13. tétel — Csoportelmélet

Csoport fogalma

Definíció: Csoport egy olyan $(G, \cdot)$ struktúra, ahol a $\cdot : G \times G \to G$ kétváltozós művelet asszociatív, van egységelem és inverz. Azaz:

$$\begin{aligned}
&(\mathrm{G1}) && \forall a,b,c \in G: && a \cdot (b \cdot c) = (a \cdot b) \cdot c \\
&(\mathrm{G2}) && \exists e \in G\, \forall a \in G: && e \cdot a = a \cdot e = a \\
&(\mathrm{G3}) && \forall a \in G\, \exists a' \in G: && a' \cdot a = a \cdot a' = e
\end{aligned}$$

Az a elem inverzét a^{-1} jelöli. Az egységelemet gyakran 1.

Definíció: A G csoport kommutatív, ha $\forall a,b \in G : a \cdot b = b \cdot a$. Ilyenkor gyakran $+$ szimbólummal jelöljük a műveletet, 0-val az egységelemet (melyet esetleg neutrális elemnek hívunk, hogy nehogy magyarul legyen) és $-a$-val az a elem inverzelemét. A kommutatív csoportokat Abel-féle vagy Abel-csoportok névvel is illethetjük (szoktuk is).

Egyszerűsítési szabály: Ha $ax = ay$ vagy $xa = ya$, akkor $x = y$. Ez minden csoportban teljesül; véges elemszám esetén – az asszociativitást feltéve – elegendő is ahhoz, hogy a csoportaxiómák teljesüljenek.

További ekvivalens megfogalmazások arra, hogy egy asszociatív művelet csoportot eredményezzen:

- $\forall a,b \in G\, \exists! x,y \in G:\ xa = ay = b$;
- $\forall a,b \in G\, \exists\, x,y \in G:\ xa = ay = b$;
- létezzen baloldali egységelem és ehhez minden elemnek létezzen balinverze (balegység és jobbinverz nem elég, pl. $xy := y$ nem ad csoportot, ha legalább kételemű az alaphalmaz).

Definíciók, jelölések

$|G|$ – A G csoport *rendje* — alaphalmazának elemszáma.

a^n – Az $a \in G$ elem $n \in \mathbf{N}$-edik *hatványa* — $n = 0$-ra az egységelem, $n > 0$ esetén az n-tényezős $a \cdot a \cdot \ldots \cdot a$ szorzat, $n < 0$-ra $(a^n)^{-1}$ avagy $\left(a^{-1}\right)$.

$o(a)$ – Az $a \in G$ elem *rendje* — az a legkisebb r pozitív egész szám, melyre $a^r = 1$; ha nincs ilyen r, akkor ∞.

p-csoport egy olyan csoport, melyben minden elem rendje az adott p prím hatványa.

komplexus A G csoportban — ez alatt azt értjük, hogy a csoport egy részhalmaza.

$K \cdot L$ – *Komplexusszorzat* — $\{k \cdot l \in G \mid k \in K, l \in L\}$, ahol $K, L \subseteq G$ komplexusok (a komplexusszorzás mindig asszociatív, kommutatív csoportban kommutatív is).

K^{-1} – a $K \subseteq G$ *komplexus inverze* — $\left\{k^{-1} \in G \mid k \in K\right\}$.

$H \leq G$ – A $\emptyset \neq H \subseteq G$ komplexus *részcsoportot* alkot G-ben — ez azt jelenti, hogy a G feletti művelet megszorításával a H halmaz csoportot alkot. Persze elég hogy zárt legyen a műveletekre, legkényelmesebb ekvivalens megfogalmazásai: $\left(HH \subseteq H, H^{-1} \subseteq H\right)$, illetve $HH^{-1} \subseteq H$.

aH, Ha – A $H \leq G$ részcsoport bal (jobb) oldali *mellékosztályai* — az $\{a\} \cdot H = \{a \cdot h \in G \mid h \in H\}$ $(\ldots)$ komplexusok. Ezek a csoport partícióját adják.

$|G : H|$ – A $H \leq G$ részcsoport *indexe* — a (pl. bal oldali) mellékosztályok halmazának számossága (egyes elvetemültek a $[G : H]$ jelölés szándékos alkalmazásától sem riadnak vissza).

$\langle X \rangle$ – Az $X \subseteq G$ komplexus által *generált részcsoport* — a (halmazelméleti tartalmazásra nézve) legszűkebb olyan $H \leq G$ részcsoport, amely tartalmazza X-et.

Z_n, Z_∞ n-edrendű illetve végtelen *ciklikus csoport* — olyan csoport, amit egyetlen elem generál, melynek rendje n illetve ∞.

Homomorfizmus a $G, \overline{G}$ csoportok közt — egy olyan $\varphi : G \to \overline{G}$ leképezés, amely művelettartó, azaz $\forall a, b \in G: \ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ (ebből már következik $\varphi(1_G) = 1_{\overline{G}}$ és $\forall a \in G: \ \varphi(a^{-1}) = \big(\varphi(a)\big)^{-1}$).

$Im\,\varphi$ – A $\varphi : G \to \overline{G}$ homomorfizmus *képe* — $\big\{\varphi(a) \in \overline{G} \mid a \in G\big\}$, mely **részcsoport** $\overline{G}$-ben.

$Ker\,\varphi$ – A $\varphi : G \to \overline{G}$ homomorfizmus *magja* — $\big\{a \in G \mid \varphi(a) = 1_{\overline{G}}\big\}$, mely **normálosztó** G-ben.

$\varphi : G \xrightarrow{\sim} \overline{G}$ — A $G, \overline{G}$ csoportok közti izomorfizmus — olyan $\varphi : G \to \overline{G}$ homomorfizmus, amely teljesíti a következő ekvivalens feltételeket:

(1) kölcsönösen egyértelmű;

(2) kölcsönösen egyértelmű és (halmazelméleti) inverze egy $\overline{G} \to G$ homomorfizmus;

(3) $Ker\,\varphi = \{1_G\}$ és $Im\,\varphi = \overline{G}$.

$G \underset{\varphi}{\simeq} \overline{G}$ – A G és $\overline{G}$ csoportok (a φ leképezéssel megadottan) *izomorfak* — létezik $\varphi : G \xrightarrow{\sim} \overline{G}$ izomorfizmus (illetve φ ilyen).

Homomorf képe a $\overline{G}$ csoport a G csoportnak — ha létezik $\varphi : G \to \overline{G}$ homomorfizmus, hogy $Im\,\varphi = \overline{G}$.

Endomorfizmus a G csoportban — $\varphi : G \to G$ homomorfizmus.

Automorfizmus a G csoportban — $\varphi : G \to G$ izomorfizmus.

$Aut\,G$ – A G csoport *automorfizmus-csoportja* — az összes $G \to G$ automorfizmusok csoportja a kompozíció műveletével (egységelem az identikus leképezés).

a^x – Az $a \in G$ elem $x \in G$-vel vett *konjugáltja* — $x^{-1}ax$, egyesek szerint xax^{-1}.

φ_x – Az $x \in G$ elemmel való *konjugálás*, más néven az x-hez tartozó *belső automorfizmus* — tehát a $\varphi_x : G \to G, \ a \mapsto a^x$ leképezés.

a^φ – Az $a \in G$ *elem képe* a $\varphi \in Aut\,G$ automorfizmusnál — (ez a jelölés néhány további jelölést leegyszerűsít majd, mellesleg így $a^x = a^{\varphi_x}$).

K^x, K^φ – A $K \subseteq G$ *komplexus képe* az $x \in G$ elemmel való konjugálásnál, illetve az $\varphi \in Aut\,G$ automorfizmusnál.

$Inn\,G$ – A G csoport *belső automorfizmus-csoportja* — G összes belső automorfizmusának halmaza, mely $Aut\,G$-nek részcsoportját, sőt, **normálosztóját** adja.

$[a]$ – Az $a \in G$ elem *konjugált osztálya* — $\{a^x \in G \mid x \in G\}$ (a konjugált osztályok a csoport egy partícióját adják).

$N \lhd G$ – Az $N \leq G$ részcsoport *normálosztó* — teljesülnek rá az alábbi ekvivalens feltételek.

(1) Bármely elemének bármely G-beli elemmel vett konjugáltját is tartalmazza, azaz $\forall a \in N, x \in G: \ x^{-1}ax \in N$;

(2) N bal- és jobboldali mellékosztályai ugyanazt a partíciót adják G-ben;

(3) $\forall x \in G: \quad N^x = N$ (avagy $\ldots \subseteq N$);

(4) $\forall \varphi \in Inn\,G: \quad N^\varphi = N$ (avagy $\ldots \subseteq N$);

(5) $\exists \overline{G}$ csoport és $\exists \varphi : G \to \overline{G}$ homomorfizmus, hogy $N = Ker\,\varphi$;

(6) $\exists X \subseteq G, \ \langle X \rangle = G \ \forall x \in X: \quad N^x = N$;

(7) $\exists X \subseteq G, \ \langle X \rangle = G \ \forall x \in X \cup X^{-1}: \quad N^x \subseteq N$;

(8) $\exists X, Y \subseteq G, \ \langle X \rangle = G, \ \langle Y \rangle = N \ \forall x \in X \cup X^{-1} \ \forall a \in Y: \quad a^x \in N$.
Például egy Abel-csoportban minden részcsoport normálosztó.

Egyszerű csoport alatt olyan $G \neq \{1\}$ csoportot értünk, melynek csak triviális normálosztói vannak ($\{1\}$ és G). Mint tudjuk, bonyolultak.

G/N – A G csoport $N \lhd G$ normálosztó szerinti *faktorcsoportja* — az a csoport, melynek elemei az N szerinti mellékosztályok, a művelet pedig a komplexusszorzás, ami szerencsére átírható $aN \cdot bN = abN$ alakba, mert $Nb = bN$ a normálosztó definíciója alapján.

ψ_N – A G/N faktorcsoportba menő *természetes homomorfizmus* — a $\psi_N : G \to G/N, \ a \mapsto aN$ leképezés.

a^S – Az $a \in G$ elem *S-orbitja*, ahol $S \leq G$ vagy $S \leq Aut\, G$ — $\{a^s \in G \mid s \in S\}$. (A jelölést esetleg olyankor is használjuk, ha S csak komplexus, az elnevezést már kevésbé.)

H^S – A $H \leq G$ részcsoport *S-konjugáltjai által generált részcsoport*, ahol $S \leq G$ vagy $S \leq Aut\, G$ — $\langle a^s \in G \mid a \in H, s \in S \rangle$ (esetleg itt is lehet S csak komplexus).

H^G, $\langle X \rangle^G$ – A $H \leq G$ részcsoport avagy $X \subseteq G$ komplexus által *generált normálosztó* — a legszűkebb normálosztó, amely tartalmazza H-t (X-et), ez éppen $\langle a^x \in G \mid a \in H\ (X), x \in G \rangle$. Akkor fontos, amikor generátorokkal és relációkkal adunk meg csoportokat.

Normállánc a G csoportban — egy $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$ alakú sorozat. Egy normállánc *faktorai* a G_i/G_{i+1} faktorcsoportok.

Kompozíciólánc egy olyan normállánc, mely nem finomítható (nem lehet elemeket közbeszúrni úgy, hogy normállán maradjon). Másképp: amelynek faktorai egyszerű csoportok.

Feloldható csoport — van olyan normállánca, melynek faktorai kommutatívak.

Invariáns lánc egy olyan normállánc, melynek elemei G-ben nemcsak részcsoportok, hanem normálosztók is. (*Szuperfeloldható* egy csoport, ha van olyan invariáns lánca, melynek faktorai kommutatívak.)

$H \underset{char}{\lhd} G$ – *H karakterisztikus részcsoport G-ben* — (részcsoport és) minden $\sigma \in Aut\, G$ automorfizmus önmagába viszi, azaz $H^{Aut\, G} = H$. (Normálosztó akkor volt, ha $H^{Inn\, G} = H$. Szokták a $H\, char G$ is jelölést is használni.

Felcserélhetőek az $a, b \in G$ elemek, ha $ab = ba$ — ez evkivalens azzal, hogy $a^b = a$.

$[a, b]$ – Az $a, b \in G$ elemek *kommutátora* — $[a, b] = [ab] = a^{-1}b^{-1}ab = a^{-1}a^b$. Arról ismerszik meg, hogy $ab = ba[ab]$. Pontosan akkor 1, ha a és b felcserélhetőek.

$[a_1, a_2, \ldots, a_k]$ – *Többszörös kommutátor*, a hiányzó zárójeleket balról kell pótolni — $[a_1, a_2, \ldots, a_k] = \big[[a_1, a_2], a_3, \ldots, a_k\big] = \ldots = \Big[\big[[a_1, a_2], a_3 \ldots\big], a_k\Big]$

$[H, K]$ – A *H, K komplexusok kommutátora* — az elkészíthető kommutátorok által generált részcsoport, azaz $\langle [h, k] \mid h \in H, k \in K \rangle$.

$[H_1, H_2, \ldots, H_k]$ – *Komplexusok többszörös kommutátora* – az, ami logikus: $\{[h_1, \ldots, h_k] \mid \ldots\}$.

$Z(G)$ – A G csoport *centruma* — a mindennel felcserélhető elemek halmaza, azaz $Z(G) = \{a \in G \mid \forall x \in G a^x = a\}$. Tehát $Z(G)$ az egyelemű konjugált-osztályok uniója.

$C_G(a)$ – Az $a \in G$ elem *centralizátora* — azon G-beli elemek halmaza, melyekkel a felcserélhető, $C_G(a) \leq G$.

$N_G(H)$ – Az $H \leq G$ részcsoport *normalizátora* — azon $x \in G$ elemek halmaza, melyekre $H^x = H$; $N_G(H) \leq G$.

$Z_r(G)$ – A G csoport *r-edrendű centruma* — rekurzívan definiált sorozat: $Z_1(G) = Z(G)$, majd $Z_r(G) = \psi^{-1}_{Z_{r-1}(G)}\big(Z(G/Z_{r-1}(G))\big)$, másképp fogalmazva azon G-beli elemek halmaza, melyeket bármely G-beli elemmel összekommutálva Z_{r-1}-beli az eredmény: $Z_r(G) = \{a \in G \mid \forall x \in G :\ [a, x] \in Z_{r-1}(G)\}$. A $Z_0(G) = \{1\} \subseteq Z(G) \subseteq Z_2(G) \subseteq \ldots$ sorozat a G felső centrális lánca, $Z_r(G) \lhd G$.

G^r – (nem tudom a nevét…) — mivel felesleges lenne a komplexusszorzatot jelölni így, ez inkább a $G = G^1 \geq G^2 \geq \ldots$ alsó centrális sorozat r-edik eleme, ahol $G^r = [G^{r-1}, G] = [G, G, \ldots, G]$ az r-szeres kommutátorok által generált részcsoport. $G^r \underset{char}{\lhd} G$.

G' – A G csoport *kommutátor-részcsoportja* avagy *derivált csoportja* — $G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle$.

$G^{(r)}$ – A G csoport *és r-edik derivált csoportja* — $G^{(1)} = G'$, $G^{(r)} = [G^{(r-1)}, G^{(r-1)}]$. $G \geq G' \geq G'' \geq \ldots$ a G derivált lánca, $G^{(r)} \underset{char}{\lhd} G$.

$d(G)$ – a G csoport *feloldható hossza* — amennyiben van olyan $r \in \mathbf{N}$, hogy $G^{(r)} = 1$, akkor a legkisebb ilyen szám; különben nem értelmezzük.

$S(\Omega)$ – Az Ω halmaz feletti *szimmetrikus csoport* — az összes $\Omega \to \Omega$ permutációk (kölcsönöses

egyértelmű leképezések) halmaza, a művelet a kompozíció, az egységelem az identitás.

$A(\Omega)$ – Az Ω véges halmaz feletti *alternáló csoport* — az összes $\Omega \to \Omega$ páros permutációk (amelyek páros sok permutáció szorzataként állnak elő) csoportja.

$G(\Omega)$ – *Permutációcsoport* az Ω halmaz felett — az $S(\Omega)$ részcsoportja. Pl. $(Aut\, G)(G)$ is permutációcsoport. Egy permutációcsoport foka $|\Omega|$.

S_n, A_n – Az *n-edfokú szimmetrikus és alternáló csoport.*

ω^g – az $\omega \in \Omega$ elem képe a $g \in G$ leképezésnél — ez is azért, hogy néhány későbbi jelölés egyszerűbb lehessen.

$G(\Omega) \underset{\psi}{\simeq} G'(\Omega')$ – a két permutációcsoport *izomorf* a $\psi : \Omega \to \Omega'$ leképezésre nézve — ψ izomorfizmust indukál a megadott csoportok közt, azaz $G'(\Omega') = \{\psi \circ g \circ \psi^{-1} \mid g \in G\}$.

ω^G – az $\omega \in \Omega$ elem *orbitja* — $\{\omega^g \mid g \in G\}$. Beszélhetünk néha H-orbitról is. Az orbitok az Ω partícióját adják.

Tranzitív egy $G(\Omega)$ permutációcsoport, ha Ω egyetlen orbitból áll, azaz $\forall \omega, \omega' \in \Omega\ \exists g \in G :\ \omega^g = \omega'$.

Δ^g, Δ^H – a $\Delta \subseteq \Omega$ részhalmaz *képe, H-orbitja.*

G_ω – az $\omega \in \Omega$ elem *stabilizátora* — azon G-elemek halmaza, melyek fixen hagyják ω-t, azaz $G_\omega = \{g \in G \mid \omega^g = \omega\}$.

Reguláris egy $G(\Omega)$ permutációcsoport, ha minden stabilizátor egyelemű, azaz $g \neq 1$ mindig fixpontmentes.

Δ *IPT* – a $\Delta \subseteq \Omega$ nemüres halmaz *imprimitivitási tartomány* — ha Δ képei az Ω partícióját adják (ehhez a csoport tranzitív kell legyen). Egy *IPT* nemtriviális, ha nem egyelemű és nem a teljes Ω. $G(\Omega)$ *imprimitív*, ha van ilyen.

G_Δ – az $\Delta \subseteq \Omega$ *IPT stabilizátora* — $G_\Delta = \{g \in G \mid \Delta^g = \Delta\}$.

Reprezentáció a G csoport homomorfizmusa egy permutációcsoportba, illetve ezen homomorfizmus képe.

Részcsoport, normálosztó, homomorfizus

Állítás: Az $a, b \in G$ elemek pontosan akkor tartoznak ugyanabba a $H \leq G$ szerinti bal (jobb) oldali mellékosztályba, ha $a^{-1}b \in H$ ($ab^{-1} \in H$).

Következmény: Egy elem konjugált osztályának mérete a centralizátorának indexe $\big|[a]\big| = \big|G : C_G(a)\big|$. (Ez többek közt azért fontos, mert a Wedderburn-tétel Witt-féle bizonyítása használja.) Hasonlóan a $H \leq G$ részcsoport különböző konjugáltjainak száma $\big|G : N_G(a)\big|$.

Lagrange-tétel: $|G| = |H| \cdot |G : H|$, ha $H \leq G$.

Következmény: Ha H a G véges csoport részcsoportja, akkor $|H| \,\Big|\, |G|$. Speciálisan, mivel $o(a) = |\langle a \rangle|$, $o(a) \,\Big|\, |G|$.

Állítás: Ha $K \leq H \leq G$, akkor $|G : K| = |G : H| \cdot |H : K|$.

Megjegyzés: Részcsoportok metszete részcsoport, ezért értelmes a generált részcsoport fogalma. Ez persze nem más, mint a generátorrendszer elemeiből képzett véges kifejezések (lehetséges értékeinek, ha nagyon precízek akarunnk lenni) halmaza, ahol a felhasználható műveletek a szorzás és az inverzképzés (avagy a szorzás és a hatványozás, hogy áttekinthetőb legyen).

Állítás: Normálosztók metszete normálosztó, ezért értelmes a generált normálosztó fogalma. Ez nem más, mint a generátorrendszer elemeinek tetszőleges konjugáltjaiból képzett véges kifejezések halmaza.

Állítás: A $H \leq G$ részcsoport által tartalmazott normálosztók közt van legbővebb, mégpedig $\bigcap\limits_{x \in G} H^x$.

Homomorfizmus-tétel: Ha $\varphi : G \to \ldots$ homomorfizmus, akkor $Ker\, \varphi \lhd G$ és $Im\, \varphi \simeq {}^{G}\!/_{Ker\, \varphi}$.

Megjegyzés: A $H, K \leq G$ részcsoportok komplexusszorzata pontosan akkor részcsoport, ha $HK = KH$. Speciálisan ha $N \lhd G$, akkor $\langle H, N \rangle = HN = NH \leq G$. Normálosztók komplexusszorzata normálosztó.

Megjegyzés: Az $N \lhd G$ normálosztó előáll, mint a $\psi_N : G \to {}^{G}\!/_{N}$ természetes homomorfizmus magja.

Az iménti tétellel egybevetve látjuk, hogy a normálosztók éppen a csoportból induló homomorfizmusok magjai, a homomorf képek pedig a faktorcsoportok.

Következmény: $Inn\,G \simeq G/Z(G)$, hiszen a $\Phi : G \to Inn\,G,\ x \mapsto \varphi_x$ leképezés magja $Z(G)$.

Megjegyzés: Egy φ homomorfizmus kölcsönösen egyértelmű megfeleltetést létesít $Im\,\varphi$ részcsoportjai, normálosztói és G azon részcsoportjai és normálosztói közt, melyek tartalmazzák $Ker\,\varphi$-t.

I. Izomorfizmus-tétel: Ha $H \leq G$, $N \lhd G$, akkor

(1) $N \lhd HN$,

(2) $(H \cap N) \lhd H$ és

(3) $HN/N \simeq H/H \cap N$.

II. Izomorfizmus-tétel: Ha $M, N \lhd G$ és $M \leq N$, akkor

(1) $M \lhd N$;

(2) $N/M \lhd G/M$;

(3) $G/N \equiv \big(G/M\big)\Big/\big(N/M\big)$.

Állítás: A G csoport pontosan akkor (belső) direkt szorzata a $\{H_i \leq G \mid i \in \mathbf{I}\}$ részcsoportoknak, ha teljesülnek a következők:

(1) $\langle H_i \mid i \in \mathbf{I}\rangle = G$;

(2) $H_i \cap \langle H_j \mid j \neq i\rangle = \{1\}$ $\qquad \forall i \in \mathbf{I}$;

(3) $[x_i, x_j] = 1$ $\qquad \forall i \neq j,\ x_i \in H_i,\ x_j \in H_j$. avagy: egyértelmű előállítás

Állítás: Legyen $G = \prod\limits_{i\in\mathbf{I}} G_i$, $H_i \leq G_i$, $H = \prod\limits_{i\in\mathbf{I}} H_i$. Ekkor a következők igazak:

- $Z(G) = \prod Z(G_i)$; $\qquad Z_r(G) = \prod Z_r(G_i)$
- $H \lhd G \iff \forall i \in \mathbf{I} :\ H_i \lhd G_i$; $\qquad$ (ebben az esetben $G/H = \prod \big(G_i/H_i\big)$);
- $H \underset{char}{\lhd} G \iff \forall i \in \mathbf{I} :\ H_i \underset{char}{\lhd} G_i$.

Lemma: Legyen P véges Abel p-csoport. Ekkor ha $A = \langle a\rangle$ maximális rendű ciklikus részcsoport P-ben (nincs a-nál nagyobb rendű elem P-ben), akkor direkt összeadandó, azaz $\exists B \leq P$, hogy $P = A \oplus B$. Ennek segítségével igazolható a következő tétel.

Véges Abel-csoportok alaptétele: Legyen A véges Abel-csoport. Ekkor egyértelműen felírható $A \simeq \prod\limits_{i\in\mathbf{I}} Z_{p_i^{s(i)}}$ alakban, ahol a p_i-k (nem feltétlenül különböző prímek) és az $s(i)$ kitevők pozitív egészek.

Megjegyzés: Ez általánosítható *végesen generált Abel-csoportok alaptételévé*, mely esetben Z_∞ tényezők is megengedettek. Egy A végesen generált Abel-csoport $rk\,A$ $Ker\,A$ rangja a szereplő Z_∞ tényezők száma, mely egyébként a legnagyobb olyan r, amelyre $Z_\infty^r \leq A$. Ebben az a jó, hogy egzakt sorozatoknál a dimenzióhoz hasonlóan viselkedik, pl. rövid egzakt sorozatra a középső elem rangja a két szélső rangjának összege.

Sylow-tételek

Cauchy-tétel: Ha a G véges csoport rendjét osztja a p prím, akkor van p rendű eleme. Speciálisan ha G rendje prím, akkor G ciklikus.

Sylow tételei: Az alábbiakban legyen a G véges csoport rendje $|G| = p^k \cdot s$, ahol p prím és $p \nmid s$.

I. Minden p-hatvány rendű részcsoport beleágyazható normálosztóként egy olyanba, melyben az indexe p — kivéve persze azokat, melyekre ez a Lagrange-tétel szerint eleve lehetetlen, azaz

$$0 \leq i < k,\ P \leq G,\ |P| = p^i \quad \Longrightarrow \quad \exists P^* \leq G :\ |P^*| = p^{i+1},\ P \lhd P^*.$$

Def. A fentiek szerint létezik olyan részcsoport G-ben, melynek rendje p^k. Ezeket a részcsoportokat nevezzük a G p-Sylowjainak, halmazukat $Syl_p(G)$ jelöli. Egy kényelmes megfogalmazás: a P részcsoport p-Sylow G-ben, ha $p \nmid |G : P|$.

II. Minden p-Sylow konjugált, azaz $\forall P, P' \in Syl_p(G)\ \exists x \in G :\ P' = P^x$.

III. A p-Sylowok száma p-vel osztva 1 maradékot ad, azaz $|Syl_p(G)| \equiv 1 \pmod p$.

Megjegyzés: Ha G véges csoport és π prímek tetszőleges halmaza, akkor a $H \leq G$ részcsoportot π-Hall

részcsoport névvel illetjük, ha $|H|$ minden prímosztója π-beli, $|G:H|$-nak viszont nincs π-beli prímosztója. (Hall-részcsoport az, amihez van ilyen π, azaz $|H|$ és $|G:H|$ relatív prímek.) Ezzel a megfogalmazással a p-Sylow részcsoportok éppen $\{p\}$-Hall részcsoportok. Ha még bevezetjük a p-től különböző összes prímek halmazára a p' jelölést, kimondhatjuk a következő tételt:

Philip Hall tétele: A G véges csoportra ekvivalensek az alábbiak:

(1) G-nek minden π-re van π-Hall részcsoportja;

(2) G-nek minden p-re van p'-Hall részcsoportja;

(3) G feloldható (ld. később).

Feloldhatóság

Megjegyzés: G kommutatív $\iff$ $Z(G)=G$ $\iff$ $G'=\{1\}$.

Megjegyzés: Egy egyszerű csoport feloldható $\iff$ kommutatív $\iff$ prímrendű ciklikus.

Lemma: Ha G/N kommutatív, akkor $N \geq G'$. Ha pedig $G' \leq H \leq G$, akkor $H \lhd G$ és G/H kommutatív.

Következmény: Ha a $G \rhd G_1 \rhd \ldots G_r$ első k faktora kommutatív, akkor $G_k \leq G^{(k)}$. Tehát a derivált lánc a „legyorsabb", amelynek kommutatívak a faktorai. Tehát G pontosan akkor feloldható, ha a derivált lánc leér $\{1\}$-be és ekkor $d(G)$ a lehető legkisebb olyan szám, amilyen hosszú normállánc már tanúsíthatja a feloldhatóságot.

Állítás: $N \lhd G$ esetén G felloldható $\iff$ N és G/N feloldható, továbbá ilyenkor $d(N), d(G/N) \leq d(G) \leq d(N)+d(G/N)$.

Megjegyzés: Ha egy $G \rhd G_1 \rhd \ldots G_r$ normállánc k-adik eleme normálosztó, akkor a normállánc kezdőszelete G/G_k egy normálláncát, vége G_k normálláncát adja. A két kis lánc faktorai (multiplicitással számolva) éppen kiadják a teljes lánc faktorait a II. izomorfizmus-tétel szerint. Ennek alapján G/N és N egy-egy normálláncából könnyű összerakni G egy normálláncát és a faktorok itt is megmaradnak.

Állítás: Az alábbiak ekvivalensek:

(1) G feloldható;

(2) G valamely normálláncának faktorai feloldhatóak;

(3) G minden normálláncának faktorai feloldhatóak;

(4) G részcsoportjának faktorcsoportjaként csak feloldható csoportok állnak elő;

(5) A derivált lánc „leér" $\{1\}$-be, azaz $d(G)<\infty$.

Ha még G véges is (ekkor biztosan van kompozíciólánca), akkor az alábbi feltételek is ekvivalensek:

(6) G részcsoportjának faktorcsoportjaként nem áll elő nemkommutatív egyszerű csoport;

(7) G-nek van olyan normállánca, melynek minden faktora prímrendű ciklikus (ez persze kompozíciólánc lesz);

(8) G minden kompozíciólláncának minden faktora prímrendű ciklikus.

Jordan–Dedekind-tétel: Legyen G véges csoport (ennek biztosan létezik kompozíciólánca a végesség miatt). Ekkor bármely két kompozíciólánc hossza azonos és a keletkező faktorok is ugyanazok, azonos multiplicitással.

Tétel: S_1, S_2, S_3, S_4 feloldhatóak; $n \geq 5$ esetén A_n egyszerű.

Feit–Thompson-tétel: Minden páratlan rendű csoport feloldható.

Következmény: Minden $4k+2$ rendű csoport feloldható. (Mellékosztály szerinti reprezentációval.)

Feloldható továbbá minden olyan csoport, melynek rendje $p^k \cdot q^l$ alakú (Burnside-tétel — következik a Sylow-tételekből és a Hall-tételből, de valójában a Hall-tétel bizonyítása a Burnside-tételre épül) vagy négyzetmentes,

Megjegyzés: A G csoport nilpotens, ha van olyan $G=G_1>G_2>\ldots>G_r=\{1\}$ lánc, melyre $[G_i,G] \leq G_{i+1}$ — ún. centrális lánc. (Ekkor persze $G_i' \leq G_{i+1}$ még inkább teljesül, ezért $G_i \rhd G_{i+1}$, tehát normálláncról van szó, a faktorok pedig kommutatívak. Igazolható, hogy ekkor $G^i \leq G_i \leq Z_{r-i}(G)$. Tehát nilpotens csoportban az alsó centrális lánc leér $\{1\}$-be, a felső centrális lánc pedig felér G-ig és minden minimális hosszúságú centrális

lánc e kettő közt halad.

Permutációcsoportok

Legyen $G(\Omega)$ tranzitív permuációcsoport.

Állítás: Az $\omega \in \Omega$ pont stabilizátorának indexe az orbit elemszáma, azaz $|G : G_\omega| = \left|\omega^G\right|$. Speciálisan egy tranzitív permutációcsoport foka osztja a rendjét. Reguláris permutációcsoport rendje osztja a fokát. Tranzitív reguláris permutációcsoport rendje és foka azonos (végtelenek számosságoknál is).

Állítás: $G(\Omega)$-ban minden stabilizátor konjugált, tehát izomorf, így van értelme egy tranzitív permutációcsoportnál „a" stabilizátorról beszélni.

Cayley-tétel: Minden csoport izomorf egy tranzitív reguláris permutációcsoporttal, mégpedig a $\Omega \stackrel{\text{def}}{=} G$, $g : \omega \mapsto \omega \cdot g$ módon. (Ha permutációk szorzatára alatt a kompozíciós jelölést használjuk, azaz jobbról kezdjük kifejteni a gh szorzatot ω helyen felvett értékét, akkor $g : \omega \mapsto g \cdot \omega$ lesz jó.) Ezt a csoport Cayley-reprezentációjának hívjuk.

Megjegyzés: Ami igazán fontos, az a mellékosztály szerinti reprezentáció. Legyen $H \leq G$ részcsoport. Legyen $\Omega \stackrel{\text{def}}{=} \{Ht \mid t \in G\}$, $\rho : G \to S(\Omega)$, $\rho_g : Ht \mapsto Htg$. Ez jóldefiniált lesz és $Ker\,\rho = \bigcap_{x \in G} H^x$ a legbővebb, H által tartalmazott normálosztó. Ennek segítségével egy $|G : H|$ fokú tranzitív reprezentációt találtunk. Következésképp ha G-ben van n indexű részcsoport, akkor van legfeljebb $n!$ indexű normálosztó is. Belátható, hogy minden tranzitív reprezentáció izomorf egy mellékosztály szerinti reprezentációval, H-nak valamelyik stabilizátort kell választani.

Még egy-két „hasznos" tudnivaló

Schreier-tétel: Szabadcsoport minden részcsoportja szabad.

Tétel: Végesen generált csoport véges indexű részcsoportja végesen generált.

Schur-tétel: Ha a centrum indexe véges, akkor a derivált csoport rendje is az.

Schur–Zassenhaus-tétel: Ha N Hall-részcsoport és normálosztó G-ben, akkor van komplementuma (olyan $H \leq G$ részcsoport, hogy $HN = G$ és $H \cap N = \{1\}$ – ekkor G a H és N szemidirekt szorzata) és minden komplementuma konjugált.

Állítás: Nyilván minden $n \in \mathbf{Z}_+$ számra létezik n elemű csoport, mégpedig a megfelelő ciklikus csoport. Pontosan akkor nincs más, ha $\big(n, \varphi(n)\big) = 1$, azaz ha n négyzetmentes és nincsenek olyan p, q prímosztói, hogy $p \equiv 1 \pmod{q}$.