és (K 32) miatt (36. o.)

[78]

$$(ab^\beta)^k = a^{\left[\frac{k\beta}{k} \right]} b^{\beta k} = a^k b^\beta .$$

Akkor egyrészt $(ab^\beta)^{k-1} = ab^\beta (ab^\beta)^{-1} = a^k b^\beta b^{-\beta} a^{-1} = a^{k-1} ,$

másrészt $(ab^\beta)^{k-1} = a^{\left[\frac{k\beta}{k-1} \right]} b^{\beta(k-1)} = a^{\left[\frac{k\beta}{k-1} \right]} .$

(Itt ismét használtuk a (K 32) – t, 36. o.)

Ezekből kapjuk, hogy $\left[\frac{k\beta}{k-1} \right] \equiv k-1 \pmod{m} . \quad (K 311)$

Térjünk vissza a 77. oldali G csoportozhoz.

Keressük b – nek azt a legkisebb kitevőjét – méghozzá $t p^\gamma, t | r, \gamma > \gamma$

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

$$t p^{\alpha+\gamma} \equiv 0 \pmod{p^\epsilon r} .$$

Ebből $t \equiv 0 \pmod{r}$ következik.

Viszont föl volt téve, hogy $t | r$, ezért végül kapjuk, hogy $t = r$. (18)

Írjuk föl a (K 311) – et :

$$\left[(sp^{\alpha-\beta} + 1)^{p^\gamma r} | sp^{\alpha-\beta} \right] \equiv sp^{\alpha-\beta} \pmod{p^\alpha q} . \quad (19)$$

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:

[79]

$$\left[(sp^{\alpha-\beta} + 1)^{p^\gamma r} | sp^{\alpha-\beta} \right] \equiv sp^{\alpha-\beta} \pmod{q} . \quad (21)$$

Mivel G_2 – re (a 77. oldalon) semmilyen kikötéssel nem éltünk, a (21) akkor lesz biztosan igaz, ha $\gamma \geq \delta$.

(Ekkor ugyanis $(sp^{\alpha-\beta} + 1)^{p^\gamma r} \equiv 1 \pmod{q}$, s így (21) automatikusan teljesül.)

Mármost $\varepsilon = \max(\beta, \delta) > \gamma \geq \delta$ -ból 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) –ból

$\gamma \geq 2\beta - \alpha$, 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 $\mathcal{A}$ – bel.

Foglaljuk össze az eddigieket:

[80]

3. LEMMA: Legyen

$G_1 = (p^\alpha \mid p^{\alpha-\beta} + 1 \mid p^\beta)$, ahol $p \in P_0$, $\alpha - 1 \geq \beta \geq 1$,

$G_2 = (q \mid k \mid r p^\delta)$, $(p, qr) = 1$, $\beta - 1 \geq \delta \geq 0$.

Akkor a $G = G_1 \otimes G_2 = (p^\alpha q \mid s p^{\alpha-\beta} + 1 \mid p^\beta r)_a^b$, $(s, p) = 1$ 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

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

és $(q \mid k \mid 2^\delta r)$, $(2, qr) = 1$, $\beta - 1 \geq \delta \geq 0$

csoportokat. Ezek fúziójának, a

$$G = (2^\alpha q \mid s 2^{\alpha-\beta} + 1 \mid 2^\beta r)_a^b, (2, s) = 1$$

csoportnak lesz egy

$$a \rightarrow ab^{2^{\gamma}r}$$

$\omega :$

$$b \rightarrow b^{\varepsilon}$$

automorfizmusa, ahol $\gamma \geq 2\beta - \alpha$ és ε alkalmas $R_{2^{\beta}r}$ – beli szám. Q. E. D.

[81]

5. LEMMA: A

$$(2^{\alpha} | 2^{\alpha-\beta} - 1 | 2^{\beta}) , \alpha \geq 4 , \alpha - 2 \geq \beta \geq 2$$

$$\text{és } (q | k | 2^{\delta} r) , (2 , qr) = 1 , \beta - 1 \geq \delta \geq 0$$

csoportok fúziójaként előálló

$$G = (2^{\alpha} q | s 2^{\alpha-\beta} + 1 | 2^{\beta} r)_a^b , (2 , s) = 1$$

csoportnak lesz egy

$$a \rightarrow ab^{r \cdot 2^{\beta-1}}$$

$\omega :$

$$b \rightarrow b^{r \cdot 2^{\beta-1} + 1}$$

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 – e $\langle b \rangle$ – 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 $b^x \cong ab^{\beta}$, 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 $G = (m \mid k \mid n) \frac{b}{a}$ 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 prímhatványrendű 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 α –
jelben $w_p(G) = \alpha$ –, ha G – ben van $(p)^\alpha$ részcsoporth, 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 részcsoporthja legfölbjebb 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 részcsoporthja abeli vagy CYCYSbeli. Ez azonban sajnos nem igaz.

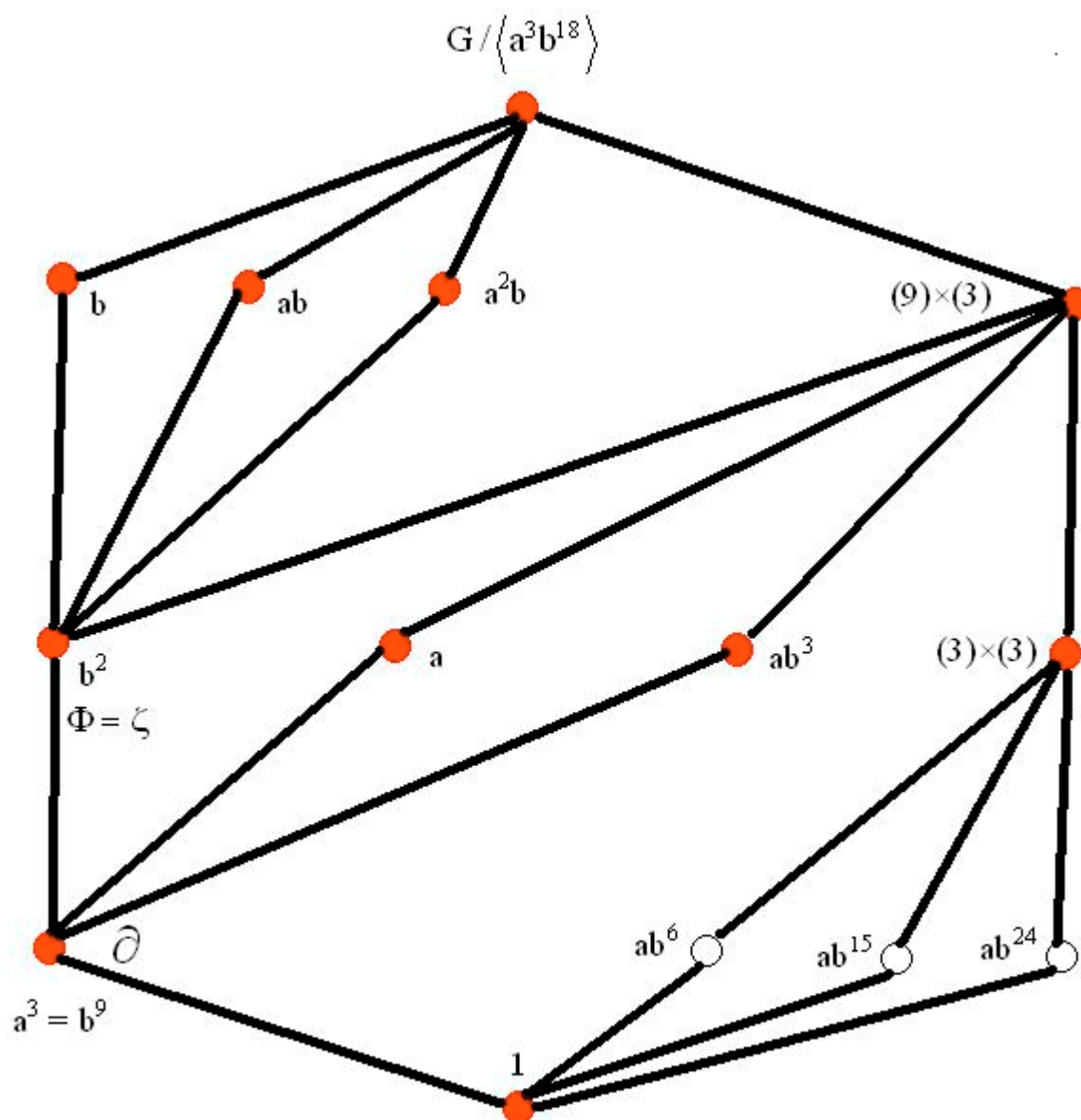
A legkisebb ellenpéllda a $(8 \mid 3 \mid 2) \begin{smallmatrix} b \\ a \end{smallmatrix}$, ahol $\langle a^2, ab \rangle \cong Q$.

Hasonlóan nem áll, hogy egy CYCYSbeli csoport minden nemabeli faktor-

csoportja CYCYSbeli. Itt a minimális ellenpéllda a $G = (4 \mid 3 \mid 4) \begin{smallmatrix} b \\ a \end{smallmatrix}$, ahol az $\langle a^2 b^2 \rangle$ szerinti faktorcsoporthja Q – val izomorf.

Egy kevésbé egyszerű ellenpéllda a $G = (9 \mid 4 \mid 27) \begin{smallmatrix} b \\ a \end{smallmatrix}$,

ahol a $G / \langle a^3 b^{18} \rangle$ 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:

$$r \neq m, r \neq n, \quad (4)$$

$$r \mid (m, n, k-1), \quad (5)$$

$$k^{\frac{n}{r}} \equiv 1 \pmod{m}. \quad (6)$$

A (4) a (2) miatt világos. A (6) a (3) –ból 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:

$$\text{A (3) –ból} \quad b a^{\frac{m}{r}} b^{-1} = a^{\frac{m}{r}k},$$

$$\text{és (2) miatt} \quad b b^{\frac{n}{r}} b^{-1} = b^{\frac{n}{r}k},$$

$$b^{\frac{n}{r}} = b^{\frac{n}{r}k}$$

$$\text{amiből} \quad 1 = b^{\frac{n}{r}(k-1)}, \text{ azaz } \frac{n}{r}(k-1) \equiv 0 \pmod{m}.$$

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 $\text{CYCYS} \subset \text{CYCEX}$,

hiszen elég (2) –ben az $r=1$ választással élni.

Végezetül még egy talány:

3. SEJTÉS: $\text{CYCYS} \subset \text{MAXPIND}$.

Függelék

A 63. oldalon felsorolt összefüggések bizonyítása:

(i) $[s p^{\alpha-\beta} + 1 \mid p^\beta] \equiv p^\beta \pmod{p^\alpha}$, ahol $p \in \mathbf{P}_0$, $0 \leq \beta \leq \alpha$, $(s, p) = 1$.

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.

(i i) $[s 2^{\alpha-\beta} + 1 \mid 2^\beta] \equiv 2^{\alpha-1} + 2^\beta \pmod{2^\alpha}$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.

Bizonyítás: $[s 2^{\alpha-\beta} + 1 \mid 2^\beta] = \frac{(s \cdot 2^{\alpha-\beta} + 1)^{2^\beta} - 1}{s \cdot 2^{\alpha-\beta}} =$

$$= 2^\beta + \binom{2^\beta}{2} s \cdot 2^{\alpha-\beta} \equiv 2^\beta + 2^{\alpha-1} (2^\beta - 1) s, \text{ de } s = 2^j + 1, j > 0 \text{ esetén}$$

$$2^\beta + 2^{\alpha-1} (2^\beta - 1) (2^j + 1) = 2^\beta + 2^{\alpha-1+\beta} \cdot 2^{\alpha-1+j} - 2^{\alpha-1+j} + 2^{\alpha-1+\beta} - 2^{\alpha-1} \equiv$$

$$\equiv 2^\beta - 2^{\alpha-1} \equiv 2^\beta + 2^{\alpha-1} \pmod{2^\alpha}, \text{ hiszen } -2^{\alpha-1} \equiv 2^{\alpha-1} \pmod{2^\alpha}. \text{ Q. E. D.}$$

(i i i) $[s 2^{\alpha-\beta} - 1 \mid 2^\beta] \equiv 2^{\alpha-1} \pmod{2^\alpha}$, ahol $\alpha > 2$, $1 \leq \beta < \alpha - 1$, $(2, s) = 1$.

[87]

Bizonyítás: $[s 2^{\alpha-\beta} - 1 \mid 2^\beta] =$

$$= [s \cdot 2^{\alpha-\beta} - 1 \mid 2] \left[(s \cdot 2^{\alpha-\beta} - 1)^2 \mid 2 \right] \dots \left[(s \cdot 2^{\alpha-\beta} - 1)^{2^{\beta-1}} \mid 2 \right] = s \cdot 2^{\alpha-\beta} \cdot 2^{\beta-1} \cdot A,$$

ahol A páratlan. Végeredményben $[s 2^{\alpha-\beta} - 1 \mid 2^\beta] \equiv 2^{\alpha-1} B \pmod{2^\alpha}$, ahol

$$B = 2j + 1, \text{ és így } 2^{\alpha-1} B = 2^{\alpha-1+j} + 2^{\alpha-1} \equiv 2^{\alpha-1} \pmod{2^\alpha}.$$

Q. E. D.

(i v) $(m \mid k \mid n) \equiv (m \mid 1 \mid n)$ esetén $[k \mid n] \equiv [1 \mid n] \pmod{m}$.

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

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

Kristóf Miklós