Tartalomjegyzék

1. Csoportkonstrukciók **2**
1.1. Direkt szorzat . . . 2
1.2. Szemidirekt szorzat . . . 3
1.3. Ciklikus csoportok automorfizmuscsoportja . . . 6

2. Permutációcsoportok **8**

3. Feloldható csoportok **13**
3.1. Kommutátor-részcsoport . . . 13
3.2. Feloldható csoportok . . . 14
3.3. Hall-részcsoportok . . . 16

4. Nilpotens csoportok **19**
4.1. Nilpotens csoportok jellemzése . . . 19
4.2. Frattini-részcsoport . . . 21
4.3. Véges p-csoportok . . . 22
4.4. Hamilton-csoportok . . . 23

5. Transzfer **26**

6. Primitív és többszörösen tranzitív permutációcsoportok **30**
6.1. k-tranzitív csoportok . . . 30
6.2. Primitív csoportok . . . 31
6.3. Tranzitív és primitív csoporthatások . . . 32
6.4. Szigorúan k-tranzitív permutációcsoportok . . . 33
6.5. Mathieu-csoportok . . . 34

7. Szabad csoportok **38**
7.1. Definiáló relációk . . . 39
7.2. Nielsen–Schreier-tétel . . . 40

Tárgymutató **43**

1. Csoportkonstrukciók

1.1. Direkt szorzat

Definíció. Két csoport, H és K *külső direkt szorzata* a $H \times K = \{(h,k) \mid h \in H,\ k \in K\}$ Descartes-szorzat a komponensenkénti szorzással:

$$(h_1,k_1)\cdot(h_2,k_2) = (h_1h_2, k_1k_2).$$

Ha $H, K \lhd G$ és $H \bigcap K = 1$, $HK = G$, akkor G-t a H és K *belső direkt szorzatának* nevezzük.

A fenti két fogalom ekvivalens abban az értelemben, hogy ha G belső direkt szorzata a H és K csoportoknak, akkor természetes módon izomorf a $H \times K$ külső direkt szorzattal, és fordítva, a $H \times K$ külső direkt szorzat belső direkt szorzata a $H \times 1 \cong H$ és $1 \times K \cong K$ normálosztóinak. A továbbiakban a két fogalmat nem fogjuk megkülönböztetni.

Definíció. A G_i $(i \in I)$ csoportok (diszkrét) *direkt szorzata* a Descartes-szorzatuk

$$\prod_{i\in I} G_i = \{(\ldots, g_i, \ldots) \mid \text{ véges sok } g_i \neq 1\}$$

részhalmaza a komponensenkénti szorzással (véges I esetén ez a teljes Descartes-szorzat). Illetve belső szorzatként: $G = \prod\limits_{i\in I} G_i$, ha $G_i \lhd G\ \forall i$, $\langle G_i \mid i \in I\rangle = G$, és $G_i \cap \langle G_j \mid j \neq i\rangle = 1\ \forall i$.

1.1. Tétel. ***Krull–Schmidt-tétel***
Ha egy véges csoportot felbontunk direkt felbonthatatlanok direkt szorzatára, akkor a felbontás a komponensek izomorfiájától és a sorrendjétől eltekintve egyértelmű.

1.2. Tétel. *S akkor és csak akkor részcsoportja a $G = G_1 \times G_2$ csoportnak, ha léteznek olyan $N_i \lhd H_i \leqslant G_i$ részcsoportok és egy $\varphi : H_1/N_1 \to H_2/N_2$ izomorfizmus a hozzájuk tartozó szeletek között, amelynek grafikonja S, azaz*

$$S = \{(h_1,h_2) \in H_1 \times H_2 \mid \bar{h_1}\varphi = \bar{h_2}\}.$$

Bizonyítás: $\Leftarrow$: Ezek a grafikonok valóban részcsoportok, ugyanis $\bar{1}\varphi = \bar{1} \implies (1,1) \in S$, és ha $(h_1,h_2),(h_1',h_2') \in S$, akkor $(h_1,h_2)^{-1}(h_1',h_2') = (\overline{h_1^{-1}h_1', h_2^{-1}h_2'}) \in S$:
$\overline{h_1^{-1}h_1'}\varphi = (\bar{h_1}^{-1}\bar{h_1'})\varphi = (\bar{h_1}\varphi)^{-1}\bar{h_1'}\varphi = \bar{h_2}^{-1}\bar{h_2'} = \overline{h_2^{-1}h_2'}$.
$\Rightarrow$: Legyen $\pi_1 :\ G_1 \times G_2 \to G_1$, $(g_1,g_2) \to g_1$ és $\pi_2 :\ G_1 \times G_2 \to G_2$, $(g_1,g_2) \to g_2$ az első, illetve második komponensre képező projekció.
Legyen a $\pi_1|_S$ homomorfizmus képe $H_1 = \{g_1 \in G_1 \mid \exists g_2 \in G_2 :\ (g_1,g_2) \in S\}$, és a $\pi_2|_S$ homomorfizmus magja (precízebben annak a G_1-re vett vetülete) $N_1 = \{g_1 \in G_1 \mid (g_1,1) \in S\}$.
Ugyanígy $H_2 = \{g_2 \in G_2 \mid \exists g_1 \in G_1 :\ (g_1,g_2) \in S\}$ és $N_2 = \{g_2 \in G_2 \mid (1,g_2) \in S\}$.
Ekkor $N_i \lhd H_i \leqslant G_i$, és $N_1 \times N_2 \leqslant S \leqslant H_1 \times H_2$.
Definiáljuk a $\varphi : H_1/N_1 \to H_2/N_2$ leképezést a

$$\bar{h}_1\varphi = \bar{h}_2 \iff (h_1,h_2) \in S$$

összefüggéssel.

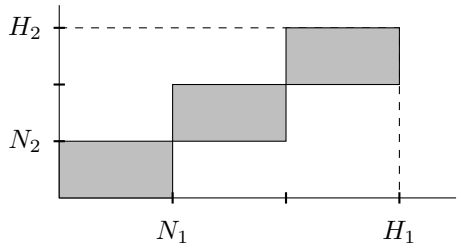
φ jól definiált, mert $\forall n_1 \in N_1,\ n_2 \in N_2$: $(h_1,h_2) \in S \iff (h_1n_1, h_2n_2) = (h_1,h_2)(n_1,1)(1,n_2) \in S$, mivel $(n_1,1),(1,n_2) \in S$.

φ nyilván szorzattartó, és szürjektív is a H_2 definíciója szerint.

φ injektív, mert $\bar{h}_1\varphi = \bar{1} \implies (h_1,1) \in S \implies h_1 \in N_1 \implies \bar{h}_1 = \bar{1}$.

Végül S a φ grafikonja a φ definíciója szerint. □

Megjegyzés. Az előző tétel konstrukciója szerint a φ grafikonjaként megkapott S részcsoport a φ által egymásnak megfeleltetett mellékosztályok Descartes-szorzatainak uniója. Következésképpen $|S| = |N_1| \cdot |N_2| \cdot |H_1 : N_1| = |N_1| \cdot |N_2| \cdot |H_2 : N_2|$.



Példa. Határozzuk meg $C_4 \times S_3$ részcsoportjait!
C_4 szeletei C_1-gyel, C_2-vel és C_4-gyel izomorfak, de S_3-nak nincs C_4-gyel izomorf szelete, mivel S_3 rendje nem osztható 4-gyel.
Egy K csoporttal izomorf szeletek között éppen $|\mathrm{Aut}(K)|$ izomorfizmus van, ezért a részcsoportok száma

$$\sum_K |\{K\text{-val izomorf szeletpárok}\}| \cdot |\mathrm{Aut}(K)|.$$

C_1-gyel izomorf szelet tartozik minden részcsoporthoz, ez $3 \cdot 6$ szeletpárt jelent, C_2-vel izomorf szelet C_4-ben kettő van, S_3-ban pedig a három másodrendű részcsoport ($N_2 = 1$ választással), és S_3/A_3 összesen négy C_2-vel izomorf szeletet ad.
Így $C_4 \times S_3$-nak $3 \cdot 6 \cdot 1 + 2 \cdot 4 \cdot 1 = 26$ részcsoportja van.

1.2. Szemidirekt szorzat

Definíció. A G csoport az N normálosztójának a H részcsoporttal vett (belső) *szemidirekt szorzata*, $G = N \rtimes H$ (vagy $G = H \ltimes N$), ha $H \cap N = 1$ és $HN = G$.

Tehát ha $G = H \ltimes N$, akkor minden $g \in G$-hez létezik egyetlen $h \in H$ és $n \in N$, amelyre $g = hn$. Az ebben a formában felírt elemek szorzata:

$$(hn)(h'n') = hh'h'^{-1}nh'n' = hh'n^{h'}n'.$$

Ennek segítségével definiálhatjuk két csoport külső szemidirekt szorzatát.

Definíció. Legyen N és H két csoport, és $\varphi : H \to \mathrm{Aut}(N)$ homomorfizmus. Ekkor N és H (külső) *szemidirekt szorzata* ($N \rtimes H$ vagy $H \ltimes N$) a H és N Descartes-szorzata a

$$(h, n) \cdot (h', n') = (hh', n^{h'\varphi}n').$$

szorzással.

Az olvasóra bízzuk annak ellenőrzését, hogy ezzel a definícióval $N \rtimes H$ valóban csoport: a szorzás asszociatív, $(1, 1)$ egységelem, és $(h, n)^{-1} = (h^{-1}, [n^{(h^{-1}\phi)}]^{-1})$.

1.3. Állítás. *A $G = N \rtimes H$ külső szemidirekt szorzat az $\tilde{N} = \{(1, n) \mid n \in N\} \cong N$ normálosztójának és $\tilde{H} = \{(h, 1) \mid h \in H\} \cong H$ részcsoportjának belső szemidirekt szorzata. (A továbbiakban ezeket azonosítjuk N-nel, illetve H-val.)*

Bizonyítás: Mivel $(h, 1)(h', 1) = (hh', 1^{h'\varphi}1) = (hh', 1)$, $(1, n)(1, n') = (1, n^{1\varphi}n') = (1, nn')$, és $(h, 1)(1, n) = (h, 1^{1\varphi}n) = (h, n)$, világos, hogy $\tilde{H} \cong H$, $\tilde{N} \cong N$, és $\tilde{H}\tilde{N} = G$, továbbá $\tilde{H} \cap \tilde{N}$ is nyilvánvaló. Mivel $G = \tilde{H}\tilde{N}$, annak belátásához, hogy $\tilde{N} \lhd G$, elég megmutatni, hogy $\tilde{N}$ elemeinek a $\tilde{H}$-beli elemekkel vett konjugáltja $\tilde{N}$-beli.

$$(1, n)^{(h,1)} = (h^{-1}, 1)(1, n)(h, 1) = (h^{-1}, n)(h, 1) = (h^{-1}h, n^{h\varphi}1) = (1, n^{h\varphi}).$$

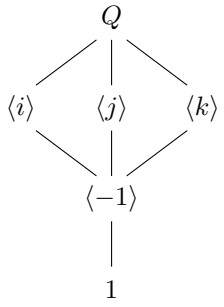
Ezzel egyúttal azt is beláttuk, hogy egy $(h, 1)$ elemmel való konjugálás az N-en megfelel a $h\varphi$ automorfizmus hatásának. □

Példa. 1. Diédercsoportok: $D_n = \langle f \rangle \rtimes \langle t \rangle \cong C_n \rtimes C_2$, ahol t hatása C_n-en $f^t = f^{-1}$ (másodrendű automorfizmus).

2. S_n előáll-e (valódi) szemidirekt szorzatként? $A_n \lhd S_n$, $|S_n : A_n| = 2$. Legyen $\tau = (12) \in S_n \setminus A_n$, ekkor $\langle\tau\rangle \cap A_n = 1$, és $\langle\tau\rangle A_n = S_n$ a rendek miatt. Tehát $S_n = A_n \rtimes \langle\tau\rangle$.

3. S_4-nek normálosztója $V = \langle(12)(34), (14)(24)\rangle \simeq C_2 \times C_2$. Az $S_3 (= \langle(12), (123)\rangle)$ részcsoport komplementuma V-nek, azaz $S_3 \cap V = 1$, és $|S_3V| = \dfrac{|S_3| \cdot |V|}{|S_3 \cap V|} = 24 = |S_4|$, így $S_4 = S_3V$. Tehát $S_4 = V \rtimes S_3$.

4. Legyen $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ a *kvaterniócsoport*, tehát $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, $i^2 = j^2 = k^2 = -1$). Q részcsoporthálója



Q-nak nincs valódi szemidirekt felbontása, mert nincs két nem triviális diszjunkt részcsoportja.
Viszont elő tudjuk állítani Q-t két ciklikus csoport szemidirekt szorzatának faktorcsoportjaként:

$$Q \cong \langle b\rangle \ltimes \langle a\rangle / \langle (b^{-2}, a^2)\rangle,$$

ahol $\langle a\rangle \cong \langle b\rangle \cong C_4$, és $a^b = a^{-1}$, ugyanis könnyen ellenőrizhető, hogy a $\psi : \langle b\rangle \ltimes \langle a\rangle \to Q$, $(b^x, a^y)\psi = j^x i^y$ leképezés szürjektív homomorfizmus, és a magja éppen $\langle (b^{-2}, a^2)\rangle$.

Ezt a konstrukciót általánosabb helyzetben is alkalmazhatjuk.

1.4. Állítás. *Tegyük fel, hogy $N \lhd G$, $H \leqslant G$ és $G = HN$. Ekkor*

$$G \cong H \ltimes N / \{(x^{-1}, x) \,|\, x \in H \cap N\},$$

ahol $\varphi : h \mapsto (n \mapsto n^h)$ a g-ből természetesen adódó homomorfizmus H-ból $AutN$-be.

Bizonyítás: Legyen $S = H \ltimes N$ a fent definiált szemidirekt szorzat, és $\psi : S \to G$ az a leképezés, amelyre $(h, n)\psi = hn$. Ez homomorfizmus: $((h, n)(h', n'))\psi = (hh', n^{h'\varphi} n')\psi = (hh', n^{h'} n')\psi = hh' n^{h'} n' = hnh'n' = (h, n)\psi \cdot (h', n')\psi$; szürjektív a $HN = G$ feltétel miatt; és $(h, n) \in \operatorname{Ker}\psi \iff hn = 1$ G-ben $\iff h = n^{-1} \in H \cap N$.

□

A következő tételben belátjuk, hogy az olyan csoportok, amelyeknek van az indexéhez relatív prím rendű Abel-féle normálosztójuk, felírhatók szemidirekt szorzatként. Ez a speciális esete a 4. fejezetben bizonyítandó Schur–Zassenhaus-tételnek (4.9. Tétel).

1.5. Tétel. *Legyen G véges csoport, és $N \lhd G$ Abel-csoport. Ha $(|G : N|, |N|) = 1$, akkor N-nek van komplementuma , azaz olyan $H \leqslant G$, amelyre $H \cap N = 1$ és $HN = G$. (Így G felírható $G = N \rtimes H$ szemidirekt szorzat alakban.)*

Bizonyítás: Egy $H \leqslant G$ részcsoport akkor és csak akkor komplementuma N-nek, ha az N mellékosztályainak teljes reprezentánsrendszerét alkotja ($H \cap N = 1 \iff$ minden mellékosztályból legföljebb 1 elemet tartalmaz, és $HN = G \iff$ minden mellékosztályból legalább egy elemet tartalmaz). Legyen $Q = G/N$, $|Q| = m$, $|N| = n$, és $G = \dot\cup_{\alpha \in X} x_\alpha N$. Ha az $X = \{x_\alpha \mid \alpha \in Q\}$ reprezentánsrendszer szorzásra zárt, akkor $X \leqslant G$ komplementuma N-nek. Ha nem, akkor keresünk egy másik reprezentánsrendszert: $y_\alpha \in x_\alpha N$, amely szorzásra zárt.

Minden $\alpha, \beta \in Q$-ra $x_\alpha x_\beta = x_{\alpha\beta} \cdot f(\alpha, \beta)$ alkalmas $f(\alpha, \beta) \in N$ elemekkel. Számítsuk ki az $x_\alpha x_\beta x_\gamma$ szorzatot kétféleképpen!

$$(x_\alpha x_\beta) x_\gamma = x_{\alpha\beta} f(\alpha, \beta) x_\gamma = x_{\alpha\beta} x_\gamma f(\alpha, \beta)^{x_\gamma} = x_{\alpha\beta\gamma} f(\alpha\beta, \gamma) f(\alpha, \beta)^{x_\gamma},$$

$$x_\alpha(x_\beta x_\gamma) = x_\alpha x_{\beta\gamma} f(\beta,\gamma) = x_{\alpha\beta\gamma} f(\alpha,\beta\gamma) f(\beta,\gamma).$$

Tehát az $f(\ ,\ )$ függvényre teljesül, hogy

$$f(\alpha\beta,\gamma) f(\alpha,\beta)^{x_\gamma} = f(\alpha,\beta\gamma) f(\beta,\gamma), \text{ minden } \alpha,\beta,\gamma \in Q\text{-ra} \tag{1.1}$$

Legyen

$$g(\beta) = \prod_{\alpha\in Q} f(\alpha,\beta).$$

Szorozzuk össze minden α-ra az 1.1 egyenlőségeket. (Itt használjuk az N kommutativitását.)

$$\prod_{\alpha\in Q} f(\alpha\beta,\gamma) \prod_{\alpha\in Q} f(\alpha,\beta)^{x_\gamma} = \prod_{\alpha\in Q} f(\alpha,\beta\gamma) f(\beta,\gamma)^m$$

$$g(\gamma) g(\beta)^{x_\gamma} = g(\beta\gamma) f(\beta,\gamma)^m, \text{ vagy átrendezve}$$

$$g(\beta\gamma) = g(\beta)^{x_\gamma} g(\gamma) f(\beta,\gamma)^{-m} \tag{1.2}$$

Mivel $(m,n) = 1$, van olyan m' egész szám, amelyre $-mm' \equiv 1 \bmod n$, így bármely $z \in N$ normálosztóbeli elemre $z^{-mm'} = z$.
Legyen $h(\alpha) = g(\alpha)^{m'}$, és $y_\alpha = x_\alpha h(\alpha)\ \forall \alpha \in Q$. Az 1.2 egyenlőséget m'-edik hatványra emelve:

$$h(\beta\gamma) = h(\beta)^{x_\gamma} h(\gamma) f(\beta,\gamma), \text{ amiből} \tag{1.3}$$

$$y_\beta y_\gamma = x_\beta h(\beta) x_\gamma h(\gamma) = x_\beta x_\gamma h(\beta)^{x_\gamma} h(\gamma) = x_{\beta\gamma} f(\beta,\gamma) h(\beta)^{x_\gamma} h(\gamma) = x_{\beta\gamma} h(\beta\gamma) = y_{\beta\gamma}$$

teljesül minden $\beta,\gamma \in Q$-ra az 1.3 egyenlőség szerint, így az $\{y_\alpha \mid \alpha \in Q\}$ reprezentánsrendszer csoport, és az N normálosztó komplementuma. □

1.3. Ciklikus csoportok automorfizmuscsoportja

A szemidirekt szorzatok megkonstruálásának alapfeltétele a csoportok automorfizmuscsoportjának ismerete. Ez sok esetben elég bonyolult, de segít, ha a csoport felbomlik relatív prím rendű kisebb csoportok direkt szorzatára.

1.6. Állítás. *Ha* $G = G_1 \times \cdots \times G_r$, *és* $(|G_i|, |G_j|) = 1$, *akkor* $\operatorname{Aut} G = \operatorname{Aut} G_1 \times \cdots \times \operatorname{Aut} G_r$.

Bizonyítás: A $(|G_i|, |G_j|) = 1$ feltétel miatt G elemei közül pontosan azok vannak G_i-ben, amelyeknek a rendje osztója $|G_i|$-nek, ugyanis egy $g = g_1 g_2 \cdots g_r$ ($g_i \in G_i$) elem rendje a G direkt szorzatban a g_i elemek rendjének legkisebb közös többszöröse. Másrészt az automorfizmusok megőrzik az elemek rendjét, így minden $\varphi \in \operatorname{Aut} G$-re $G_i\varphi = G_i$.

Legyen $\psi : \operatorname{Aut} G \to \operatorname{Aut} G_1 \times \cdots \times \operatorname{Aut} G_r$ az a leképzés, amely minden $\varphi \in \operatorname{Aut} G$ izomorfizmust a $(\varphi|_{G_1}, \ldots, \varphi|_{G_r})$ elembe képez. Ez nyilván szorzattartó, injektív, mert az automorfizmusokat meghatározza a G-t generáló G_i-ken való hatásuk, és szürjektív, mert tetszőleges $\varphi_i \in \operatorname{Aut} G_i$-kre $\varphi : g_1 \cdots g_r \mapsto (g_1)\varphi_1 \cdots (g_r)\varphi_r$, automorfizmus G-n, és a megszorítása G_i-re φ_i. □

Az előző állítás miatt a ciklikus csoportok automorfizmuscsoporjának meghatározásához elég a prímhatványrendű ciklikus csoportokat vizsgálni.

1.7. Lemma. *Ha* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *kanonikus alak, akkor* $C_n \cong C_{p_1^{\alpha_1}} \times \cdots \times C_{p_r^{\alpha_r}}$

Bizonyítás: Ha $a_1, \ldots, a_r$ az egyes komponensek generátorelemei, akkor az $(a_1, \ldots, a_r)$ elem rendje $l.k.k.t.\{o(a_1), \ldots, o(a_r)\} = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = n$. □

1.8. Lemma. $\operatorname{Aut} C_n$ *izomorf* $\mathbb{Z}_n^\times$*-tel, a modulo* n *vett redukált maradékosztályok multiplikatív csoportjával, következésképpen* $\varphi(n)$ *rendű Abel-csoport.*

Bizonyítás: Az $\langle a \rangle \cong C_n$ csoport automorfizmusai a generátorelemet generátorelembe képező hatványozások, azaz amelyek a-t a^k-ba, egy tetszőleges a^m elemet a^{mk}-ba képeznek, ahol $(k, n) = 1$. Ha $\sigma, \tau \in \operatorname{Aut}\langle a \rangle$-ra $\sigma : a \mapsto a^k$ és $\tau : a \mapsto a^\ell$, akkor $\sigma\tau : a \mapsto (a^k)^\ell = a^{k\ell}$, továbbá $\sigma = \tau \iff a^k = a^\ell \iff k \equiv \ell (\bmod n)$, így az $a \mapsto a^k$ által megadott automorfizmushoz k-t rendelő leképezés izomorfizmus $\operatorname{Aut}\langle a \rangle$-ból $\mathbb{Z}_n^\times$-be. □

1.9. Tétel. *Egy test multiplikatív csoportjának bármely véges részcsoportja ciklikus.*

Bizonyítás: Legyen K test, $G \leqslant K^\times$ és $|G| < \infty$. A véges Abel-csoportok alaptétele szerint G felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. Ha a prímek között lenne egyenlő, akkor $C_p \times C_p \lesssim C_{p^{n_1}} \times C_{p^{n_2}} \leqslant G$, de ennek a p^2 rendű részcsoportnak minden eleme gyöke az $x^p - 1$ polinomnak, aminek legfeljebb p gyöke lehet egy testben. Így G ciklikus az 1.7 Lemma alapján. □

1.10. Következmény. $\mathbb{Z}_p^\times \cong C_{p-1}$.

1.11. Tétel. $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *kanonikus alakú természetes számra* $\operatorname{Aut} C_n \cong \prod_{i=1}^{r} \operatorname{Aut} C_{p_i^{\alpha_i}}$, *és*

$$\operatorname{Aut}(C_{p^n}) \cong \begin{cases} C_{(p-1)p^{n-1}}, & \text{ha } p > 2 \text{ prím} \\ C_{2^{n-2}} \times C_2, & \text{ha } p = 2,\ n \geqslant 2 \end{cases}$$

Bizonyítás: A felbontás következik az 1.6. és 1.7. állításokból, ezért az 1.8. lemma szerint csak a $\mathbb{Z}_{p^n}^\times$ csoportokkal kell foglalkoznunk.

1. Először belátjuk, hogy $p > 2$ esetén $\mathbb{Z}_{p^n}^\times$-ben van $p - 1$ rendű elem. Jelölje $o_k(g)$ egy $g \in \mathbb{N}$ szám rendjét modulo k. Az 1.10. következmény miatt van olyan $g \in \mathbb{N}$ szám, amelyre $o_p(g) = p - 1$. Ha $m = o_{p^n}(g)$, akkor $g^m \equiv 1 \pmod{p^n} \implies g^m \equiv 1 \pmod{p} \implies p - 1 | m$, és így $o_{p^n}(g^{m/(p-1)}) = p - 1$.

2. $\mathbb{Z}_{p^n}^\times$-ben van p^{n-1} rendű elem, ha $p > 2$, és van 2^{n-2} rendű elem, ha $p = 2$. Ennek bizonyításához a következő lemmát használjuk.

> **Lemma.** Ha $c \equiv 1 + p^m \pmod{p^{m+1}}$, akkor $c^p \equiv 1 + p^{m+1} \pmod{p^{m+2}}$, feltéve, hogy $p > 2$ és $m \geqslant 1$ vagy $p = 2$ és $m \geqslant 2$.

Bizonyítás: Először vegyük észre, hogy ha $a \equiv b \pmod{p^m}$, akkor $a^p \equiv b^p \pmod{p^{m+1}}$, ugyanis $a \neq b$ esetén $\dfrac{a^p - b^p}{a-b} = a^{p-1} + a^{p-2}b + \ldots + b^{p-1} \equiv pa^{p-1} \pmod{p}$. Másrészt $(1+p^m)^p = 1 + p^{m+1} + \binom{p}{2}p^{2m} + \ldots \equiv 1 + p^{m+1} \pmod{p^{m+2}}$, mert $p > 2$ esetén $p \mid \binom{p}{2}$, $p = 2$ esetén pedig $m \geqslant 2$ miatt $p^{2m} \geqslant m+2$. □

Legyen p páratlan prím, és $c = 1 + p$. Ekkor $c \equiv 1 + p \pmod{p^2}$-re iterálva a lemmát

$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n} \not\equiv 1 \pmod{p^n}$, és

$(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}} \equiv 1 \pmod{p^n}$, tehát $o_{p^n}(1+p) = p^{n-1}$.

A $p = 2$ esetben legyen $c = 5$. Ekkor $c \equiv 1 + 2^2 \pmod{2^3}$-re iterálva a lemmát

$(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n} \not\equiv 1 \pmod{2^n}$, és

$(1+2^2)^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}} \equiv 1 \pmod{2^n}$, tehát $o_{2^n}(5) = 2^{n-2}$, ha $n \geqslant 3$.

3. $p > 2$-re $\mathbb{Z}_{p^n}^\times \gtrsim C_{p-1}$, és $\gtrsim C_{p^{n-1}}$, és ez a két csoport relatív prím rendű, így $\mathbb{Z}_{p^n}^\times \gtrsim C_{p-1} \times C_{p^{n-1}}$, s mivel $\mathbb{Z}_{p^n}^\times$ és $C_{p-1} \times C_{p^{n-1}}$ azonos rendűek, izomorfak is.

4. $p = 2$-re $n \geqslant 3$ esetén $\mathbb{Z}_{2^n}^\times \gtrsim C_{2^{n-2}}$, és $\mathbb{Z}_{2^n}^\times$-ben egynél több másodrendű elem van (nyilvánvaló, hogy $-1, 1+2^{n-1}$ és $-1+2^{n-1}$ is másodrendű), így a 2^{n-1} rendű $\mathbb{Z}_{2^n}^\times$ csoport ciklikusokra való felbontása csak $C_{2^{n-2}} \times C_2$ lehet. Végül $\operatorname{Aut} C_2 = 1$, és $\operatorname{Aut} C_4 \cong C_2$ nyilvánvaló. □

Megjegyzés. A teljesség kedvéért jegyezzük meg, hogy a végtelen ciklikus csoport automorfizmuscsoportja C_2-vel izomorf, mert az $\langle a \rangle \cong C_\infty$ csoportnak csak a és a^{-1} a generátorelemei.

Példa. Izomorfia erejéig hány $C_5 \rtimes C_4$ csoport van?
Legyen $\langle a \rangle \cong C_5$ és $\langle b \rangle \cong C_4$. Mivel $\operatorname{Aut} C_5 \cong C_4$, és C_4-ből C_4-be négy homomorfizmus megy, legfeljebb négy ilyen csoport lehet. Legyen $G_k = \langle a \rangle \rtimes \langle b \rangle$ az $a^b = a^k$ hatással, ahol $k = 1, 2, 3, 4$. Ha $a^b = a^2$, akkor $a^{b^{-1}} = a^{b^3} = a^8 = a^3$, tehát az $a \mapsto a,\ b \mapsto b^{-1}$ leképezés izomorfizmust indukál G_2-ből G_3-ba. Viszont G_1, G_2 és G_4 közül semelyik kettő nem izomorf: könnyen ellenőrizhető például, hogy $|Z(G_1)| = 20$, $|Z(G_2)| = 1$, és $|Z(G_4)| = 2$.

2. Permutációcsoportok

Az S_Ω *szimmetrikus csoport* az Ω halmaz permutációinak csoportja a kompozícióra mint szorzásra nézve. S_n az $\{1, 2, \ldots, n\}$ halmazon ható szimmetrikus csoport (vagy általánosabban egy n elemű halmaz permutációinak csoportja). Az $(\alpha_1\alpha_2\ldots\alpha_r)$ ciklus az $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_r \to \alpha_1$ permutációt jelöli. A permutációkat mindig jobbról hattatjuk, így a szorzatukat is balról jobbra haladva számítjuk ki. A ciklusfelbontás tulajdonságait (szorzás, elemrend, invertálás, konjugálás), és a szimmetrikus és alternáló csoportról korábban tanult állításokat a függelékben foglaljuk össze.

Definíció. S_Ω részcsoportjait *permutációcsoportoknak* nevezzük. Egy $\varphi : G \to S_\Omega$ homomorfizmus a G csoport *permutációreprezentációja* vagy *csoporthatása* . A csoporthatás *hűséges*, ha $\operatorname{Ker}\varphi = 1$. (Ekkor $G \lesssim S_\Omega$.) A G csoport hatására is többnyire itt is az egyszerűsített $\omega g := \omega(g\varphi)$ jelölést használjuk.

Definíció. Egy $G \to S_\Omega$ csoporthatásra $\omega \in \Omega$ *stabilizátora*

$$G_\omega = \{g \in G \,|\, \omega g = \omega\} \leqslant G.$$

Egy $\omega \in \Omega$ elem *orbitja*

$$\omega G = \{\omega g \,|\, g \in G\} \subseteq \Omega.$$

Egy $g \in G$ elem *fixpontjainak* halmaza

$$Fix(g) = \{\omega \in \Omega \,|\, \omega g = \omega\} \subseteq \Omega.$$

2.1. Állítás. *Az orbitok Ω egy partícióját adják.*

Bizonyítás: Ω nyilván előáll az orbitok uniójaként. Másrészt a metsző orbitok megegyeznek, ugyanis ha $\alpha g = \beta h \in \alpha G \cap \beta G$, akkor $\alpha = \beta h g^{-1} \in \beta G$, így $\alpha G \subseteq \beta G$, és ugyanígy $\beta G \subseteq \alpha G$. □

2.2. Állítás. *A G_ω stabilizátor bármely jobb mellékosztálya az ω-t az orbitjának egy adott elemébe vivő permutációk halmaza.*

Bizonyítás: Az x csoportelem ωh-ba viszi ω-t $\Leftrightarrow \omega x = \omega h \Leftrightarrow \omega x h^{-1} = \omega \Leftrightarrow x h^{-1} \in G_\omega \Leftrightarrow x \in G_\omega h$ □

2.3. Következmény. *$|\omega G| = |G : G_\omega|$, azaz $|G| = |G_\omega| \cdot |\omega G|$*

2.4. Állítás. *$G_{\omega g} = (G_\omega)^g$, tehát ha a csoporthatás tranzitív, akkor minden stabilizátor konjugált egymással, így azonos rendűek is.*

Bizonyítás: $(\omega g)h = \omega g \iff \omega g h g^{-1} = \omega \iff g h g^{-1} \in G_\omega \iff h \in g^{-1} G_\omega g,$ □

2.5. Lemma. ***Burnside-lemma***
Egy véges G csoport véges halmazon való csoporthatásánál a G orbitjainak száma a fixpontok számának átlaga: $\frac{1}{|G|}\sum_{g\in G} Fix(g)$.

Bizonyítás: Legyen $\mathcal{H} := \{(\omega, g) \,|\, \omega \in \Omega,\ g \in G,\ \omega g = \omega\}$, és k az orbitok száma. Ekkor $|\mathcal{H}| = \sum_{\omega\in\Omega} |G_\omega| = \sum_{\omega\in\Omega} \frac{|G|}{|\omega G|} = \sum_{O \text{ orbit}} \frac{|G|}{|O|}|O| = |G| \cdot k$, másrészt $|\mathcal{H}| = \sum_{g\in G} |Fix(g)|$. □

Definíció. Egy csoporthatás tranzitív, ha egyetlen orbitja van.

Példa. Néhány fontos csoporthatás:

	jobbról szorzás elemeken	jobbról szorzás mellékosztályokon	konjugálás elemeken	konjugálás részcsoportokon
Ω	G	$\{Hx \mid x \in G\}$	G	$\{H \mid H \leqslant G\}$
g hatása	$x \mapsto xg$	$Hx \mapsto Hxg$	$x \mapsto x^g$	$H \mapsto H^g$
tranzitív	igen	igen	nem	nem
orbitok	G	$\{Hx \mid x \in G\}$	$\mathcal{K}(g)$	$\{H^g \mid g \in G\}$
1 elemű orbit	nincs	nincs	$Z(G)$ elemei	normálosztók
stabilizátor	1	H^x	$C_G(x)$	$N_G(H)$
orbit mérete	$\lvert G\rvert$	$\lvert G : H\rvert$	$\lvert\mathcal{K}(g)\rvert$	$\lvert G : N_G(H)\rvert$
mag	1	$\bigcap_{x\in G} H^x$	$Z(G)$	$\bigcap_{H\leqslant G} N_G(H)$

2.6. Következmény.

(1) Egy G-beli x elem konjugáltosztályának, $\mathcal{K}(x) = x^G$-nek az elemszáma $|\mathcal{K}(x)| = |G : C_G(x)|$.

(2) Mivel G tranzitív a p-Sylow-részcsoportokon a konjugálással, $|Syl_p(G)| = |G : N_G(P)|$, ahol $P \in Syl_p(G)$.

Definíció. A G csoport két csoporthatása, $\varphi : G \to S_\Omega$ és $\psi : G \to S_{\Omega'}$ *ekvivalens*, ha van olyan $b : \Omega \to \Omega'$ bijekció, hogy

$$(\omega(g\varphi))b = (\omega b)(g\psi) \ \forall g \in G, \ \omega \in \Omega.$$

Általánosabban, két csoporthatás, $\varphi : \ G \to S_\Omega$ és $\psi : \ H \to S_{\Omega'}$ *ekvivalens*, ha van olyan $\sigma : \ G \to H$ izomorfizmus és $b : \ \Omega \to \Omega'$ bijekció, hogy

$$(\omega(g\varphi))b = (\omega)(g\sigma\psi) \ \forall g \in G, \ \omega \in \Omega.$$

2.7. Tétel. *Egy G csoport minden tranzitív csoporthatása ekvivalens egy olyan csoporthatással, amely G valamely H részcsoportjának a mellékosztályain hat a jobbszorzással.*

Bizonyítás: Legyen Ω a csoporthatás alaphalmaza, és α az Ω egy tetszőleges eleme. Legyen H az α stabilizátora G-ben, és Ω' álljon a H jobb oldali mellékosztályaiból. Ekkor a 2.2. Állítás miatt a $b : Hx \mapsto \alpha x$ leképezés bijekció Ω'-ből Ω-ba, és tetszőleges $g \in G$-re $(Hx)b = \alpha(xg) = (\alpha x)g = ((Hx)b)g$, így az eredetileg megadott csoporthatás ekvivalens a H mellékosztályain vett csoporthatással. □

Még egy egyszerű alkalmazást mutatunk a tanult csoporthatások egyikére, az elemeken való jobbszorzással ható Cayley-reprezentációra.

2.8. Tétel. *Ha G véges, $|G| > 2$ és páros, továbbá G 2-Sylowja ciklikus, akkor G nem egyszerű.*

Bizonyítás: Tegyük fel, hogy G egyszerű, $\langle a\rangle \in Syl_2(G)$, $o(a) = 2^k$, és $|G| = 2^k m$, ahol $2 \nmid m$. Legyen $\varphi : G \to S_G$ a jobbszorzással való hatás G elemein. Láttuk, hogy ez a csoporthatás hűséges, sőt mindegyik stabilizátora triviális, vagyis a nemtriviális elemek hatása fixpontmentes. Ebből következik, hogy $o(a\varphi) = 2^k$, és $a\varphi$ minden 2^k-nál kisebb kitevős hatványa is fixpontmentes, így $a\varphi$ ciklusfelbontása csak 2^k hosszú ciklusokat tartalmaz. Mivel a csoporthatás alaphalmaza $2^k m$ elemű, $a\varphi$ pontosan m darab, tehát páratlan sok 2^k hosszú diszjunkt ciklus szorzata, így páratlan permutáció, vagyis nincs benne az alternáló csoportban, A_G-ben. Tehát $\operatorname{Im}\varphi \not\leqslant A_G$, következésképpen $A_G \cap \operatorname{Im}\varphi$ valódi normálosztója $\operatorname{Im}\varphi$-nek. Mivel $\operatorname{Im}\varphi \cong G$ egyszerű, ebből $A_G \cap \operatorname{Im}\varphi = 1$ következik, így $|G| = |\operatorname{Im}\varphi| \leqslant |S_G : A_G| = 2$, ami ellentmond a tétel feltételeinek. □

Feladat. Csoporthatások segítségével bizonyítsuk be a Sylow-tételeket a következő útmutatások alapján!

(1) Legyen $|G| = p^a m$, ahol a p prím nem osztója m-nek, és hattassuk G-t a jobbszorzással a $\binom{p^a m}{p^a}$ darab p^a elemű részhalmazon. Mutassuk meg, hogy ekkor minden orbit

(a) vagy egyrétegűen fedi le G-t, m elemű, és pontosan egy részcsoport van az orbit elemei között,

(b) vagy átfedéssel fedi le G-t, p-vel osztható elemszámú, és nincs benne részcsoport.

Így $\binom{p^a m}{p^a} \equiv |Syl_p(G)| \cdot m \pmod p$.

(2) Bizonyítsuk be, hogy $\binom{p^a m}{p^a} \equiv m \pmod p$ (alkalmazzuk az előző feladatot a $p^a m$ rendű ciklikus csoportra), és lássuk be ebből, hogy $|Syl_p(G)| \equiv 1 \pmod p$.

(3) Tekintsük G hatását $Syl_p(G)$-n a konjugálással. Lássuk be, hogy

(a) egy Q p-részcsoport akkor és csak akkor hagy helyben egy P p-Sylowot, ha $Q \leqslant P$;

(b) minden p-részcsoport beágyazható egy p-Sylowba;

(c) G tranzitívan hat $Syl_p(G)$-n.

A fejezet további részében a szimmetrikus és az alternáló csoport szerkezetét és automorfizmusait vizsgáljuk.

2.9. Állítás. *$Z(S_n) = 1$, ha $n \geqslant 3$, és $Z(A_n) = 1$, sőt $C_{S_n}(A_n) = 1$, ha $n \geqslant 4$.*

Bizonyítás: Legyen $1 \neq g \in S_n$. Ekkor $g : \alpha \mapsto \beta$ valamely $\alpha \neq \beta$-ra. Ha γ egy α-tól és β-tól különböző elem az alaphalmazban, akkor $x = (\beta\gamma)$-ra $g^x : \alpha \mapsto \gamma$, így $g^x \neq g$, vagyis g nem cserélhető fel minden S_n-beli elemmel, tehát $g \notin Z(S_n)$.

A második állítás bizonyításához A_n-beli x-et kell találnunk. Legyen $x = (\beta\gamma\delta)$, ahol γ, δ egymástól és az α, β elemektől is különböznek. Ekkor $g^x : \alpha \mapsto \gamma$, tehát $g^x \neq g$, és így $g \notin C_{S_n}(A_n)$. Ebből következik, hogy $Z(A_n) \leqslant C_{S_n}(A_n) = 1$. □

2.10. Tétel. *A_n egyszerű, ha $n \neq 4$. A_4-nek az 1-en és A_4-en kívül csak egy normálosztója van: a másodrendű elemek által generált Klein-csoport, $V \cong C_2 \times C_2$.*

Bizonyítás: $n \leqslant 3$ esetén az állítás nyilvánvaló. Legyen $n \geqslant 5$, és tegyük fel, hogy $1 \neq N \lhd A_n$. Belátjuk, hogy ekkor $N = A_n$. Minthogy A_n-et generálják a 3-ciklusok, és $n \geqslant 5$ esetén ezek mind konjugáltak egymással, elég megmutatni, hogy N tartalmaz 3-ciklust. Legyen $1 \neq g \in N$.

1. Ha g ciklusfelbontásában van k-ciklus valamely $k \geqslant 4$-re: $g = (a_1a_2a_3a_4\ldots)x$, ahol $x \in S_n$ elem jelöli a g-ben $(a_1a_2a_3a_4\ldots)$ ciklustól diszjunkt ciklusok szorzatát, akkor $h = (a_1a_2a_3)$-ra $g^{-1}g^h = (a_1a_2a_3a_4\ldots)^{-1}x^{-1}(a_2a_3a_1a_4\ldots)x = (a_1a_2a_4) \in N$.

2. Ha g-ben nincs 3-nál hosszabb ciklus, és csak egy 3-ciklus van benne, akkor g^2 3-ciklus.

3. Ha g-ben van két 3-ciklus: $g = (a_1a_2a_3)(b_1b_2b_3)\ldots$, akkor $h = (a_1a_2b_1)$-re $g^{-1}g^h = (a_1a_2b_2a_3b_1) \in N$, tehát az 1. eset feltétele teljesül erre az elemre.

4. Ha g-ben csak 2-ciklusok vannak, akkor ezekből legalább kettő van: $g = (a_1a_2)(b_1b_2)\cdots$. $n \geqslant 5$ miatt van a_1, a_2, b_1, b_2-től különböző c elem. Ekkor $h = (a_1b_1c)$-re $g^{-1}g^h$-ban van egy $(a_1b_1c...)$ ciklus, így a korábbi esetek valamelyike teljesül $g^{-1}g^h$-ra.

Végül $n = 4$ esetén a másodrendű elemek konjugáltak, ezért ha egy benne van N-ben, akkor $V \leqslant N \leqslant A_4$, és $|A_4 : V| = 3$ miatt $N = V$ vagy A_4. Ha viszont $1 \neq N$ páratlan rendű, akkor csak harmadrendű lehet, de a harmadrendű részcsoportok nem normálosztók A_4-ben. □

2.11. Állítás. *S_n normálosztói 1, A_n, S_n, ha $n \neq 4$, és S_4 normálosztói 1, V, A_4 és S_4.*

Bizonyítás: $n \leqslant 3$-ra nyilván igaz az állítás. Tegyük fel, hogy $n \geqslant 4$, és $N \lhd S_n$. Ha $A_n \leqslant N$, akkor $N = A_n$ vagy S_n.
Ha $A_n \not\leqslant N$, akkor $A_n \cap N \neq A_n$ normálosztó A_n-ben, így $A_n \cap N = 1$ vagy (az $n = 4$ esetben) $A_n \cap N = V$. Ha $A_n \cap N = 1$, akkor $A_nN = A_n \times N$, így $N \leqslant C_{S_n}(A_n) \leqslant 1$ a 2.9. Állítás szerint. Ha $n = 4$, és $A_4 \cap N = V$, akkor $N/V \lhd S_4/V \cong S_3$, amelynek az előzőek alapján csak három normálosztója van, így ekkor N csak V, A_4 vagy S_4 lehet. □

2.12. Tétel. ***Kis indexű részcsoportok***
Legyen $n \geqslant 5$.

(1) Ha $H \leqslant S_n$, $|S_n : H| < n$, akkor $H = A_n$ vagy $H = S_n$.

(2) Ha $H \leqslant A_n$, $|A_n : H| < n$, akkor $H = A_n$.

Bizonyítás: (1): Tegyük fel, hogy $|S_n : H| = k < n$. Ekkor létezik egy $\varphi : S_n \to S_k$ csoporthatás a H mellékosztályain, amely nem hűséges, mert $n! > k!$.
A 2.11. Állítás alapján $A_n \leqslant \operatorname{Ker}\varphi$, és a mellékosztályokon való csoporthatás tulajdonságaiból tudjuk, hogy $\operatorname{Ker}\varphi = \bigcap_{x\in G} H^x \leqslant H$, ezért $H = A_n$ vagy S_n.
(2): Legyen $|A_n : H| = k < n$. Ekkor létezik egy $\varphi : A_n \to S_k$ csoporthatás a H mellékosztályain. Ha $n > 2$, akkor $\frac{n!}{2} > k!$, így $\operatorname{Ker}\varphi \neq 1$. Az 2.11 Állítás miatt $\operatorname{Ker}\varphi = A_n$, és $\operatorname{Ker}\varphi \leqslant H$, tehát $H = A_n$. □

Példa. S_4-ben van 3 indexű részcsoport: a 2-Sylowok ilyenek.

2.13. Tétel. *Ha $n \geqslant 3$ és $n \neq 6$, akkor $\operatorname{Aut} S_n = \operatorname{Inn} S_n \cong S_n$.*

Bizonyítás: A 2.9. Állítás szerint $Z(S_n) = 1$, így $\operatorname{Aut} S_n \geqslant \operatorname{Inn} S_n \cong S_n/Z(S_n) = S_n$. Az $n = 3$ és $n = 4$ esetben egyszerű becsléssel láthatjuk, hogy az automorfizmuscsoportnak nem lehet 6-nál, illetve 24-nél több eleme. Vegyük S_3-nak az $\{(12), (123)\}$ generátorrendszerét, S_4-ben pedig az $\{(1234), (1243)\}$ generátorrendszert. Az adott rendű elemek számából láthatjuk, hogy ezeknek a képe legfeljebb $3 \cdot 2 = 6$-féle, illetve $6 \cdot 4 = 24$-féle lehet (a másik negyedrendű elempár sem lehet egymás inverze, ezért a második választására nem 5, csak 4 lehetőségünk van), és ezek képe már meghatározza az automorfizmust.

Legyen most $n \geqslant 5$. Az automorfizmusok megtartják az elemrendet, és konjugáltosztályt konjugáltosztályba képeznek, tehát a másodrendű elemek konjugáltosztályait (azaz az adott ciklusfelbontású másodrendű elemek osztályait) is egymás között permutálják. Szeretnénk belátni, hogy a transzpozíciók osztálya önmagába megy minden automorfizmusnál. Hasonlítsuk össze a másodrendű elemek konjugáltosztályainak méretét!

$$|\mathcal{K}_1| = |\mathcal{K}((12))| = \binom{n}{2}, \text{ és}$$

$$|\mathcal{K}_k| = |\mathcal{K}((12)(34)\cdots((2k-1)\,2k))| = \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}}{k!}$$

Nézzük meg, hogy lehet-e ez a két konjugáltosztály azonos méretű, ha $k > 1$!

$$\begin{array}{rcl} \frac{n(n-1)}{2} = |\mathcal{K}_1| & = & |\mathcal{K}_k| = \frac{n(n-1)\cdots(n-2k+2)(n-2k+1)}{2^k\cdot k!} \\ & \Updownarrow & \\ 2^{k-1}k! & = & (n-2)\cdots(n-2k+1) \end{array}$$

Könnyen láthatjuk, hogy
$k = 2$-re a $4 = (n-2)(n-3)$ egyenletnek nincs megoldása a pozitív egészek körében,
$k = 3$-ra pedig $24 = (n-2)(n-3)(n-4)(n-5) \iff n = 6$, a kivételes eset.
$k \geqslant 4$-re belátjuk, hogy a bal oldal kisebb a jobb oldalnál. Ezt elég a jobb oldal minimumára, az $n = 2k$ esetre bebizonyítani.

$$\begin{array}{rcl} 2^{k-1}\cdot k! & < & (2k-2)\cdots 1 \\ & \Updownarrow & \\ 2\cdot 4\cdots(2k-2)\cdot k & < & (2k-2)\cdots 1 \\ & \Updownarrow & \\ k & < & 1\cdot 3\cdots(2k-3) \\ & \Uparrow & \\ k & < & 2k-3 \\ & \Updownarrow & \\ k & > & 3 \end{array}$$

Tehát $n \neq 6$ esetén minden automorfizmus önmagába képezi a transzpozíciók $\mathcal{K}_1$ konjugáltosztályát.

Definiáljunk egy gráfot a $\mathcal{K}_1$ alaphalmazon: az (ab) és (cd) transzpozíciókat akkor köti össze él, ha $|\{a,b\} \cap \{c,d\}| = 1$, vagy ami ezzel ekvivalens, ha a szorzatuk rendje 3. Legyen $\sigma \in \operatorname{Aut} S_n$ tetszőleges automorfizmus. Ekkor σ permutálja a gráf csúcsait, s mivel rendtartó, az éleket egymásnak felelteti meg, vagyis automorfizmust ad meg a gráfon is. A gráf $(n-1)$ csúcsú teljes részgráfjai $n \geqslant 5$ esetén éppen a

$$\mathcal{G}_a = \{(a,x)\,|\,x \in \{1,\ldots,n\} \setminus \{a\}\}$$

csúcshalmazok által kifeszített részgráfok, így definiálhatunk egy $g \in S_n$ permutációt úgy, hogy

$$g : a \mapsto a' \iff \sigma : \mathcal{G}_a \to \mathcal{G}_{a'}.$$

Vegyük észre, hogy $a \neq b$-re

$$\{(ab)\} = \mathcal{G}_a \cap \mathcal{G}_b, \text{ tehát } (ab)\sigma = (ag\ bg) = (ab)^g.$$

Vagyis a g-vel való konjugáláshoz tartozó φ_g automorfizmus hatása megegyezik a σ hatásával a transzpozíciókon, s mivel ezek generálják S_n-et, a teljes S_n-en is. Ezzel beláttuk, hogy S_n minden automorfizmusa belső automorfizmus, így $\operatorname{Aut} S_n \cong S_n$. □

Feladat. A következő részfeladatok segítségével bizonyítsuk be, hogy $\operatorname{Aut} S_6 > S_6$.

(1) Tekintsük S_5 hatását a konjugálással az 5-Sylowjain! Bizonyítsuk be, hogy ez S_5-nek olyan beágyazását adja S_6-ba, ahol S_5 képének harmadrendű elemei fixpontmentesek.

(2) Legyen $H, K \leqslant S_n$ úgy, hogy $|S_n : H| = |S_n : K| = n$. Bizonyítsuk be, hogy van olyan $\sigma \in \operatorname{Aut} S_n$, amelyre $H\sigma = K$.

3. Feloldható csoportok

3.1. Kommutátor-részcsoport

Egy csoport két eleme, a és b felcserélhető, ha $ab = ba$, vagy átrendezve az egyenlőséget, $a^{-1}b^{-1}ab = 1$. Ezt az $[a, b] = a^{-1}b^{-1}ab$ elemet az a és b *kommutátorának* hívjuk. Tehát egy csoport pontosan akkor Abel-csoport, ha minden kommutátoreleme 1. Az alább definiált kommutátor-részcsoport azt méri, milyen messze van a G csoport attól, hogy Abel-csoport legyen.

Definíció. A $H, K \subseteq G$ részhalmazok kommutátora $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$. A G csoport *kommutátor-részcsoportja* $G' = [G, G]$.

Megjegyzés. G' elemei nem feltétlenül kommutátorok, csak ilyenek szorzatai. Könnyen látható, hogy $[x, y]^{-1} = [y, x]$, és így $[H, K] = [K, H]$ bármely H, K részhalmazra.

3.1. Állítás. *Legyen $H \leqslant G$. Egy $K \subseteq G$ részhalmaz akkor és csak akkor van $N_G(H)$-ban, ha $[K, H] \leqslant H$.*

Bizonyítás. $[K, H] \leqslant H \iff k^{-1}h^{-1}kh \in H \ \forall k \in K, h \in H \iff k^{-1}h^{-1}k \in Hh^{-1} = H \ \forall k \in K, h \in H \iff K \subseteq N_G(H)$ □

3.2. Következmény. *G egy N részcsoportja pontosan akkor normálosztó, ha $[N, G] \leqslant N$.*

Definíció. Egy $H \leqslant G$ részcsoport *karakterisztikus részcsoportja* G-nek, ha G bármely automorfizmusa helyben hagyja: $\forall \sigma \in Aut(G)$-re $H\sigma = H$. Jelölése $H \operatorname{char} G$.

3.3. Lemma.

(1) Minden karakterisztikus részcsoport normálosztó.

(2) Ha $H \operatorname{char} N \lhd G$, akkor $H \lhd G$.

(3) Ha $H \lhd N \lhd G$, akkor H nem feltétlenül normálosztó G-ben.

(4) Ha $H \operatorname{char} K \operatorname{char} G$, akkor $H \operatorname{char} G$.

Bizonyítás. (1) Egy elemmel való konjugálás automorfizmus.
(2) Tetszőleges $g \in G$-vel való konjugálás automorfizmus G-n, és helyben hagyja N-et, így N-nek is automorfizmusa. Következésképpen helyben hagyja H-t is.
(3) Például $\langle (12) \rangle \lhd V \lhd A_4$, de $\langle (12) \rangle \not\lhd A_4$.
(4) $\sigma \in \operatorname{Aut} G \implies K\sigma = K \implies \sigma|_K \in \operatorname{Aut} K \implies H\sigma = H\sigma|_K = H$. □

3.4. Állítás.

(1) $G' \lhd G$, sőt G' karakterisztikus részcsoport G-ben.

(2) G/G' Abel csoport.

(3) G' a legkisebb olyan normálosztó, amellyel vett faktor Abel-csoport.

Bizonyítás. (1): Tetszőleges $\sigma \in Aut(G)$-re G' generátorainak a képe benne van G'-ben:
$[x, y]\sigma = (x^{-1}y^{-1}xy)\sigma = (x\sigma)^{-1}(y\sigma)^{-1}x\sigma y\sigma = [x\sigma, y\sigma] \in G'$. Tehát $G' \operatorname{char} G$, és a 3.3/1. Lemma miatt ebből $G' \lhd G$ is következik.
(2) és (3) helyett a következő erősebb állítást bizonyítjuk:
(3') Egy $H \leqslant G$ részcsoport pontosan akkor tartalmazza G'-t, ha $H \lhd G$, és G/H Abel-csoport.
$G' \leqslant H \implies [H, G] \leqslant [G, G] \leqslant H \implies H \lhd G$, ezért mindkét irány bizonyításánál feltehetjük, hogy $H \lhd G$, és így G/H értelmezve van.
$G' \leqslant H \iff \forall x, y \in G$-re $[x, y] \in H \iff \forall xH, yH \in G/H$-ra $[xH, yH] = [x, y]H = H \iff G/H$ Abel-csoport.

□

Példa. Számítsuk ki S_4 kommutátor-részcsoportját!
Tudjuk, hogy S_4 normálosztói $1 < V < A_4 < S_4$, az ezekkel vett faktorok pedig $S_4/1 \cong S_4$ nem Abel; $S_4/V \cong S_3$ nem Abel; $S_4/A_4 \cong C_3$ Abel. Tehát $S_4' = A_4$.

Példa. Legyen G nem Abel, p^3-rendű csoport. Bizonyítsuk be, hogy ekkor $Z(G) = G'$ p-edrendű csoport!

Tudjuk, hogy prímhatvány rendű csoport centruma nem lehet triviális, így $|G : Z(G)| \,|\, p^2$. Másrészt $G/Z(G)$ nem lehet 1- vagy p-elemű, mert ha $G/Z(G)$ ciklikus, akkor $G/Z(G) = \langle aZ(G)\rangle \implies G = \langle Z(G), a\rangle$ generátorelemei felcserélhetők egymással, tehát G Abel-csoport lenne. Ezért $|G/Z(G)| = p^2$, amiből következik az is, hogy $G/Z(G)$ Abel-csoport, így $G' \leqslant Z(G)$. Viszont G' sem lehet 1, ha G nem Abel, ezért $G' = Z(G)$ p-edrendű részcsoport.

3.5. Állítás.

(1) Ha $H \leqslant G$, akkor $H' \leqslant G'$.

(2) Ha $\varphi : G \to H$ szürjektív, akkor $G'\varphi = H'$.

(3) $(G_1 \times G_2)' = G_1' \times G_2'$

Bizonyítás: (1) közvetlenül adódik a definícióból.
(2): $G'\varphi \leqslant H'$ nyilván teljesül: $\forall x, y \in G$-re $[x, y]\varphi = [x\varphi, y\varphi] \in H'$. Másrészt a φ szürjektivitása miatt minden $u, v \in H$-nak van $x, y \in G$ ősképe, így $[u, v] = [x\varphi, y\varphi] = [x, y]\varphi \in G'\varphi$, tehát $H' \leqslant G'\varphi$.
(3): Az (1) állítás miatt $G_1', G_2' \leqslant (G_1 \times G_2)'$, így $\langle G_1', G_2'\rangle = G_1' \times G_2' \leqslant (G_1 \times G_2)'$. Másrészt a (2) állítást alkalmazva a $\pi_i : G_1 \times G_2 \to G_i$, $(g_1, g_2) \mapsto g_i$ homomorfizmusokra azt kapjuk, hogy $(G_1 \times G_2)'\pi_i = G_i'$ $(i = 1, 2)$, így $(G_1 \times G_2)' \leqslant G_1' \times G_2'$. □

3.2. Feloldható csoportok

Definíció. Egy G csoport *kommutátorlánca*

$$G \rhd G' \rhd G'' \rhd \cdots \rhd G^{(i)} \rhd \ldots,$$

ahol $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

3.6. Állítás. *A kommutátorlánc tulajdonságai:*

(1) $G^{(i)} \lhd G$ minden i-re, sőt $G^{(i)}$ char G

(2) $G^{(i)}/G^{(i+1)}$ Abel-csoport.

Bizonyítás. Az (1) állítás i-re vonatkozó indukcióval következik abból, hogy a kommutátor-részcsoport karakterisztikus: $G^{(i+1)}$ char $G^{(i)}$ char $G \implies G^{(i+1)}$ char G a 3.3/4. Állítás szerint.
A (2) pedig a $G^{(i+1)}$ definíciójából közvetlenül adódik. □

Definíció. *Normálláncnak* nevezzük részcsoportoknak egy $G = N_0 \rhd N_1 \rhd \cdots \rhd N_k = 1$ sorozatát.

Definíció. G csoport *feloldható*, ha létezik olyan normállánca, amelynek minden faktora kommutatív: N_i/N_{i+1} Abel-csoport $i = 0, \ldots, k-1$-re.

Példa. Az Abel-csoportok nyilván feloldhatók.
A D_n diédercsoport nem Abel, de feloldható: az $1 \lhd \langle f\rangle \lhd D_n$ normállánc mindegyik faktora ciklikus, tehát kommutatív.

3.7. Állítás. *Ha $G = N_0 \rhd N_1 \rhd \cdots \rhd N_k = 1$ normállánc Abel faktorokkal, akkor $N_i \geqslant G^{(i)}$ minden i-re. Következésképpen G akkor és csak akkor feloldható, ha a kommutátorlánca leér az 1-ig, és az összes Abel faktorú normállánc közül a kommutátorlánc a legrövidebb.*

Bizonyítás. Teljes indukcióval bizonyítjuk, hogy $N_i \geqslant G^{(i)}$. $N_0 = G = G^{(0)}$, és ha valamely i-re $N_i \geqslant G^{(i)}$, akkor N_i/N_{i+1} kommutativitása miatt

$$N_{i+1} \geqslant N_i' \geqslant (G^{(i)})' = G^{(i+1)}.$$

Tehát ha van k hosszúságú kommutatív faktorú normállánc, akkor $G^{(k)} = 1$, és fordítva, ha a kommutátorlánc leér, akkor az is kommutatív faktorú normállánc, tehát a csoport feloldható. □

Definíció. G *feloldhatósági hossza* k, ha $G^{(k)} = 1$, de $G^{(k-1)} \neq 1$.

Definíció. Egy P Abel-csoport *elemi Abel p-csoport*, ha minden elemének a rendje p vagy 1.

Megjegyzés. Egy P (nem feltétlenül véges) csoport akkor és csak akkor elemi Abel p-csoport, ha C_p-k diszkrét direkt szorzata, ugyanis ekkor P vektortér a p elemű test fölött (ahol az összeadás helyett szorzás, a skalárral való szorzás helyett hatványozás a művelet), és ennek egy bázisa adja a ciklikus faktorok generátorelemeit.

3.8. Állítás. *Ha G véges feloldható csoport, akkor létezik olyan normálosztókból álló normállánca, melynek minden faktora Abel p-csoport, sőt elemi Abel p-csoport.*

Bizonyítás. Finomítsuk a kommutátorláncot, amíg lehet úgy, hogy a tagjai továbbra is normálosztók legyenek (a faktorai Abel-csoportok szeletei, tehát szintén kommutatívak):

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_k = 1.$$

Ekkor minden faktorcsoport *karakterisztikusan egyszerű*, azaz nincs 1-től és az egésztől különböző karakterisztikus részcsoportja, ugyanis $H/N_{i+1} \operatorname{char} N_i/N_{i+1} \lhd G/N_{i+1} \implies H/N_{i+1} \lhd G/N_{i+1} \implies H \lhd G$, tehát $H/N_{i+1} \neq 1, N_i/N_{i+1}$ esetén a normálláncot tovább tudnánk finomítani.

Legyen $\overline{N} = N_i/N_{i+1}.$, és $p \,|\, |\overline{N}|$. Mivel $\overline{N}$ Abel-csoport, a p-edrendű elemek az 1-gyel együtt részcsoportot, sőt karakterisztikus részcsoportot alkotnak, így $\overline{N}$ minden $\neq 1$ eleme p-edrendű, vagyis $\overline{N}$ elemi Abel p-csoport. □

3.9. Állítás.

(1) Ha G feloldható és $H \leqslant G$, akkor H feloldható.

(2) Ha $N \lhd G$ és G feloldható, akkor G/N is feloldható.

(3) Ha $N \lhd G$ olyan, hogy N és G/N is feloldható, akkor G is feloldható.

Bizonyítás. (1): A 3.5. Állítás többszöri alkalmazásával azt kapjuk, hogy $H^{(i)} \leqslant G^{(i)}\ \forall i$, ezért $G^{(k)} = 1$ esetén $H^{(k)} = 1$.
(2): Legyen $\varphi : G \to G/N$ a természetes szürjektív homomorfizmus. Ekkor a 3.5/2. Állítás alapján $G'\varphi = (G\varphi)'$, ezért $G^{(i)}\varphi = (G\varphi)^{(i)} = (G/N)^{(i)}$ minden i-re. Így ha $G^{(k)} = 1$, akkor $(G/N)^{(k)} = 1$.
(3): N-nek egy Abel faktorú normállánca és G/N egy Abel faktorú normállánca tagjainak ősképei összerakhatók G-nek egy N-en keresztül menő normálláncává, ahol a faktorok az N-beli, illetve G/N-beli kommutatív faktorokkkal izomorfak, így G is feloldható, és feloldhatósági hossza legfeljebb a két feloldhatósági hossz összege. □

Példa. A szimmetrikus csoportok közül S_1, S_2, S_3, S_4 feloldhatók: S_1 és S_2 Abel-csoport, S_3-nak $S_3 \rhd A_3 \rhd 1$, S_4-nek $S_4 \rhd A_4 \rhd V \rhd 1$ a kommutátorlánca. $n \geqslant 5$-re viszont A_n egyszerű, nem kommutatív csoport, így $A_n' = A_n$ miatt A_n nem feloldható, és ezért az ezt tartalmazó S_n csoport sem lehet feloldható. (S_n kommutátorlánca $S_n \rhd A_n \rhd A_n \rhd A_n \cdots$)

3.10. Tétel. *Minden prímhatványrendű csoport feloldható.*

Bizonyítás. Legyen $|G| = p^n$, ahol p prím. Az n kitevőre vonatkozó teljes indukcióval bizonyítjuk az állítást. $n = 1$-re $G \cong C_p$ Abel, így feloldható. Egy G prímhatványrendű csoport centruma nem triviális: $1 \neq Z(G) \lhd G$. $Z(G)$ feloldható, mert Abel, $G/Z(G)$ pedig az indukciós feltevés szerint feloldható, így a 3.9/3. Állítás értelmében G is feloldható. □

3.11. Tétel. ***Burnside-tétel***
Ha $|G| = p^\alpha q^\beta$, ahol p, q prímek, akkor G feloldható.

Bizonyítás. Erre a bizonyításra a reprezentációelméleti fejezetben kerül sor. □

3.3. Hall-részcsoportok

Legyen $\mathcal{P}$ a pozitív prímek halmaza. $\pi \subseteq \mathcal{P}$ részhalmazra $\pi' = \mathcal{P} \setminus \pi$. n-et π-számnak nevezzük, ha n minden prímosztója π-ben van. Egy véges G csoport π-csoport, ha $|G|$ π-szám.

Definíció. $H \leqslant G$ *π-Hall-részcsoport*, ha $|H|$ π-szám és $|G:H|$ π'-szám. Jelölés: $H \in Hall_\pi(G)$.
Másképpen, ha $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\pi \cap \{p_1, \dots, p_r\} = \{p_{i_1}, \dots, p_{i_k}\}$ és $H \in Hall_\pi(G)$, akkor $|H| = p_{i_1}^{\alpha_{i_1}} \dots p_{i_k}^{\alpha_{i_k}}$.
Ha $\pi = \{p\}$, akkor a $Hall_\pi(G) = Hall_p(G)$, $Hall_{\pi'}(G) = Hall_{p'}(G)$ jelöléseket is használjuk. Ebben az esetben $Hall_p(G) = Syl_p(G)$.

Megjegyzés. Ha $H \leqslant G$ és $(|H|, |G:H|) = 1$, akkor H π-Hall részcsoport, valamilyen $\pi \subseteq \mathcal{P}$-re.

Példa. S_4-ben minden π-hez létezik π-Hall részcsoport: ha $2, 3 \notin \pi$, akkor az 1; ha π a $2, 3$ közül pontosan egyet tartalmaz, akkor a megfelelő Sylow részcsoport; ha $2, 3 \in \pi$, akkor S_4 lesz π-Hall részcsoport.

Példa. S_5-ben nem létezik $2'$-Hall-részcsoport:
Ha $H \in Hall_{2'}(S_5)$, akkor $|H| = 15$, mivel $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$. Az egyetlen 15-ödrendű csoport a C_{15}, mert egy 15-ödrendű csoportnak mindkét Sylowja ciklikus és normálosztó. Ekkor viszont S_5-ben léteznie kellene 15-ödrendű elemnek. De annak a ciklusfelbontásában vagy van 15-ciklus, vagy van diszjunkt 3 és 5 hosszúságú ciklus, és S_5-ben egyik eset sem fordulhat elő.

3.12. Állítás. *Ha $H, K \leqslant G$, akkor $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$, ahol a HK komplexusszorzat nem feltétlenül részcsoport.*

Bizonyítás. $HK = \{hk \mid h \in H, k \in K\}$, és ebben $hk = h'k' \iff (h')^{-1}h = k'k^{-1} = x \in H \cap K \iff (h', k') = (hx^{-1}, xk)$,azaz a $H \times K$ Descartes szorzatban pontosan $H \cap K$ darab elempár adja ugyanazt a hk szorzatot. Így $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$. □

3.13. Állítás. *Ha $H \in Hall_\pi(G)$ és $N \lhd G$, akkor $H \cap N \in Hall_\pi(N)$ és $HN/N \in Hall_\pi(G/N)$.*

Bizonyítás. $|N \cap H| \mid |H|$, tehát π-szám, másrészt a 3.12. Állítás alapján $\frac{|N|}{|H\cap N|} = \frac{|HN|}{|H|}$, ami osztója a $\frac{|G|}{|H|}$ π'-számnak ($HN \leqslant G$), így $H \cap N \in Hall_\pi(N)$.
A faktorcsoportban pedig $|HN/N| = |H/(H\cap N)|$ osztója a $|H|$ π-számnak, és $|G/N : HN/N| = |G:HN|$ osztója a $|G:H|$ π'-számnak ($H \leqslant HN$). Ezért $HN/N \in Hall_\pi(G/N)$ □

Definíció. A $H, K \leqslant G$ részcsoportok *felcserélhetők*, ha $HK = KH$.

3.14. Állítás. *H és K pontosan akkor felcserélhetők, ha $HK = \langle H, K\rangle$*

Bizonyítás. $\Rightarrow$:

$$\langle H, K\rangle = \bigcup_{n=1}^{\infty} (HK)^n \overset{HK=KH}{=} \bigcup_{n=1}^{\infty} H^n K^n = \bigcup_{n=1}^{\infty} HK = HK.$$

$\Leftarrow$: $KH \subseteq \langle H, K\rangle = HK$, és ezt felhasználva, $HK = H^{-1}K^{-1} = (KH)^{-1} \subseteq (HK)^{-1} = K^{-1}H^{-1} = KH$. □

3.15. Állítás. *Ha $H, K \leqslant G$, akkor*

(1) $(|G:H|, |G:K|) = 1 \Rightarrow |G:(H\cap K)| = |G:H|\cdot|G:K|$

(2) $H \cap K = 1 \Rightarrow |HK| = |H|\cdot|K|$. *(Speciálisan $(|H|, |K|) = 1$ esetén is igaz.)*

Bizonyítás. (1): $H \cap K \leqslant H, K$, ezért $|G:H|, |G:K| \mid |G:H\cap K|$, s mivel $|G:H|$ és $|G:K|$ relatív prímek, ebből következik, hogy $|G:K|\cdot|G:H| \mid |G:(H\cap K)|$.
Másrészt $|G:H|\cdot|G:K| = \frac{|G|^2}{|H|\cdot|K|} \geqslant \frac{|HK|}{|H|} \cdot \frac{|G|}{|K|} \overset{3.12.}{=} \frac{|K|}{|H\cap K|} \cdot \frac{|G|}{|K|} = |G:H\cap K|$.
Így $|G:H|\cdot|G:K| = |G:H\cap K|$.
(2) Közvetlen következménye a 3.12. Állításnak. □

Definíció. Legyen $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ kanonikus alak. A $P_1, \dots, P_r$ részcsoportok *Sylow-bázist* alkotnak, ha $P_i \in Syl_{p_i}(G)$ (minden i-re) és bármely $i \neq j$-re P_i és P_j felcserélhető.

3.16. Következmény. *Ha létezik Sylow-bázis, akkor minden π-re létezik π-Hall részcsoport is. A megfelelő Sylow-részcsoportok komplexusszorzata részcsoport lesz a felcserélhetőség miatt, és éppen megfelelő rendű a 3.15/2. Állítás szerint.*

3.17. Állítás. *Ha $\{P_1, \dots, P_r\}$ Sylow-bázis G-ben, és N normálosztó G-ben, akkor*

(1) $\{P_1 \cap N, \dots, P_r \cap N\}$ Sylow-bázis N-ben,

(2) $\{P_1N/N, \dots, P_rN/N\}$ Sylow-bázis G/N-ben.

Bizonyítás. A 3.13. Állításból következik, hogy $P_i \cap N \in Syl_{p_i}(N)$, és $P_iN/N \in Syl_{p_i}(G/N)$ minden i-re. Így csak a felcserélhetőséget kell belátni.
Ha $|N| = p_1^{\beta_1} \cdots p_r^{\beta_r}$, a $\langle P_i, P_j \rangle = P_iP_j$-ben levő $(P_i \cap N)(P_j \cap N)$ részcsoport rendje az $|N|$-et osztó maximális $\{p_i, p_j\}$-szám, tehát osztója $p_i^{\beta_i} p_j^{\beta_j}$-nek. Másrészt $|(P_i \cap N)(P_j \cap N)| = |P_i \cap N| \cdot |P_j \cap N| = p_i^{\beta_i} p_j^{\beta_j}$ a 3.12. Állítás miatt, ezért a $(P_i \cap N)(P_j \cap N) \subseteq \langle (P_i \cap N)(P_j \cap N) \rangle$ tartalmazás egyenlőség, és így $P_i \cap N$ és $P_j \cap N$ felcserélhetők.
A második esetben a felcserélhetőség az ősképek felcserélhetőségéből következik: $(P_iN)(P_jN) = P_iP_jN = P_jP_iN = (P_jN)(P_iN)$. □

3.18. Tétel. *Ha G véges csoport a következő állítások ekvivalensek:*

(1) G feloldható;

(2) G-nek minden π-re létezik π-Hall-részcsoportja;

(3) G-nek minden p prímre létezik p'-Hall-részcsoportja;

(4) G-ben létezik Sylow-bázis.

Bizonyítás. (1) $\Rightarrow$ (2): A G rendjére vonatkozó teljes indukcióval bizonyítjuk. Ha G p-csoport, akkor nyilván teljesül az állítás. Most legyen G tetszőleges véges feloldható csoport. Ekkor a 3.8. Állítás szerint van olyan $1 \neq N \lhd G$, amely Abel p-csoport (N_{k-1} az ottani jelöléssel). Az indukciós feltevés szerint G/N-ben létezik π-Hall részcsoport. Legyen ez H/N.

- Ha $p \in \pi$, akkor H π-csoport és $|G : H| = |G/N : H/N|$ π'-szám. Azaz H π-Hall-részcsoport.
- Ha $p \notin \pi$, akkor $(|N|, |H : N|) = 1$, ezért az 1.5. Tétel szerint létezik $H_1 \leqslant H$, hogy $H = N \rtimes H_1$. Ekkor H_1 π-Hall részcsoport, hiszen $|H_1| = |H/N|$ π-szám és $|G : H_1| = |N| \cdot |G : H|$ π'-szám.

(2) $\Rightarrow$ (3): Nyilvánvaló.
(3) $\Rightarrow$ (4): Legyen $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ és $R_i \in Hall_{p_i'}(G)$, azaz $|G : R_i| = p_i^{\alpha_i}$. Legyen $P_i = \bigcap_{j \neq i} R_j$.
Megmutatjuk, hogy $\{P_i \mid i = 1, \dots, r\}$ Sylow-bázisa G-nek.
Az 3.15/1. Állítást felhasználva indukcióval belátható, hogy

$$|G : \ R_{i_1} \cap \dots \cap R_{i_k}| = p_{i_1}^{\alpha_{i_1}} \cdot \dots \cdot p_{i_k}^{\alpha_{i_k}}, \tag{3.1}$$

ha $i_1, \dots, i_k$ különbözőek. Azaz $|P_i| = p_i^{\alpha_i}$, tehát P_i-k p_i-Sylow részcsoportok. Már csak a felcserélhetőséget kell ellenőrizni: a 3.15. Állítás alapján

$$p_i^{\alpha_i} p_j^{\alpha_j} = |P_iP_j| \leqslant |\langle P_i, P_j \rangle| = |\langle \bigcap_{t \neq i} R_t, \bigcap_{t \neq j} R_t \rangle| \leqslant \Big| \bigcap_{t \neq i,j} R_t \Big| = p_i^{\alpha_i} p_j^{\alpha_j}.$$

Tehát $P_iP_j = \langle P_i, P_j \rangle$, ezért P_i és P_j felcserélhetők.
(4) $\Rightarrow$ (1): Ezt is a csoport rendjére vonatkozó teljes indukcióval bizonyítjuk. Ha G p-csoport, akkor tudjuk, hogy feloldható. Tegyük fel, hogy kisebb csoportokra igaz az állítás, és $\{P_1, \dots, P_r\}$ Sylow-bázisa G-nek.

Elég megmutatni, hogy létezik $1 \neq N$ valódi normálosztó G-ben, mert ekkor ekkor N-ben és G/N-ben is lesz Sylow-bázis a 3.17. Állítás alapján. Az indukciós feltevés szerint ebből következik N és G/N feloldhatósága, és a 3.9/3. Állítás miatt G is feloldható lesz.

Legyen $H = P_1P_2$ (ez csoport a 3.14. Állítás miatt). Ekkor $|H| = p_1^{\alpha_1}p_2^{\alpha_2}$, így a Burnside-tétel (3.11. Tétel) miatt H feloldható, ezért a 3.8. Állítás alapján létezik M normális p-részcsoportja. Az általánosság megszorítása nélkül feltehetjük, hogy M p_1-csoport. Az M normálosztó H minden p_1-Sylowjában benne van (valamelyikben benne van, és ez átkonjugálható bármelyik p_1-Sylowba, miközben az M normálosztó önmagába képződik). Így $M \leqslant P_1$.

Mivel $G = P_1P_2 \cdots P_r$ a Sylow-bázis tulajdonságai alapján, tetszőleges $g \in G$ felírható $g = hg'$ alakban, ahol $h \in H = P_1P_2$, és $g' \in P_3 \cdots P_r$. Ekkor $M^g = M^{hg'} = M^{g'} \leqslant \langle P_1, P_3, \ldots, P_r\rangle = P_1P_3 \ldots P_r < G$, így $N = \langle M^g \mid g \in G\rangle$ valódi normálosztó G-ben. □

3.19. Tétel. ***Hall-tételek.***
Ha G feloldható, akkor

(1) minden $K \leqslant G$ π-részcsoporthoz létezik H π-Hall-részcsoport, amely tartalmazza K-t;

(2) bármely két π-Hall-részcsoport átkonjugálható egymásba;

Bizonyítás. A két állítást összevonva elég a következőt bizonyítani:

(3) Bármely $K \leqslant G$ π-részcsoportra és $H \leqslant G$ π-Hall-részcsoportra létezik $g \in G$, hogy $K \leqslant H^g$.

(Minthogy a 3.18. Tétel szerint G-nek van π-Hall-részcsoportja, (1) & (2) $\iff$ (3).)

Tegyük fel, hogy nem igaz a (3) állítás, és legyen G minimális elemszámú ellenpélda a megfelelő K, H részcsoportokkal.

Mivel G feloldható, a 3.8. Állítás miatt van olyan $N \neq 1$ normálosztója, amely p-csoport. A G minimalitása miatt G/N-re teljesül a (3) állítás.

$|KN/N| = |K/(K \cap N)|$ osztója $|K|$-nak, ami π-szám $\implies$ KN/N π-csoport,

$|HN/N| = |H/(H \cap N)|$ osztója $|H|$-nak, ami π-szám, és

$|G/N : HN/N| = |G : HN|$ osztója $|G : H|$-nek, ami π'-szám, így $HN/N \in Hall_\pi(G/N)$.

Tehát van olyan $g \in G$, amelyre $KN/N \leqslant (HN/N)^g$, és ezt az ősképekre alkalmazva azt kapjuk, hogy $K \leqslant KN \leqslant (HN)^g = H^gN$.

1. N nem lehet π-csoport,
ugyanis akkor $|HN|\,||H| \cdot |N|$ π-szám lenne, de ebben az esetben $H \in Hall_\pi(G)$ miatt $H = HN$, és $K \leqslant (HN)^g = H^g$ ellentmondana G választásának.

2. $HN = G$,
ugyanis különben $H^gN = (HN)^g < G$, és így a H^gN csoport K π-részcsoportjára és H^g π-Hall-részcsoportjára alkalmazhatjuk a (3) állítást, azt kapva, hogy valamely $x \in HN < G$-re $K \leqslant H^{gx}$, ami megint ellentmondás.

3. $K \in Hall_\pi(G)$,
mert ha $|K| < |H|$ lenne, akkor $|KN| = |K|\cdot|N| < |H|\cdot|N| = |G|$ miatt a KN csoport K π-részcsoportjára és $H \cap KN$ π-Hall-részcsoportjára alkalmazhatjuk a (3) Állítást:

$H \cap KN \leqslant H$ π-csoport, és

$|KN : (H \cap KN)| = |HKN : H| = |G : K|$ π'-szám,

tehát $H \cap KN$ valóban π-Hall-részcsoport KN-ben. Ezért van olyan $x \in KN \leqslant G$, amelyre $K \leqslant (H \cap KN)^x \leqslant H^x$, ellentmondás.

4. Belátjuk, hogy van olyan $M < G$ részcsoport, amely tartalmazza K-t és a H egy konjugáltját.
A G/N π-csoport feloldhatósága miatt van olyan $1 \neq L/N$ normálosztó G/N-ben, amely q-részcsoport valamely $q \in \pi$-re. Ekkor $L \lhd G$, és $|L| = p^\alpha q^\beta$, ahol $\alpha, \beta > 0$.
$K, H \in Hall_\pi(G) \implies K \cap L, H \cap L \in Hall_\pi(L)$, és mindkettő $\{p, q\}$-csoport $\implies K \cap L, H \cap L \in Syl_q(L)$ $\implies \exists x \in L$: $K \cap L = (H \cap L)^x = H^x \cap L =: S$. Ez az S csoport nem lehet normálosztó G-ben, mert akkor a bizonyítás első pontját N helyett S-re alkalmazva azt kapnánk, hogy $q \notin \pi$. Viszont S normálosztó K-ban és H^x-ben is (mert az L normálosztó metszi ki belőlük), így $M := N_G(S)$-re $K, H^x \leqslant M < G$.

5. Végül M-re alkalmazhatjuk a (3) állítást a K és H^x π-Hall-részcsoportokkal, és így $K \leqslant H^{xy}$ valamely y-ra, ami ellentmond a G választásának. □

4. Nilpotens csoportok

4.1. Nilpotens csoportok jellemzése

Definíció. Egy $1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$ normálláncot *centrállláncnak* nevezünk, ha minden i-re $N_i \lhd G$ és $N_{i+1}/N_i \leqslant Z(G/N_i)$, vagy a két feltételt összevonva, ha $[N_{i+1}, G] \leqslant N_i$ minden i-re.

Definíció. G csoport *nilpotens*, ha létezik véges centrállánca.

4.1. Következmény. *Ha G nilpotens, akkor feloldható.*

Bizonyítás: Egy centrállánc faktorai kommutatívak, mert $Z(G/N_i)$ Abel-csoport, így N_{i+1}/N_i is az. □

Definíció. *Felső centrállánc*: $1 = Z_0(G) \lhd Z_1(G) \lhd \cdots \lhd Z_k(G) \lhd \ldots$, ahol $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.

Definíció. *Ferde kommutátorlánc*: $G = K_1(G) \rhd K_2(G) \rhd \ldots$ lánc, ahol $K_i(G) = [K_{i-1}(G), G]$.

A centrállánc kétféle definíciójából azonnal látszik, hogy a felső centrállánc és a ferde kommutátorlánc is centrállánc, ha végesek, és elérik a G-t, illetve az 1-et. A következő néhány állításból kiderül, hogy ez a két centrállánc "közrefogja" az összes többit.

4.2. Állítás. *Ha $1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$ centrállánc, akkor $N_i \leqslant Z_i(G)$ minden i-re.*

Bizonyítás: Az állítást indukcióval bizonyítjuk. $i = 0$-ra igaz: $N_0 = 1 = Z_0(G)$.
Ha $N_i \leqslant Z_i(G)$, akkor $[N_{i+1}, G] \leqslant N_i \leqslant Z_i(G)$, tehát $[N_{i+1}/Z_i(G), G/Z_i(G)] = 1$,
azaz $N_{i+1}/Z_i(G) \leqslant Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$, amiből $N_{i+1} \leqslant Z_{i+1}(G)$. □

4.3. Állítás. *Ha $G = N_1 \rhd N_2 \rhd \cdots \rhd N_{k+1} = 1$ centrállánc, akkor $N_i \geqslant K_i(G)$ minden i-re.*

Bizonyítás: Itt a centrállánc tagjainak számozását a könnyebb összehasonlítás kedvéért a ferde kommutátorlánc számozásához igazítottuk, így a centrállánc definíciójában szereplő feltétel is $[N_i, G] \leqslant N_{i+1}$ alakú.
Ezt az állítást is indukcióval bizonyítjuk: $i = 1$-re $N_1 = G = K_1$, és ha $N_i \geqslant K_i(G)$,
akkor $N_{i+1} \geqslant [N_i, G] \geqslant [K_i(G), G] = K_{i+1}(G)$. □

4.4. Következmény. *Ha G nilpotens, akkor a felső centrállánca és a ferde kommutátorlánca is véges, és minden centrállánca ugyanolyan hosszú.*

Bizonyítás: Az 4.2. és 4.3. Állítás következtében a felső centrállánc és a ferde kommutátorlánc is minimális hosszúságú centrállánc, tehát megegyezik a hosszuk, s mivel bármely más centrállánc köztük halad, azok is ugyanolyan hosszúságúak. □

Definíció. *G nilpotenciaosztálya $cl(G)$* egy tetszőleges centrálláncának a hossza.

Példa. Minden Abel-csoport nilpotens, és a nilpotenciaosztálya 1.

4.5. Állítás. *Minden véges p-csoport nilpotens.*

Bizonyítás: Ha $|G| = p^n$, akkor $Z(G) > 1$, azaz $p \,|\, |Z(G)|$, így G felső centrállánca legfeljebb n lépésben felér a G-hez. (Sőt, mint később látni fogjuk, $n \geqslant 2$-re legfeljebb $n - 1$ lépés is elég.) □

Feladat. Legyen $G = \langle a \rangle \rtimes \langle b \rangle \cong C_4 \rtimes C_4$, ahol $a^b = a^{-1}$. Számítsuk ki G felső centrálláncát és ferde kommutátorláncát!
Felső centrállánc: $a^2, b^2 \in Z(G) \implies \langle a^2, b^2 \rangle \leqslant Z(G)$, így $|Z(G)| \in \{4, 8\}$ és $|G : Z(G)| \in \{4, 2\}$. Ha $G/Z(G)$ ciklikus lenne, akkor G Abel-csoport lenne, tehát $|G : Z(G)| = 4$, és $Z(G) = \langle a^2, b^2 \rangle$. Mivel $|G/Z(G)| = 4$, a $G/Z(G) = G/Z_1(G)$ faktorcsoport kommutatív, így $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) = G/Z_1(G)$, és ebből $Z_2(G) = G$. Tehát $cl(G) = 2$, és a felső centrállánc $1 \lhd \langle a^2, b^2 \rangle \lhd G$.
Ferde kommutátorlánc: $\langle a^2 \rangle \lhd G$, és $G/\langle a^2 \rangle$-ben $[\overline{a}, \overline{b}] = 1$, ugyanis $a^{-1}b^{-1}ab = a^{-1}a^{-1} = a^2 \in \langle a^2 \rangle$. Ezért $G/\langle a^2 \rangle$ Abel-csoport, tehát $G' \leqslant \langle a^2 \rangle$, és G' kisebb már nem lehet, így $K_1(G) = G' = \langle a^2 \rangle$. Minthogy $a^2 \in Z(G)$, a ferde kommutátorlánc következő tagja $K_2(G) = [K_1(G), G] = [\langle a^2 \rangle, G] = 1$. Így a ferde kommutátorlánc: $G \rhd \langle a^2 \rangle \rhd 1$.

4.6. Állítás.

(1) Ha G nilpotens, és $H \leqslant G$, akkor H is nilpotens.

(2) Ha G nilpotens, és $N \lhd G$, akkor G/N is nilpotens.

(3) Ha $N \lhd G$-re N és G/N is nilpotens, abból nem következik, hogy G is nilpotens.

(4) Ha G_1 és G_2 nilpotens, akkor $G_1 \times G_2$ is az.

Bizonyítás: (1): Legyen $\{K_i(H)\}$ és $\{K_j(G)\}$ a H, illetve G csoport ferde kommutátorlánca. $K_1(H) = H \leqslant G = K_1(G)$, és ha $K_i(H) \leqslant K_i(G)$, akkor $K_{i+1}(H) = [K_i(H), H] \leqslant [K_i(G), G] = K_{i+1}(G)$. Tehát ha $cl(G) = k$, akkor $K_{k+1}(H) \leqslant K_{k+1}(G) = 1$ miatt $cl(H) \leqslant k$.
(2): Legyen $\varphi : G \to G/N$ a természetes homomorfizmus. Mivel tetszőleges $A, B \leqslant G$-re $[A, B]\varphi = [A\varphi, B\varphi]$, a ferde kommutátorlánc ferde kommutátorláncba megy át. Ezért ha $K_{k+1}(G) = 1$, akkor $K_{k+1}(G/N) = K_{k+1}(G\varphi) = (K_{k+1}(G))\varphi = 1$.
(3): S_3 nem nilpotens ($Z(S_3) = 1$ miatt el sem indul a felső centrállánc), pedig $A_3 \cong C_3$ és $S_3/A_3 \cong C_2$ nilpotens.
(4): A ferde kommutátorlánc komponensenként számítható, mivel $A_i, B_i \leqslant G_i$-re $[A_1 \times A_2, B_1 \times B_2] = [A_1, B_1] \times [A_2, B_2]$, tehát $cl(G_1 \times G_2) = \max\{cl(G_1), cl(G_2)\}$. □

4.7. Tétel. ***Frattini-elv***
Ha G véges, $N \lhd G$, és $P \in Syl_p N$, akkor $G = N_G(P)N$.

Bizonyítás: Tetszőleges $g \in G$-re $P^g \leqslant N^g = N \implies P, P^g \in Syl_p(N) \implies \exists n \in N$, hogy $P^n = P^g \implies P = P^{gn^{-1}} \implies gn^{-1} \in N_G(P) \implies g \in N_G(P)n \subseteq N_G(P)N$. □

4.8. Tétel. *Ha G véges csoport, akkor a következő állítások ekvivalensek.*

(1) G nilpotens.

(2) Minden $H < G$-re $H < N_G(H)$.

(3) G minden maximális részcsoportja prím indexű normálosztó.

(4) G minden Sylow-részcsoportja normálosztó.

(5) Ha $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ és $P_i \in Syl_{p_i}(G)$, akkor $G = \prod_{i=1}^{r} P_i$.

(6) Ha $x, y \in G$, és $(o(x), o(y)) = 1$, akkor $[x, y] = 1$.

Bizonyítás: (1) ⇒ (2): Legyen $1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$ centrállánc és i a legkisebb index, amelyre $N_i \not\leqslant H$ (ilyen i létezik, mert $H < G$). Ekkor $[N_i, H] \leqslant [N_i, G] \leqslant N_{i-1} \leqslant H$, ezért $N_i \leqslant N_G(H)$, és így $H < N_i H \leqslant N_G(H)$.
(2) ⇒ (3): Ha $H < G$ maximális részcsoport, akkor $H < N_G(H) \leqslant G$ miatt $N_G(H) = G$, azaz $H \lhd G$. Továbbá H maximalitásából következik, hogy G/H-nak nincs valódi részcsoportja, tehát $|G/H|$ prím.
(3) ⇒ (4): Tegyük fel, hogy valamelyik P p-Sylow nem normálosztó G-ben. Ekkor $N_G(P) < G$ miatt van olyan H maximális részcsoport G-ben, amelyre $N_G(P) \leqslant H < G$. A (3) állítás szerint $H \lhd G$, és P nyilván H-nak is p-Sylowja, tehát a Frattini-elv azt adja, hogy $N_G(P)H = G$, ami ellentmond annak, hogy $N_G(P)H \leqslant HH = H < G$.
(4) ⇒ (5): Legyen $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, és $P_i \in Syl_{p_i}(G)$. A (4) állítás szerint $P_i \lhd G$ minden i-re. A rendekből következik az is, hogy $P_i \cap (P_1 \dots P_{i-1} P_{i+1} \dots P_r) = 1$ minden i-re és $P_1 \cdots P_r = G$, így $G = P_1 \times \cdots \times P_r$.
(5) ⇒ (1): A Sylow-csoportok nilpotensek a 4.5. Állítás szerint, és a 4.6/4. Állítás következtében a $G = P_1 \times \cdots \times P_r$ direkt szorzat is nilpotens.
(5) ⇒ (6): Legyen $G = P_1 \times \cdots \times P_r$, $x = (x_1, \dots, x_r)$ és $y = (y_1, \dots, y_r)$. Ha $(o(x), o(y)) = 1$, akkor minden i-re $x_i = 1$ vagy $y_i = 1$, így $[x, y] = 1$.
(6) ⇒ (4): Legyen $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, és $P_i \in Syl_{p_i}(G)$ minden i-re. Ekkor a (6) állítás miatt $P_j \leqslant C_G(P_i) \leqslant N_G(P_i)$ minden $j \neq i$-re, és $P_i \leqslant N_G(P_i)$ nyilvánvaló, ezért $H := \langle P_1, \dots, P_n \rangle \leqslant N_G(P_i)$. Mivel $p_i^{\alpha_i} \,|\, |H|$ minden i-re, $H = G$, így $P_i \lhd G$. □

Az 1. fejezetben bebizonyítottuk a Schur–Zassenhaus-tételt Abel normálosztó esetére. Most megvannak az eszközeink ahhoz, hogy befejezzük a tétel bizonyítását.

4.9. Tétel. ***Schur–Zassenhaus-tétel***
(1) Legyen $|G|$ véges. Ha $N \lhd G$, és $(|N|, |G:N|) = 1$, akkor létezik N-nek komplementuma G-ben, így G felírható $G = N \rtimes H$ alakban.
(2) Ha N vagy G/N feloldható, akkor N bármely két komplementuma konjugált egymással. Továbbá minden $K \leqslant G$-re, melyre $(|N|, |K|) = 1$, létezik H komplementum, amely tartalmazza K-t.

Megjegyzés. Ha G feloldható, akkor a Schur–Zassenhaus-tétel állításai következnek a Hall-tételekből. A második állítás tetszőleges G-re igaz az "N vagy G/N feloldható" feltétel nélkül is a Feit–Thompson-tétel miatt, mely szerint minden páratlan rendű csoport feloldható.

Bizonyítás: Csak az (1) állítást bizonyítjuk. Vegyük észre, hogy az $(|N|, |G:N|) = 1$ feltétel miatt egy $H \leqslant G$ részcsoport akkor és csak akkor komplementuma N-nek, ha $|H| = |G:N|$.

Tegyük fel, hogy nem igaz az állítás, és legyen G minimális elemszámú ellenpélda, N pedig olyan normálosztó G-ben, amelynek nincs komplementuma.
1. N nilpotens:
Tegyük fel, hogy nem az, tehát van olyan $P \in Syl_p(N)$, amely nem normálosztó N-ben, így G-ben sem, ezért $N_G(P) < G$. A Frattini-elv szerint $G = N_G(P)N$. A $|G|$ minimalitása miatt $N_G(P)$-re igaz az (1) állítás az $N \cap N_G(P) \lhd N_G(P)$ normálosztóval, ugyanis

$$|N \cap N_G(P)| \mid |N|,$$

$$|N_G(P) : (N \cap N_G(P)| = |N_G(P)N : N| = |G:N|$$

relatív prímek. Ezért van olyan $H \leqslant N_G(P)$, amelyre $|H| = |N_G(P) : N| = |G:N|$, és ez N-nek is komplementuma G-ben, ami ellentmond G választásának.
2. N Abel:
N nilpotens, így N feloldható is, tehát $N' < N$. Ha N nem lenne Abel-csoport, akkor $N' > 1$ lenne. Mivel N' char $N \lhd G$, azt kapjuk, hogy $N' \lhd G$, és $|G|$ minimalitása miatt G/N'-re igaz az (1) állítás. $N/N' \lhd G/N'$, továbbá

$$|N/N'| \mid |N| \text{ és}$$

$$|G/N' : N/N'| = |G:N|$$

relatív prímek, ezért N/N'-nek van komplementuma G/N'-ben, azaz van olyan $H_1 \geqslant N'$, amelyre $|H_1/N'| = |G/N' : N/N'| = |G:N|$. Ekkor $|H_1| = |G:N||N'| < |G|$, mert $N' < N$, tehát ismét felhasználva $|G|$ minimalitását, most a H_1-re alkalmazhatjuk az (1) állítást: $N' \lhd H_1$, továbbá

$$|N'| \mid |N| \text{ és}$$

$$|H_1 : N'| = |G:N|$$

relatív prímek, ezért van olyan $H \leqslant H_1$, amelyre $|H| = |H_1 : N'| = |G:N|$, ellentmondva a G választásának.
3. Ezzel ellentmondásra jutottunk, mert az 1.5. Tételben már bizonyítottuk, hogy Abel-féle normálosztó esetén igaz az (1) állítás. □

4.2. Frattini-részcsoport

Definíció. $H \leqslant G$ maximális részcsoportja G-nek (jele: $H \underset{max}{<} G$), ha $H \neq G$, és minden $H < K \leqslant G$-re $K = G$. Egy G csoport *Frattini-részcsoportja* G maximális részcsoportjainak a metszete: $\Phi(G) = \bigcap_{M \underset{max}{<} G} M$. Ha G-nek nincs maximális részcsoportja, akkor $\Phi(G) = G$.

Megjegyzés. A Frattini-részcsoport nyilván karakterisztikus részcsoport.

4.10. Állítás. *Legyes G tetszőleges csoport. Egy $x \in G$ elem akkor és csak akkor van $\Phi(G)$-ben, ha G minden generátorrendszeréből elhagyható.*

Bizonyítás: $\Rightarrow$: Legyen $x \in \Phi(G)$, és tegyük fel, hogy x nem hagyható el minden generátorrendszerből, azaz létezik $K < G$, hogy $\langle K, x\rangle = G$. A G csoport K-t tartalmazó valódi részcsoportjaira alkalmazható a Zorn-lemma, mert az ilyen csoportok nem tartalmazzák x-et, így ilyenek felszálló láncának uniója sem tartalmazza x-et, tehát az is valódi részcsoport. Ez azt jelenti, hogy van olyan $M \underset{max}{<} G$, amelyre $K \leqslant M$. De akkor $x \in \Phi(G) \leqslant M$, így $M \geqslant \langle K, x\rangle = G$, ami ellentmondás.
$\Leftarrow$: Legyen $x \in G$ olyan, amely minden generátorrendszerből elhagyható. Tegyük fel, hogy $x \notin \Phi(G)$. Ekkor létezik M maximális részcsoport G-ben, hogy $x \notin M$. De ez azt jelenti, hogy $\langle M, x\rangle = G$, így x mégsem hagyható el az $M \cup \{x\}$ generátorrendszerből, ami ellentmond a feltevésnek. □

4.11. Tétel. *Minden véges csoport Frattini-részcsoportja nilpotens.*

Bizonyítás: A 4.8. Tétel 4. pontja szerint elég belátni, hogy egy G véges csoportra minden $P \in Syl_p(\Phi(G))$ normálosztója $\Phi(G)$-nek. Mivel $\Phi(G) \lhd G$, alkalmazhatjuk rá a Frattini-elvet:

$$\Phi(G)N_G(P) = G.$$

Tehát $\Phi(G) \cup N_G(P)$ generátorrendszere G-nek, de ebből a $\Phi(G)$ elemei egyenként elhagyhatók (ehhez is kell a végesség!), ezért $N_G(P) = G$, azaz $P \lhd G$, és így $P \lhd \Phi(G)$. □

4.12. Állítás. *Egy G véges csoport akkor és csak akkor nilpotens, ha $G' \leqslant \Phi(G)$.*

Bizonyítás: $\Rightarrow$: Elég belátni, hogy G' benne van minden maximális részcsoportban. Legyen $M \underset{max}{<} G$. Mivel G nilpotens, $M \lhd G$ és $|G : M| = p$ (a 4.8. Tétel 3. pontja miatt). Így $G/M \cong C_p$ Abel-csoport, és ebből $G' \leqslant M$ következik.
$\Leftarrow$: Belátjuk, hogy ha $G' \leqslant \Phi(G)$, akkor minden M maximális részcsoport p-indexű normálosztó, és így a 4.8. Tétel 3. pontja szerint G nilpotens. Legyen $M \underset{max}{<} G$. Ekkor $G' \leqslant \Phi(G) \leqslant M$. A G'-t tartalmazó részcsoportok normálosztók a 3.4. Állítás bizonyításában szereplő (3') állítás szerint, így $M \lhd G$. Mivel M maximális részcsoport, a G/M faktorcsoportnak nincs valódi részcsoportja, azaz $|G/M|$ prím. □

4.13. Állítás. *$G' \cap Z(G) \leqslant \Phi(G)$ minden G véges csoportra.*

Bizonyítás: Elég megmutatni, hogy minden maximális részcsoportnak része a $G' \cap Z(G)$ metszet. Tegyük fel, hogy létezik M maximális részcsoport úgy, hogy $G' \cap Z(G) \nleqslant M$. Ekkor $(G' \cap Z(G))M = G$. Mivel $G' \cap Z(G)$ és M is normalizálja M-et, $G \leqslant N_G(M)$, azaz $M \lhd G$. Minthogy M maximális részcsoport, G/M prímrendű, tehát Abel-csoport, amiből $M \geqslant G' \geqslant G' \cap Z(G)$ következik, ellentmondva a feltevésünknek. □

4.3. Véges p-csoportok

4.14. Állítás. *Ha G véges p-csoport, akkor $G/\Phi(G)$ elemi Abel p-csoport ($C_p \times \cdots \times C_p$). Sőt $\Phi(G)$ a legkisebb olyan normálosztó mellyel vett faktor elemi Abel.*

Bizonyítás: Ha G p-csoport, akkor nilpotens is. A 4.12 Állítás miatt $G' \leqslant \Phi(G)$, és így $G/\Phi(G)$ Abel. Ezért bármely M maximális részcsoport normálosztó, és $G/M \cong C_p$ (4.8/3. Tétel). Ez azt jelenti, hogy $x^p \in M$ tetszőleges $x \in G$-re. Ez igaz minden M maximális részcsoportra, így $x^p \in \Phi(G)$ minden $x \in G$-re. Tehát a véges Abel-csoportok alaptétele szerint $G/\Phi(G) \cong C_p \times \cdots \times C_p$.
Az állítás további részének igazolásához legyen $N \lhd G$ olyan, hogy G/N elemi Abel p-csoport. Megmutatjuk, hogy ekkor $\Phi(G) \leqslant N$.
A feltételből következik, hogy $\Phi(G/N) = 1$, azaz $\bigcap_{\overline{M} \underset{max}{<} \overline{G}} \overline{M} = 1$, így az ősképekre $\bigcap_{\overline{M} \underset{max}{<} \overline{G}} M \leqslant N$. Mivel maximális részcsoportok ősképe is maximális, $\Phi(G)$ pedig az összes maximális részcsoport metszete, ebből $\Phi(G) \leqslant N$ következik. □

4.15. Tétel. *Ha G véges p-csoport és $|G/\Phi(G)| = p^d$, akkor G minden minimális generátorrendszere d elemű.*

Bizonyítás: A 4.14 Állítás alapján $G/\Phi(G) = C_p^d$. Legyen $a_1, \dots, a_d$ olyan, hogy $G/\Phi(G) = \langle \overline{a}_1, \dots, \overline{a}_d \rangle$. Ekkor $G = \langle a_1, \dots, a_d, \Phi(G) \rangle$. A 4.10. Állítás szerint ebből a generátorrendszerből elhagyhatók a $\Phi(G)$ elemei, ezért $G = \langle a_1, \dots, a_d \rangle$, tehát G-nek létezik d-elemű generátorrendszere. Megmutatjuk, hogy kisebb elemszámú nem létezik, és minden generátorrendszerből kiválasztható egy d elemű generátorrendszer.
Tegyük fel, hogy $\langle b_1, \dots, b_k \rangle = G$. Ekkor $\langle \overline{b_1}, \dots, \overline{b_k} \rangle = G/\Phi(G)$.
A $C_p \times \cdots \times C_p$ (additív) csoportot tekinthetjük d-dimenziós $\mathbb{F}_p$ feletti vektortérnek. Ezért $k \geqslant d$, és $\{\overline{b}_1, \dots, \overline{b}_k\}$-ból kiválasztható egy $\{\overline{b}_{i_1}, \dots, b_{i_d}\}$ bázis, amelyből az előző rész alapján $\langle b_{i_1}, \dots, b_{i_d} \rangle = G$. □

Definíció. A G p-csoport *extraspeciális*, ha $G' = \Phi(G) = Z(G) \cong C_p$.

4.16. Állítás. *Minden p^3-rendű nem kommutatív csoport extraspeciális.*

Bizonyítás: Legyen $|G| = p^3$, és tegyük fel, hogy G nem Abel. Véges p-csoport centruma nem triviális, így $|G/Z(G)| \in \{1, p, p^2\}$. Viszont $G/Z(G)$ nem lehet ciklikus, mert akkor G Abel-csoport lenne, tehát $|G/Z(G)| = p^2 \implies G/Z(G)$ Abel-csoport $\implies G' \leqslant Z(G)$. De G' sem lehet triviális, így $G' = Z(G) \cong C_p$. Végül abból, hogy $G/Z(G)$ nem ciklikus, az is következik, hogy $G/G' = G/Z(G) \cong C_p \times C_p$, így a 4.14. Állítás alapján $\Phi(G) = G'$. □

4.17. Állítás. *Ha $|G| = p^n$, és $n > 1$, akkor $cl(G) \leqslant n-1$, és minden $n > 1$-hez létezik G, amelyre $|G| = p^n$, és $cl(G) = n-1$.*

Bizonyítás: Legyen $1 = Z_0 < Z_1 < \cdots < Z_r = G$ a G csoport felső centrállánca. Ez legfeljebb n hosszú lehet, mert minden faktor legalább p-edrendű. Viszont $|G : Z_{r-2}| \geqslant p^3$, mert különben $Z_{r-1}/Z_{r-2} = Z(G/Z_{r-2}) = G/Z_{r-2}$, így $Z_{r-1} = G$, ami ellentmondás. Tehát $r \leqslant n-1$.
Tekintsük a $G = D_{2^{n-1}} = \langle f \rangle \rtimes \langle t \rangle \cong C_{2^{n-1}} \rtimes C_2$ diédercsoportot. Ennek a centruma $Z(G) = \langle f^{2^{n-2}} \rangle \cong C_2$, ha $n \geqslant 3$, és $G/Z(G) \cong D_{2^{n-2}}$. Így indukcióval bizonyítható, hogy $cl(G) = n-1$. □

4.4. Hamilton-csoportok

Definíció. *G Hamilton-csoport*, ha nem Abel, de minden részcsoportja normálosztó.

A Q kvaterniócsoportról tudjuk, hogy Hamilton-csoport. A fejezet hátralevő részében a Hamilton-csoportok szerkezetét fogjuk leírni. Kezdjük néhány egyszerű észrevétellel!

4.18. Lemma. *Ha G Hamilton-csoport, és $H = \langle x, y \rangle \leqslant G$, akkor $H' \leqslant Z(H)$.*

Bizonyítás: $\langle x \rangle, \langle y \rangle \lhd G \implies [x, y] \in \langle x \rangle \cap \langle y \rangle \leqslant C_H(x) \cap C_H(y) = Z(H)$, és $H/\langle [x,y] \rangle = \langle \overline{x}, \overline{y} \rangle$-ban $[\overline{x}, \overline{y}] = 1$, ezért $H/\langle [x,y] \rangle$ Abel-csoport, tehát $H' \leqslant \langle [x,y] \rangle \leqslant Z(H)$. □

4.19. Lemma. *Ha egy G csoportra $G' \leqslant Z(G)$, akkor minden x, y, z-re és $n \in \mathbb{N}$-re*

(1) $[xy, z] = [x, z][y, z]$,

(2) $[x, yz] = [x, y][x, z]$, *és*

(3) $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$.

Bizonyítás: (1): Egyszerűen ellenőrizhető az $[xy, z] = [x, z]^y [y, z]$ általános összefüggés, amiből $[x, z] \in Z(G)$ miatt $[xy, z] = [x, z][y, z]$.
(2): Az $[x, yz] = [x, z][x, y]^z$ általános összefüggést $[x, z], [x, y] \in Z(G)$ miatt tovább alakíthatjuk:
$[x, yz] = [x, z][x, y] = [x, y][x, z]$.
(3): Az $yx = xy[y, x]$ összefüggést használva az $(xy)^n = xyxy \cdots xy$ szorzatban az x-eket a szorzat elejére léptethetjük az y-okon keresztül, minden alkalommal egy (centrumbeli, tehát a végére rakható) $[y, x]$ taggal toldva meg a szorzatot. Mivel összesen $1+2+\ldots+(n-1) = \binom{n}{2}$ átléptetés kell, a végső alak $x^n y^n [y, x]^{\binom{n}{2}}$.
□

4.20. Állítás. *Ha G Hamilton-csoport, akkor G minden eleme véges rendű.*

Bizonyítás: Először azt látjuk be, hogy ha mégis lenne végtelen rendű elem, akkor az benne lenne a csoport centrumában.
Legyen $x, y \in G$, és $o(x) = \infty$. Ekkor a 4.18. Lemmából következik, hogy $[[x, y], y] = 1$. Másrészt $\langle x \rangle \lhd G$ miatt $[x, y] = x^r$ valamely r-re, így $1 = [[x, y], y] = [x^r, y] = [x, y]^r = (x^r)^r = x^{r^2}$ (felhasználva a 4.19/1. azonosságot), tehát $o(x) = \infty$ miatt $r = 0$, azaz $[x, y] = 1$.
Most tegyük fel, hogy $o(c) = \infty$ (így $c \in Z(G)$), és $o(x) < \infty$. Ekkor $o(cx) = \infty$, ugyanis $(cx)^{o(x)} = c^{o(x)}$ is végtelen rendű, ebből pedig az előző rész miatt következik, hogy $cx \in Z(G)$, tehát x is centrumbeli. Arra jutottunk, hogy ha van végtelen rendű elem, akkor G végtelen és véges rendű elemei is a centrumban vannak, így G Abel-csoport lenne, ami ellentmond a feltételeknek. □

4.21. Állítás. *Minden Hamilton-csoport felbontható különböző prímekhez tartozó p-csoportok direkt szorzatára.*

Bizonyítás: Egy adott p prímre a G Hamilton-csoport p-hatványrendű elemei részcsoportot (és így normálosztót is) alkotnak, ugyanis $xy \in \langle x, y \rangle = \langle x \rangle \langle y \rangle$, és az utóbbinak a rendje osztója $|\langle x \rangle| \cdot |\langle y \rangle|$-nak, ami p-hatvány, ha $o(x)$ és $o(y)$ p-hatványok. Legyen G_p a G p-hatványrendű elemei által alkotott normálosztó. Ekkor $G_p \cap G_q = 1$, ha $p \neq q$, így a G_p normálosztók centralizálják egymást, továbbá a $\langle G_q \,|\, q \neq p \rangle$ csoport elemeinek a rendje nem osztható p-vel, így ez is diszjunkt G_p-től. Végül G minden eleme véges rendű a 4.20. Állítás miatt, és ezek előállíthatók prímhatványrendű elemek (az elem alkalmas hatványai) szorzataként (ld. az 1.7. Lemmát), így $G = \langle G_p \,|\, p \text{ prím} \rangle = \prod_{p \text{ prím}} G_p$. □

A továbbiakban elegendő a Hamilton-féle p-csoportokat meghatározni.

4.22. Lemma. *Tegyük fel, hogy a G p-csoportra $G' \leqslant Z(G)$, és $|G'| = p$.*
Ekkor $x, y \in G$-re $(xy)^{p^k} = x^{p^k} y^{p^k}$, ha az alábbi három feltétel valamelyike teljesül:

(i) $p > 2$ *és* $k \geqslant 1$*;*

(ii) x *vagy* y *felírható valamely G-beli elem p-edik hatványaként;*

(iii) $p = 2$ *és* $k \geqslant 2$.

Bizonyítás: A 4.19. Lemma szerint $(xy)^{p^k} = x^{p^k} y^{p^k} [y, x]^{\binom{p^k}{2}}$.
Az (i) esetben $\binom{p^k}{2}$ osztható p-vel, így $|G'| = p$ miatt $[y, x]^{\binom{p^k}{2}} = 1$.
A (ii) esetben ha $y = y_1^p$, akkor a 4.19. Lemma 1. azonossága szerint szerint $[y, x] = [y_1^p, x] = [y_1, x]^p = 1$, ha pedig $x = x_1^p$, akkor $[y, x] = [y, x_1^p] = [y, x_1]^p = 1$ ugyanannak a lemmának a 2. azonossága miatt.
A (iii) esetben $k \geqslant 2$-re $\binom{2^k}{2}$ osztható 2-vel, tehát $[y, x]^{\binom{2^k}{2}} = 1$. □

4.23. Lemma. *Ha $G = \langle x, y \rangle$ Hamilton-féle p-csoport, amelyre $|G'| = p$, akkor $p = 2$, és $G \cong Q$.*

Bizonyítás: Feltehető, hogy $o(x) \geqslant o(y)$, és $\langle x \rangle \cap \langle y \rangle = \langle c \rangle$, ahol $x^{p^n} = c = y^{p^k}$ ($\implies n \geqslant k$). Legyen $y_1 = x^{-p^{n-k}} y$. Ekkor $\langle x, y_1 \rangle = G$, és $y_1^{p^k} = (x^{-p^{n-k}} y)^{p^k} = x^{-p^n} y^{p^k} = 1$ a 4.22. Lemma (i) miatt, ha $p > 2$, vagy (ii) miatt, ha $p = 2$ és $n > k \geqslant 1$, vagy (iii) miatt, ha $p = 2$ és $n \geqslant k \geqslant 2$. Mivel $|G/\langle x \rangle| = p^k$, és $|\langle y_1 \rangle| \leqslant p^k$, ebben az esetben $\langle x \rangle \cap \langle y_1 \rangle = 1$, és ezért $G = \langle x \rangle \times \langle y_1 \rangle$ Abel-csoport, ami ellentmond a feltételeknek.
Az egyetlen megmaradó eset az, amikor $p = 2$, és $n = k = 1$, azaz $o(x) = o(y)$, és $x^2 = y^2$. Az y elem helyett vehetnénk az $x^{-1}y$ elemet is, amely a 4.22. Lemma (iii) esete miatt legfeljebb negyedrendű lehet, vagyis feltehető, hogy $o(y) = 4$, és akkor $o(x) = 4$. Végül abból, hogy $\langle x \rangle \lhd G$, de G nem Abel, következik, hogy $x^y = x^{-1}$, így G csak a kvaterniócsoport lehet. □

4.24. Tétel. *Egy G (nem feltétlenül véges) csoport akkor és csak akkor Hamilton-csoport, ha $G \cong Q \times A \times B$, ahol A elemi Abel-2-csoport, és B olyan Abel-csoport, amelynek minden eleme véges és páratlan rendű.*

Bizonyítás: Először lássuk be, hogy az ilyen csoportok valóban Hamilton-csoportok. Legyen $G = Q \times A \times B$ a fenti jelöléssel. Az 1.2. Tétel szerint G minden részcsoportja $Q \times A$ és B egy-egy részcsoportjának direkt szorzata, ugyanis ennek a két csoportnak az elemei relatív prím rendűek, ezért a triviálison kívül nincs izomorf szeletük. A B Abel-csoportnak minden részcsoportja normálosztó, így elég a $H = Q \times A$

csoportról belátni, hogy Hamilton-csoport.
Legyen $K \leqslant Q \times A$. Ha $K \cap Q = 1$, akkor K beágyazható a $H/Q \cong A$ csoportba, így K minden eleme legfeljebb másodrendű. Következésképpen $K \leqslant Z(Q) \times A = Z(H)$, és így $K \lhd H$.
Ha viszont $K \cap Q \neq 1$, akkor $K \geqslant Z(Q)$, és akkor $K/Z(Q) \leqslant H/Z(Q)$, de az utóbbi csoport kommutatív, ezért ebből $K/Z(Q) \lhd H/Z(Q)$, azaz $K \lhd H$ következik.

A másik irány bizonyításához legyen G egy Hamilton-csoport. A 4.21. Lemma szerint G felírható $G = \prod_{p \text{ prím}} G_p$ direkt szorzat alakban, ahol G_p a G p-hatványrendű elemeinek halmaza. Azt kell belátnunk, hogy G_p Abel-csoport, ha $p > 2$, és hogy $G_2 \cong Q \times A$.

Tegyük fel, hogy $p > 2$, és G_p nem kommutatív. Legyen $x, y \in G_p$ két olyan elem, amelyre $[x, y] \neq 1$, és $o(x) + o(y)$ minimális erre a tulajdonságra nézve. Ha $[x, y]^p \neq 1$, akkor $o(x) + o(y)$ nem lenne minimális: a 4.19. Lemma azonosságai alapján $[x^p, y] = [x, y]^p \neq 1$, és $o(x^p) + o(y) < o(x) + o(y)$. Tehát $\langle x, y\rangle' = \langle [x, y]\rangle$ p-edrendű, és ez ellentmond a 4.23. Lemma állításának.

Most vegyünk $H := G_2$-ben olyan x, y elemeket, amelyekre $[x, y] \neq 1$, és $o(x) + o(y)$ minimális (ilyen van, mert az összes többi komponens kommutatív, így G_2-nek kell nem kommutatívnak lennie). Ugyanúgy, mint a páratlan p esetében, azt kapjuk, hogy $\langle x, y\rangle'$ 2-elemű, és a 4.23. Lemma szerint ekkor $\langle x, y\rangle \cong Q$. Azonosítsuk ezt a részcsoportot a $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ csoporttal. Vegyük észre, hogy $C_H(i)$ és $C_H(j)$ is 2 indexű, ugyanis $[i, j] \neq 1$ miatt 1 indexű nem lehet, viszont $G/C_H(i)$ beágyazható $\mathrm{Aut}\langle i\rangle \cong C_2$-be, és ugyanígy $G/C_H(j)$ is $\mathrm{Aut}\langle j\rangle \cong C_2$-be. Minthogy $C_H(i) \neq C_H(j)$, ebből következik, hogy $C_H(Q) = C_H(i) \cap C_H(j)$ 4 indexű H-ban, és $C_H(Q) \cap Q = Z(Q) = \langle -1\rangle$. $C_H(Q)$ nem tartalmazhat negyedrendű g elemet, mert akkor $\langle i, jg\rangle$ 16-odrendű csoport lenne, ami kielégíti a 4.23. Lemma feltételeit. Tehát $C_H(Q)$ elemi Abel-2-csoport, azaz egy multiplikatív vektortér, ezért ebben a $Z(Q)$ részcsoportnak van komplementuma, legyen ez A. Az így kapott A csoportra $|H : A| = |H : C_H(Q)| \cdot |C_H(Q) : A| = 8$, és $Q \cap A \leqslant Q \cap C_H(Q) \cap A = Z(Q) \cap A = 1$, ezért $H = Q \times A$. □

5. Transzfer

Definíció. Legyen $H \leqslant G$, amelyre $|G:H| = n < \infty$. Vegyünk egy $\{x_1, \dots, x_n\}$ reprezentánsrendszert a H jobb oldali mellékosztályain: $\dot{\bigcup_{i=1}^{n}} Hx_i$. A G elemeivel való jobbszorzás permutálja ezeket a mellékosztályokat: egy $g \in G$ elemre legyen $Hx_ig = Hx_{i\alpha}$, ahol $\alpha \in S_n$, azaz $x_ig = h_ix_{i\alpha}$ alkalmas $h_i \in H$ elemekkel (ezek a g-vel való szorzás „hibái"). A

$$\begin{aligned} T_{G:H}: \quad & G \to H/H' \\ & g \mapsto (\textstyle\prod_{i=1}^{n} h_i)H' = \prod_{i=1}^{n}(x_igx_{i\alpha}^{-1})H' \end{aligned}$$

leképezést *transzfernek* nevezzük.

A transzfer definíciójában nyilván nem számít a reprezentánselemek (és így a h_i elemek) sorrendje, mert H/H' kommutatív.

5.1. Állítás. *Legyen $H \leqslant G$, $|G:H| = n$. Ekkor*

(1) $T = T_{G:H}$ definíciója független a reprezentánsrendszer választásától.

(2) $T : G \to H/H'$ homomorfizmus, és $\operatorname{Ker} T \geqslant G'$.

Bizonyítás. (1) Legyen a H mellékosztályainak két reprezentánsrendszere $\{x_1, \dots, x_n\}$ és $\{y_1, \dots, y_n\}$, ahol $y_i = c_ix_i$ valamely $c_i \in H$ elemekkel. Ha $x_ig = h_ix_{i\alpha}$, akkor

$$y_ig = c_ix_ig = c_ih_ix_{i\alpha} = c_ih_ic_{i\alpha}^{-1}y_{i\alpha}.$$

Ha T az x_i-kkel, T' pedig az y_i-kkel definiált transzfer, akkor

$$gT' = \Big(\prod_{i=1}^{n} c_ih_ic_{i\alpha}^{-1}\Big)H' = \Big(\prod_{i=1}^{n} c_i\Big)H'\Big(\prod_{i=1}^{n} c_{i\alpha}^{-1}\Big)H'\Big(\prod_{i=1}^{n} h_i\Big)H' = \Big(\prod_{i=1}^{n} h_i\Big)H' = gT.$$

Az átrendezéseknél többször felhasználtuk, hogy a c_i, h_i elemek mindegyike H-beli, és hogy H/H' kommutatív.
(2) Legyen $g, g' \in G$-re $x_ig = h_ix_{i\alpha}$ és $x_ig' = h_i'x_{i\beta}$. Ekkor

$$x_igg' = h_ix_{i\alpha}g' = h_ih_{i\alpha}'x_{i\alpha\beta}, \text{ amiből}$$

$$(gg')T = \Big(\prod_{i=1}^{n} h_ih_{i\alpha}'\Big)H' = \Big(\prod_{i=1}^{n} h_i\Big)H'\Big(\prod_{i=1}^{n} h_{i\alpha}'\Big)H' = gTg'T,$$

tehát T homomorfizmus.
Mivel H/H' Abel, a $G/\operatorname{Ker} T \cong \operatorname{Im} T \leqslant H/H'$ faktorcsoport is Abel, és így a 3.4. Állítás szerint $\operatorname{Ker} T \geqslant G'$. □

Feladat. Mivel $G' \leqslant \operatorname{Ker} T_{G:H}$, a $T_{G:H}$ transzfer indukál egy $T_{G:H}^* : G/G' \to H/H'$ homomorfizmust. Mutassuk meg, hogy ha $K \leqslant H \leqslant G$ és $|G:K| < \infty$, akkor $T_{G:H}^*T_{H:K}^* = T_{G:K}^*$.

5.2. Állítás. *Legyen $T = T_{G:H}$, és $g \in G$. Ekkor $gT = (\prod_{i=1}^{r} y_ig^{n_i}y_i^{-1})H'$ alkalmas $y_i \in G$ elemekkel és n_i pozitív egészekkel úgy, hogy $\sum_{i=1}^{r} n_i = n = |G:H|$, és $y_ig^{n_i}y_i^{-1} \in H$ $\forall i$.*

Bizonyítás. A g elemet mint a H mellékosztályain ható permutációt bontsuk fel diszjunkt ciklusok szorzatára. Legyen r a ciklusok száma, az 1 hosszú ciklusokat is beleszámítva. Az i. ciklus hossza legyen n_i, és a ciklus egyik eleme Hy_i. A ciklus tagjainak reprezentánselemét választhatjuk sorra y_i, y_ig, y_ig^2,…, $y_ig^{n_i-2}$, $y_ig^{n_i-1}$-nek. Ekkor az adott ciklushoz tartozó hibák rendre: $1, 1, \dots, 1, y_ig^{n_i}y_i^{-1} \in H$, és

$$gT = \Big(\prod_{i=1}^{r} y_ig^{n_i}y_i^{-1}\Big)H'.$$

□

5.3. Következmény. *Ha $H \leqslant Z(G)$, akkor $gT = g^n$*

Bizonyítás. $H \leqslant Z(G)$ miatt $H' = 1$, és $T : G \to H$. Az előző állítás szerint $gT = (\prod_{i=1}^{r} y_i g^{n_i} y_i^{-1})H'$, és $y_i g^{n_i} y_i^{-1} \in H \leqslant Z(G) \implies y_i g^{n_i} y_i^{-1} = (y_i g^{n_i} y_i^{-1})^{y_i} = g^{n_i} \implies gT = \prod_{i=1}^{r} g^{n_i} = g^n$. □

5.4. Tétel. *Legyen $G = \langle g_1, \dots, g_m \rangle$ végesen generált csoport, és $H \leqslant G$ indexe $n < \infty$. Ekkor H-nak van nm elemű generátorrendszere.*

Bizonyítás. Legyen $\{x_i\}_{i=1}^{n}$ a H jobb mellékosztályainak egy reprezentánsrendszere, ahol $x_1 = 1$.
Rögzített i, j indexekre létezik (egyetlen) k index, hogy $x_i g_j \in H x_k$, azaz $x_i g_j x_k^{-1} \in H$. Jelöljük ezt $k_{i,j}$-vel. Legyen S a következő halmaz:

$$S := \{x_i g_j x_{k_{i,j}}^{-1} \,|\, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m\} \subseteq H.$$

Megmutatjuk, hogy ez a (legfeljebb) mn elemű S halmaz generátorrendszere H-nak.
Egy tetszőleges $h \in H$ elem felírható G generátorrendszeréből

$$h = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \dots g_{i_r}^{\varepsilon_r}$$

alakban, ahol $\varepsilon_s = \pm 1$. Ezt tovább alakíthatjuk:

$$h = \overbrace{(x_1 g_{i_1}^{\varepsilon_1} x_{i_1}^{-1})}^{\in H} \overbrace{(x_{i_1} g_{i_2}^{\varepsilon_2} x_{i_2}^{-1})}^{\in H} \dots \overbrace{(x_{i_r} g_{i_r}^{\varepsilon_r} x_{i_r}^{-1})}^{\in H} x_{i_r},$$

ahol $x_1 = 1$ a H-beli reprezentánselem, és $s \geqslant 1$-re $x_{i_{s+1}}$ az a reprezentánselem, amelyre $x_{i_s} g_{i_s}^{\varepsilon_s} \in H x_{i_{s+1}}$. A kapott H-beli tényezők $S \cup S^{-1}$-ből valók, ugyanis ha $\varepsilon_s = 1$, akkor $x_{i_s} g_{i_s} x_{i_{s+1}}^{-1} \in S$ az S definíciója szerint, ha pedig $\varepsilon_s = -1$, akkor $x_{i_s} g_{i_s}^{-1} x_{i_{s+1}}^{-1} = (x_{i_{s+1}} g_{i_s} x_{i_s}^{-1})^{-1}$ egy S-beli elem inverze.

Végül a felírás utolsó tagja, x_{i_r} szükségképpen H-beli, mert minden más tag és a szorzat is az. Mivel a H-nak mint mellékosztálynak a reprezentánselemét $x_1 = 1$-nek választottuk, $x_{i_r} = x_1 = 1$, tehát h-t felírtuk $S \cup S^{-1}$-beli elemek szorzataként. Ezzel beláttuk, hogy $\langle S \rangle = H$. □

5.5. Tétel (Schur-tétel). *Ha $|G : Z(G)| < \infty$, akkor $|G'| < \infty$.*

Bizonyítás. Legyen $|G : Z(G)| = n$. Ha $\{x_i\}_{i=1}^{n}$ a $Z(G)$ mellékosztályainak egy reprezentánsrendszere, akkor $G' = \langle [x_i, x_j] \,|\, 1 \leqslant i, j \leqslant n \rangle$, ugyanis minden $g, g' \in G$ felírható $g = x_i z$ és $g' = x_j z'$ alakban, ahol $z, z' \in Z(G)$, és ezért $[g, g'] = [x_i z, x_j z'] = [x_i, x_j]$. Következésképpen G' végesen generált.

$$G'/(G' \cap Z(G)) \overset{\text{1. izom. t.}}{\cong} G'Z(G)/Z(G) \leqslant G/Z(G) \text{ véges.}$$

Tehát $|G' :\ G' \cap Z(G)| < \infty$, és G' végesen generált, így az 5.4 Tétel miatt $G' \cap Z(G)$ is végesen generált. Tekintsük a $T = T_{G:Z(G)}$ transzfert. Az 5.3 Következmény szerint $gT = g^n\ \forall g \in G$, és $G' \leqslant \operatorname{Ker} T$, ezért $g^n = 1\ \forall g \in G'$. Így $G' \cap Z(G)$ olyan végesen generált Abel-csoport, amelyben minden elem n-edik hatványa 1, tehát minden eleme a generátorelemek legfeljebb $(n-1)$-edik hatványának szorzata, ezért $G' \cap Z(G)$ véges csoport. Ebből következik, hogy

$$|G'| = |G' :\ G' \cap Z(G)| \cdot |G' \cap Z(G)| < \infty.$$

□

5.6. Tétel (Burnside-féle normál-p-komplementumtétel). *Legyen G véges csoport és $P \in Syl_p(G)$. Ha $C_G(P) = N_G(P)$, akkor létezik $N \lhd G$, amely komplementuma P-nek.*

A tétel bizonyításához szükségünk lesz a következő lemmára.

5.7. Lemma. *Legyen $P \in Syl_p(G)$, és $K, L \subseteq P$.*

$$\left.\begin{array}{l} \text{Ha } K^x = K \text{ és } L^x = L\ \forall x \in P \\ \text{és } \exists g \in G :\ K^g = L \end{array}\right\} \implies \exists y \in N_G(P) :\ K^y = L.$$

Bizonyítás. A feltételek miatt $P \leqslant N_G(K), N_G(L)$ és $P^g \leqslant N_G(K^g) = N_G(L)$. Ezért $P, P^g \in Syl_p(N_G(L))$, és mivel a Sylow-részcsoportok konjugáltak, van olyan $z \in N_G(L)$, amelyre $(P^g)^z = P$. Legyen $y = gz$. Ekkor $y = gz \in N_G(P)$, és $K^y = K^{gz} = L^z = L$. □

A tétel bizonyítása. Mivel $P \leqslant N_G(P) = C_G(P)$, P Abel-csoport, és így $P' = 1$.
Tekintsük a $T = T_{G:P} : G \to P/P' = P$ transzfert. Legyen $N = \operatorname{Ker} T \lhd G$. Belátjuk, hogy N komplementuma P-nek.
Legyen $u \in P$ tetszőleges. Az 5.2 Állítás miatt $uT = \prod_{i=1}^{r} x_i u^{n_i} x_i^{-1}$ alkalmas $x_i \in G$ elemekkel, ahol $x_i u^{n_i} x_i^{-1} \in P$ minden i-re. Rögzítsünk egy i-t, és alkalmazzuk az 5.7. Lemmát a $K = \{u^{n_i}\}$ és $L = \{x_i u^{n_i} x_i^{-1}\}$ egyelemű halmazokra. Mivel P kommutatív, és $L = K^{x_i^{-1}}$, a K és L halmazok kielégítik a lemma feltételeit. Tehát van olyan $y_i \in N_G(P)$, amelyre $K^{y_i} = L$. Az $N_G(P) = C_G(P)$ feltétel miatt ebből következik, hogy $L = K$, azaz $x_i u^{n_i} x_i^{-1} = u^{n_i}$, így

$$uT = \prod_{i=1}^{r} x_i u^{n_i} x_i^{-1} = \prod_{i=1}^{r} u^{n_i} = u^n \text{ minden } u \in P\text{-re.}$$

Mivel $n = |G : P|$ nem osztható p-vel, a P Abel-csoportban az n. hatványra emelés injektív homomorfizmus, így P végessége miatt automorfizmus is. Tehát egyrészt $N \cap P = \operatorname{Ker} T \cap P = 1$, másrészt $T\,|_P$ szürjektivitása miatt $T : G \to P$ is szürjektív, amiből

$$|N| = |\operatorname{Ker} T| = \frac{|G|}{|\operatorname{Im} T|} = |G : P|$$

következik, ezért N valóban komplementuma P-nek. □

A Burside-féle normál-p-komplementumtétel feltételének biztosításához gyakran hasznosnak bizonyul az alábbi lemma.

5.8. Lemma. *Ha $H \leqslant G$, akkor $N_G(H)/C_G(H) \lesssim \operatorname{Aut}(H)$.*

Bizonyítás. Az $N_G(H)$ csoport elemeivel való konjugálások automorfizmusként hatnak a H csoporton, így van egy $\varphi : N_G(H) \to \operatorname{Aut}(H)$ homomorfizmus. $\operatorname{Ker}\varphi = \{g \in N_G(H) \mid h^g = h\ \forall h \in H\} = \{g \in G \mid h^g = h\ \forall h \in H\} = C_G(H)$, így a homomorfizmustétel szerint $\operatorname{Im}\varphi \cong N_G(H)/C_G(H)$. □

5.9. Következmény. *$N \lhd G$ esetén $G/C_G(N) \lesssim \operatorname{Aut}(N)$, speciálisan $N = G$-re $G/Z(G) \cong \operatorname{Inn}(G) \lhd \operatorname{Aut}(G)$ a belső automorfizmusok csoportja.*

5.10. Állítás. *Legyen p a G véges csoport rendjének legkisebb prímosztója. Ha $P \in Syl_p(G)$ ciklikus, akkor P-nek van normál p-komplementuma.*

Bizonyítás. Legyen $P \cong C_{p^n}$. Mivel P Abel-csoport, benne van a centralizátorában, tehát $P \leqslant C_G(P) \leqslant N_G(P)$. Az 5.8. Lemma szerint $N_G(P)/C_G(P) \lesssim \operatorname{Aut}(P)$, ahol $|\operatorname{Aut}(P)| = \varphi(p^n) = p^{n-1}(p-1)$ az 1.8. Lemma miatt. Viszont $|N_G(P)/C_G(P)| \mid |G : P|$ sem p-vel, sem p-nél kisebb prímekkel nem osztható, így $N_G(P)/C_G(P) = 1$, tehát alkalmazható P-re a Burnside-féle normál p-komplementumtétel. □

5.11. Tétel. *Ha $|G|$ négyzetmentes, azaz nincs olyan p prím, amelyre $p^2 \mid |G|$, akkor G feloldható.*

Bizonyítás. A prímosztók számára vonatkozó teljes indukcióval bizonyítjuk az állítást.
Legyen $|G| = \prod_{i=1}^{r} p_i$, ahol $p_1 > p_2 > \cdots > p_r$ prímek. Ha $r = 1$, akkor G Abel-csoport, tehát feloldható. Tegyük fel, hogy $r > 1$, és $r-1$-ig igaz az állítás. Legyen $P \in Syl_{p_r}(G)$. Az 5.10. Állítás szerint létezik $N \lhd G$, hogy $G = N \rtimes P$. Minthogy $G/N \cong P \cong C_{p_r}$, az N normálosztó pedig az indukciós feltevés miatt feloldható, G is feloldható (3.9). □

Definíció. *G metaciklikus*, ha G/G' és G' is ciklikus.

Bebizonyítjuk, hogy ha $|G|$ négyzetmentes, akkor G metaciklikus. Ehhez szükségünk lesz a következő lemmára

5.12. Lemma. *Ha G feloldható csoport, akkor a kommutátorláncában nem lehet G' alatt két egymás utáni nem triviális ciklikus faktor, azaz ha $G^{(i)}/G^{(i+1)}$ és $G^{(i+1)}/G^{(i+2)}$ is ciklikus valamilyen $i > 0$-ra, akkor $G^{(i+1)} = G^{(i+2)} = 1$.*

Bizonyítás. Legyen $H = G^{(i-1)}/G^{(i)}$. A feltétel szerint H'/H'' és H'' ciklikus, így $H''' = 1$.
$H/C_H(H'') = N_H(H'')/C_H(H'') \lesssim \operatorname{Aut} H''$, és H'' ciklikus, ezért $H/C_H(H'')$ Abel-csoport.
Így $C_H(H'') \leqslant H' \implies H'' \leqslant Z(H') \implies H'/Z(H') \cong (H'/H'')/(Z(H')/H'')$ ciklikus $\implies H'$ kommutatív $\implies H'' = 1$.
Ez az eredeti G csoportra nézve azt jelenti, hogy $G^{(i+1)}/G^{(i+2)} = 1$, azaz $G^{(i+1)} = G^{(i+2)}$, így az $(i+1)$-edik tagtól kezdve a kommutátorlánc tagjai megegyeznek, s mivel G feloldható, ebből következik, hogy $G^{(i+1)} = 1$. □

5.13. Tétel. *Ha $|G|$ négyzetmentes, akkor G metaciklikus.*

Bizonyítás. G feloldható az 5.11. Tétel miatt. Továbbá G kommutátorláncának a faktorai négyzetmentes rendű Abel-csoportok, így az 1.7. Lemma szerint ciklikusok is, és ebből az 5.12. Lemma miatt az is következik, hogy $G'' = 1$. Ezzel beláttuk, hogy G metaciklikus. □

6. Primitív és többszörösen tranzitív permutációcsoportok

6.1. k-tranzitív csoportok

Egy $G \leqslant S_\Omega$ permutációcsoport akkor és csak akkor tranzitív, ha minden $\alpha, \beta \in \Omega$-hoz van olyan $g \in G$, amelyre $\alpha g = \beta$. Ezt általánosítva kapjuk a k-tranzitivitás fogalmát.

Definíció. Egy $G \leqslant S_\Omega$ csoport *k-tranzitív*, ha bármely különböző $\alpha_1, \ldots, \alpha_k \in \Omega$-hoz és különböző $\beta_1, \ldots, \beta_k \in \Omega$-hoz létezik $g \in G$, hogy $\alpha_i g = \beta_i$ minden i-re. Vagy az

$$\Omega^{(k)} = \{(\alpha_1, \ldots, \alpha_k) \,|\, \text{az } \alpha_i \in \Omega \text{ elemek különbözők}\}$$

jelöléssel: G k-tranzitív Ω-n, ha tranzitív az $\Omega^{(k)}$ halmazon.

Definíció. Egy $\Delta \subseteq \Omega$ részhalmaz *halmazstabilizátora* $G_\Delta = \{g \in G \,|\, \delta g \in \Delta \ \forall \delta \in \Delta\text{-ra}\}$, és *elemenkénti stabilizátora* $G_{(\Delta)} = \{g \in G \,|\, \delta g = \delta \ \forall \delta \in \Delta\text{-ra}\}$. Ha $\Delta = \{\delta_1, \ldots, \delta_k\}$, akkor a $G_\Delta = G_{\{\delta_1,\ldots,\delta_k\}}$ és $G_{(\Delta)} = G_{\delta_1,\ldots,\delta_k}$ jelölést is használjuk.

6.1. Állítás. *Legyen $|\Omega| \geqslant k \geqslant 2$. A következő állítások ekvivalensek egy $G \leqslant S_\Omega$ csoportra:*

(i) *G k-tranzitív;*

(ii) *G tranzitív és G_α $k-1$-tranzitív az $\Omega \setminus \{\alpha\}$-n mindegyik α-ra;*

(iii) *G tranzitív és G_α $k-1$-tranzitív az $\Omega \setminus \{\alpha\}$-n valamelyik α-ra.*

Bizonyítás. *(i)* $\implies$ *(ii)*: G nyilván tranzitív, mert α-t és β-t kiegészíthetjük $\alpha_2, \ldots, \alpha_n$-nel és $\beta_2, \ldots \beta_n$-nel. Továbbá ha rögzítünk egy tetszőleges α-t, akkor minden $(\beta_1, \ldots \beta_{k-1}), (\gamma_1 \ldots \gamma_{k-1}) \in (\Omega \setminus \{\alpha\})^{(k-1)}$-hez van olyan $g \in G$, amely az $(\alpha, \beta_1, \ldots, \beta_{k-1}) \in \Omega^{(k)}$ k-ast az $(\alpha, \gamma_1, \ldots, \gamma_{k-1}) \in \Omega^{(k)}$ k-asba viszi, így G_α $(k-1)$-tranzitív $\Omega \setminus \{\alpha\}$-n.
(ii) $\implies$ *(iii)*: Nyilvánvaló.
(iii) $\implies$ *(i)*: Legyen $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega^{(k)}$. Mivel G tranzitív, $\exists x, y \in G: \ \alpha_1 \overset{x}{\mapsto} \alpha$ és $\alpha \overset{y}{\mapsto} \beta_1$. Ekkor

$$(\alpha_1, \alpha_2, \ldots, \alpha_k) \overset{x}{\mapsto} (\alpha, \alpha_2 x, \ldots, \alpha_k x) \overset{g}{\mapsto} (\alpha, \beta_2 y^{-1}, \ldots, \beta_k y^{-1}) \overset{y}{\mapsto} (\beta_1, \beta_2, \ldots, \beta_k)$$

alkalmas $g \in G_\alpha$-val a G_α $k-1$-tranzitivitása miatt. □

Definíció. Ha V vektortér, akkor az *általános lineáris csoport*, $GL(V)$ a V invertálható lineáris transzformációinak csoportja a kompozícióra nézve. Ha V n-dimenziós vektortér egy K test felett, akkor használjuk a $GL_n(K)$, illetve $|K| = q < \infty$ esetén a $GL_n(q)$ jelölést is.

Definíció. A V vektortér fölötti *affin általános lineáris csoport*

$$AGL(V) = \{v \mapsto Av + b \mid A \in GL(V), \ b \in V\}.$$

Példa. $GL(V)$ nem tranzitív V-n a 0 miatt, de $V \setminus \{0\}$-n tranzitív.

Példa. $AGL(V)$ 2-tranzitív V-n, ugyanis tranzitív (tetszőleges $v_1, v_2 \in V$-re az $A = I$-hez és $b = v_2 - v_1$-hez tartozó affin transzformáció v_1-et v_2-be viszi), és a 0 stabilizátora, $GL(V)$ tranzitív $V \setminus \{0\}$-n.

Egy K test feletti n-dimenziós vektortér egydimenziós alterei alkotják a K feletti $(n-1)$-dimenziós projektív tér pontjait, az egyenesek pedig a kétdimenziós alterek.
Vegyük észre, hogy az $n = 3$ esetben valóban teljesülnek a projektív sík axiómái:

(i) Bármely két ponton keresztül egyetlen egyenes húzható.

(ii) Bármely két különböző egyenes pontosan egy pontban metszi egymást.

(iii) Van négy olyan pont, amelyek közül semelyik kettő nincs egy egyenesen.

$GL(V)$ 2-tranzitívan hat a kapott projektív téren: V tetszőleges két különböző egydimenziós alterét átviheti tetszőleges két különböző egydimenziós altérbe, mert az altereket kifeszítő vektorok mindkét párnál függetlenek.
A hatás magját $GL(V)$ azon elemei alkotják, amelyek minden egydimenziós alteret helyben hagynak, azaz amelyeknek minden vektor sajátvektora. Ez pedig pontosan akkor teljesül, ha minden vektor ugyanahhoz a λ sajátértékhez tartozó sajátvektor, azaz a transzformáció mátrixa a λI skalármátrix. Ezek a transzformációk éppen a $GL(V)$ centrumának elemei. Így a projektív téren 2-tranzitívan hat a $GL(V)/Z(GL(V))$ csoport.

Definíció. *Projektív általános lineáris csoport*: $PGL(V) := GL(V)/Z(GL(V))$.

Az előbbiek szerint $PGL(V)$ 2-tranzitív a V-hez tartozó projektív téren.

Definíció. Legyen V n-dimenziós vektortér egy K test felett. Ekkor

$$SL(V) = \{A \in GL(V) \,|\, \det(A) = 1\} \lhd GL(V)$$

a V fölötti *speciális lineáris csoport*, és

$$PSL(V) = SL(V)/Z(SL(V))$$

a *projektív speciális lineáris csoport*. Az előzőekhez hasonlóan használjuk az $SL_n(K)$, $SL_n(q)$ és $PSL_n(K)$, $PSL_n(q)$ jelöléseket is.

$PSL(V)$ is 2-tranzitív a V-hez tartozó projektív téren, mert a $PGL(V)$ 2-tranzitivitásának bizonyításánál választott két vektorpárból az egyik vektort helyettesíthetjük alkalmas skalárszorosával úgy, hogy a determináns 1 legyen.

6.2. Primitív csoportok

Definíció. Legyen $G \leqslant S_\Omega$. Az Ω halmaz egy $\cup_i \Omega_i$ partíciója *G-invariáns*, ha $\forall i$-re és $\forall g \in G$-re létezik j, hogy $\Omega_i g = \Omega_j$. A partíció valódi, ha több, mint egy osztályból áll, és nem minden osztálya egyelemű.

Definíció. $G \leqslant S_\Omega$ *primitív*, ha Ω-nak nincs G-invariáns valódi partíciója. G *imprimitív*, ha tranzitív, de nem primitív.

Példa. D_4 mint a négyzet négy csúcsán ható permutációcsoport imprimitív, mert tranzitív (már a forgatások is), de átlót csak átlóba vihet, tehát a csúcsok átlók szerinti csoportosítása valódi invariáns partíció.

Megjegyzés. Vegyük észre, hogy egy imprimitív csoporthoz tartozó invariáns partíció osztályai azonos számosságúak: a tranzitivitás miatt minden Ω_i-hez és Ω_j-hez van olyan g, amelyre $\Omega_i g = \Omega_j$.

6.2. Állítás.

(1) Minden primitív permutációcsoport tranzitív.

(2) Minden 2-tranzitív csoport primitív.

(3) Ha G prím fokú tranzitív csoport, akkor primitív is.

Bizonyítás: (1): Az orbitokra bontás is invariáns partíció, és ha a csoport nem triviális, akkor van az orbitok között egynél több elemű.
(2): Ha egy G-invariáns partíciónak egyik osztálya tartalmaz legalább két elemet: $\alpha, \beta \in \Omega_i$ különbözők, és van másik osztálya is: $\gamma \in \Omega_j \neq \Omega_i$, akkor a 2-tranzitivitás miatt létező $g \in G$ elem, amelyre $\alpha g = \beta$ és $\beta g = \gamma$, nem hagyja invariánsan a partíciót: $\Omega_i g$ két osztályba is belemetsz.
(3): Ha $|\Omega| = p$ prím, és van egy G-invariáns partíció, annak a tranzitivitás miatt minden osztálya azonos számosságú, így elemszámuk osztója p-nek: 1 vagy p. De akkor ez a partíció nem lehet valódi. □

Definíció. Legyen $G \leqslant S_\Omega$. A $\Delta \subseteq \Omega$ részhalmaz *blokk* a G-re nézve, ha $\forall g \in G$-re $\Delta \cap \Delta g \neq \emptyset \implies \Delta = \Delta g$. A Δ blokk valódi blokk, ha $\Delta \neq \Omega$, és $|\Delta| \neq 1$.

6.3. Állítás. *Legyen $G \leqslant S_\Omega$ tranzitív. A G csoport akkor és csak akkor primitív, ha nem létezik valódi blokkja.*

Bizonyítás. Azt fogjuk bizonyítani, hogy G imprimitív $\Leftrightarrow \exists$ valódi blokkja.
$\Rightarrow$: Legyen $\Omega = \cup_i \Omega_i$ egy valódi G-invariáns partíció. Ekkor tetszőleges Ω_i blokkja G-nek.
$\Leftarrow$: Legyen Δ valódi blokk. Megmutatjuk, hogy ekkor $\{\Delta g \mid g \in G\}$ valódi partíció (bár a partíciónak ugyanazt az osztályát esetleg többször is felsoroltuk). A tranzitivitás miatt $\cup_{g\in G}\Delta g = \Omega$. Ahhoz, hogy G-invariáns partíció legyen, be kell látnunk, hogy

$$\forall g, h \in G: \ \Delta g \cap \Delta h \neq \emptyset \ \Rightarrow \ \Delta g = \Delta h.$$

Tegyük fel, hogy$\Delta g \cap \Delta h \neq \emptyset$. Ekkor $\Delta g h^{-1} \cap \Delta \neq \emptyset$, ezért a blokk definíciója szerint $\Delta g h^{-1} = \Delta$, és így $\Delta g = \Delta h$. Mivel Δ valódi blokk, a kapott partíció valódi. □

6.4. Tétel. *Egy tranzitív $G \leqslant S_\Omega$ csoport akkor és csak akkor primitív, ha a G_α stabilizátor maximális részcsoport G-ben bármely/valamely α-ra.*

Bizonyítás. A tranzitivitás miatt minden stabilizátor konjugált egymással (2.4), tehát egyszerre maximálisak vagy nem maximálisak. Azt látjuk be, hogy tranzitív G-re

$$G \text{ imprimitív } \Leftrightarrow G_\alpha \text{ nem maximális } G\text{-ben.}$$

$\Rightarrow$: Legyen Δ valódi blokk, $\alpha \in \Delta$, és $M := \{g \in G \mid \Delta g = \Delta\} \leqslant G$.
Ekkor $G_\alpha \leqslant M$, mert $\alpha g = \alpha \implies \Delta g \cap \Delta \neq \emptyset \implies \Delta g = \Delta$,
sőt $G_\alpha < M$, mert $\exists \beta \in \Delta \setminus \{\alpha\}$, és $\exists g : \alpha \mapsto \beta$, így $\beta \in \Delta \cap \Delta g \implies \Delta g = \Delta \implies g \in M \setminus G_\alpha$.
Másrészt $M < G$, mert $\exists \gamma \in \Omega \setminus \Delta$, és $g : \alpha \mapsto \gamma$-ra $\Delta g \neq \Delta \implies g \notin M$.
$\Leftarrow$: Tegyük fel, hogy G_α nem maximális: $G_\alpha < M < G$. Legyen $\Delta =: \alpha M \subseteq \Omega$.
Ekkor $|\Delta| > 1$, mert $G_\alpha < M$, és $\Delta \neq \Omega$, mert G_α mellékosztályai az α-t adott helyre vivő permutációk halmazai (2.2), és M nem tartalmaz minden mellékosztályt. Végül ha $\Delta \cap \Delta g \neq \emptyset$, akkor $\alpha m = \alpha m' g$ alkalmas $m, m' \in M$ elemekkel $\implies \alpha m' g m^{-1} = \alpha \implies m' g m^{-1} \in G_\alpha \leqslant M \implies g \in M \implies \Delta g = \Delta$. □

6.5. Tétel. *Ha G primitív és $1 \neq N \lhd G$, akkor N tranzitív.*

Bizonyítás. Tegyük fel, hogy N nem tranzitív. Mivel $N \neq 1$, létezik N-nek egy legalább kételemű orbitja: $\Delta = \alpha N \neq \Omega$.
Ez a Δ részhalmaz blokkja (és így valódi blokkja) G-nek, mert $\forall g \in G$-re $\Delta g = \alpha N g = \alpha g N$ miatt Δg is orbit, így vagy diszjunkt Δ-tól, vagy megegyezik vele. Ez ellentmond a feltevésnek, hogy G primitív. □

6.3. Tranzitív és primitív csoporthatások

Az előző alfejezetben a primitív permutációcsoportokról kimondott definíciók és tételek természetes módon általánosíthatók csoporthatásokra, csak a 6.5. Tételt kell módosítanunk: az $N \neq 1$ feltétel helyett azt kell megkövetelnünk, hogy N ne legyen benne a csoporthatás magjában.

Korábban bizonyítottuk (2.7), hogy egy G csoport valamely részcsoportjának mellékosztályain a G elemeivel való jobbszorzás hatása tranzitív csoporthatás, sőt G minden tranzitív csoporthatása ekvivalens egy ilyennel. Vizsgáljuk meg, milyen feltételek mellett lesz a kapott csoporthatás hűséges, illetve primitív.

6.6. Tétel. *Egy G csoport minden hűséges, tranzitív csoporthatása ekvivalens egy olyan $H \leqslant G$ mellékosztályain való hatással, amely nem tartalmazza G-nek valódi normálosztóját.*

Bizonyítás. A 2.7. Tételben bizonyítottuk, hogy van az adott csoporthatással ekvivalens, H mellékosztályain ható csoporthatás. Ennek a magja a H-ban levő legnagyobb normálosztó, $N = \bigcap_{x\in G} H^x$. Tehát a hatás pontosan akkor hűséges, ha $N = 1$, azaz ha H-ban nincs G-nek valódi normálosztója. □

6.7. Tétel. *G minden primitív csoporthatása ekvivalens egy olyan H mellékosztályain való hatással, amely maximális G-ben.*

Bizonyítás. A H mellékosztályain való csoporthatásnál a H stabilizátora éppen H, tehát a 6.4. Tétel csoporthatásokra alkalmazott változata szerint ez a csoporthatás pontosan akkor primitív, ha H maximális G-ben. □

A 6.6 és 6.7. Tétel összevonásával kapjuk a primitív hűséges csoporthatások jellemzését.

6.8. Tétel. *G minden hűséges, primitív csoporthatása ekvivalens egy olyan H mellékosztályain való hatással, amely maximális G-ben és nem tartalmazza G valódi normálosztóját.*

Példa. D_4-nek nem létezik hűséges, primitív permutációreprezentációja, mert minden maximális részcsoportja normálosztó. Sőt, általánosabban:
Véges nilpotens csoportnak nincs hűséges, primitív permutációreprezentációja, mert ezeknek minden maximális részcsoportja normálosztó (4.8).

A primitív csoportok tárgyalását fejezzük be egy olyan konstrukcióval, amellyel tranzitív csoportokból imprimitív csoportokat készíthetünk, illetve imprimitív permutációcsoportokat beágyazhatunk ilyen módon előállított permutációcsoportokba.

Definíció. Legyen $G \leqslant S_\Delta$, $H \leqslant S_\Omega$, $|\Delta| = n$ és $|\Omega| = k$. Ekkor G és H *koszorúszorzatának* nevezzük a

$$G \wr H = \{(g_1, \dots, g_k, h) \mid g_1, \dots, g_k \in G, h \in H\} \leqslant S_{\Delta \times \Omega}$$

$(G \times \cdots \times G) \rtimes H$ alakú permutációcsoportot, ahol az elemek hatása $\Omega = \{\omega_1, \dots, \omega_k\}$ esetén

$$(\delta, \omega_i)(g_1, \dots, g_k, h) = (\delta g_i, \omega_i h).$$

Feladat. Lássuk be, hogy ha G és H tranzitív, akkor $G \wr H$ imprimitív, és $\cup_i \{\Delta \times \omega_i\}$ egy $G \wr H$-invariáns valódi partíció.

6.4. Szigorúan k-tranzitív permutációcsoportok

Definíció. A $G \leqslant S_\Omega$ permutációcsoport *reguláris*, ha $\forall \alpha, \beta \in \Omega$-ra létezik egyetlen $g \in G$, hogy $\alpha g = \beta$. *G szigorúan k-tranzitív*, ha $\forall (\alpha_1, \dots, \alpha_k), (\beta_1, \dots, \beta_k) \in \Omega^{(k)}$-ra létezik egyetlen $g \in G$, hogy minden i-re $\alpha_i g = \beta_i$, azaz ha G reguláris az $\Omega^{(k)}$-n.

6.9. Állítás. *A következő állítások ekvivalensek:*

(1) G csoport szigorúan k-tranzitív;

(2) G k-tranzitív és $G_{\alpha_1, \dots, \alpha_k} = 1$;

(3) G tranzitív és G_α szigorúan $(k-1)$-tranzitív az $\Omega \setminus \alpha$-n.

Bizonyítás. Az (1) $\Leftrightarrow$ (2) ekvivalencia nyilvánvaló, a (2) $\Leftrightarrow$ (3) ekvivalencia következik a k-tranzitivitás rekurzív jellemzéséből (6.1). □

Példa. S_n szigorúan n-tranzitív és szigorúan $(n-1)$-tranzitív is.
A_n szigorúan $(n-2)$-tranzitív, mert ha $n-2$ elemen megadjuk egy permutáció hatását, akkor a maradék két elemen csak kétféleképpen hathat, és a kapott permutációk közül pontosan az egyik páros (az egyiket a másikból egy transzpozícióval való szorzással kapjuk).

6.10. Állítás. *Ha G reguláris csoporthatás Ω-n, akkor $|G| = |\Omega|$.*

Bizonyítás. Ha rögzítünk egy $\alpha \in \Omega$ elemet, akkor Ω és G között bijekciót ad az, ha minden $\beta \in \Omega$-hoz hozzárendeljük azt a g_β elemet, amelyre $g_\beta : \alpha \mapsto \beta$. □

6.11. Állítás. *Ha $G \leqslant S_n$ szigorúan k-tranzitív, akkor $|G| = n(n-1)\cdots(n-k+1)$.*

Bizonyítás. G reguláris az $\Omega^{(k)}$ halmazon, így $|G| = |\Omega^{(k)}| = n(n-1)\cdots(n-k+1)$. □

Példa. Az K testen mint önmaga feletti vektortéren az affin általános lineáris csoport , $AGL(K) = \{x \mapsto ax + b \mid a, b \in K,\ a \neq 0\}$ szigorúan 2-tranzitív:
Korábban láttuk, hogy $AGL(V)$ 2-tranzitív. Másrészt, ha egy $g : x \mapsto ax + b$ elem helyben hagyja 0-t és 1-et, akkor $b = 0$ és $a + b = 1$, amiből $g = 1$. Így $AGL_{0,1} = 1$.

Feladat. Tekintsük a $G = \{x \to \frac{ax+b}{cx+d} \mid a, b, c, d \in K,\ ad - bc \neq 0\}$ csoportot a $K \cup \{\infty\}$ kibővített testen, ahol $\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$, ha $a, c \neq 0$, $= \infty$, ha $c = 0$ és $a \neq 0$, $= 0$, ha $a = 0$ és $c \neq 0$, továbbá $\frac{a}{0} = \infty$, ha $0 \neq a \in K$. Bizonyítsuk be, hogy ez a csoport szigorúan 3-tranzitív. (Útmutatás: Érdemes a 0, G_0-ban a ∞, majd $G_{0,\infty}$-ben az 1 orbitját és stabilizátorát nézni.)

6.5. Mathieu-csoportok

6.12. Tétel (**Jordan-tétel**).
Legyen $G \leqslant S_n$ szigorúan k-tranzitív és $k \geqslant 4$. Ha $G \neq A_n, S_n$, akkor
$k = 4$ *és* $n = 11$ *vagy*
$k = 5$ *és* $n = 12$

A bizonyításhoz szükségünk lesz a következő lemmára.

6.13. Lemma. *Ha $g, h \in G \leqslant S_\Omega$ felcserélhető elemek, akkor* $\mathrm{Fix}(g)h = \mathrm{Fix}(g)$.

Bizonyítás. Ha $\alpha \in \mathrm{Fix}(g)$, akkor $(\alpha h)g = (\alpha g)h = \alpha h$, így $\mathrm{Fix}(g)h \subseteq \mathrm{Fix}\, g$, és ugyanígy $\mathrm{Fix}(g)h^{-1} \subseteq \mathrm{Fix}(g)$, amiből $\mathrm{Fix}(g) \subseteq \mathrm{Fix}(g)h$. □

A Jordan-tétel bizonyítása.
A $k = 4$ eset:

A bizonyításban sokszor használjuk a szigorú 4-tranzitivitás alábbi következményeit.

- Tetszőlegesen előírhatjuk egy $g \in G$ elem hatását az alaphalmaz 4 elemén.
- Ha G két eleme ugyanúgy hat az alaphalmaz 4 elemén, akkor azok megegyeznek.

1. *Feltehetjük, hogy $n \geqslant 8$:*
   Ugyanis ha $n \leqslant 7$, akkor $|G| = n(n-1)(n-2)(n-3)$ miatt $|S_n : G| = (n-4)! < n$, és $n \geqslant 5$ esetén S_n-nek nincs A_n-től és S_n-től különböző n-nél kisebb indexű részcsoportja (2.12).

2. *Bármely két másodrendű elem konjugált egymással:*
   Mivel az 1-től különböző elemeknek legfeljebb 3 fixpontja van, és $n \geqslant 8$, minden másodrendű elem ciklusfelbontásában van legalább két transzpozíció:
   $$\begin{aligned} x &= (12)(34)\dots \\ y &= (ab)(cd)\dots \end{aligned}.$$
   $\exists z = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \dots \\ a & b & c & d & \dots \end{smallmatrix}\right)$, és ezzel $x^z = (ab)(cd)\dots$, tehát a szigorú 4-tranzitivitás miatt $x^z = y$.

A 4-tranzitivitás miatt $\exists g = (12)(3)(4)\cdots$ és $h = (1)(2)(34)\cdots$. Legyen $H = \langle g, h\rangle \leqslant G$.

3. $H \cong C_2 \times C_2$:
   $g^2 = (1)(2)(3)(4)\cdots$ és $h^2 = (1)(2)(3)(4)\cdots \implies g^2 = h^2 = 1$.
   $gh = (12)(34)\cdots$ és $hg = (12)(34)\cdots \implies gh = hg$.

4. *H orbitjai $\{1,2\}, \{3,4\}, \{5,6\}, \{"7"\}, X, X', \dots$,*
   ahol $5, 6$ később definiálandó pontok, a 7 esetleg nem létezik, és $X, X', \dots$ mind 4-elemű orbitok:
   g-nek legfeljebb 3 fixpontja van, tehát a $3, 4$-en kívül legfeljebb még egy, ezt jelöljük 7-tel. A 7-et idézőjelbe tesszük, hogy egyúttal azt az esetet is kezeljük, amikor nincs harmadik fixpont.
   Minthogy g és h felcserélhető, h helyben hagyja a $\mathrm{Fix}(g) = \{3, 4, "7"\}$ halmazt, de ebből 3-at és 4-et felcseréli, ezért $"7"$, ha van, h-nak is fixpontja. Végül gh-nak $"7"$ szintén fixpontja, ha g-nek és h-nak fixpontja volt, és a konjugáltság miatt emellett kell lennie még két fixpontjának, legyenek ezek 5 és 6: $\mathrm{Fix}(gh) = \{5, 6, "7"\}$.
   Mivel g és h felcserélhetők gh-val, mindkettő helyben hagyja a $\mathrm{Fix}(gh) = \{5, 6, "7"\}$ halmazt, ezért

mindkettő felcseréli az 5-öt és a 6-ot (minthogy fixen nem hagyhat több elemet). Tehát a g, h, gh ciklusfelbontása:

$$\begin{aligned} g = &\quad (12)(3)(4)(56)(\text{"7"})\cdots \\ h = &\quad (1)(2)(34)(56)(\text{"7"})\cdots \\ gh = &\quad (12)(34)(5)(6)(\text{"7"})\cdots, \end{aligned}$$

és több fixpontjuk nincs.
Végül az $\Omega = \{1, \ldots, n\}$ halmazon g, h, gh egyikének sincs több fixpontja, azaz H regulárisan hat a többi orbiton, így a többi orbit 4-elemű (6.10).

5. $C_G(H) = H$:
Tegyük fel, hogy $1 \neq a \in C_G(H)$. Mivel a felcserélhető H minden elemével, helyben hagyja a H elemeinek fixponthalmazait, így az ezek metszetéből és különbségeikből kapott $\{1,2\}$, $\{3,4\}$, $\{5,6\}$ és $\{\text{"7"}\}$ halmazokat is. De a-nak is legfeljebb 3 fixpontja lehet, ezért a három kételemű halmaz közül legalább kettőn transzpozicióval hat:

$$a = (12)(34)\ldots \text{ vagy } a = (12)(56)\ldots \text{ vagy } a = (34)(56)\ldots.$$

Ez azt jelenti, hogy a legalább négy elemen megegyezik a g, h, gh elemek valamelyikével, így $a \in \{g, h, gh\} \subseteq H$.

6. $G_X = N_G(H)$ *minden* $X \subseteq \Omega \setminus \{1, 2, \ldots, 7\}$ H*-orbitra:*
Tudjuk, hogy $|X| = 4$. Tekintsük a G_X halmazstabilizátor hatását az X-en:
$\varphi : G_X \to S_X \simeq S_4$ homomorfizmus a $\sigma \mapsto \sigma|_X$ megfeleltetéssel. Mivel X-en tetszőlegesen megadhatjuk egy G-beli permutáció hatását, φ szürjektív, azaz $\operatorname{Im}\varphi \cong S_4$, másrészt az X négyelemű halmazon való hatás meghatározza a permutációt, tehát φ injektív is. Azt kaptuk, hogy $G_X \cong S_X \cong S_4$, és a $H \cong C_2 \times C_2$ részcsoport csak az S_4-beli V normálosztóba képződhet. Tehát $H\varphi \lhd S_X$, amiből $H \lhd G_X$, azaz $G_X \leqslant N_G(H)$.
A $G_X = N_G(H)$ egyenlőséghez ezen kívül elég belátnunk, hogy $|N_G(H)| \leqslant |G_X|$.
$N_G(H)/H = N_G(H)/C_G(H) \overset{5.8}{\lesssim} \operatorname{Aut}(H) \cong S_3$, tehát $|N_G(H) : H| \leqslant 6$, így $|N_G(H)| \leqslant 6 \cdot |H| = 24 = |G_X|$.

7. H*-nak egyetlen* 4 *hosszú orbitja van:*
Mivel $n \geqslant 8$, legalább egy 4 hosszú orbitnak kell lennie. Tegyük fel, hogy van kettő is: $X = \{i, j, k, l\}$ és $X' = \{i', j', k', l'\}$. Tudjuk, hogy $H|_X$ és $H|_{X'}$ fixpontmentesek, és az elemeik

$$\{1, (ij)(kl), (ik)(jl), (il)(jk)\} \text{ és } \{1, (i'j')(k'l'), (i'k')(j'l'), (i'l')(j'k')\}.$$

A 4-tranzitivitás miatt $\exists b \in G$, hogy $b|_X = (ij)(k)(l)$. Az előző pont szerint $b \in G_X = N_G(H) = G_{X'}$. Mivel $b^2|_X = 1$, b másodrendű elem. Már láttuk, hogy k, l fixpont és $b \neq 1$, ezért a k, l-en kívül legfeljebb 1 fixpontja lehet. Ezért $b|_{X'}$ két transzpozícióból áll. Ekkor viszont $b|_{X'} \in H|_{X'}$, amiből $b \in H$ következne, de H másodrendű elemei fixpontmentesen hatnak az X-en. Ellentmondásra jutottunk abból a feltevésből, hogy H-nak van két különböző 4-elemű orbitja.

Azt kaptuk, hogy H orbitjai: $\{1,2\}, \{3,4\}, \{5,6\}, \{\text{"7"}\}, \{i,j,k,l\}$. Tehát $n = 10$ vagy 11. De a később bizonyítandó 6.15. Állítás szerint a $k = 4$, $n = 10$ eset lehetetlen, ezért $n = 11$.

A $k \geqslant 5$ eset:
Teljes indukcióval bizonyítjuk. Mivel $G \leqslant S_n$ szigorúan k-tranzitív, az n stabilizátora, $G_n \leqslant S_{n-1}$ szigorúan $k-1$-tranzitív, így az indukciós feltevés szerint
vagy $k - 1 = 4$ és $n - 1 = 11 \implies k = 5$ és $n = 12$,
vagy $k - 1 = 5$ és $n - 1 = 12 \implies k = 6$ és $n = 13$.
A később bizonyítandó 6.16. Állítás szerint a $k = 6$, $n = 13$ eset nem lehetséges, tehát ezzel bebizonyítottuk a Jordan-tétel állítását. □

A két kimaradó eset kezeléséhez szükségünk lesz a következő lemmára.

6.14. Lemma. *Legyen $G \leqslant S_n$ k-tranzitív, $P \in Syl_p(G)$ és $\Gamma = Fix(P) = \bigcap_{x\in P} \mathrm{Fix}(x)$. Ha $|\Gamma| \geqslant k$, akkor $N_G(P)$ k-tranzitív Γ-n.*

Bizonyítás. Ha $g \in N_G(P)$ és $\gamma \in \Gamma$, akkor $\gamma gP = \gamma Pg = \gamma g$. Tehát γg is fixpontja P-nek, azaz $\gamma g \in \Gamma$. Ezért $\Gamma N_G(P) = \Gamma$.
Legyen $(\alpha_1, \dots, \alpha_k), (\beta_1, \dots \beta_k) \in \Gamma^{(k)}$.
A G k-tranzitivitásából következik, hogy $\exists g \in G$: $\alpha_i \overset{g}{\mapsto} \beta_i \ \ \forall i$-re.

$$\left.\begin{array}{c} P \leqslant G_{\beta_1,\dots,\beta_k} \text{ és} \\ P^g \leqslant (G_{\alpha_1,\dots,\alpha_k})^g = G_{\beta_1,\dots,\beta_k}, \ (2.4) \end{array}\right\} \quad \Longrightarrow \quad P, P^g \in Syl_p(G_{\beta_1,\dots,\beta_k}),$$

tehát $\exists h \in G_{\beta_1,\dots,\beta_k}$, hogy $P^{gh} = P$, azaz $gh \in N_G(P)$, és $\alpha_i gh = \beta_i$ minden i-re. □

6.15. Állítás. *Nem létezik $G \leqslant S_{10}$ szigorúan 4-tranzitív csoport.*

Bizonyítás. Tegyük fel, hogy van ilyen $G \leqslant S_{10}$. Ekkor $|G| = 10 \cdot 9 \cdot 8 \cdot 7$. A G csoport 7-Sylowja ciklikus, ezért feltehető, hogy $P = \langle(1234567)\rangle \in Syl_7(S_{10})$.
Az előző 6.14 Lemma alapján $N_G(P)$ 3-tranzitív $Fix(P) = \{8, 9, 10\}$-en. Ezért van olyan $g, h \in N_G(P)$, amelyre

$$\begin{array}{l} g = \tau(8\ 9)(10) \\ h = \pi(8\ 10)(9), \end{array} \quad \text{ahol } \tau, \pi \in S_7, \text{ így } \tau, \pi \in N_{S_7}(P).$$

A $\tau, \pi, \tau\pi$ permutációk egyike sem 1, mert különben g-nek, h-nak, illetve gh-nak 8, illetve 7 fixpontja lenne, ami ellentmond a szigorú 4-tranzitivitásnak.
Ha τ-ban van ℓ-ciklus, ahol $\ell > 1$ páratlan, akkor $g^\ell \neq 1$, de van legalább $\ell + 1 \geqslant 4$ fixpontja, ami megint ellentmondás.
Mivel τ 7 elemen hat, és csupa páros ciklusból áll, τ-nak van fixpontja, így g^2-nek van négy, tehát $g^2 = 1$, és ugyanígy $h^2 = 1$. Ebből következik, hogy τ és π is másodrendűek.
$\tau, \pi \notin P = C_{S_7}(P)$, így $g, h \notin C_G(P)$.

$$N_G(P)/C_G(P) \lesssim Aut C_7 \cong C_6 \ \ (\text{ld. } 5.8,\ 1.11)$$

C_6-ban csak egy másodrendű elem van $\Longrightarrow$ $gh = gh^{-1} \in C_G(P) \Longrightarrow \tau\pi \in C_{S_7}(P) = P \Longrightarrow o(\tau\pi) = 1$ vagy 7. Tudjuk, hogy $\tau\pi \neq 1$, ha pedig $o(\tau\pi) = 7$, akkor $(gh)^7 = (\tau\pi)^7(8\ 9\ 10)^7 = (8\ 9\ 10) \neq 1$-nek pontosan 7 fixpontja lenne, ellentmondva a szigorú 4-tranzitivitásnak. □

6.16. Állítás. *Nem létezik $G \leqslant S_{13}$ szigorúan 6-tranzitív csoport.*

Bizonyítás. Tegyük fel, hogy van ilyen $G \leqslant S_{13}$. Ekkor $|G| = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.
A G 5-Sylowja, $P \in Syl_5(G)$ ciklikus, és a generátorelemének legfeljebb 5 fixpontja van, ezért feltehető, hogy $P = \langle(1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)\rangle$.
A 6.14 Lemma miatt $N_G(P)$ 3-tranzitívan hat a $\{11,\ 12,\ 13\}$ halmazon, ezért $\exists h = \sigma(11\ 12\ 13) \in N_G(P)$, ahol $\sigma \in N_{S_{10}}(P)$. Viszont $|N_{S_{10}}(P)| = 4 \cdot |C_{S_{10}}(P)| = 4 \cdot 2 \cdot 5^2 = 200$, tehát $h^{200} = \sigma^{200}(11\ 13\ 12) = (11\ 13\ 12)$-nek 10 fixpontja lenne, ami ellentmond a szigorú 6-tranzitivitásnak. □

Nem térünk ki annak a bizonyítására, hogy a Jordan-tételben szereplő 11-edfokú 4-tranzitív, illetve 12-edfokú 5-tranzitív csoportok valóban léteznek, és izomorfia erejéig (sőt permutációcsoportok ekvivalenciája erejéig is) egyértelműek. Ezek az M_{11} és M_{12} *Mathieu-csoportok*.

6.17. Tétel. *Az M_{11} és M_{12} csoportok egyszerűek.*

Bizonyítás. Legyen $G \simeq M_{11}$, azaz $G \leqslant S_{11}$ szigorúan 4-tranzitív. Ekkor $|G| = 11 \cdot 10 \cdot 9 \cdot 8$.
Tegyük fel, hogy G nem egyszerű, azaz létezik egy $N \neq 1$ valódi normálosztója, és N minimális ilyen.
G 4-tranzitív $\Longrightarrow$ G primitív $\overset{6.5}{\Longrightarrow}$ N tranzitív $\Longrightarrow$ $11 \mid |N|$.
Legyen $P \in Syl_{11}(N)$. Feltehető, hogy $P = \langle(1\ 2\ 3\ \dots 10\ 11)\rangle$, és P nyilván G-nek is Sylow-részcsoportja.
Vegyük észre, hogy $C_{S_{11}}(P) = P$, így $P = C_N(P) = C_G(P)$ is teljesül. Továbbá

$$P \leqslant N_N(P) \leqslant N_G(P) \leqslant N_{S_{11}}(P), \qquad \text{ahol } \ N_{S_{11}}(P)/P \overset{5.8}{\lesssim} \mathrm{Aut}\, C_{11} \cong C_{10}.$$

Ha $N_N(P) = N_G(P)$,
akkor a Frattini-elv (4.7) szerint $G = N \cdot N_G(P) = N \cdot N_N(P) = N$, ellentmondás.
Ha $P = N_N(P)$,
akkor a Burnside-féle p-komplementumtétel (5.6) szerint $\exists K \lhd N$, hogy K komplementuma P-nek N-ben, azaz $K \in Hall_{11'}(N)$. De akkor $K \operatorname{char} N \lhd G \implies K \lhd G$, így N minimalitása miatt $K = 1$. Ebből következik, hogy $P = N \lhd G$, tehát $G \leqslant N_G(P)$, így $|G| = |N_G(P)| \leqslant |N_{S_{11}}(P)| \leqslant 10 \cdot 11$, ellentmondás.
Tehát

$$P < N_N(P) < N_G(P) \leqslant N_{S_{11}}(P),$$

s mivel $|N_{S_{11}}(P)/P|$ osztója 10-nek, ez csak úgy lehet, hogy $N_G(P) = N_{S_{11}}(P)$.
De akkor $(1\ 11)(2\ 10)\cdots(5\ 7)(6) \in N_{S_{11}}(P) \leqslant G$, holott a Jordan-tétel (6.12) bizonyítása során kiderült, hogy G-ben minden másodrendű elemnek pontosan 3 fixpontja van. Tehát ellentmondásra jutottunk abból a feltevésből, hogy G nem egyszerű.

Most legyen $G \simeq M_{12}$, azaz $G \leqslant S_{12}$ szigorúan 5-tranzitív csoport, és legyen $H \leqslant S_{11}$ az egyik stabilizátora. Ekkor H szigorúan 4-tranzitív, tehát a bizonyítás első része alapján H egyszerű csoport.
Tegyük fel, hogy $1 \neq N \lhd G$ minimális normálosztó. Ekkor $N \cap H \lhd H$, tehát H egyszerűsége miatt vagy $N \cap H = 1$, vagy $N \geqslant H$. Az első esetben $|N| \leqslant |G : H| = 12$, de G primitivitása miatt N tranzitív, így legalább 12-elemű, vagyis $|N| = 12$. De 12-elemű karakterisztikusan egyszerű csoport nem létezik (vagy a 3-Sylow, vagy a 2-Sylow karakterisztikus részcsoport benne), és ez ellentmond N minimalitásának. Ha viszont $N \geqslant H$, akkor $H \neq N$ következik például abból, hogy N tranzitív, tehát H maximalitása miatt $N = G$. □

7. Szabad csoportok

Egy X halmaz elemeiből mint *betűkből szavakat* képezünk a következő módon. Legyen $x^1 = x$, és legyen x^{-1} új jel minden $x \in X$-re. Egy $w = a_1 a_2 \dots a_n$ jelsorozat szó, ha minden i-re $a_i = x_i^{\varepsilon_i}$, ahol $x_i \in X$, és $\varepsilon_i = \pm 1$. Az üres szó jele 1. Ezek a szavak egységelemes félcsoportot alkotnak a szavak egymás után írására mint szorzásra nézve.

Legyen w és w' két szó ebből a félcsoportból. Azt mondjuk, hogy w és w' *szomszédosak*, ha vannak olyan u, v szavak, x betű, és $\varepsilon = \pm 1$, amelyekre $\{w, w'\} = \{ux^\varepsilon x^{-\varepsilon} v, uv\}$. A w és w' szavak *ekvivalensek* ($w \sim w'$), ha létezik szavaknak olyan $w = w_0, \dots, w_n = w'$ sorozata, amelyben w_i és w_{i+1} szomszédos minden i-re. A $\sim$ nyilván ekvivalenciareláció. Jelöljük w ekvivalenciaosztályát $[w]$-vel. Egy w szót *redukált szónak* hívunk, ha nincs benne $x^\varepsilon x^{-\varepsilon}$ alakú részszó.

7.1. Állítás. *Minden ekvivalenciaosztály egyetlen redukált szót tartalmaz.*

Bizonyítás. Először belátjuk, hogy a „balról jobbra redukálás" minden szóhoz egy egyértelmű, vele ekvivalens redukált szót rendel. Legyen $w = a_1 \dots a_n$, ahol $a_i = x_i^{\varepsilon_i}$. Definiáljuk w_i szomszédos szavak sorozatát a következő módon: $w_1 := a_1$, és ha $w_i = ux^\varepsilon$, akkor

$$w_{i+1} := \begin{cases} u & \text{ha } a_{i+1} = x^{-\varepsilon}, \\ ux^\varepsilon a_{i+1} & \text{különben.} \end{cases}$$

Ekkor $w_n \sim w$, és w_n redukált. Nevezzük az így kapott w_n szót $\operatorname{red}(w)$-nek. Az algoritmusból adódik, hogy $w_i = \operatorname{red}(a_1 \dots a_i)$ minden i-re.

Megmutatjuk, hogy szomszédos szavak redukáltja, és így az ekvivalens szavak redukáltja is megegyezik. Tekintsük a $w = ux^\varepsilon x^{-\varepsilon} v$ és $w' = uv$ szomszédos szavakat. Ha u hossza i, akkor $w_i = w'_i = \operatorname{red}(u)$.
Ha $\operatorname{red}(u) = rx^{-\varepsilon}$ valamilyen r szóra, akkor $w_{i+1} = \operatorname{red}(rx^{-\varepsilon}x^\varepsilon) = r$, és $w_{i+2} = \operatorname{red}(rx^{-\varepsilon})$. Viszont $rx^{-\varepsilon}$ a feltétel miatt redukált, így $w_{i+2} = rx^{-\varepsilon} = w'_i$, amiből $\operatorname{red}(w) = \operatorname{red}(w_{i+2}v) = \operatorname{red}(w'_i v) = \operatorname{red}(w')$.
Ha $w_i = \operatorname{red}(u)$ nem $rx^{-\varepsilon}$ alakú, akkor $w_{i+1} = \operatorname{red}(w_i x^\varepsilon) = w_i x^\varepsilon$, és $w_{i+2} = \operatorname{red}(w_i x^\varepsilon x^{-\varepsilon}) = w_i$. Ismét arra jutottunk, hogy $w_{i+2} = w'_i$, tehát $\operatorname{red}(w) = \operatorname{red}(w')$.

Végül vegyük észre, hogy a redukált szavakat változatlanul hagyja az előbbi algoritmus, tehát egy ekvivalenciaosztályban nem lehet két különböző redukált szó. □

7.2. Állítás. *Az X halmazból alkotott szavak ekvivalenciaosztályai csoportot alkotnak az $[u] \cdot [v] = [uv]$ szorzással.*

Bizonyítás. Elsőként megmutatjuk, hogy a szorzás jól van definiálva. Ha $u \sim u'$ és $v \sim v'$, akkor $\operatorname{red}(u) = \operatorname{red}(u')$ és $\operatorname{red}(v) = \operatorname{red}(v')$. Viszont egy szót egy részszavának redukálása is ekvivalens szóba visz, tehát $uv \sim \operatorname{red}(u)\operatorname{red}(v) = \operatorname{red}(u')\operatorname{red}(v') \sim u'v'$.

Az asszociativitás ezek után következik a szavak félcsoportjának asszociativitásából, az [1] nyilván egységelem, és egy $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ inverze $w' = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$, mivel $\operatorname{red}(ww') = \operatorname{red}(w'w) = 1$. □

Definíció. Az X által generált *szabad csoport* $F(X) = \{[w] \mid w \text{ szó az } X\text{-en}\}$. Tekinthetjük úgy is, hogy a szabad csoport elemei a redukált szavak, és az u, v redukált szavak szorzata $\operatorname{red}(uv)$. Így $F(X) = \langle X \rangle$.

Példa. Ha $X = \{x\}$, akkor $F(X) = \{1, x, x^{-1}, x^2, x^{-2}, \dots\} \cong C_\infty$.
Ha $X = \{x, y\}$, akkor $F(X) = \{x^{a_1} y^{b_1} \cdots x^{a_n} y^{b_n} \mid n \geqslant 1,\ a_1, b_n \in \mathbb{Z},\ a_2, \dots, a_n, b_1, \dots, b_{n-1} \in \mathbb{Z} \setminus \{0\}\}$.

7.3. Állítás. *Legyen G csoport és $\varphi : X \to G$ egy leképezés. Ekkor φ egyértelműen kiterjeszthető $F(X)$-ből G-be menő csoporthomomorfizmussá, azaz létezik egyetlen $\overline{\varphi} : F(X) \to G$ csoporthomomorfizmus úgy, hogy $\overline{\varphi}|_X = \varphi$.*

Bizonyítás. A szavakra kiterjesztett $(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})\overline{\varphi} := (x_1\varphi)^{\varepsilon_1} \dots (x_n\varphi)^{\varepsilon_n}$ leképezés szomszédosakat ugyanoda visz, és nyilván művelettartó, tehát indukál egy művelettartó leképezést a szavak ekvivalenciaosztályairól, amely kiterjesztése az X-en értelmezett φ leképezésnek. Mivel X generálja $F(X)$-et, a kiterjesztés egyértelmű. □

7.4. Állítás. *Az előző állításban leírt kiterjesztési tulajdonság izomorfia erejéig meghatározza az X generátorrendszerhez tartozó $F(X)$ szabad csoportot. Sőt, ha $|X| = |Y|$, akkor $F(X) \cong F(Y)$.*

Bizonyítás. Tegyük fel, hogy egy G csoport Y generátorrendszere azonos számosságú az X halmazzal, és G szintén kielégíti a 7.3 Állítás kiterjeszthetőségi feltételét az Y generátorrendszerre nézve. Legyen $\alpha : X \to Y$ egy bijekció. Ekkor α és α^{-1} is kiterjeszthető csoporthomomorfizmussá, azaz léteznek olyan $\varphi : F(X) \to G$, $\psi : G \to F(X)$ homomorfizmusok, amelyekre $\varphi|_X = \alpha$ és $\psi|_Y = \alpha^{-1}$. Mivel $\varphi\psi$ és $id_{F(X)}$ is az id_X kiterjesztése, a kiterjesztés egyértelműsége miatt $\varphi\psi = id_{F(X)}$, és ugyanígy $\psi\varphi = id_G$. Tehát $F(X) \cong G$, speciálisan, $F(X) \cong F(Y)$. □

Definíció. Legyen X a G csoport egy generátorrendszere. Azt mondjuk, hogy X szabadon generálja G-t, ha G az X részhalmazzal kielégíti a 7.3. Állításban megfogalmazott kiterjesztési tulajdonságot, vagy ami ezzel ekvivalens, az id_X leképezést kiterjesztő $F(X) \to G$ csoporthomomorfizmus izomorfizmus.

Definíció. $A(X) = \langle X \rangle$ az X halmaz által generált *szabad Abel-csoport*, ha minden B Abel-csoportra és a $\varphi : X \to B$ leképezésre létezik egyetlen $\overline{\varphi} : A(X) \to B$ csoporthomomorfizmus, amely kiterjesztése φ-nek.

7.5. Állítás. *$A(X) \cong F(X)/F(X)' \cong \prod_{x\in X} C_\infty$, ahol a szorzat a diszkrét direkt szorzatot jelenti.*

Bizonyítás. A 7.4. Állítás bizonyításához hasonlóan látható, hogy az $A(X)$ szabad Abel-csoport izomorfia erejéig (pontosabban X-et helyben hagyó izomorfia erejéig) egyértelmű. Tehát elég megmutatnunk, hogy $F(X)/F(X)'$ és $\prod_{x\in X} C_\infty$ is kielégíti az $A(X)$ definíciójában szereplő kiterjesztési tulajdonságot, ahol X-et azonosítjuk az $F(X)/F(X)'$ faktorcsoportbeli képével, illetve a direkt szorzatban az egyes komponensek egy-egy generátorából alkotott halmazzal.

Legyen $\varphi : X \to B$ egy tetszőleges Abel-csoportba menő leképezés. Ez a 7.3 Állítás miatt kiterjeszthető egy $\widetilde{\varphi} : F(X) \to B$ csoporthomomorfizmussá. Mivel $\mathrm{Im}(\widetilde{\varphi})$ Abel, $F(X)'$ benne van a leképezés magjában. Tehát $\widetilde{\varphi}$ definiál egy $\overline{\varphi} : F(X)/F(X)' \to B$ homomorfizmust. Ez a kiterjesztés egyértelmű, mivel X képe generálja az $F(X)/F(X)'$ csoportot.
Ha a_x-szel jelöljük az x. komponens generátorelemét a $G = \prod_{x\in X} C_\infty$ direkt szorzatban, akkor minden g elem egyértelműen írható $(\ldots, a_x^{n_x}, \ldots)$ alakban, tehát a $\widetilde{\varphi}(g) = \prod_{x\in X} \varphi(a_x)^{n_x}$ leképezés jól van definiálva, és nyilván művelettartó is. (A szorzat értelmezve van, mert a g előállításában csak véges sok komponens nem 1.) A kiterjesztés itt is egyértelmű, mert a g_x elemek generálják a G csoportot. □

7.6. Állítás. *Az X és Y halmazok által generált szabad csoportok pontosan akkor izomorfak, ha $|X| = |Y|$.*

Bizonyítás. A 7.4 Állításban már láttuk az egyik irányt. Most tegyük fel, hogy $F(X) \cong F(Y)$. Ekkor természetesen $A(X) \cong F(X)/F(X)' \cong F(Y)/F(Y)' \cong A(Y)$ is teljesül, azaz $\prod_{x\in X} C_\infty \cong \prod_{y\in Y} C_\infty$. Belátjuk, hogy ebből következik, hogy $|X| = |Y|$.
Tetszőleges B Abel-csoport esetén $B^2 = \{b^2\}_{b\in B} \lhd B$ és B/B^2 2-exponensű csoport lesz, azaz (multiplikatívan írt) $\mathbb{F}_2$ fölötti vektortér. Így a

$$\prod_{x\in X} C_2 \cong A(X)/A(X)^2 \cong A(Y)/A(Y)^2 \cong \prod_{y\in Y} C_2$$

izomorfiából azt kapjuk, hogy

$$|X| = \dim_{\mathbb{F}_2}(A(X)/A(X)^2) = \dim_{\mathbb{F}_2}(A(Y)/A(Y)^2) = |Y|.$$

□

Definíció. Az X által generált szabad csoport *rang*ja $|X|$.

7.1. Definiáló relációk

Definíció. Legyen $G = \langle g_1, \ldots, g_n \rangle$ végesen generált csoport és $F(X)$ az $X = \{x_1, \ldots, x_n\}$ által generált szabad csoport. Ekkor létezik egyetlen $\varphi : F(X) \to G$ leképezés, amely az $x_i \to g_i$ kiterjesztése. Jelöljük N-nel a leképezés magját és a magnak mint normálosztónak a generátorait r_i-vel. ($Ker(\varphi) = N = \langle r_1, r_2, \ldots \rangle_\lhd$ az r_i-k összes konjugáltja által generált részcsoport.) Így

$$G \cong \langle x_1, \ldots, x_n \mid r_1 = 1, r_2 = 1, \ldots \rangle.$$

Az r_i-ket a G csoport *definiáló relációi*nak nevezzük.

Példa. $C_n \cong \langle x \mid x^n = 1\rangle$

7.7. Tétel (Dyck). *Legyen $G = \langle x_1, \dots, x_n \mid r_1 = 1, r_2 = 1, \dots\rangle$ és $H = \langle h_1, \dots, h_n\rangle$. Ha minden r_j-ben az x_i-ket h_i-kkel helyettesítve a H egységelemét kapjuk, akkor G-nek H homomorf képe.*

Bizonyítás. Legyen a $\varphi: F(X) \to H$ homomorfizmus az $x_i \mapsto h_i$ leképezés egyértelmű kiterjesztése, ahol $X = \{x_1, \dots, x_n\}$, és N az r_i-k által generált normálosztó $F(X)$-ben, azaz $G = F(X)/N$. A feltétel szerint φ minden r_j-t az egységelembe képez, ezért $N = \langle r_1, r_2, \dots\rangle_\lhd \leqslant \operatorname{Ker}(\varphi)$. Tehát

$$H \cong F(X)/\operatorname{Ker}(\varphi) \cong F(X)/N \Big/ \operatorname{Ker}(\varphi)/N = G \Big/ \operatorname{Ker}(\varphi)/N.$$

□

Feladat. Bizonyítsuk be, hogy $G = \langle x, y \mid x^2 = 1,\ y^4 = 1,\ xyx = y^{-1}\rangle \cong D_4$.
Megoldás: Legyen $D_4 = \langle f, t\rangle = \{1, f, f^2, f^3, t, tf, tf^2, tf^3\}$, ahol f a 90° fokos forgatás, és t az egyik tükrözés. A (7.7) Dyck tételt alkalmazhatjuk, hiszen x helyére t-t, y helyére f-et helyettesítve a relációkban 1-et kapunk. Így létezik $\varphi: G \to D_4$ szürjektív leképezés.
Megmutatjuk, hogy $|G| \leqslant |D_4|$, tehát φ csak izomorfizmus lehet. Az $\langle y\rangle$ részcsoport normálosztó G-ben, mivel $y^x = x^{-1}yx \overset{x^2=1}{=} xyx = y^{-1}$ miatt $x \in N_G(\langle y\rangle)$, y pedig nyilván normalizálja $\langle y\rangle$-t. Következésképpen

$$|G| = |\langle x, y\rangle| = |\langle x\rangle\langle y\rangle| \leq |\langle x\rangle| \cdot |\langle y\rangle|,$$

és az utóbbi legfeljebb 8 az $x^2 = 1$ és $y^4 = 1$ feltételek miatt.

7.2. Nielsen–Schreier-tétel

7.8. Tétel (Nielsen-Schreier). *Szabad csoport részcsoportja is szabad.*

Definíció. Egy G csoporthoz és adott X generátorrendszeréhez tartozó $\Gamma(G, X)$ *Cayley-gráf* csúcshalmaza $V(\Gamma(G, X)) = G$, élei pedig $E(\Gamma(G, X)) = \{(g, xg) \mid x \in X, g \in G\}$.

A $\Gamma(G, X)$-et tekinthetjük egy X elemeivel színezett irányított gráfnak, ahol $g \xrightarrow{x} xg$. Mivel X generátorrendszere G-nek, a gráf összefüggő, és minden csúcsból pontosan egy x színű él indul, és pontosan egy x színű él érkezik bele. Jelöljük $\operatorname{Aut}_c(\Gamma(G, X))$-szel a Cayley-gráf színezéstartó automorfizmusainak a csoportját.

7.9. Állítás. $G \cong \operatorname{Aut}_c(\Gamma(G, X))$.

Bizonyítás. Tetszőleges $g \in G$ elemnek feleltessük meg a $\varphi_g : h \mapsto hg$ permutációt G-n, azaz a g-vel való jobbszorzást. A $\psi : g \mapsto \varphi_g$ leképezés nyilvánvalóan injektív csoporthomomorfizmus G-ből az S_G szimmetrikus csoportba. Az alábbi ábra mutatja, hogy φ_g a gráf éleit ugyanolyan színű élekbe képezi, s mivel φ_g inverze, $\varphi_{g^{-1}}$ is ilyen tulajdonságú, φ_g a nem-éleket pedig nem-élekbe viszi, azaz $G \cong \operatorname{Im}\psi \leq \operatorname{Aut}_c(\Gamma(G, X))$.

$$\begin{array}{ccc} h & \xrightarrow{x} & xh \\ \downarrow{\scriptstyle \varphi_g} & & \downarrow{\scriptstyle \varphi_g} \\ hg & \xrightarrow{x} & xhg \end{array}$$

A szürjektivitás bizonyításához vegyük észre, hogy $\operatorname{Aut}_c(\Gamma(G, X))$ minden nem triviális eleme fixpontmentes, ugyanis ha egy gráfhomomorfizmus helyben hagy egy csúcsot, akkor a vele szomszédosakat is helyben kell hagynia (adott színű be-élből és ki-élből is csak egy van), tehát az összefüggő $\Gamma(G, X)$ gráf minden csúcsa helyben marad. Legyen most $\varphi \in \operatorname{Aut}_c(\Gamma(G, X))$ és $g = 1\varphi$. Ekkor 1 fixpontja a $\varphi\varphi_g^{-1}$ automorfizmusnak, így $\varphi\varphi_g^{-1} = 1$, azaz $\varphi = \varphi_g$. □

7.10. Lemma. *G-t akkor és csak akkor generálja szabadon az X részhalmaz, ha $\Gamma(G, X)$ fa.*

Bizonyítás. Egyrészt X pontosan akkor generátorrendszer, ha $\Gamma(G,X)$ összefüggő. Másrészt ha X generátorrendszer, akkor

a Cayley-gráfban létezik kör
$\iff \exists\, a \in G$, hogy $x_n^{\varepsilon_n} \dots x_1^{\varepsilon_1} a = a$ valamely X-beli betűkből álló $x_n^{\varepsilon_n} \dots x_1^{\varepsilon_1}$ nem üres redukált szóra
$\iff$ van olyan nem üres redukált szó az X elemeiből mint betűkből, amely G-ben 1-gyel egyenlő
$\iff$ X nem szabad generátorrendszere G-nek.

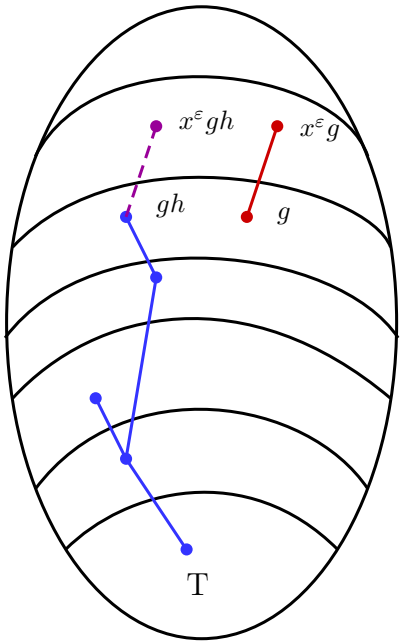
Tehát G-t pontosan akkor generálja szabadon az X, ha a $\Gamma(G,X)$ Cayley-gráf összefüggő és körmentes, azaz fa. □

Bizonyítás. (a Nielsen-Schreier-tétel (7.8) bizonyítása)
Legyen G az X által generált szabad csoport és $H \leqslant G$. Az előző Lemma szerint ez fa, és azt kell megmutatnunk, hogy H-nak is van olyan Cayley-gráfja, amelyik fa. Tekintsük a Γ azon összefüggő feszített részgráfjainak S halmazát, amelyek a H minden mellékosztályából legfeljebb egy elemet tartalmaznak.

Zorn-lemma Ha egy részben rendezett, nem üres S halmazban minden teljesen rendezett részhalmaznak van felső korlátja S-ben, akkor S-ben van maximális elem.

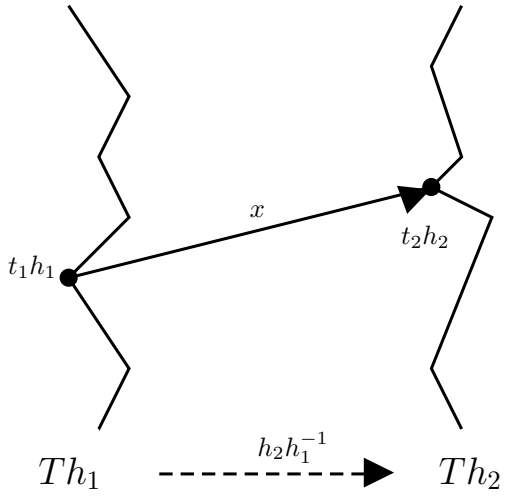
A Zorn-lemma miatt S-nek van a tartalmazásra nézve maximális eleme, ha ugyanis vesszük ilyen részgráfok teljesen rendezett halmazát, azok uniója is S-ben van: az unió két tetszőleges elemét tartalmazó S-beli gráfok közül a bővebbikben össze lehet kötni a két pontot, így az unióban is, és ha ezek egy H-mellékosztályban lennének, akkor már a nagyobbik S-beli gráf is több pontban metszette volna az adott mellékosztályt. Legyen ez a maximális részgráf T.

A T részgráf alaphalmaza transzverzálisa H-nak, azaz H minden mellékosztályát egyetlen elemben metszi. Ha ugyanis lenne olyan mellékosztály, amit T nem ér el, akkor Γ összefüggősége miatt lenne olyan is, amelyet elér, de egy vele éllel összekötött másik mellékosztályt nem: $(g, x^\varepsilon g)$ él, és van olyan $h \in H$, amelyre $gh \in T$. De akkor $(gh, x^\varepsilon gh)$ is él, és így kibővíthetnénk a T gráfot. Feltehetjük azt is, hogy T tartalmazza az 1-et, mert ha H-ból a h elemet tartalmazza, akkor vehetjük helyette a Th^{-1} vele izomorf, ugyanolyan tulajdonságú részgráfot. Tekintsük a T eltoltjait: $\mathcal{T} = \{Th \,|\, h \in H\}$. Ezek diszjunkt transzverzálisai a H-nak, amelyek lefedik G-t; a Th transzverzálisok által kifeszített részgráfok egymással izomorf fák; és Th egyetlen H-beli eleme h, vagyis a $h \mapsto Th$ természetes bijekció H és $\mathcal{T}$ között.



A $\mathcal{T}$ alaphalmazon definiálhatunk egy irányított, H-beli elemekkel színezett részgráfot. Ehhez vegyük észre először, hogy $h_1 \neq h_2$-re legfeljebb egy olyan éle van Γ-nak, amely Th_1 és Th_2 valamelyik pontját köti össze egymással valamilyen irányban. Ha ugyanis lenne két ilyen él is, akkor azt az összefüggő Th_1-ben és Th_2-ben menő utakkal Γ-beli körré egészíthetnénk ki.

Ha egy x színű élre $x(t_1h_1) = t_2h_2$, azaz $t_2^{-1}xt_1 = h_2h_1^{-1}$, akkor legyen (Th_1, Th_2) él, $h_2h_1^{-1} \in H$ színnel színezve.

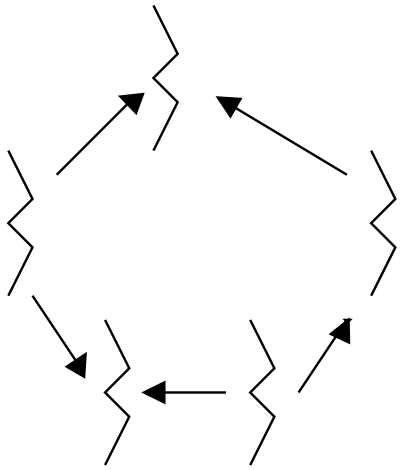


Az így kapott színek halmazát jelöljük Y-nal. Ekkor

$$\Gamma(H, Y) \cong \mathcal{T}$$

a $h \mapsto Th$ megfeleltetéssel. Ha ugyanis $t_2^{-1}xt_1 = h_2h_1^{-1} \in Y$, akkor tetszőleges $h \in H$-ra $(h_2h_1^{-1})h = (t_2^{-1}xt_1)h = t_2^{-1}x(t_1h)$, azaz $x(t_1h) = t_2(h_2h_1^{-1}h) \in Th_2h_1^{-1}h$, ezért Th-ból $Th_2h_1^{-1}h$-ba is megy $h_2h_1^{-1}$ színű él.

A $\mathcal{T}$ gráf összefüggő, mert Γ is az, és fa, ugyanis ha lenne benne kör, akkor a $\mathcal{T}$ elemei között menő éleket kiegészítve a transzverzálisokon belül menő utakkal, Γ-ban is kört kapnánk.



Ebből következik, hogy Y szabadon generálja a H részcsoportot. □

Tárgymutató

k-tranzitív, 30

AGL, 30

blokk, 31
Burnside-lemma, 8

Cayley-gráf, 40
centrállánc, 19
csoporthatás, 8
    hűséges, 8

definiáló relációk, 39
direkt szorzat, 2
direkt szorzat, diszkrét, 2
Dyck-tétel, 40

elemi Abel p-csoport, 15
extraspeciális p-csoport, 23

felcserélhető részcsoportok, 16
feloldható csoport, 14
feloldhatósági hossz, 14
felső centrállánc, 19
ferde kommutátorlánc, 19
fixpont, 8
Frattini-elv, 20
Frattini-részcsoport, 21

GL, 30

Hall-részcsoport, 16
Hall-tételek, 18
Hamilton-csoport, 23

imprimitív, 31
invariáns partíció, 31

Jordan-tétel, 34

karakterisztikus részcsoport, 13
karakterisztikusan egyszerű, 15
kiterjesztési tulajdonság, 38
kommutátor, 13
kommutátor-részcsoport, 13
kommutátorlánc, 14
komplementum, 4
koszorúszorzat, 33
Krull–Schmidt-tétel, 2
kvaterniócsoport, 4

Mathieu-csoportok, 36
metaciklikus, 28

Nielsen–Schreier-tétel, 40

nilpotenciaosztály, 19
nilpotens csoport, 19
normállánc, 14

orbit, 8

permutációcsoport, 8
PGL, 31
primitív, 31
PSL, 31

redukált szó, 38
reguláris, 33

Schur–Zassenhaus-tétel, 21
    Abel normálosztóval, 4
Schur-tétel, 27
SL, 31
stabilizátor, 8
    elemenkénti, 30
    halmaz-, 30
Sylow-bázis, 16
szabad Abel-csoport, 39
szabad csoport, 38
szemidirekt szorzat, belső, 3
szemidirekt szorzat, külső, 3
szigorúan k-tranzitív, 33
szimmetrikus csoport, 8

transzfer, 26