Huber László

Véges ciklikus csoportoknak véges ciklikus csoportokkal való szétesző bővítéseiről

1995

Barátomnak és Uranita testvéremnek szeretettel

Mota
1995. 12. 08.

TARTALOM

Köszönetnyilvánítás

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

$\boldsymbol{N}$	A természetes számok halmaza.
$\boldsymbol{Q}$	kvaterniócsoport.
$\boldsymbol{Z}_m$	az m-nél kisebb nemnegatív egészek additív csoportja: {0,1,2,…, m-1}.
$\boldsymbol{R}_m$	az m-nél kisebb, az m-hez relatív prím pozitív egészek multiplikatív csoportja.
$\boldsymbol{P}$	a prímszámok halmaza.
$\boldsymbol{P}_0$	a páratlan prímek halmaza.
$\boldsymbol{P}$R	olyan számok halmaza, amelyekhez létezik primitív gyök.
$\boldsymbol{D}_m$	a 2m-edrendű diédercsoport.
$\boldsymbol{S}_m$	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 $\boldsymbol{R}_m$-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 lnko-ja (legnagyobb közös osztó).
[m,n]	az m és n számok lkkt-je (legkisebb közös többszörös).
max $(m_1, ..., m_r)$	az $m_1, \ldots, m_r$ egészek legnagyobbika.
EU(m)	az EULER-féle függvény: EU(m) = $\|\boldsymbol{R}_m\|$
$\pi(m)$	az m prímosztóinak halmaza.
pr(m)	az m-hez tartozó primitív gyökök halmaza.
$k \overset{.n}{\equiv} 1(m)$	„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.
$a \longrightarrow b$	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.
$G = \langle \Gamma(G) \mid \Delta_{\Gamma(G)} \rangle$	a G megadása a $\Gamma(G)$ generátorokkal és a $\Delta_{\Gamma(G)}$ relációkkal.

Hom (G,H)	a G csoportot a H-ba leképező homomorfizmusok halmaza.
Hom (n,H)	az (n) ciklust a H-ba leképező homomorfizmusok halmaza.
Aut G	a G teljes automorfizmuscsoportja.
Inn G	a G belső automorfizmusainak halmaza.
Hol G	a G holomorfja.
∂(G)	a G kommutátora.
ζ(G)	a G centruma.
ζ_e (G)	a G elsőcentruma és
ζ_h (G)	hátsócentruma (ld. 21. old..)
Φ (G)	a G Frattini-részcsoportja.
Φ_e (G)	lásd a 23. oldalt..
Φ_h (G)	lásd a 23. oldalt..
(m | k | n)	lásd a 2. oldalt..
$(m \mid k \mid n)_a^b$	lásd a 2. oldalt..
(m | k |· n)	lásd a 10. oldalt..
(m | r,k | n)	lásd a 84. oldalt..
$(m \mid r,k \mid n)_a^b$	lásd a 84. oldalt..
[k | α]	lásd az 5. oldalt..
CYCYS	1. oldal..
ABEL	a kommutatív csoportok osztálya NIL a nilpotens csoportok osztálya SOL a feloldható csoportok osztálya DIV az osztható csoportok osztálya: legyen $\|G\|=n$, és $n_1 \| n$. Akkor $\exists H \leq G : \|H\| = n_1$.
TODIV	a totálisan osztható csoportok osztálya: $G \in$ TODIV ha $\forall\ H \leq G : H \in$ DIV.
MAXPIND	azon csoportok osztálya, amelyekben minden maximális részcsoport prím indexű.
CYCEX	85. oldal.
MAX (G)	a G csoport maximális részcsoportjainak halmaza.
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) x (p) x … x (p)
α-tényező	$\underbrace{\qquad\qquad}_{\alpha}$
w_p (G)	83. oldal.
w (G)	83. oldal.
H / ~	a H halmazon a ~ ekvivalenciareláció által létesített osztályozás osztályainak halmaza (a H-nak a ~ 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 szétesõ 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 szétesõ bővítése, amelyet a

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

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 $G \in$ CYCYS, akkor

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

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

$$\mathrm{Hom}(B, \mathrm{Aut}\, A) = \mathrm{Hom}(n, \boldsymbol{R}_m),$$

és a kísérő homomorfizmus

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

ahol

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

[2]

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

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

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

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

azaz

$$k^n \equiv 1\ (m) \qquad (3)$$

más szóval $|k|_m \mid n$ következik.

A (2) csoport pont akkor lesz nemabeli, ha

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

azaz

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

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 | k | n)} halmaz között nincs bijekció, hiszen (1)-ből következik, hogy

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

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

[3]

azaz

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

1. TÉTEL (PRET = PREZENTÁCIÓTÉTEL)

Az (m | k | n) és (m | l | n) által szimbolizált CYCYS-csoportok pont akkor izomorfok, ha k és l ugyanazt a részcsoportot generálja $\boldsymbol{R}_m$-ben:

$$(m \mid k \mid n) \cong (m \mid l \mid n) \quad \Leftrightarrow \quad \langle k \rangle = \langle l \rangle \leq \boldsymbol{R}_m.$$

Bizonyítás: Az (5) miatt elegendő a $\Rightarrow$ implikációt igazolni.

Világos, hogy bármely φ izomorfizmusnál a

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

φ (G) képét egy

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

cikluspár fogja generálni.

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

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

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

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

másrészt a (6) prezentáció szerint

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

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

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

majd $\gamma \in \boldsymbol{R}_m$ miatt $k \equiv l^{\delta} \quad (m)$, végül

[4]

$\delta \in \boldsymbol{R_n}$ miatt $\langle k \rangle = \langle l \rangle \leq \boldsymbol{R_m}$ következik.

Q . E . D .

Vezessünk be a Hom (n , $\boldsymbol{R_m}$) halmazon egy $\leftrightarrow$ relációt:

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

$\forall\, \Theta_1 , \Theta_2 \in$ Hom (n , $\boldsymbol{R_m}$) : $\Theta_1 \leftrightarrow \Theta_2 \Leftrightarrow \Theta_1 (\langle b \rangle) = \Theta_2 (\langle b \rangle)$.

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

Az (m) -nek az (n) -nel való összes nem izomorf szétető bővítései bijektíven megfelelnek a Hom (n , $\boldsymbol{R_m}$) / $\leftrightarrow$ elemeinek,

vagyis a Hom (n , $\boldsymbol{R_m}$) halmazon a $\leftrightarrow$ reláció által létesített

osztályozás osztályainak.

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

{ (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.

[5]

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

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

(II) $\forall\, g \in G\ \exists\, \alpha \in \boldsymbol{Z_m}\ \exists\, \beta \in \boldsymbol{Z_n}$: $g = a^{\alpha} b^{\beta}$.

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

(IV) $\forall\, \alpha_1 , \alpha_2 \in \boldsymbol{Z_m}$ $\forall\, \beta_1 , \beta_2 \in \boldsymbol{Z_n}$:

$$\left(a^{\alpha 1} \cdot b^{\beta 1}\right) \cdot \left(a^{\alpha 2} \cdot b^{\beta 2}\right) = a^{\alpha_1 + \alpha_2 \cdot k^{\beta_1}} \cdot b^{\beta_1 + \beta_2} .$$

(V) $\forall\, \alpha \in \boldsymbol{Z_m}$ $\forall\, \beta \in \boldsymbol{Z_n}$ $\forall\, \gamma \in \boldsymbol{N}$:

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

$\forall\, s \mid m$, $\forall\, t \mid n$:

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

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

Q . E . D .

Az (V) -ben szereplő [|] 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

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

[6]

Akkor

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

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

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

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

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

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

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

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

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

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

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

$[k^{\beta 1} \mid \alpha] \equiv [k^{\beta 2} \mid \alpha] \quad (m)$. Q . E . D .

Az $(m_1 \mid k_1 \mid n_1) \cong (m_2 \mid k_2 \mid n_2)$ reláció fennállásának feltételeit vizsgálva a PRET csak az $m_1 = m_2$ esetben igazít el. Meglepő módon ez a reláció akkor is fönnállhat, ha $m_1 \neq m_2$ (s ekkor persze $n_1 \neq n_2$ is) .

Némi számolással pl. megmutatható, hogy

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

2. TÉTEL (PART = PARTÍCIÓTÉTEL)

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

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

Ezt a műveletet úgy nevezzük hogy (konstanssal) szorzás elölről,

illetve (konstans) kiemelés(e) elölről.

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

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

E műveletre úgy hivatkozunk, mint (konstanssal való) szorzásra hátulról,

illetve (konstans) kiemelés(é)re hátulról .

(c) $(m_1 \mid k_1 \mid n_1)_{a1}^{b1} \times (m_2 \mid k_2 \mid n_2)_{a2}^{b2} \cong (m_1 \cdot m_2 \mid k \mid n_1 \cdot n_2)_a^b$

akkor és csak akkor, ha

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

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

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

Ekkor az $a \longrightarrow d^s$, $b \longrightarrow b$, $c \longrightarrow d^m$ leképezésről könnyen látható,

hogy izomorfizmus .

(b) $a \longrightarrow a , b \longrightarrow d^s , c \longrightarrow d^n$. 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 $k \equiv l (m)$ 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 $k \equiv k_i (m_i) , i = 1, 2$.

Ekkor az $a_1 \longrightarrow a^{m2} , a_2 \longrightarrow a^{m1} , b_1 \longrightarrow b^{n2} , b_2 \longrightarrow b^n$

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 $x \equiv a_i \quad (n_i)$ 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 $[n_1 , n_2 , ... n_r]$.

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

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

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

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

Akkor a $(b_1 \cdot b_2)^x = b_1{}^x \cdot b_2{}^x = b_1{}^{t1} \cdot b_2{}^{t2}$ relációból folyó

$$x \equiv t_i \quad (n_i) , i = 1, 2$$

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

$$x \in \boldsymbol{R}\, n_1.n_2 , \qquad \text{hogy}$$

$$(m1 \mid k1^{t1} \mid n1)_{a1}{}^{b_1^{t..1}} \times (m2 \mid k2^{t2} \mid n2)_{a2}{}^{b_2^{t..2}} \cong (m1 \cdot m2 \mid k^x \mid n1 \cdot n2)_a{}^{b^x} .$$

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, **felbonthatatlan**oknak 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 felbonthatatlan faktorú direkt felbontása izomorf. Q . E . D .

4. DEFINÍCIÓ Azon CYCYS - csoportok halmazát, amelyeknek létezik olyan (m | k | n) prezentációjuk, ahol n = $|k|_m$, $\mathfrak{S}$ - sel jelöljük. ($\mathfrak{S}$ - csoportok) . Ha n = $|k|_m$, akkor használni fogjuk az (m | k | $\dot{n}$) , (m | k | · n) , (m | k | (· n) s) , vagy (m | k | $\dot{n}$ s) jelöléseket is. Az (m | k | $\dot{n}$) az ún. $\mathfrak{S}$ - prezentáció.

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

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

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

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

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

s így (m | k | n) ≅ (m | k | $|k|_{m)}$ × (s) , de az (s) konstans előre nem vihető be,

vagy $$\pi (s) \subseteq \pi (|k|_m) , \qquad (12)$$

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 részcsoportként sem tartalmaz (4 | 3 | 2) ≅ $\boldsymbol{D}_4$ csoportot.

5. DEFINÍCIÓ Az (m | k | · n) csoport homológjainak nevezzük az (m | k | (· 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, . . . r számok páronként relatív prímek.

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

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

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

$k^{\cdot n_i} \equiv 1 (m_i) \Rightarrow k^{\cdot [n1, n2, \ldots n_r]} \equiv 1 (m_1 \cdot m_2 \cdot \ldots \cdot m_r)$.

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

(Látnivaló, hogy ha az $n_1 , n_2 , \ldots , n_r$ 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 :

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

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

és $b = b_1 \, b_2 \ldots b_r$, akkor

$b a b^{-1} = b_1 a_1 b_1^{-1} b_2 a_2 b_2^{-1} \ldots . b_r a_r b_r^{-1} = a_1^{k1} a_2^{k2} \ldots a_r^{kr} = a$,

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

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

[13]

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

$G \lhd G^*$. (14)

Mivel a 6. definícióban az n_i -k (i = 1, 2, . . . 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

$(63\,|\,25\,|\,3)$ nem izomorf $(63\,|\,4\,|\,3)$ - mal.

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

jelben $G_1 \sim G_2$, ha fúziós felbontásukban azonos számú tényező van, és e tényezők csak a prezentációjukban különböznek

egymástól . (Az izostrukturalitás nyilván ekvivalenciareláció .)

A közelebbi vizsgálat azt mutatja, hogy izostruktúrális csoportok

részcsoporthálója ugyanolyan, az egymásnak megfelelő hálószemek vagy izostruktúrálisak, vagy izomorfak. Ezen felül az izostruktúrális csoportok automorfizmuscsoportjai is izomorfak.

A $(63\,|\,4\,|\,3)$ és $(63\,|\,25\,|\,3)$ csoportok esetében például a hálók megfelelő szemei - a legfelső kivételével - izomorfak egymással.

A fúziót azért kellett $\mathcal{S}$ - 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

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

8. DEFINÍCIÓ: Az $(m\,|\,k\,|\cdot\,n)$ csoportot magnak nevezzük pont akkor, ha

az m egy prím hatványa. A magok halmazát $\mathcal{K}$ fogja jelölni.

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

Bármely $\mathcal{S}$ 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 fúziónak 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 $(5 \mid 3 \mid 4) \otimes (7 \mid 3 \mid 6) = (35 \mid 3 \mid 12)$,

$\boldsymbol{D}_5 \leq (5 \mid 3 \mid 4)$, $\boldsymbol{D}_7 \leq (7 \mid 3 \mid 6)$, de

$\boldsymbol{D}_5 \otimes \boldsymbol{D}_7 = \boldsymbol{D}_{35} \not\leq (35 \mid 3 \mid 12)$.

Diédercsoportok fúziója – már ha egyáltalán elvégezhető – ismét diédercsoport.

E sajátságok 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) $G \in$ SOL,

(ii) $G \in$ DIV.

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

A legkézenfekvőbb arra hivatkozni, hogy a

$$G \rhd \langle a \rangle \rhd 1$$

egy olyan normállánc, melynek faktorai abeliek.

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 | m és t | n , akkor

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

4. LEMMA

(a) Minden G ∈ CYCYS előáll egy alkalmas $\mathcal{S}$ csoport részeként.

(b) Minden G ∈ CYCYS része valamely ciklus holomorfjának.

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

ezért tegyük föl, hogy G = (m | k | $\dot{n}$ · s) , és s > 1.

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

p > m, és ns | p – 1 .

Tekintsük az

$$(m \mid k \mid \dot{n}) \otimes (p \mid k_p \mid \sqcup(n\, s)) = (mp \mid l \mid \sqcup(n\, s)) \begin{matrix} a \\ b \end{matrix}$$

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

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

Nyilvánvaló, hogy

$$(m \mid k \mid \dot{n}) \leq \mathrm{Hol}\,(m) \cong (m) \cdot \boldsymbol{R}_m , \qquad (15) ,$$

hiszen $\left\langle k \right\rangle \leq \boldsymbol{R}_m$.

(Később meg fogjuk mutatni, hogy (15) –ben pontosan akkor van egyenlőség, ha (m | k | $\dot{n}$) speciális tulajdonságú, ld. 84 – 89 oldal.) Q. E. D.

II. rész
Reprezentációk

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

A szorzási szabály:

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

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

Könnyen kiszámolható, hogy az

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

generátorokkal valóban az $(\, m \mid k \mid n)_a^b$ csoportot kapjuk.

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

mátrixokkal való reprezentáció az $(\, m \mid k \mid \dot{n})_a^b$ 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 $G = (\, m \mid k \mid \dot{n})_a^b$ csoportnak létezik izomorf képe az $\boldsymbol{S}_m$ – ben .

Bizonyítás: Két általános csoportelméleti tételre támaszkodunk:

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

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

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

Mármost jelölje B a $\langle b \rangle$ összes konjugáltját G – ben . Nyilván $B \lhd G$, 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 $G \in \mathcal{S}$, 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. Hassanak az A, B, …Z permutációk az Ω jegyhalmazon, és legyen $i \in \Omega$. Akkor

A B …Z (i) = A(B(….(Z (i)) …) .

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

$\boldsymbol{Z}_m = \{ 0, 1, 2, 3, \ldots m - 1 \}$.

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

az a és a b hatása legyen az alábbi:

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

b (i) = k·i mod 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 $i \in \boldsymbol{Z}_m$, és tegyük fel, hogy

$b^x (i) = i$,

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

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

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

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

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

Legyen ugyanis $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_r^{\alpha_r}$, ahol a p_i –k páronként különböző prímek (i = 1, 2, …r) , és legyen $m' = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \ldots p_r^{\beta_r}$, $0 \leq \beta_i \leq \alpha_i$ (i = 1, 2, ..r)

Akkor triviális, hogy

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

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:

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

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

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

[20]

kaptunk.

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

Ezt egy konkrét példán keresztül érthetjük meg a legjobban.

Legyen az ábrázolandó csoport a

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

Készítsük el a fúziós tényezők reprezentációit az előbb ismertetett módon:

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

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

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

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 $(60\,|\,23\,|\,4)\,{}^{b}_{a}$ csoportot

kaptuk, mégpedig $\boldsymbol{S}_{60}$ helyett az $\boldsymbol{S}_{3+4+5} = \boldsymbol{S}_{12}$ –ben .

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

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

$(m\,|\,k\,|\,\dot{n})$ csoportot az $\boldsymbol{S}_{m_1 + m_2 + \ldots + m_r}$ szimmetrikus csoportban sikerül

ábrázolni az $\boldsymbol{S}_{m_1 \cdot m_2 \cdot \ldots \cdot m_r} = \boldsymbol{S}_m$ helyett.

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

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

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

Akkor az $(m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_r \mid k \mid \dot{n})$ csoportnak létezik az

$\boldsymbol{S}_{m_1 + m_2 + \ldots + m_r}$ 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

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

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

ahol b a $(m \mid k \mid \dot{n})_a^b$ csoporthoz a szokásos módon megszerkesztett permutáció és a $(\beta_1\ \beta_2\ \beta_3\ \ldots.\ \beta_{ns})$ diszjunkt a –val és b –vel is.

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

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

III. rész
Nevezetes részcsoportok

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

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

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

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

1. DEFINÍCIÓ: A G –t $\mathfrak{Z}$ – csoportnak nevezzük pont akkor, ha

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

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

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

Mind a kommutátor szerinti faktorcsoportja ciklikus.

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

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

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

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

Bizonyítás: közvetlen számolással. Q. E. D.

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

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

Az 1. és 2. lemmákból kiolvasható, hogy

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

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

(ζ_e (G)) közötti sajátos „komplementaritást”.

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

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

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

(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 $\boldsymbol{R}_{m_1}$ – beli lehet, vagyis $k \equiv 1 \ (2^{\alpha})$.

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

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

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

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

csoportot értjük.

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

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

Ha pedig $\beta \in \boldsymbol{R}_n$, akkor $\langle a, a^{\alpha} b^{\beta} \rangle \in \mathrm{MGR}\ (G)$.

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

Tegyük föl, hogy $\alpha \notin \boldsymbol{R}_m$ és $\beta \notin \boldsymbol{R}_n$.

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

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

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

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

[24]

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

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

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

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

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

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

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

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

amiből máris következik, hogy

$$\Phi (G) = \langle a^{p_1 \cdot p_2 \cdot \ldots \cdot p_r}, b^{\gamma} \rangle , \qquad (\bigstar)$$

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

A következőket láttuk be:

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

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

Általában $\Phi_h (G) \neq \Phi (b)$. Ha például $G = (p \mid k \mid \cdot (p - 1))$, $p \in \boldsymbol{P}_0$, akkor Könnyen kiszámolható, hogy $\Phi_h (G) = 1$. Biztosan nagyobb lesz azonban a

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

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

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

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

Bizonyítás: Mivel $\left\langle b^n \right\rangle \lhd G$ és $\left\langle b^n \right\rangle \leq \Phi(b) = \left\langle b^{q_1 \ldots q_t} \right\rangle$, alkalmazhatjuk azt Az általános csoportelméleti tételt, miszerint ha $A \leq G$ és $N \leq \Phi(A)$, akkor

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

8. LEMMA:

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

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

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 ($p \in$ ***P)*** halmazát $\mathcal{P}$,
a nilpotensekét $\mathcal{N}$ fogja jelölni.

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

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

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

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

$(2^\alpha \mid 2^\alpha - 1 \mid 2) \cong \boldsymbol{D}\, 2^\alpha$, $\alpha \geq 2$. (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:
$| s \cdot p^{\alpha-\beta} + 1 |\, p^\alpha = p^\beta$, ahol $(s,p) = 1$.

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

$$\left(s \cdot p^{\alpha-\beta}+1\right)^{p^{\beta-\gamma}} - 1 = s \cdot p^{\alpha-\beta} \cdot [\, s \cdot p^{\alpha-\beta}+1 \mid p^{\beta-\gamma}\,] =$$

$$= s \cdot p^{\alpha-\beta} \cdot [\, s \cdot p^{\alpha-\beta}+1 \mid p\,] \cdot [\, \left(s \cdot p^{\alpha-\beta}+1\right)^{p} \mid p\,] \cdot \ldots . [\, \left(s \cdot p^{\alpha-\beta}+1\right)^{p^{\beta-\gamma-1}} \mid p\,] .$$

Elemi módon kiszámolható, hogy

$$p \parallel [\, \left(s \cdot p^{\alpha-\beta}+1\right)^{p^{\delta}} \mid p\,] , \; 0 \le \delta \le \beta-\gamma-1 ,$$

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

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

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

[27]

Legyen ismét $0 \le \gamma < \beta$.

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

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

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

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

Könnyű kiszámolni, hogy

$$2 \parallel [\, \left(s \cdot 2^{\alpha-\beta}-1\right)^{2^{\delta}} \mid 2\,] , \; 1 \le \delta \le \beta-\gamma-1 ,$$

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

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

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

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

Q. E D.

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

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

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

alakban, ahol p_i –k páronként különböző prímek (i = 1, 2, …r), valamint

$(p_1 , p_2 , p_3 , \ldots p_r , q) = 1$.

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

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

Bizonyítás: Legyen $G = (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_r^{\alpha_r} \mid k \mid n)$, ahol a p_i –k páronként

különböző prímek (i = 1,2, . . . r). Elemi számolással adódik hogy $\partial(G) \leq \zeta_e (G)$ $\Leftrightarrow (k-1)^2 \equiv 0 \ (p_1^{\alpha_1} \ldots p_r^{\alpha_r})$.

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

Eszerint $k = s \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \ldots p_r^{\varepsilon_r} + 1$, (s, p_1 p_2 . . . 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, . . . r. Akkor

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

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

$k - 1 \equiv 0 \quad (p_1^{\alpha_1 - 1} \ldots . . p_r^{\alpha_r - 1})$.

Ámde ekkor $|\partial(G)| = \dfrac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_r^{\alpha_r}}{\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_r^{\alpha_r}, k-1\right)} = d$,

$|\Phi_e(G)| = p_1^{\alpha_1 - 1} \ldots . p_r^{\alpha_r - 1} = f$, és $d \mid f$, tehát $\partial(G) \leq \Phi_e(G)$. 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 , ($p \in$ ***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 $G = (p^\alpha \mid k \mid \cdot p^\beta q)_a^b$, ($p \in$ ***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 (★) szerint (24. o.) $p \mid \gamma$.

Mivel $\Phi(G) = \langle a^p, b^\gamma \rangle \lhd G$, ezért $k^\gamma \equiv 1$ (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, … r .

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

$\left(p_1 p_2 \ldots p_r, \bar{q}_i\right) = 1$, i = 1, 2, …r .

(Ha föltesszük, hogy $p_1 < p_2 < \ldots < p_r$, akkor világos, hogy

$j \geq i$ esetén $\delta_{ji} = 0$.)

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

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

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

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

A (3) magok fúziója tehát így írható fel:

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

Tudjuk, hogy $\Phi(G) = \left\langle a^p, b^\gamma \right\rangle$, ahol most $p = p_1 p_{2\ldots} p_r$.

$\Phi(G) \lhd G$ miatt $k^\gamma \equiv 1$ (p) , és ebből következik, hogy $q_i \mid \gamma$, i = 1, 2, …r , tehát $\left[q_1, q_2, \ldots q_r\right] \mid \gamma$.

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

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

15. LEMMA:

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

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

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

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

Bizonyítás: (i) Ha $G_i \in \mathfrak{R} \cap \mathfrak{S}$, i = 1, 2, …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 , …r .

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

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

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

adódik az állítás. Q. E . D .

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

$G_1 = (p_1^{\alpha 1} \mid k_1 \mid \bullet p_i^{\beta_i} q_i)$,

$G2 = (p_2^{\alpha 2} \mid k_2 \mid \bullet p_2^{\beta 2} p_1^{\delta} q_2)$ magokat, ahol

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

A két mag fúziója $G = G_1 \otimes G_2 = (p_1^{\alpha 1} p_2^{\alpha 2} \mid k \mid \bullet p_2^{\beta 2} p_1^{\varepsilon} q)_a^b$,

ahol $\varepsilon = \max(\beta 1, \delta)$, $q = [q_1, q_2]$. Mi lesz a Φ (G) ?

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

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

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

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

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

másrészt H nilpotens, hiszen $H = (p_1^{\alpha 1} p_2^{\alpha 2} \mid k^{p_1^{\delta} q} \mid p_2^{\beta_2})_a^{b^{p_1^{\delta} q}}$,

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

[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

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

(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 = $\left\langle a, b^{p_1^{\beta_1} q} \right\rangle$ részcsoportot.

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

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

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

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

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

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

Részletesen ez azt jelenti, hogy

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

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

$$\varphi(b)\,\varphi(a) = \varphi(a)^k\,\varphi(b) \qquad (3)$$

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

Előfordulhatnak a következő esetek is:

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

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

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

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

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

(Az (5 d) – nél mindkét eset fönnáll.) Ez nyilvánvalóan csak úgy lehetséges,

ha a mondott részek centrálisak, izomorfok, és mind $\langle a \rangle$ - nak, mind $\langle b \rangle$ - nek direkt faktorai. Az alábbit láttuk be:

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

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

Q . E . D .

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

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

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

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

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

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

$$\varphi(a) = a^{\alpha} b^{\beta} \text{ ,}$$

$$\varphi(b) = a^{\gamma} b^{\delta} \qquad (7)$$

alakú, ahol az α , $\gamma \in \boldsymbol{Z}_m$, β , $\delta \in \boldsymbol{Z}_n$ számoknak az (1) , (2) , (3) – ból következőleg ki kell elégíteniük az alábbi relációkat:

Az m a legkisebb pozitív egész, amelyre

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

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

Az n a legkisebb pozitív egész, amelyre

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

és $\quad \delta\, n \equiv 0\ (n)\,, \qquad (K\,22)$

valamint

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

$$\beta\,(k-1) \equiv 0\ (n)\,, \qquad (K\,32)$$

Ezt a kissé riasztó kongruenciarendszert KÁNON-nak is nevezzük.

Később látni fogjuk, hogy fontos esetekben ezek a relációk jelentősen

egyszerűsíthetők.

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

Világos, hogy az identikus automorfizmus egyszerű, és egyszerű auto-

morfizmus nem lehet keresztező.

Egy egyszerű automorfizmus megadásánál nem tüntetjük föl azt a generátort,

amelyen identikusan hat. Például φ: $a \rightarrow a^{\alpha}\, b^{\beta}$, $b \rightarrow b$ helyett csak annyit írunk, hogy φ: $a \rightarrow a^{\alpha}\, b^{\beta}$.

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: $\quad \varphi = \varphi_1 \otimes \varphi_2$.

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 $\mathscr{C}$ – vel jelöljük.

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

$\varphi_1 \otimes \varphi_2 \neq \varphi_1$ o φ_2 . Az is nyilvánvaló, hogy $\varphi_1 \otimes \varphi_2 = \varphi_2 \otimes \varphi_1$, és

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

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

A G – nek ugyanis van egy φ: $a \rightarrow a\, b^2$, $b \rightarrow b^3$ automorfizmusa, ámde sem a φ_1: $a \rightarrow a\, b^2$, sem a φ_2: $b \rightarrow b^3$ nem automorfizmusa G – nek.

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

(A . 1) A G – nek az $a \to a^{\mu}$, $\mu \in \boldsymbol{R}_m$ egyszerű automorfizmusai egy

$\boldsymbol{R}_m$ - mel izomorf részcsoportot generálnak Aut G – ben.

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

$$\varphi: \quad a \to a\, b^{\beta}\,, \ \beta \downarrow n$$
$$b \to b^{\delta}\,, \quad \delta \in \boldsymbol{R}_n$$

automorfizmusa.

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

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

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

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

Bizonyítás: (A . 1) triviális.

(A . 2) Ha $\langle a \rangle$ nem karakterisztikus G – ben, akkor mindenesetre léteznie kell egy ψ: $a \to a^{\alpha} b^{\beta}$, $\beta \neq 0$,

$$b \to b^{\delta}\,, \quad \delta \in \boldsymbol{R}_n$$

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

Először mutassuk ki, hogy $\alpha \in \boldsymbol{R}_m$. 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 $\alpha\alpha' \equiv 1 \ (m)$, amiből következik, hogy $\alpha \in \boldsymbol{R}_m$.

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

Ilyen fölírás mindig lehetséges.

Ekkor tehát $\psi(a) = a^{\alpha} (b^t)^{\beta 1}$.

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

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

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

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

Ekkor valóban

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

$\quad b \to b^{\delta}$, $\quad \delta \in \boldsymbol{R}_n$.

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

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

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

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

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

Legyen ω: $b \to a^{\gamma}\, b^{\delta}$, A $\delta \in \boldsymbol{R}_n$. 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 $\delta \in \boldsymbol{R}_n$ mellett csak $G \notin \mathfrak{S}$ mellett lehetséges.

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

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

TÉTEL: Ha a $G = (m \mid k \mid n)_a^{\,b}$ csoportnak a

φ_1: $a \to a^{\alpha}\, b^{\beta}$

φ_2: $b \to a^{\gamma}\, b^{\delta}$

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

automorfizmusa G –nek.

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

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

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

valamint a $[\, k^{\beta} \mid k\,] \equiv k\ (m)$ $\qquad (K_1\, 31)$

relációkból áll.

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

$\qquad k^{\delta} \equiv k\ (m)$ $\qquad (K_2\, 31)$

lesznek.

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

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

Fölhasználva a $(K_1\, 31)$ és $(K_2\, 31)$ – et, megfelelő átrendezés után ebből a

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

relációt nyerjük. Vegyük figyelembe, hogy

[41]

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

(itt ismét felhasználtuk a (K_1 31) - et) .

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

$$\gamma\,(k-1)\,[\,k \mid \beta] \equiv 0 \quad (m) \qquad (\oplus)$$

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

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

A (K_1 31) és (K 32) – ből

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

$\equiv [\,k^{\beta} \mid k-1] + 1 \equiv k\ (m)$, azaz

$$[\,k^{\beta} \mid k-1] \equiv k-1\ (m) \qquad (9)$$

Írjuk be ide (8) – at a baloldalra:

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

A (K 21) és (K_2 32) – ből nyerjük, hogy $\gamma\,[\,k \mid n] \equiv 0 \quad (m)$,

S így $\gamma\,s\,[\,k \mid n] \equiv \gamma\,s\,[\,k \mid \beta]\,[\,k^{\beta} \mid \frac{n}{s}] \quad \equiv 0 \quad (m)$.

Alkalmazva a (10) – et:

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

tehát a ($\oplus$) teljesül.

Ha most β helyett egy $\beta\,t$ többszöröst veszünk, akkor

[42]

$[\,k \mid \beta\,t] \equiv [\,k \mid \beta]\,[\,k^{\beta} \mid t] \quad (m)$, és

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

mert $\Gamma \equiv 0\ (m)$, 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 $\left\langle a^{\alpha} b^{\beta} \right\rangle \bigcap \left\langle a^{\gamma} b^{\delta} \right\rangle = 1$,

tehát φ valóban automorfizmusa G – nek. Q. E. D.

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

$$\text{Inn } G \cong \left\langle a^{k-1}, b^{n/n_0} \right\rangle \text{, ahol } n_0 = \mid k \mid_m .$$

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

akár abból, hogy Inn $G \cong G / \zeta(G)$. Q. E. D.

[43]

V. rész
Ch – csoportok

1. DEFINÍCIÓ: A $G = (m \mid k \mid n)_a^b$ csoportot $\mathcal{Ch}$ – csoportnak nevezzük,

ha $\langle a \rangle$ char G , vagyis $\langle a \rangle$ karakterisztikus G – ben.

Világos, hogy $G \in \mathcal{Ch}$ esetén a G minden, a IV. rész (7) – ben (36. o.)

adott automorfizmusánál $\beta = 0$. Ekkor G automorfizmusai az

$$\begin{pmatrix} \alpha & 0 \\ \gamma & 1 \end{pmatrix}, \alpha \in \boldsymbol{R}_m, \gamma \in \boldsymbol{Z}_m$$

mátrixokkal reprezentálhatók. Az automorfizmusok összetételének megfelel

a fenti mátrixok szokásos szorzása, mint azt könnyű kiszámolni.

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

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

Bizonyítás: Legyen $G = (m \mid k \mid n)_a^b$. 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 $(m \mid k \mid \dot{n}) \in \mathcal{Ch}$, és $(m , s) = 1$, akkor

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

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

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

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

Mivel ciklikus csoportnak minden részcsoportja karakterisztikus, kapjuk, hogy

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

amiből $\langle a_1 \rangle$ char G_s .

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

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

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

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

A VI. rész 1. lemmája (71. o.) mutatja, hogy az iménti állításban miért volt szükség $\mathfrak{S}$ – csoportokra szorítkozni.

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

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

$G_1 = (m_1 \mid k_1 \mid n_1) \begin{matrix} b_1 \\ a_1 \end{matrix} \in \mathfrak{Ch}$, és $G_2 = (m_2 \mid k_2 \mid n_2) \begin{matrix} b_2 \\ a_2 \end{matrix} \in \mathfrak{Ch}$.

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

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

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

$$\varphi : \begin{matrix} a_1 a_2 \longrightarrow a_1 a_2 (a_1 a_2)^{\beta} \\ b_1 b_2 \longrightarrow (b_1 b_2)^{\delta} \end{matrix}$$

automorfizmusa. tekintsük ennek a φ – nek mondjuk a G_1 – re való megszorítását. Mivel $G_1 \in \mathfrak{Ch}$, ezért a $\varphi(\langle a_1 \rangle) = \langle a_1 \rangle$ relációnak teljesülnie kell. Ámde $(m_1, m_2) = 1$, s így $\langle a_1 \rangle = \langle a_1^{m2} \rangle$, és

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

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

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

Ebből $[k^{\beta} \mid m_2] \equiv 0 \ (m_2)$ (1 a)

és $\beta m_2 \equiv 0 \ (n_2)$ (1 b)

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

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

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

$$[\, k^{\beta} \mid k \,] \equiv k^{\delta} \ (m_1\, m_2) \qquad (1\ c)$$

$$\beta\,(k-1) \equiv 0 \ \ (n)\ . \qquad (1\ d)$$

Vegyük a k – t mod m_2 , a β és δ – t mod n_2 , azaz legyen

$$k = k_2 + m_2\, x,$$

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

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

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

Az (1 a) – ból:

$$\left[k^{\beta} \mid m_2\right] \equiv \left[k_2^{\beta_2 + n_2 y} \mid m_2\right] \equiv \left(k_2^{n_2 y} \equiv 1 \ (m_2) \text{ miatt }\right) \equiv$$

$$\equiv \left[k_2^{\beta_2} \mid m_2\right] \equiv 0 \ (m_2) \qquad (1\ a\ a)$$

Az (1 b) – ből:

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

Az (1 c) – nél a [|] bal felében közvetlenül áttérhetünk k – ról k_2 – re :

$$\left[k^{\beta} \mid k\right] \equiv \left[k_2^{\beta_2 + n_2 y} \mid k\right] \equiv k_2^{\delta_2 + n_z} \ (m_2)\ ,$$

amiből $k_2^{ny} \equiv k_2^{nz} \equiv 1$ (m_2) miatt

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

Meg kell még mutatni, hogy

$$\left[k_2^{\beta_2} \mid k\right] \equiv \left[k_2^{\beta_2} \mid k_2\right] \ (m_2)\ .$$

Íme: $\left[k_2^{\beta_2} \mid k\right] \equiv \left[k_2^{\beta_2} \mid k_2 + m_2 x\right] \equiv \left[k_2^{\beta_2} \mid k_2\right] + k_2^{\beta_2 k_2} \left[k_2^{\beta_2} \mid m_2 x\right] \equiv$

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

mivel (1 a a) miatt $\left[k_2^{\beta_2} \mid m_2 \right] \equiv 0 \ (m_2)$.

Kaptuk tehát, hogy

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

Az (1 d) – ből:

$$\beta (k - 1) \equiv (\beta_2 + ny) (k_2 + m_2 x - 1) \equiv$$

$$\equiv \beta_2 (k_2 - 1) \equiv 0 \quad (n_2) , \qquad (1 \text{ d d})$$

hiszen $\beta_2 m_2 \equiv 0 \quad (n_2)$ az (1 b b) szerint.

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

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

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

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

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

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

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

$$[k \mid n] \equiv 0 \quad (m) .$$

4. LEMMA:

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

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

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

Bizonyítás: egyszerű számolással. Q. E. D.

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

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

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

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

Ekkor a G – nek létezik egy

$$a \to a\, b^{\beta},\ \beta \downarrow n$$

$$\varphi:$$

$$b \to b^{\delta},\ \delta \in \boldsymbol{R}_n$$

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

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

$$[\, k^{\beta} \mid k \,] \equiv k^{\delta} \quad (m)\,.$$

Ebből a (K 32) – vel (36. o.) :

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

azaz $[\, k^{\beta} \mid k - 1] \equiv k^{\delta} - 1 \ (m)\,.$

Most $k - 1 = s\dfrac{n}{\beta}$,

mivel $\beta \downarrow n$, ezért

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

Mivel $G \in \mathfrak{B}$, ezért $[\, k \mid n\,] \equiv 0 \ (m)$, s így

$$s\,[\, k \mid n\,] \equiv s\,[\, k \mid \beta\,]\,[\, k^{\beta} \mid \frac{n}{\beta}\,] \equiv 0 \ (m)\,.$$

Használjuk föl itt a (2) – t :

$$[\, k \mid \beta\,]\,(k^{\delta} - 1) \equiv 0 \ (m)\,. \qquad (3)$$

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

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

és a (3) – mal nyerjük, hogy

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

Ebből következik, hogy

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

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

Az 1. lemma és az 1. tétel szerint

$$\mathfrak{B} \cup \mathfrak{Q} \cup \mathfrak{R} \cup \mathfrak{Z} \subset \mathfrak{Ch}\,.$$

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

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

(m, k – 1) = 1, és így a $k^n - 1 = (k-1)\,[\,k \mid n\,] \equiv 0 \ (m)$ relációból $(\lhd)$

$[\,k \mid n\,] \equiv 0 \ (m)$ következik.)

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

(i) $\left(\frac{m}{\gamma}\right) \cdot \boldsymbol{R}_m \cong \mathrm{Aut}(m \mid k \mid \dot{n}) \leq \mathrm{Hol}(m)$, ahol $\gamma = \frac{m}{(m, \lfloor k \mid n \rfloor)}$;

(i i) $\mathrm{Aut}(m \mid k \mid \dot{n}) \cong \mathrm{Hol}(m)$ pontosan akkor, ha $(m \mid k \mid \dot{n}) \in \mathcal{BS}$;

(i i i) $\mathrm{Hol}(m) \in \mathrm{CYCYS} \Leftrightarrow m \in \boldsymbol{P}\mathrm{R}$.

Bizonyítás:

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

$$\varphi: \begin{array}{l} a \to a^{\alpha}, \quad \alpha \in \boldsymbol{R}_m \\ b \to a^{\gamma} b, \ \gamma \in \boldsymbol{Z}_m \end{array}$$

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

$$\varphi_\alpha : a \to a^{\alpha}, \quad \alpha \in \boldsymbol{R}_m$$

$$\varphi_\gamma : b \to a^{\gamma} b, \ \gamma \in \boldsymbol{Z}_m$$

egyszerű automorfizmusok.

Nyilvánvaló, hogy $\left\langle \{\varphi_\alpha \mid \alpha \in R_m\} \right\rangle \cong \boldsymbol{R}_m$.

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

$$\gamma\,[\,k \mid n\,] \equiv 0 \ (m).$$

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

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

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

[51]

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

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

(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 $[\, k \mid n \,] \equiv 0 \ (m)$, tehát $(m \mid k \mid \dot{n}) \in \mathcal{B}$.

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

$$\mathrm{Aut}\, \boldsymbol{D}_m \cong (m) \cdot \boldsymbol{R}_m .$$

Az $\boldsymbol{R}_m$ pedig pontosan akkor ciklikus, ha $m \in \boldsymbol{P}R$. Q. E. D.

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

5. LEMMA: $\mathcal{T} = \{ (p^\alpha \mid k \mid p^{\alpha-1}(p-1)) \}$, ahol $p \in \boldsymbol{P}_0$, $k \in \mathrm{pr}(p^\alpha)$.

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

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

$$\mathrm{Aut}\, G \cong \mathrm{Inn}\, G \cong G .$$

Ha $G \in$ 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. ($\lhd$)).

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

$$\mathrm{Aut}\, G = \left\langle \varphi, \{\varphi_\alpha\} \right\rangle,$$

[52]

ahol $\varphi : b \longrightarrow ab$,

$$\varphi_\alpha : a \longrightarrow a^\alpha , \ \alpha \in \boldsymbol{R}_m .$$

A φ nyilván belső automorfizmus, hiszen

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

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

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

$$\left\langle k \right\rangle \cong \boldsymbol{R}_m ,$$

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

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

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

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

(i i) $G = (2p^\alpha \mid k \mid p^{\alpha-1}(p-1))_a^b$, $p \in \boldsymbol{P}_0$, $k \in pr(2p^\alpha)$,

(i i i) $G \cong \boldsymbol{D}_4$.

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 elölről 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 Aut $G = \left\langle \varphi, \varphi_k \right\rangle$, ahol

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

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

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

tehát valóban $\left\langle \varphi, \varphi_k \right\rangle \cong G$. Q. E. D.

A fentiekből levonható az a következtetés, hogy azokra a $G = (m \mid k \mid \dot{n})_a^b$

csoportokra, ahol $m \in \boldsymbol{P}R$, $k \in pr(m)$, 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 $\left\langle b \right\rangle$ - nek akkor és csak akkor van m számú különböző automorf képe, ha $[k \mid n] \equiv 0 \ (m)$.

Bizonyítás: Tekintsük a

$$a \longrightarrow a ,$$

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

leképezést. Ezzel

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

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

ami azt jelenti, hogy $| a^{\gamma} b | = n$ esetén φ (egyszerű) automorfizmusa lesz G – nek. Tekintve, hogy $(a^{\gamma} b)^n = a^{\gamma[k|n]}$,

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

[54]

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

Ekkor azonban

$$\left\langle a^{\gamma_1} b \right\rangle = \left\langle a^{\gamma_2} b \right\rangle \qquad (4)$$

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

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

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

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

Innen $x \equiv 1$ (n), de mivel $x \in \boldsymbol{Z}_n$, 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 $\left\langle b \right\rangle$ 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 $\left\langle b \right\rangle$ bármely konjugáltjával összemetsz ebben a nem triviális hátsó centrumban.

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

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

Bizonyítás: Az 5. definícióval ekvivalens állítás ez:

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

[55]

automorf képével csak triviálisan metsződik, vagyis

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

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

Az (5) mármost csakis akkor teljesül, ha

$$\forall \gamma \in \boldsymbol{Z}_m \; \forall \nu \downarrow n : \; \gamma \left[k \mid \nu \right] \not\equiv 0 \; (m) .$$

Innen pedig azonnal kapjuk az

$\forall \nu \downarrow n$: (m, [k | ν]) = 1 feltételt. Q. E. D.

6. DEFINÍCIÓ: Ha $\mu \downarrow m$ és $\nu \downarrow n$, akkor a $G = (m \mid k \mid n)_a^b$ csoportnak az $\langle a^{\mu}, b^{\nu} \rangle$ 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 $G = (m \mid k \mid n)_a^b$, $\mu \downarrow m$, $\nu \downarrow n$, és

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

$M \in \mathcal{M}^*$ pontosan akkor, ha $\forall \nu_0 \downarrow \frac{n}{\nu} : \left(\frac{m}{\mu}, \left[k^{\nu} \mid \nu_0 \right] \right) = 1$.

Tegyük föl, hogy valamely ν_0 – ra $\left(\frac{m}{\mu}, \left[k^{\nu} \mid \nu_0 \right] \right) > 1$.

Akkor nyilván $\left(m, \left[k^{\nu} \mid \nu_0 \right] \right) > 1$ is fönnáll.

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

$$\left(m, \left[k^{\nu} \mid \nu_0 \right] \right) = \left(m, \left[k \mid \nu \right] \left[k^{\nu} \mid \nu_0 \right] \right) = \left(m, \left[k \mid \nu\nu_0 \right] \right) > 1 ,$$

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

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

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

(a) β = 1 és r = 1 , vagy

(b) β = 0 .

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

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

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

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

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

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

$$x (k-1) [k \mid y] \equiv x (k^y - 1) \equiv 0 \ (p^\alpha) \qquad (6)$$

[57]

következik.

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

tehát $y \equiv 0$ (n), ellentmondásban az $y \in \boldsymbol{Z}_n$ föltevéssel.

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

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

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

k most a (p – 1) ciklusból való, s ezért k rendje r minden $1 \le \delta \le \alpha - 1$

esetén is.

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

Azt kell még megmutatni, hogy más eset6ekben viszont G ∉ $\mathcal{M}^*$.

Ismét két lehetőség van:

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

(d) $\beta \ge 2$.

A (c) – nél elég látni, hogy a (p | k | 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 $n \in \boldsymbol{P}$, akkor (m | k | n) minden további megszorítás nélkül $\in \mathcal{M}^*$.

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

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

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

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

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

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

Bizonyítás: (A) triviális.

(B) Mindenekelőtt jegyezzük meg, hogy

$$(n , p_{i)} = 1, i = 1, 2, \ldots r . \qquad (7)$$

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 ($p_i^{\alpha_i} \mid k \mid p_i^{\beta_i} n_{i)}$ főrész 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 ($p_i^{\alpha_i} \mid k \mid n$) főrész

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

Már csak az s – re vonatkozó kirovást kell indokolni.

Az $(s, p_1 p_2 \ldots p_{r)} = 1$ természetesen az elölről 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.

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

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

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

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

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

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

(s , $[\, l \mid \nu \,]$) = 1 csakis úgy teljesülhet, ha (s , ν) = 1.

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

kapjuk, hogy (s , n) = 1 . Q. E. D.

7. DEFINÍCIÓ: Azokat az $(\, m \mid k \mid n)_a^{\,b}$ 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 $\boldsymbol{D}_m \in \mathcal{M}$ minden $m \geq 3$ számmal, így a multiédercsoport fogalma a diédercsoport fogalmának természetes általánosítása.

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

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

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

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

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

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

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

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

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

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

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

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

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

(A) (p) × $(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \mid k \mid \cdot p)$, ahol

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

p | ($p_1 - 1$, $p_2 - 1$, . . . $p_r - 1$) ;

(B) $(p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r} \mid k \mid \cdot n)$, ahol

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

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

[61]

Bizonyítás: A (9) – et figyelembe véve elegendő az $\mathcal{M}^*$ – csoportok közül kikeresni azokat, amelyek $\mathcal{B}$ – ben is benne vannak (segítségül híva 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, . . . prímeket, amelyekre

$n \mid p_i - 1$, i = 1 , 2 , ...

(A DIRICHLET – tétel szerint végtelen sok ilyen prímet találhatunk.)

Tegyük föl, hogy a p_1 , p_2 , . . . p_r alkalmas prímek.

Akkor tetszőleges $\alpha_i \geq 1$, i = 1 , 2 , . . . r számokkal könnyen

megszerkeszthetők a $(p_i^{\alpha_i} \mid k_i \mid \overline{n})_{a_i}^{b_i}$ 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: $\left\langle a, b_1^{t_1} b_2^{t_2} ... b_r^{t_r} \right\rangle$, (11)

ahol $a = a_1 a_2 \ldots a_r$, és $t_i \in \boldsymbol{R}_{ni}$, i = 1 , 2 , . . . r .

A (11) összesen $\prod_{i=1}^{r} EU(n_i)$ számú csoportot ad, ámde

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

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

$\mathcal{M}$ – csoportok száma

[62]

(a) összetett n esetén $\prod_{i=1}^{r} EU(n_i) / EU(n)$,

(b) $n \in \boldsymbol{P}$ esetén a fenti szám kétszerese,

hiszen ha $(p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}\,|\,k\,|\,p) \in \mathcal{M}$, akkor a 4. tétel (A) szerint

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

12. LEMMA: Legyen p ∈ $\boldsymbol{P}$, 1 < r | p – 1 , $s \geq 1$. Akkor

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

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

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

alakban, akkor a III. rész 9. lemma szerint (25. o.)

$$|\,k\,|_{p^{\alpha}} = p^{\alpha-\beta}$$ volna.

De most $|\,k\,|_{p^{\alpha}} = p^{\beta}r$, ahol r > 1 , így (p^{α}, k – 1) = 1,

és ez a tény független s – től. Q. E. D.

5. TÉTEL: Az alábbi csoportok $\mathcal{P} \cap \mathcal{C}h$ – ban vannak:

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

(b) $\boldsymbol{D}_{2^{\alpha}}$, $\alpha \geq 2$.

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

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

(b) $\boldsymbol{D}_{2^{\alpha}} \in \mathcal{M} \subset \mathcal{B} \subset \mathcal{C}h$. Q. E. D.

VI. rész
Csoportok a Ch – n kívül

TÉTEL: Az V. rész 5. tételében fölsoroltakon kívül minden más p – csoport

a $\mathcal{Ch}$ – n kívül van.

Bizonyítás: A következőkben erősen támaszkodunk az alábbi összefüggésekre:

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

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

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

(i v) Ha $(m \mid k \mid n) \cong (m \mid l \mid n)$, akkor $[\, k \mid n\,] \equiv [\, l \mid n\,]\ (m)$.

Ezen kongruenciák igazolását lásd a Függelékben.

Rátérünk a tétel bizonyítására.

(A) $G = (p^{\alpha} \mid p^{\alpha-\beta}+1 \mid p^{\beta+\delta})\ \begin{matrix} b \\ a \end{matrix}$, ahol $p \in \boldsymbol{P}_0$, $\alpha \ge 2$, $\alpha-1 \ge \beta \ge 1$, $\delta \ge 0$.

Azt fogjuk vizsgálni, hogy melyik az a legkisebb nemnegatív γ , amellyel létezik az $\omega : a \to ab^{p^{\gamma}}$ egyszerű automorfizmus. Azért keressük a lehető legkisebb γ – t , mert annak birtokában kaphatjuk meg a legnagyobb

$\langle \omega \rangle$ ciklust az Aut G – ben.

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

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

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

Ezért $\left[(p^{\alpha-\beta}+1)^{p^{\gamma}} \mid p^{\beta-\gamma+\delta}\right] \equiv \left[p^{\alpha-(\beta-\gamma)}+1 \mid p^{\beta-\gamma+\delta}\right] \equiv$

$$\equiv \left[p^{\alpha-(\beta-\gamma)}+1 \mid p^{\beta-\gamma}\right]\left[(p^{\alpha-(\beta-\gamma)}+1)^{p^{\beta-\gamma}} \mid p^{\delta}\right] \equiv$$

$$\equiv p^{\delta}\left[p^{\alpha-(\beta-\gamma)}+1 \mid p^{\beta-\gamma}\right] \equiv p^{\beta-\gamma+\delta} \quad (p^{\alpha}) ,$$

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

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

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

ha $\beta - \gamma + \delta \le \alpha$, azaz $\gamma \ge \beta - \alpha + \delta$. (3)

Tegyük föl, hogy γ kielégíti a (3) – at, s így (2) fönnáll.

Vizsgáljuk meg, hogy a $\partial(G) = \left\langle a^{p^{\alpha-\beta}} \right\rangle \le \left\langle ab^{p^\gamma} \right\rangle$ (4)

reláció milyen feltételek mellett teljesülhet.

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

amiből nyerjük, hogy $\alpha - \beta \ge \beta - \gamma + \delta$, azaz $\gamma \ge 2\beta - \alpha + \delta$ (5)

A továbbiakban tehát föl kell tennünk, hogy γ az (5) – öt is kielégíti.

Annak igazolása van hátra, hogy teljesül – e az alábbi reláció:

$$bab^{p^\gamma}b^{-1} = (ab^{p^\gamma})^{p^{\alpha-\beta}+1} \ . \qquad (6)$$

Ha (5) – ben egyenlőség van, akkor $\alpha - \beta = \beta - \gamma + \delta$,

s így $bab^{p^\gamma}b^{-1} = a^{p^{\alpha-\beta}+1}b^{p^\gamma} = a^{p^{\alpha-\beta}}ab^{p^\gamma} = a^{p^{\beta-\gamma+\delta}}ab^{p^\gamma} =$

$= (ab^{p^\gamma})^{p^{\beta-\gamma+\delta}}ab^{p^\gamma} = (ab^{p^\gamma})^{p^{\alpha-\beta}}ab = (ab^{p^\gamma})^{p^{\alpha-\beta}+1}$,

tehát (6) fönnáll.

[65]

Ha 2β – α + δ negatív, akkor γ = 0, és α – 2β – δ pozitív. Ekkor

$bab^{p^\gamma}b^{-1} = ba = a^{p^{\alpha-\beta}+1}b$, és $(ab^{p^\gamma})^{p^{\alpha-\beta}+1} = (ab)^{p^{\alpha-\beta}+1} = ((ab)^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}}ab =$

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

$(a^{p^{\beta+\delta}})^{p^{\alpha-2\beta-\delta}} \cdot ab = a^{p^{\alpha-\beta}+1}b$, tehát (6) ismét teljesül.

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

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

Ekkor viszont $\zeta_h(G) = \left\langle b^{p^\beta} \right\rangle$, s így $b^{p^\gamma} \in \zeta_h(G)$. 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 $a\rightleftharpoons b^{p^\gamma}$, ezért most is fönnáll (1) , és a (4) – et vizsgálva ismét az (5) – re jutunk.

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

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

E két oldal tehát akkor egyezik meg, ha

$p^{\alpha-\beta+\gamma}+p^\gamma\equiv p^\gamma \quad (p^{\beta+\delta})$.

Ebből $\alpha-\beta+\gamma\geq\beta+\delta$ következik, ami az (5) – tel ekvivalens.

[66]

Tehát a (6) most is fönnáll, az $\omega: a\rightarrow ab^{p^\gamma}$ leképezés az (5) teljesülése esetén akkor is automorfizmusa G – nek, ha $\gamma\geq\beta$.

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

E csoportnak létezni fog egy

$$\varphi:\quad \begin{matrix} a\rightarrow ab^{2^\gamma} \\ b\rightarrow b^\varepsilon \end{matrix}$$

automorfizmusa, ahol γ a legkisebb nemnegatív szám, amelyre

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

és ε – t az alábbi kongruenciával lehet kiszámítani:

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

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

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

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 fönnáll, hiszen γ nemnegatív.

Mármost $\partial(G) = \left\langle a^{2^{\alpha-\beta}} \right\rangle$, és annak föltétele, hogy $\partial(G) \le \left\langle ab^{2^{\gamma}} \right\rangle$ legyen, ez:

$$a^{2^{\alpha-\beta}} \in \left\langle a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)} \right\rangle = \left\langle ab^{2^{\beta-\gamma}} \right\rangle .$$

Ebből nyerjük az $\alpha-\beta \ge \beta-\gamma$, tehát a $\gamma \ge 2\beta-\alpha$ feltételt.

Igazolandó, hogy fönnáll a definiáló reláció:

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

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

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

Ha most $\gamma > 2\beta-\alpha$, akkor γ minimalitása miatt $\gamma = 0$ és $\alpha - 2\beta$ pozitív.

Ekkor a $(**)$ jobboldala így alakul:

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

$$= a^{2^{2\alpha-2\beta-1}+2^{\alpha-\beta}+1}b = a^{2^{\alpha-\beta}+1}b,$$

hiszen $2^{2\alpha-2\beta-1} \equiv 0 \quad (2^{\alpha})$ pont azért, mert most $\alpha - 2\beta$ pozitív.

Jelen esetben tehát a $(**)$ az $\varepsilon = 1$ választással kielégül.

Ha a $G = (2^{\alpha} \mid 2^{\alpha-\beta}+1 \mid 2^{\beta+\delta})\ \begin{matrix} b \\ a \end{matrix}$ homológot vizsgáljuk, ahol $\delta > 0$, akkor a fentiekkel teljesen analóg okoskodás a $\gamma \ge 2\beta-\alpha+\delta$ relációt fogja adni,

akárcsak e tétel (A) pontjában.

A homológképzésnél megszűnhet a csatolás. Pl. a $(16 \mid 5 \mid 4)\ \begin{matrix} b \\ a \end{matrix}$ – nek egy $a \to ab^2, b \to b^3$ csatolt automorfizmusa van, ám a $(16 \mid 5 \mid 4)\ \begin{matrix} b \\ a \end{matrix}$ – nek az $a \to ab^2$ leképezés egyszerű automorfizmusa.

(C) $G = (2^{\alpha} \mid 2^{\alpha-\beta}-1 \mid 2^{\beta})\ \begin{matrix} b \\ a \end{matrix}$, ahol $\alpha \ge 4$, $\alpha-2 \ge \beta \ge 2$.

E csoportnak létezik egy

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

ω :

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

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

A bizonyítás stratégiája az eddigiekével azonos:

vizsgáljuk az ab^{2^γ} elemet :

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

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

Ez azért van így, mert az $\boldsymbol{R}_{2^\alpha} \cong (2^{\alpha-2}) \times (2)$, $\alpha \geq 3$ 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:

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

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 $\partial(G) = \left\langle a^{2^{\alpha-\beta}-2} \right\rangle = \left\langle a^2 \right\rangle$, és ahhoz, hogy

$a^2 \in \left\langle a^{2^{\beta-\gamma}(2^{\alpha-(\beta-\gamma)-1}+1)} \right\rangle = \left\langle a^{2^{\beta-\gamma}} \right\rangle$ teljesüljön, kell $\beta - \gamma \leq 1$, azaz $\gamma \geq \beta - 1$.

Ámde $\beta - 1 \geq \gamma$ is fönnáll, így kapjuk, hogy $\gamma = \beta - 1$.

Még azt kell belátni, hogy

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

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

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

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

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

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

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

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

$$\equiv 2^{2\alpha-\beta-1}+2^{\alpha-\beta}-2^{\alpha-1}-1 \ (2^{\alpha}) . \qquad (9)$$

A (8) – beli kitevővel hosszabb a számolás:

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

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

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

$$\equiv (2^{\alpha-1}+2)(2^{\alpha-\beta-1}-1) \equiv 2^{2\alpha-\beta-2}+2^{\alpha-\beta}-2^{\alpha-1}-1 \qquad (2^{\alpha}) . \quad (10)$$

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

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

Ámde ez triviális, hiszen e kongruencia mindkét oldala osztható 2^{α} – val – abból kifolyólag, hogy $\alpha-2 \geq \beta$.

Az $|\omega| = 2$ közvetlen számolással adódik.

(D) $G = (2^{\alpha} \mid 2^{\alpha-\beta}-1 \mid 2^{\beta+\delta}) \begin{matrix} b \\ a \end{matrix}$, ahol $\alpha \geq 3$, $\alpha-2 \geq \beta > 1$, $\delta \geq 1$.

G – nek létezik egy ω : $a \to ab^{2^{\beta+\delta-1}}$ egyszerű automorfizmusa.

A bizonyításnál ugyanúgy járunk el, mint (A) – nál: az ω – t $a \to ab^{2^{\gamma}}$ alakban keressük, szétválasztva a $\gamma < \beta$ és $\gamma \geq \beta$ eseteket.

(E) $G = (2^{\alpha} \mid 2^{\alpha}-1 \mid 2^{1+\delta}) \begin{matrix} b \\ a \end{matrix}$, ahol $\alpha \geq 2$, $\delta \geq 1$.

Itt a következő számolás fogja mutatni egy ω : $a \to ab^{2^{\delta}}$ automorfizmus meglétét: vizsgáljuk meg az $ab^{2^{\gamma}}$ elemet .

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

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

Az $(ab^{2^{\gamma}})^{2^{l-\gamma+\delta}} = a^{2^{l-\gamma+\delta}}$ 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.

$\partial(G) = \left\langle a^{2^{\alpha-2}} \right\rangle = \left\langle a^2 \right\rangle$, és $\left\langle a^2 \right\rangle \leq \left\langle ab^{2^{\gamma}} \right\rangle$ pontosan akkor, ha $a^2 \in \left\langle a^{1-\gamma+\delta} \right\rangle$.

Ez azonban csakis úgy teljesülhet, ha $2^{1-\gamma+\delta} \mid 2$, azaz $1 \geq 1-\gamma+\delta$,

amiből $\gamma \geq \delta$ következik.

Csakhogy $1 + \delta > \gamma$ is fönnáll, ezért végül $\gamma = \delta$.

Mivel most $\zeta_h(G) = \left\langle b^2 \right\rangle$, 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 $2^{\alpha+\delta} - 2^{\delta} \equiv 2^{\delta}$ $(2^{1+\delta})$, 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 $(s) \times (m \mid k \mid \dot{n}\ s) \notin \mathcal{U}$.

Bizonyítás: Legyen $(s) \times G = (ms \mid l \mid \dot{n}\ s)\frac{b}{a} = G_s$.

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

hogy $\mathcal{X} \cap \mathcal{U} = \varnothing$.

Tegyük föl ezért, hogy $\pi(s) \subset \pi(n)$. (11)

(Az $(n , s) \neq 1$ nem elég, mert ettől még előfordulhat, hogy az s – nek egy valódi osztójára, s' – re $(n , s') = 1$, ami megint a $G_s \in \mathcal{X}$ esetre vezetne.)

Tekintsük az ab^n elemet G_s – ben. Egyrészt $(ab^n)^s = a^s b^{ns} = a^s$,

és így $| ab^n | = ms$, másrészt $1 \equiv 1$ (s), ezért $a^{1-1} \in \left\langle a^s \right\rangle$, vagyis $\partial(G_s) \leq \left\langle a^s \right\rangle$.

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

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

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

Mindebből az következik, hogy a G_s – nek létezik egy

$$\varphi : \begin{matrix} a \to ab^n \\ b \to b \end{matrix}$$

egyszerű automorfizmusa. Q. E. D.

E lemma kapcsán fölmerülhet a kérdés, hogy az $a^s b^n$ elem miért ne lehetne az a – nak automorf képe? Hiszen most is $|a^s b^n| = ms$,

és $(a^s b^n)^s = a^{s^2}$, $|a^{s^2}| = m$ miatt $\partial(G_s) \leq \langle a^{s^2} \rangle$.

Tehát az $\langle a^s b^n \rangle$ is egy ms – rendű ciklus, mely tartalmazza a kommutátort.

Ugyanakkor $(a^s b^n)^m = b^{mn}$, és mivel $\langle b^n \rangle \cong (s)$, és $(m, s) = 1$,

ezért $\langle b^{mn} \rangle = \langle b^n \rangle$. Tehát $\langle a^s b^n \rangle \cap \langle b \rangle = \langle b^n \rangle$.

Eszerint az $a^s b^n$ az a – nak csak valamilyen x – automorfizmusnál lehetne a képe, ami megint a $G_s \in \mathfrak{X}$ esetre vezetne.

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

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

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

$b a b^{-1} = a^l$, (12 c)

$a^s b^n = 1$. (12 d)

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

$a^s = 1$ (12 e)

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

$b^n = 1$ (12 f)

relációt adja.

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

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

Látnivaló, hogy a (12 e, f, g) relációk egy (s) × (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 $G_s \in \mathfrak{X}$.

[74]

E fejtegetések melléktermeke, hogy $\mathfrak{X} \cap \mathfrak{C} = \varnothing$.

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

$\mathfrak{C}$ – ba nem tartozó csoportot készíthessünk. A legegyszerűbb példa:

$G = (6 \mid 5 \mid 4)\begin{matrix} b \\ a \end{matrix}$. Ennél Aut G = $\langle \varphi, \psi, \sigma, \omega \rangle$, ahol

$$\varphi : a \to a^5 \ , \mid \varphi \mid = 2 \ ,$$
$$\psi : b \to ab \ , \mid \psi \mid = 6 \ ,$$
$$\sigma : b \to b^3 \ , \mid \sigma \mid = 2 \ ,$$
$$\omega : a \to ab^2 \ , \mid \omega \mid = 2 \ .$$

Több – kevesebb számolással kimutatható, hogy Aut $(6 \mid 5 \mid 4) \cong \boldsymbol{D}_3 \times \boldsymbol{D}_4$.

Nem látszik sokkal bonyolultabbnak a $G = (21 \mid 4 \mid 9)\begin{matrix} b \\ a \end{matrix}$ sem, holott itt Aut G = $\langle \varphi_3, \varphi_7, \psi_3, \psi_7, \sigma, \omega \rangle$, ahol

$$\varphi_3 : a \to a^8 \ , \mid \varphi_3 \mid = 2 \ ,$$
$$\varphi_7 : a \to a^{19} \ , \mid \varphi_7 \mid = 6 \ ,$$
$$\psi_3 : b \to a^7 b \ , \mid \psi_3 \mid = 3 \ ,$$
$$\psi_7 : b \to a^3 b \ , \mid \psi_7 \mid = 7 \ ,$$
$$\sigma : b \to b^4 \ , \mid \sigma \mid = 3 \ ,$$
$$\omega : a \to ab^3 \ , \mid \omega \mid = 3 \ .$$

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

[75]

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

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

Bizonyítás: Ha $(m \mid k \mid n) \begin{matrix} b \\ a \end{matrix} \notin \mathcal{C}$, akkor a 38. o. (A 2) szerint van egy

$$\varphi: \quad a \longrightarrow a\, b^{\beta} , \beta \downarrow n$$
$$b \longrightarrow b^{\delta}, \quad \delta \in \boldsymbol{R}_n$$

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

$$[k^{\beta} \mid m] \equiv 0 \ (m) , \qquad (KR\ 1)$$
$$\beta\, m \equiv 0 \ (n) , \qquad (KR\ 2)$$
$$[k^{\beta} \mid k - 1] \equiv k^{\delta} - 1 \ (m) , \qquad (KR\ 3)$$
$$\beta\, (k - 1) \equiv 0 \ (n) . \qquad (KR\ 4)$$

(A $\mathcal{B}$ – tétel (48. o.) bizonyításában láthattuk, hogy $[k^{\beta} \mid k] \equiv k^{\delta} \ (m)$ és $\beta\, (k - 1) \equiv 0 \ (n)$ relációkból hogyan következik (KR 3) .)

Most e lemmában azt kell bizonyítani, hogy ha (KR 1 – 4) – ben áttérünk m – ről ms – re, k – ról j –re, ahol $(m , s) = 1$, és $j \equiv k \ (s)$, akkor a (KR 1 – 4) relációk továbbra is érvényben maradnak. Rögtön látszik, hogy csak a (KR 3) – at kell közelebbről megvizsgálni. Világos, hogy

$$[j^{\beta} \mid j - 1] \equiv j^{\delta} - 1 \ (ms)$$

pontosan akkor teljesül, ha

$$[j^{\beta} \mid j - 1] \equiv j^{\delta} - 1 \ (m) , \qquad (13)$$

[76]

és $$[j^{\beta} \mid j - 1] \equiv j^{\delta} - 1 \ (s) . \qquad (14)$$

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

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

$$[k^{\beta} \mid j - 1] \equiv k^{\delta} - 1 \ (m) ,$$

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

Legyen $j = k + mx$. Akkor

$[k^{\beta} \mid j - 1] = [k^{\beta} \mid k - 1 + mx] = [k^{\beta} \mid k - 1] + k^{\beta (k-1)} \ [k \mid mx] =$

$=$ (a (KR 4) miatt) $= [k^{\beta} \mid k - 1] + [k^{\beta} \mid mx] =$

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

mert (KR 1) miatt $[k^{\beta} \mid m] \equiv 0 \ (m)$. Q. E. D.

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

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

a fúzió lehet $\mathcal{Ch}$ – beli, dacára annak, hogy egy vagy minden tényezője $\mathcal{Ch}$ – n

kívül esik. Tekintsük például ezeket:

$(5 \mid 3 \mid 4) \in \mathfrak{Ch}$,

$(7 \mid 3 \mid 6) \in \mathfrak{Ch}$,

$(9 \mid 4 \mid 3) \notin \mathcal{Ch}$,

$(16 \mid 5 \mid 4) \notin \mathcal{Ch}$.

Kihasználva a fúzió asszociativitását, a fenti csoportok fúziója

kétféleképpen is felírható:

$[(7 \mid 3 \mid 6) \otimes (16 \mid 5 \mid 4)] \otimes [(5 \mid 3 \mid 4) \otimes (9 \mid 4 \mid 3)]$ (15)

$[(7 \mid 3 \mid 6) \otimes (9 \mid 4 \mid 3)] \otimes [(5 \mid 3 \mid 4) \otimes (16 \mid 5 \mid 4)]$ (16)

A (15) fölírásnál a szögletes zárójelben álló csoportok nincsenek $\mathcal{Ch}$ – ban,

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

szerint ez a négyes fúzió $\mathcal{Ch}$ – beli lesz. Magyarán szólva

$$G_1 , G_2 \notin \mathcal{Ch} \not\Rightarrow G_1 \otimes G_2 \notin \mathcal{Ch} .$$

Legyen

$G_1 = (p^{\alpha} \mid p^{\alpha-\beta} + 1 \mid p^{\beta}) , p \in \boldsymbol{P}_0$,

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

Ekkor $G = G_1 \otimes G_2 = (p^{\alpha} q \mid j \mid rp^{\varepsilon}) \begin{matrix} b \\ a \end{matrix}$,

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

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

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

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

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

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

A továbbiak előtt jegyezzük meg a következőket:

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

[78]

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

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

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

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

Ezekből kapjuk, hogy [k^{β} | k – 1] ≡ k – 1 (m) . (K 311)

Térjünk vissza a 77. oldali G csoporthoz.

Keressük b – nek azt a legkisebb kitevőjét – méghozzá $t\, p^{\gamma}$, t | r , $\varepsilon > \gamma$ alakban, amellyel a $\varphi : a \to ab^{tp^{\gamma}}$ egyszerű automorfizmusa lesz G – nek.

A (K 12) – be (36. o.) írjuk be a megfelelő adatokat, akkor kapjuk, hogy

$$t\, p^{\alpha+\gamma} \equiv 0 \ (p^{\varepsilon} r) \ .$$

Ebből $t \equiv 0$ (r) következik.

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

Írjuk föl a (K 311) – et :

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

Régebbi vizsgálódásainkból (ld. TÉTEL (A) – ban az (5) δ = 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]

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

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

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

Mármost $\varepsilon = \max(\beta,\delta) > \gamma \geq \delta$ - ból következik, hogy ε = β ,

s mivel nyilván ε > γ , végül nyerjük, hogy $\beta - 1 \geq \gamma \geq \delta$. (22)

A φ leképezésünk tehát mindenesetre olyan lesz, hogy benne b kitevője

(19) miatt r p^{γ} alakú, ahol γ – nak ki kell elégítenie a (20) és (22)

relációkat. (Nem vizsgáltuk az $ab^{rp^{\gamma}}$ rendjét, mert (K 311) biztosítja, hogy ez a rend $p^{\alpha}q$.)

Írjuk föl még (K 32) – t is (36. o.) ; kapjuk belőle, hogy

$\alpha - \beta + \gamma \geq \varepsilon$, azaz $\gamma \geq \varepsilon - \alpha + \beta$ (23)

A megfelelő γ – nak tehát a (20) , (22) és (23) relációkat ki kell elégítenie.

De ez csak látszólag három reláció, ugyanis most ε = β , és így a (23) – ból

$\gamma \geq 2\beta - \alpha$, ami a (20) – szal azonos.

Az elmondottakból most már világos, hogy a

(7 | 4 | 3) ⊗ (9 | 4 | 3) = (63 | 4 | 3) miért lesz $\mathcal{C}\mathcal{U}$ – beli.

Foglaljuk össze az eddigieket:

3. LEMMA: Legyen

$G_1 = (p^{\alpha} \mid p^{\alpha-\beta} + 1 \mid p^{\beta})$, ahol $p \in \boldsymbol{P}_0$, $\alpha - 1 \geq \beta \geq 1$,

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

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 $\varphi : a \to ab^{rp^{\gamma}}$

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

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

ω :

$$b \to b^{\varepsilon}$$

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

[81]

5. LEMMA: A

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

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

csoportok fúziójaként előálló

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

csoportnak lesz egy

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

ω :

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

c – automorfizmusa, és $|\omega| = 2$. Q. E. D.

Az e részbeli tételben, illetve a 3. , 4. , és 5. lemmákban külön nem vizsgáltuk, hogy a szereplő $(m \mid k \mid n)_{a}^{b}$ 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 $\boldsymbol{S}$ – csoportok szerepelnek, a következő két lemma segít a fenti probláma megoldásában.

6. LEMMA: Ha $(m \mid k \mid n) \in \boldsymbol{S}$, akkor tetszőleges $b \in \boldsymbol{Z}_{n}$ esetén

$$\langle ab^{\beta} \rangle \cap \langle b \rangle = 1 \ .$$

Bizonyítás: Tegyük föl, hogy $b^{x} \in \langle ab^{\beta} \rangle$. Ekkor nyilván $b^{x} \rightleftharpoons ab^{\beta}$, ezért

$b^x a b^\beta b^{-x} = a b^\beta$. Másrészt $b^x a b^\beta b^{-x} = a^{k^x} b^\beta$, ahonnan $k^x \equiv 1$ (m) következik, ami a csoport $\mathcal{S}$ – belisége miatt csak x = 0 – val elégíthető ki.

Q. E. D.

7. LEMMA: Legyen a G = (m | k | n) $\begin{matrix} b \\ a \end{matrix}$ csoportban az m egy prím hatványa, és tegyük föl, hogy | ab^β | = m, valamint $\partial(G) \leq \langle ab^\beta \rangle$. Akkor

$$\langle ab^\beta \rangle \cap \langle b \rangle = 1 .$$

Bizonyítás: Ha $b^x \in \langle ab^\beta \rangle$ valamely $x \neq 0$ számmal, akkor $\langle b \rangle \cap \partial(G) = 1$ miatt $\langle b^x \rangle \cap \partial(G) = 1$, s mivel $\partial(G) \leq \langle ab^\beta \rangle$, azt kapjuk, hogy egy prímhatvány-rendű ciklusban diszjunkt valódi részek vannak, ami nyilván lehetetlen.

Q. E. D.

VII. rész
Nyitott kérdések

1. DEFINÍCIÓ: Legyen G tetszőleges véges csoport, | G | = n .

Azt mondjuk, hogy a G – nek a $p \in \pi(n)$ prímre vonatkozó bősége α –

jelben $w_p(G) = \alpha$ – , ha G – ben van $(p)^{\alpha}$ részcsoport, 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 $G \in$ CYCYS, akkor $w(G) \leq 2$.

Ez ekvivalens azzal, hogy ha $G \in$ CYCYS, akkor G bármely részcsoportja

legföljebb két generátorral prezentálható.

Az I. rész 3. lemmában (15. o.) megállapítottuk, hogy CYCYS $\subset$ DIV .

2. SEJTÉS: CYCYS $\subset$ TODIV .

E sejtésre rögvest igent mondhatnánk, ha kiderülne, hogy a $G \in$ CYCYS minden részcsoportja abeli vagy CYCYSbeli. Ez azonban sajnos nem igaz.

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

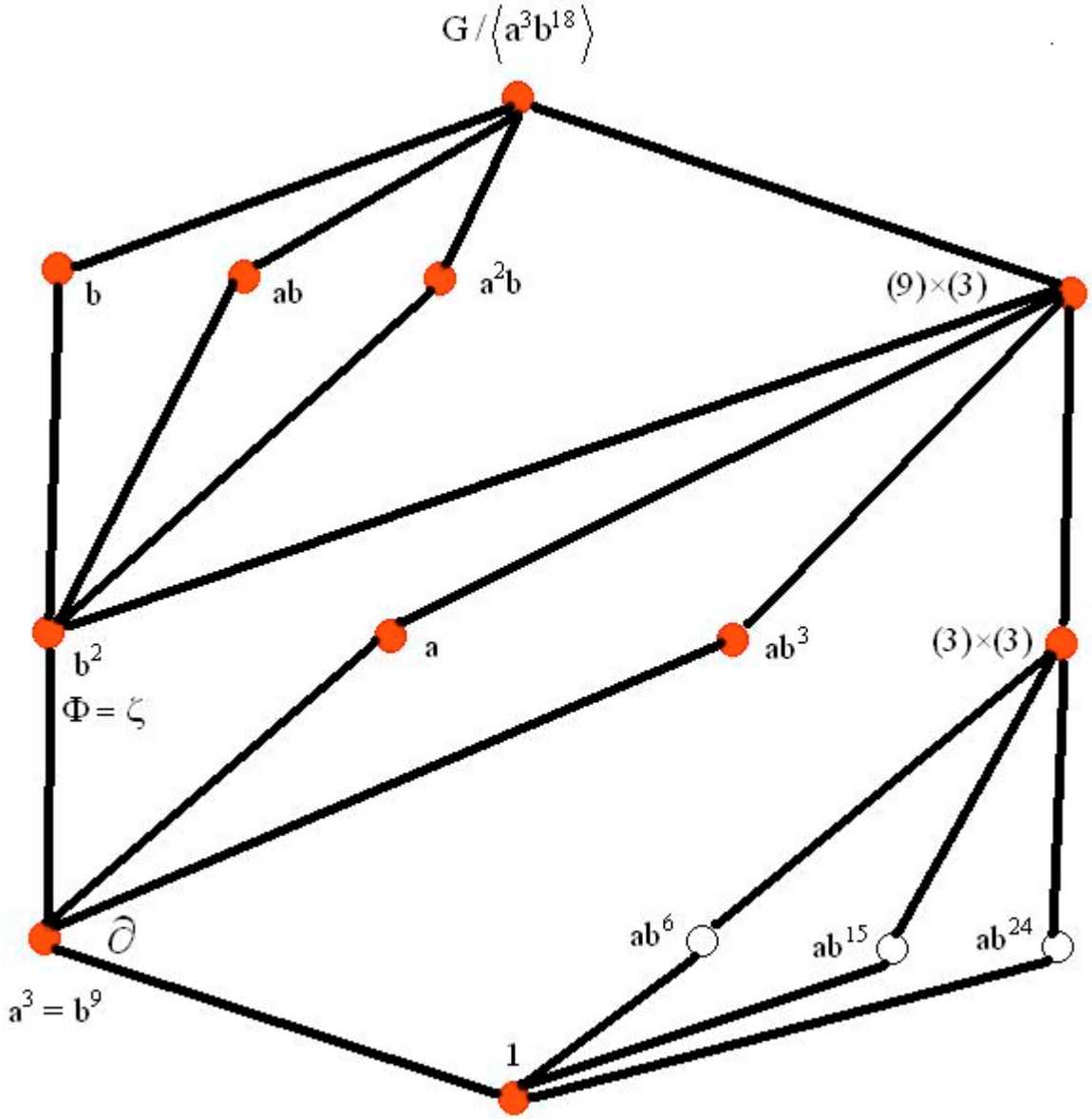
Hasonlóan nem áll, hogy egy CYCYSbeli csoport minden nemabeli faktor-

csoportja CYCYSbeli. Itt a minimális ellenpélda a $G = (4 \mid 3 \mid 4)\ \begin{matrix} b \\ a \end{matrix}$, ahol az $\langle a^2 b^2 \rangle$ szerinti

faktorcsoportja $\boldsymbol{Q}$ – val izomorf.

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

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 szétesők bővítéseként sem.

Az imént vázolt csoport a következő csoportosztályba tartozik:

2. DEFINÍCIÓ: $(m \mid r , k \mid n)\ \begin{matrix} b \\ a \end{matrix}$ – vel jelöljük a következő prezentációt:

$$a^m = b^n = 1 , \qquad (1)$$

$$a^{\frac{m}{r}} = b^{\frac{n}{r}} , \qquad (2)$$

$$b\, a\, b^{-1} = a^k . \qquad (3)$$

E relációk konzisztenciájához az alábbiak szükségesek:

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

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

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

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 | m és r | n a (2) – ből világos.

Az r | k – 1 – hez gondoljuk meg a következőket:

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

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

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

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

Innen adódik az r | k – 1 .

Az (1), (2), (3) által prezentált csoportok halmazát CYCEX – nek nevezzük.

Rendkívül érdekes, hogy a CYCEX csoportok CYCYSbeli csoportok faktorcsoportjaiként kaphatók, ugyanakkor CYCYS $\subset$ CYCEX ,

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

Végezetül még egy talány:

3. SEJTÉS: CYCYS $\subset$ MAXPIND .

Függelék

A 63. oldalon fölsorolt összefüggések bizonyítása:

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

Bizonyítás: $[\, s\, p^{\alpha-\beta}+1 \mid p^{\beta}\,] = \dfrac{(sp^{\alpha-\beta}+1)^{p^{\beta}}-1}{sp^{\alpha-\beta}} =$

$$= p^{\beta} + \sum_{k=2}^{p^{\beta}} \binom{p^{\beta}}{k} s^{k-1} p^{(k-1)(\alpha-\beta)} ,$$

ahol a szumma minden tagja osztható p^{α} – val. Q. E. D.

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

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

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

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

$\equiv 2^{\beta} - 2^{\alpha-1} \equiv 2^{\beta} + 2^{\alpha-1}$ (2^{α}) , hiszen $-2^{\alpha-1} \equiv 2^{\alpha-1}$ (2^{α}) . Q. E. D.

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

[87]

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

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

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

$B = 2j + 1$, és így $2^{\alpha-1} B = 2^{\alpha} j + 2^{\alpha-1} \equiv 2^{\alpha-1}$ (2^{α}) . Q. E. D.

(i v) $(m \mid k \mid n) \cong (m \mid l \mid n)$ esetén $[\, k \mid n\,] \equiv [\, l \mid n\,]$ (m) .

Bizonyítás: egészen triviális. Q. E. D.

Irodalom

Kuros: Csoportelmélet

Niven – Zuckerman: Bevezetés a számelméletbe

Huppert: Endliche gruppen i.

Coxeter – Moser: Generators and relations for discrete groups

Itt végződik a CYCYS eredeti kézirata.

Utóirat

Huber László 1997 július 2-án meghalt, 42 éves volt. Kézirata 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