6. Csoportelmélet

6.1 Csoportaxiómák, alapfogalmak

6.1.1 Definíció: csoport egy olyan $(G,\cdot)$ rendezett páros, ahol G egy halmaz, $\cdot$ pedig egy $G\times G\to G$ művelet, amely teljesíti a csoportaxiómákat:

(G1) a művelet asszociatív, azaz $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(G2) van jobb és bal egységelem (neutrális elem), azaz $\exists e_R,e_L\in G\colon \forall a\in G\colon a\cdot e_R=e_L\cdot a=a$. (Ezek egyenlőek, mert $e_R=e_L\cdot e_R=e_L$).

(G3) minden elemnek van jobb és bal oldali inverze, azaz $\forall g\in G\colon \exists g_L^{-1},g_R^{-1}\in G\colon g\cdot g_R^{-1}=g_L^{-1}\cdot g=e$. Ezek egyenlőek, mert $g_L^{-1}=g_L^{-1}(gg_R^{-1})=(g_L^{-1}g)g_R^{-1}=g_R^{-1}$.

6.1.2 Állítás: ezzel ekvivalensek az alábbi feltételek:

(G1) a művelet asszociatív.

(GL2) van bal oldali egységelem.

(GL3) van bal oldali inverz.

Bizonyítás: tegyük fel, hogy e bal oldali egységelem és a bal oldali inverze a_0, a_0 bal inverze a_1. Ekkor $aa_0=e(aa_0)=(a_1a_0)(aa_0)=a_1(a_0a)a_0=a_1(ea_0)=a_1a_0=e$, tehát $a_0a=e\Rightarrow aa_0=e$, minden elem bal inverze egyben jobb inverz is. Ekkor $\forall x\in G\colon xe=x(x^{-1}\cdot x)=(x\cdot x^{-1})x=ex=x$, azaz e jobb oldali egységelem is egyben.

6.1.3 Megjegyzés: bal egység és jobb inverz még kevés lenne, mert az $xy=y$ művelet asszociatív, minden elem bal egység, ráadásul bármely elemhez és bármely e bal egységhez e megfelel jobb inverznek; márpedig így egynél több elem esetén nem kapunk csoportot.

6.1.4 Jelölés: az egységelemet 1, $a\in G$ inverzét a^{-1} jelöli. (Additív csoportban 0 illetve $(-a)$.)

6.1.5 Megjegyzés: $(ab)^{-1}=b^{-1}a^{-1}$.

6.1.6 Definíció: ha a G csoportban a szorzás kommutatív, azaz $\forall a,b\in G\colon ab=ba$, akkor G kommutatív avagy Abel-csoport.

6.1.7 Állítás: ha G csoport, akkor $\forall a,b\in G$-re pontosan egy megoldása van az $ax=b$ ill. az $ya=b$ egyenleteknek.

Bizonyítás: nyilván elég az egyik egyenlettel foglalkozni. $ax=b\Rightarrow x=a^{-1}ax=a^{-1}b$, tehát más nem lehet jó megoldás; ez pedig az.

6.1.8 Állítás: **6.1.1**-el ekvivalens definíció az alábbi:

(G1) a művelet asszociatív.

(G2′) az $ax=b, ya=b$ egyenletek $\forall a,b\in G$-re megoldhatóak.

Bizonyítás: ha G csoport, akkor ezek **6.1.7** szerint igazak. Lássuk a másik irányt: legyen e az $ya=a$ egyenlet megoldása. Ekkor $\forall x\in G\colon eax=ax$. Minden b felírható ax alakban, tehát $\forall b\in G\colon eb=b\Rightarrow e$ bal egység. $\forall a\in G\colon ya=e$ megoldható, tehát **(GL3)** is teljesül.

6.1.9 Definíció: a G csoport rendje a G halmaz elemeinek száma. Jelölése $|G|$. Ha ez véges, akkor G véges csoport.

6.1.10 Megjegyzés: véges elemszám esetén G pontosan akkor csoport, ha a művelet asszociatív és teljesül rá az ún. „egyszerűsítési szabály”: $ax_1=ax_2\Rightarrow x_1=x_2$ és $y_1a=y_2a\Rightarrow y_1=y_2$. Végtelen elemszámnál ez szükséges, de nem elégséges feltétel, hiszen pl. a pozitív egészek az összeadással kielégítik, asszociatívak, ráadásul még kommutatívak is, de nincs köztük egység.

6.1.11 Definíció: G csoportban az a elem n-edik hatványa (n egész) a következő: $n>0$ esetén G azon eleme, melyet a n-szeri összeszorzásával kapunk; $n=0$-ra 1; $n<0$ esetben a^{-1} $|n|$-edik hatványa. Jelölése a^n. Könnyen ellenőrizhetően $a^na^m=a^{n+m}$. Ebből következik, hogy egy elem hatványai tetszőleges csoportban felcserélhetőek.

6.1.12 Definíció: legyen a a G csoport egy eleme. Vegyük a összes hatványát. Ezek vagy mind különbözőek, vagy vannak köztük azonosak, pl. $a^i=a^j$ $(i<j)$. A második esetben $a^{j-i}=1$, tehát van egy legkisebb pozitív k, melyre $a^k=1$. Legyen a rendje végtelen, ha minden hatvány különböző, egyébként legyen $\mathbf{min}\{k\in\mathbb{Z}^+ \,|\, a^k=1\}$. Jelölése $o(a)$.

6.1.13 Definíció: komplexusnak nevezzük egy G csoport részhalmazait. Az alábbi műveleteket definiáljuk rajtuk: $K_1K_2=\{k_1k_2 \,|\, k_1\in K_1, k_2\in K_2\}$, $K^{-1}=\{k^{-1} \,|\, k\in K\}$. A $K\cdot\{a\}$ és $\{a\}\cdot K$ komplexusszorzatokat az egyszerűség kedvéért aK ill. Ka jelöli. A komplexusszorzás asszociatív, az egység $\{1\}$. Az alábbiak teljesülnek:

$$\textbf{(1)}\ (K^{-1})^{-1}=K\,,\ \textbf{(2)}\ (K_1K_2)^{-1}=K_2^{-1}K_1^{-1}\,,\ \textbf{(3)}\ K_1\subseteq K_2\Rightarrow K_1^{-1}\subseteq K_2^{-1}, K'K_1K''\subseteq K'K_2K''\,,$$
$$\textbf{(4)}\ (\bigcap_{\alpha\in\mathbf{I}}K_\alpha)\cdot(\bigcap_{\beta\in\mathbf{J}}K_\beta)=\bigcap_{(\alpha,\beta)\in\mathbf{I}\times\mathbf{J}}(K_\alpha\cdot K_\beta)\,,\ \textbf{(5)}\ (\bigcup_{\alpha\in\mathbf{I}}K_\alpha)\cdot(\bigcup_{\beta\in\mathbf{J}}K_\beta)=\bigcup_{(\alpha,\beta)\in\mathbf{I}\times\mathbf{J}}(K_\alpha\cdot K_\beta)\,,$$
$$\textbf{(6)}\ (\bigcap_{\alpha\in\mathbf{I}}K_\alpha)^{-1}=\bigcap_{\alpha\in\mathbf{I}}K_\alpha^{-1}\ \text{és}\ \textbf{(7)}\ (\bigcup_{\alpha\in\mathbf{I}}K_\alpha)^{-1}=\bigcup_{\alpha\in\mathbf{I}}K_\alpha^{-1}\,.$$

6.1.14 Definíció: a H komplexus részcsoportja G-nek, ha csoport a G-beli műveletre nézve. Jelölése $H\leq G$.

6.1.15 Állítás: H komplexus pontosan akkor részcsoport G-ben, ha nem üres, tartalmazza bármely két elemének szorzatát és bármely elemének inverzét is. Ekkor persze az G egységét is tartalmazza.

Bizonyítás: ha részcsoport, akkor a csoport definíciója alapján zárt a szorzásra nézve és van benne egy e egység. Ez csak G egysége lehet, mert akkor $e\cdot e=e=1\cdot e$ és az egyszerűsítési szabály alapján $e=1$. Hasonlóan belátható, hogy egy $a\in H$ elem H-beli inverze azonos kell legyen G-beli inverzével, tehát H-nak tartalmaznia kell minden elemének inverzét is. Ha pedig H teljesíti ezeket a feltételeket, akkor láthatóan teljesíti **6.1.1** feltételeit.

6.1.16 Állítás: legyen H komplexus a G csoportban. Ekkor az alábbi feltételek ekvivalensek:

$$\overset{(1)}{H\leq G} \Leftrightarrow \begin{matrix}H\neq\emptyset\\ HH\subseteq H\\ H^{-1}\subseteq H\end{matrix}\overset{(2)}{} \Leftrightarrow \begin{matrix}H\neq\emptyset\\ HH=H\\ H^{-1}=H\end{matrix}\overset{(3)}{} \Leftrightarrow \begin{matrix}H\neq\emptyset\\ HH^{-1}\subseteq H\end{matrix}\overset{(4)}{} \Leftrightarrow \begin{matrix}H\neq\emptyset\\ HH^{-1}=H\end{matrix}\overset{(5)}{}$$

Bizonyítás: **(2)** egyszerűen **6.1.15** feltételeinek megfogalmazása komplexusszorzattal, tehát **(1)** $\Leftrightarrow$ **(2)**. **(1)**-ből következik **(3)**, mert $1\in H\Rightarrow H=\{1\}\cdot H\subseteq H\cdot H$ és **(2)** szerint $H\supseteq H\cdot H$, ezeket összevetve $H=H\cdot H$. Másrészt **(2)**-ből **6.1.13.1** és **6.1.13.3** alapján $H=(H^{-1})^{-1}\subseteq H^{-1}\subseteq H$, azaz $H=H^{-1}$. Eddig **(1)** $\Leftrightarrow$ **(2)** $\Rightarrow$ **(3)**. Ha **(3)** teljesül, akkor $HH^{-1}=HH=H$, azaz **(3)** $\Rightarrow$ **(5)**. **(5)** $\Rightarrow$ **(4)** nyilvánvaló. Ha **(4)** teljesül, akkor $\exists a\in H\Rightarrow 1=aa^{-1}\in HH^{-1}\subseteq H$, azaz $1\in H$. Ekkor $b\in H\Rightarrow b^{-1}=1\cdot b^{-1}\in HH^{-1}\subseteq H$, azaz $b\in H\Rightarrow b^{-1}\in H$. Ezt alkalmazva $a,b\in H\Rightarrow b^{-1}\in H\Rightarrow ab=a(b^{-1})^{-1}\in HH^{-1}\subseteq H$, azaz $a,b\in H\Rightarrow ab\in H$. Összesítve **(4)** $\Rightarrow$ **(2)**. Ezzel az állítást beláttuk.

6.1.17 Állítás: ha G csoport és az $\mathbf{I}$ indexhalmazra $\forall\alpha\in\mathbf{I}$: $H_\alpha\leq G$, akkor $\bigcap_{\alpha\in\mathbf{I}}H_\alpha\leq G$.

Bizonyítás: **6.1.13.4**, **6.1.13.6** és **6.1.16.4** felhasználásával $(\bigcap H_\alpha)\cdot(\bigcap H_\alpha)^{-1}=(\bigcap H_\alpha)\cdot(\bigcap H_\alpha^{-1})=\bigcap(H_\alpha H_\alpha^{-1})=\bigcap H_\alpha$. Mivel $\bigcap H_\alpha$ tartalmazza G egységelemét – hiszen minden részcsoport tartalmazza –, nem üres, tehát teljesül rá a **6.1.16.5** feltétel, azaz részcsoport.

6.1.18 Definíció: G csoportban a K komplexus által generált részcsoport a legszűkebb olyan részcsoport, amely tartalmazza K-t. Jelölése $\langle K\rangle$. Ez létezik, mert $\langle K\rangle=\bigcap_{K\subseteq H\leq G}H$ az előző pont szerint részcsoport, tehát megfelel a feltételeknek. Látható, hogy $K_1\subseteq K_2\Rightarrow\langle K_1\rangle\subseteq\langle K_2\rangle$.

6.1.19 Állítás: $a\in\langle K\rangle$ $\Leftrightarrow$ előáll véges sok K-beli elem hatványainak szorzataként.

Bizonyítás: ha előáll ilyen alakban, akkor benne kell legyen minden $H\supseteq K$ részcsoportban, mert H-nak zártnak kell lennie a műveletekre. A véges sok K-beli elem hatványai szorzataként előállítható G-beli elemek komplexusa pedig részcsoport, mert zárt a szorzásra és az inverzképzésre. Ez tehát tényleg a legszűkebb $H\supseteq K$ részcsoport.

6.1.20 Definíció: G csoport egy K komplexusa generátorrendszer G-ben, ha $\langle K\rangle=G$. G végesen generált, ha van véges elemszámú generátorrendszere.

6.1.21 Állítás: G csoport a elemére $o(a)=|\langle a\rangle|$.

Bizonyítás: ha $o(a)=k$ véges, akkor $a^{j+kn}=a^j$, ezért $A=\{a^0=1,a,a^2,\ldots,a^{k-1}\}$-ben szerepel a összes hatványa, tehát $A=\langle a\rangle$. Ezek valóban különböző elemek, így $|A|=k$ és ezt akartuk bizonyítani. Ha a rendje végtelen, akkor az a által generált részcsoport hasonló meggondolások alapján $\{a^n \,|\, n\in\mathbb{Z}\}$, ennek rendje valóban végtelen.

6.1.22 Definíció: legyenek G_1 és G_2 csoportok, $\varphi: G_1\to G_2$. φ homomorfizmus, ha $\forall a,b\in G_1$: $(a\varphi)(b\varphi)=(ab)\varphi$.

6.1.23 Definíció: a $\varphi: G_1\to G_2$ homomorfizmus képe $Im\,\varphi=\{a\in G_2 \,|\, \exists x\in G_1: x\varphi=a\}$, magja $Ker\,\varphi=\{a\in G_1 \,|\, x\varphi=1\}$.

6.1.24 Definíció: a φ homomorfizmus epimorfizmus, ha $Im\varphi=G_2$, jelölése $\varphi: G_1 \twoheadrightarrow G_2$. Monomorfizmus, ha φ G_1 képén invertálható, jelölése $\varphi: G_1 \rightarrowtail G_2$. Izomorfizmus, ha mindkettő, azaz bijekció, jelölése $\varphi: G_1 \xrightarrow{\sim} G_2$. Ekkor G_1 és G_2 izomorfak, jelölése $G_1 \simeq G_2$ vagy $G_1 \overset{\varphi}{\simeq} G_2$.

6.1.25 Megjegyzés: az izomorfia ekvivalencia-reláció, hiszen izomorfizmusok inverze és kompozíciója, továbbá a $G \to G$ identikus leképezés is izomorfizmus, tehát az izomorfia tranzitív, szimmetrikus és reflexív.

6.1.26 Állítás: a $\varphi: G_1 \to G_2$ homomorfizmus képe részcsoport G_2-ben. Ugyanis $Im\varphi$ két tetszőleges elemét felírva $a\varphi, b\varphi$ alakban $(a\varphi)(b\varphi)^{-1}=(ab^{-1})\varphi$ is eleme a képnek, tehát **6.1.16.4** szerint $Im\varphi$ részcsoport.

6.1.27 Definíció: $n \times n$-es latin négyzet egy olyan $n \times n$-es táblázat, melyben összesen n különböző elem szerepel, minden sorban és minden oszlopban minden elem pontosan egyszer. Két latin négyzet akkor ekvivalens, ha az alaphalmazaik között létezik olyan bijekció, ami egymásba viszi őket. Az **A** és **B** latin négyzetek ortogonálisak, ha az (a_{ij}, b_{ij}) rendezett párok mindegyike különböző.

6.1.28 Definíció: legyenek G (lehetőleg véges) csoport elemei $g_1=1, g_2, g_3, \ldots$. Ekkor G szorzás- vagy Cayley-táblázata az a táblázat, melyben az i-edik sor j-edik eleme $g_i \cdot g_j$. Ez **6.1.8** szerint latin négyzet, viszont nem minden latin négyzet áll elő csoport Cayley-táblázataként, mert az asszociativitás nem mindig teljesül. (És nagyon problémás ellenőrizni egy szorzástáblázatról, hogy asszociatív-e.)

6.2 Példák

Az egyelemű csoport jelölése 1.

Az n-elemű ciklikus csoport az az n-elemű csoport, melynek van olyan eleme, ami generálja. Ez kommutatív, mert egy elem hatványai felcserélhetőek, jelölése Z_n. A Z_∞ végtelen ciklikus csoport az egy elem által generált végtelen rendű csoport. A Z_{p^∞} kváziciklikus avagy Prüfer-csoport (p prím) a p^k-adik egységgyökök csoportja a szorzásra, ahol k befutja a nemnegatív egészeket. (Másként megfogalmazva: könnyen ellenőrizhetően Z_{p^2}-ben pontosan $(p-1)$ p-edrendű elem van, azaz Z_{p^2}-nek pontosan egy Z_p-vel izomorf részcsoportja van. Hasonlóan egyértelműen foglalható bele $Z_{p^{k+1}}$-be Z_{p^k}. Tehát értelmes a $Z_{p^\infty}=\bigcup_{k\in\mathbb{N}}(Z_p \le Z_{p^2} \le Z_{p^3} \le \ldots \le Z_{p^k})$ definíció.) Ez kommutatív és $|Z_{p^\infty}|=\aleph_0$.

A D_n diédercsoport $(n \ge 3)$ a szabályos n-szög egybevágóságainak csoportja. Ennek elemei a forgatások: $1, f, f^2, \ldots, f^{n-1}$ és a tükrözések: $t, tf, tf^2, \ldots, tf^{n-1}$. Nem kommutatív, hiszen $ft=tf^{-1} \ne tf$. Rendje $2n$. D_n-nek pontosan akkor részcsoportja D_m, ha $m \mid n$.

Az S_n szimmetrikus csoport az n-elemű permutációk csoportja. Ez sem kommutatív, ha $n \ge 3$. $|S_n|=n!$ és $m \le n \Rightarrow S_m \le S_n$. Az A_n alternáló csoport elemei az n-elemű páros permutációk. A_n nem kommutatív, ha $n \ge 4$. $|A_n|=\frac{1}{2}n!$ és $m \le n \Rightarrow A_m \le A_n$.

Egy $(K, +, \cdot)$ testre K additív csoportja $(K, +)$, multiplikatív csoportja $(K \setminus \{0\}, \cdot)$, mindkettő kommutatív. Ez utóbbit $mul(K)$ vagy K^* jelöli. $GL_n(K)$ a K feletti $n \times n$-es invertálható mátrixok csoportja a mátrixszorzásra; ez $n=1$-re K^*, egyébként nem kommutatív. $SL_n(K)$ a K feletti 1 determinánsú $n \times n$-es mátrixok csoportja a mátrixszorzásra. Ez $n=1$-re érdektelen, egyébként nem kommutatív (ugyanis $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}2&1\\1&1\end{smallmatrix}\right)\ne\left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$). A K feletti affín csoport $Aff(K)=\{x \mapsto ax+b \mid a, b \in K; a \ne 0\}$ a függvénykompozícióra. Speciálisan $Aff(p)=Aff(\mathbb{F}_p)$, ez $p>2$-re nem kommutatív. $PGL_2(K)=\{x \mapsto \frac{ax+b}{cx+d} \mid ad-bc \ne 0\}$. Hogy ezek bijektívek legyenek, nem $K \to K$ vesszük őket, hanem $K \cup \{\infty\} \to K \cup \{\infty\}$, ahol $x \mapsto \frac{ax+b}{cx+d}$ az $x=-\frac{d}{c}$ helyen ∞, ∞-ben pedig $\frac{a}{c}$. Ekkor ismét egy nem kommutatív csoportot kapunk. $PSL_2(K)$ azon $PGL_2(K)$-beli elemek csoportja, ahol $ad-bc=1$.

A Q kvaterniócsoport az $\{1, -1, i, -i, j, -j, k, -k\}$ kvaterniók csoportja a kvaterniószorzásra. Rendje 8, nem kommutatív. A Klein-féle csoport az a négyelemű csoport, melynek Cayley-táblázata $\begin{smallmatrix}1&a&b&c\\a&1&c&b\\b&c&1&a\\c&b&a&1\end{smallmatrix}$, kommutatív.

6.3 Mellékosztályok. Lagrange- és Wilson-tételek

6.3.1 Definíció: legyen $H \leq G$. Ekkor $a \cdot H$-t ill. $H \cdot a$-t az a elem H szerinti bal ill. jobb oldali mellékosztályának hívjuk. A mellékosztályokra az alábbiak teljesülnek:

(1) $a \in aH \cap Ha$, mert $a = a \cdot 1 = 1 \cdot a$.

(2) $|aH| = |H|$, mert $ah \mapsto h$ az egyszerűsítési szabály szerint bijekció a két halmaz között.

(3) két H szerinti azonos oldali mellékosztály vagy azonos, vagy diszjunkt.

Bizonyítás: nyilván elég az állítást pl. bal oldali mellékosztályokra belátni. Ha aH és bH diszjunktak, akkor az állítás igaz. Ha $s \in aH \cap bH$, akkor $s = ah_1 = bh_2 : h_1, h_2 \in H$. Ekkor $b = ah_1 h_2^{-1}$, azaz $\forall h \in H: bh = a(h_1 h_2^{-1} h) \in aH$, ezért $bH \subseteq aH$. Ugyanígy $aH \subseteq bH$, tehát $aH \subseteq bH$. Ezzel az állítást beláttuk. Következmény:

(4) egy részcsoport azonos oldali mellékosztályai a csoport egy partícióját adják. Ennek eleme $H = H \cdot 1 = 1 \cdot H$.

(5) $aH = H \Leftrightarrow a \in H$, triviális.

(6) a és b pontosan akkor van ugyanabban a H szerinti bal oldali mellékosztályban, ha $b^{-1}a \in H$, mert felhasználva. Ugyanis **(3)** szerint pontosan akkor vannak egy mellékosztályban, ha $aH = bH$-val, amivel a komplexusszorzás asszociativitása miatt ekvivalens $b^{-1}aH = b^{-1}bH = H$, ez pedig **(5)** szerint ekvivalens $b^{-1}a \in H$-val. Jobb oldali mellékosztállyal $ba^{-1} \in H$ a feltétel.

6.3.2 Állítás: a H szerinti jobb és bal oldali mellékosztályok számossága azonos.

Bizonyítás: **6.3.1.6** szerint a és b pontosan akkor vannak ugyanabban a bal oldali mellékosztályban, ha a^{-1} és b^{-1} ugyanabban a jobb oldali mellékosztályban vannak. Eszerint az $f: a \mapsto a^{-1}$ bijekció a bal és a jobb oldali mellékosztályok között is bijekciót létesít, ezek tehát ugyanannyian vannak.

6.3.3 Definíció: a H részcsoport indexe G-ben a H szerinti mellékosztályok számossága G-ben. Jelölése $|G:H|$.

6.3.4 Lagrange-tétel: $|G| = |G:H| \cdot |H|$.

Bizonyítás: válasszunk ki minden baloldali mellékosztályból egy elemet, legyen ezek halmaza K. Ekkor G minden eleme egyértelműen áll elő $g = k \cdot h : k \in K, h \in H$ alakban. Előáll, mert véve a g-vel azonos mellékosztályban lévő $k \in K$ elemet $k^{-1}g = h \in H$ **6.3.1.6** szerint. Egyértelműen, mert ha $g = kh$, akkor k és g azonos mellékosztályban vannak, azaz k egyértelmű és ha g és k adott, akkor h már csak egyféle lehet az egész G-ben az egyszerűsítési szabály szerint. K és a mellékosztályok között $k \mapsto kH$ bijekció és az előbbiek szerint $K \times H$ és G között $(h,k) \mapsto hk$ szintén bijekció. Összevetve $|G:H| \cdot |H| = |K| \cdot |H| = |G|$, ez volt bizonyítandó. (Ebből véges csoporton belüli mellékosztályokra következik **6.3.2**. Végtelenre viszont nem, mert pl. $\aleph_0 \cdot \aleph_0 = 2 \cdot \aleph_0$, pedig $\aleph_0 \neq 2$.)

6.3.5 Következmény: ha G véges csoport és $H \leq G$, akkor $|H| \,\big|\, |G|$. Speciálisan $o(a) \,\big|\, |G|$.

6.3.6 Korrolárium: ha p prím és a p-hez relatív prím, akkor $\mathbb{F}_p^*$-ban a rendje osztja a csoport rendjét, azaz $(p-1)$-et. Eszerint $a^{p-1} \equiv 1 \pmod{p}$.

6.3.7 Állítás: véges Abel-csoportban az összes elem szorzata egyenlő a másodrendű elemek szorzatával. (Nem kommutatív vagy végtelen csoportban nincs is értelme az összes elem szorzatának.)

Bizonyítás: a kommutativitás miatt ezt a szorzatot át szabad rendeznünk. 2-nél kisebb rendű elem csak az egység, ami a szorzatot nem változtatja. Elég tehát belátnunk, hogy a 2-nél nagyobb rendű elemek szorzata egy. Ezek pedig párba állíthatóak úgy, hogy mindegyik elem párja az inverze, hiszen mindegyik pontosan egy elem inverze, az szintén nem másodrendű és nem önmaga. A szorzat tehát átrendezve és átzárójelezve néhány 1 szorzata lesz, ami még mindig 1. Ezzel az állítást beláttuk.

6.3.8 Következmény (Wilson-tétel): $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás: ha $p = 2$, akkor az állítás igaz. Ha $p > 2$, akkor alkalmazzuk az előző állítást $\mathbb{F}_p$ multiplikatív csoportjára: $(p-1)! = \prod_{x \in \mathbb{F}_p} x = \prod_{o(x)=2} x = \prod_{x^2-1=0, x \neq 1} x = \prod_{(x-1)(x+1)=0, x \neq 1} x$. Testben egy másodfokú polinomnak legfeljebb két gyöke van. 1 és -1 két különböző gyök, tehát a feltételeknek csak a -1 felel meg ($\Rightarrow$ez az egyetlen másodrendű elem). Eszerint $(p-1)! = \prod_{x \in \mathbb{F}_p, x=-1} x = -1$.

6.4 Konjugált, konjugált osztály, normálosztó. Homomorfizmus-tétel, izomorfizmus-tételek

6.4.1 Definíció: $a,b\in G$ elemek konjugáltak, ha $\exists x\in G: x^{-1}ax=b$. Ez ekvivalencia-reláció, mert $1^{-1}\cdot a\cdot 1=a$ miatt reflexív, $x^{-1}ax=b \Rightarrow (x^{-1})^{-1}b(x^{-1})=a$ miatt szimmetrikus és $b=x_1^{-1}ax_1, c=x_2^{-1}bx_2 \Rightarrow c=(x_1x_2)^{-1}a(x_1x_2)$ miatt tranzitív. Ezek szerint a reláció ekvivalencia-osztályokra bontja G-t, ezek a konjugált osztályok. A K komplexus x elemmel vett konjugáltja $x^{-1}Kx=\{x^{-1}kx \mid k\in K\}$. Az a elem konjugált osztályát néha $[a]$-val jelöljük. (Néha meg $cl(a)$-val.) Nyilván $[1]=\{1\}$, hiszen $x^{-1}\cdot 1\cdot x=x^{-1}x=1$.

6.4.2 Jelölés: a^x-el illetve K^x-el jelöljük a elem ill. K komplexus x-el vett konjugáltját. Ha $H\le G, K\subseteq G$, akkor H^K $\langle k^{-1}hk \mid h\in H, k\in K\rangle=\langle k^{-1}Hk \mid k\in K\rangle$-t jelöli, azaz a H komplexus K-beli elemekkel vett konjugáltjai által generált részcsoportot. (Szerencsére így $H^{\{x\}}=H^x$, mert $H^x\le G$.)

6.4.3 Definíció: G egy H részcsoportja normálosztó (esetleg normális részcsoport), ha bal és jobb mellékosztályai megegyeznek, azaz $\forall a\in G: aH=Ha$. Jelölése $H\triangleleft G$.

6.4.4 Megjegyzés: $H\triangleleft G$-hez elég, hogy H jobb és baloldali mellékosztályai ugyanazt a partíciót adják. Ugyanis ekkor aH felírható Hb alakban, így **6.3.1.1** szerint $a\in aH=Hb \Rightarrow a\in Hb \Rightarrow Ha=Hb=aH$. Ez alapján $|G:H|=2 \Rightarrow H\triangleleft G$, hiszen H bármely oldali mellékosztályai a $\{H, G\setminus H\}$ partíciót adják.

6.4.5 Definíció: G csoport egyszerű, ha csak triviális normálosztója van, azaz $H\triangleleft G \Rightarrow (H=\{1\}$ vagy $H=G)$.

6.4.6 Állítás: H részcsoportra pontosan akkor teljesül $H\triangleleft G$, ha H konjugált osztályok uniója.

Bizonyítás: $H\triangleleft G \Leftrightarrow \forall a\in G: aH=Ha \Leftrightarrow \forall a\in G: a^{-1}Ha=H$. Ehhez szükséges $\forall a\in G: a^{-1}Ha\subseteq H$ és elég is, mert ha teljesül, akkor $\forall a^{-1}\in G: (a^{-1})^{-1}H(a^{-1})\subseteq H$, azaz $\forall a\in G: aHa^{-1}\subseteq H \Rightarrow H\subseteq a^{-1}Ha$. Összevetve $H\subseteq a^{-1}Ha\subseteq H$, eszerint azonosak. Tehát $H\triangleleft G \Leftrightarrow \forall a\in G: a^{-1}Ha\subseteq H \Leftrightarrow \forall a\in G, h\in H: a^{-1}ha\in H$, ami azt jelenti, hogy H minden elemének minden konjugáltja benne van H-ban. Ezzel az állítást beláttuk.

Észrevehetjük, hogy $H\triangleleft G \Leftrightarrow (H\le G$ és $(ab\in H \Rightarrow ba\in H))$.

Az állításból látható, hogy a „Lagrange-tétel megfordítása" – ha G véges csoportra $k\,\big|\,|G|$, akkor G-nek van k elemű részcsoportja – nem igaz. Ugyanis $6\,\big|\,12=|A_4|$, de A_4-nek nincs hatelemű részcsoportja, mert ha lenne, akkor az 2 indexű, tehát normálosztó lenne, azaz teljes konjugált osztályokból állna. Viszont A_4 konjugált osztályai rendre $1,3,4,4$ eleműek, ebből nem lehet hatelemű részcsoportot építeni. Kommutatív csoportban a megfordítás igaz, ld. véges Abel-csoportok alaptétele.

6.4.7 Definíció: legyen $N\triangleleft G$. Ekkor a G/N faktorcsoport elemei az N szerinti mellékosztályok (mivel normálosztó, mindegy, hogy bal vagy jobb oldali), a művelet pedig a komplexusszorzás. Két mellékosztály komplexusszorzata valóban mellékosztály, ugyanis $(aN)(bN)=a(Nb)N=a(bN)N=(ab)(NN)=(ab)N$. (Ez nem függ attól, hogy az adott mellékosztályok mely elemeit választottuk ki; egy N szerinti mellékosztály bármely elemének komplexusszorzata N-el maga a mellékosztály.) Az asszociativitás következik a G feletti szorzás asszociativitásából. A faktorcsoport egységeleme N. Inverz is van, mégpedig $(aN)^{-1}=N^{-1}a^{-1}=Na^{-1}=a^{-1}N$.

6.4.8 Megjegyzés: legyen $N\triangleleft G$. Ekkor a $\psi: G\to G/N$ „természetes homomorfizmus" legyen $\psi: g\mapsto gN$. Ennek képe a teljes faktorcsoport, hiszen minden N szerinti mellékosztály előáll egy elem N-el vett komplexusszorzataként; erre a mellékosztály bármely eleme alkalmas. Magja **6.3.1.5** szerint N.

6.4.9 Homomorfizmus-tétel: ha $\varphi: G_1\to G_2$ homomorfizmus, akkor $Ker\,\varphi\triangleleft G_1$ és $Im\,\varphi\simeq G/Ker\,\varphi$.

Bizonyítás: legyen $a\in Ker\,\varphi, x\in G_1$. Ekkor $(x^{-1}ax)\varphi=(x^{-1}\varphi)(a\varphi)(x\varphi)=(x\varphi)^{-1}\cdot 1\cdot(x\varphi)=1$, azaz $x^{-1}ax\in Ker\,\varphi$. Eszerint a mag teljes konjugált osztályok uniója, tehát – mivel részcsoport – normálosztó. Vizsgáljuk meg, mikor lesz az $a,b\in G_1$ elemek képe azonos: $a\varphi=b\varphi \Leftrightarrow a\varphi=(a(a^{-1}b))\varphi \Leftrightarrow a\varphi=a\varphi\cdot(a^{-1}b)\varphi \Leftrightarrow (a^{-1}b)\varphi=1 \Leftrightarrow a^{-1}b\in Ker\,\varphi$. Pontosan akkor, ha ugyanabban a $Ker\,\varphi$ szerinti mellékosztályban vannak, azaz φ bijekció a kép és a faktorcsoport között. Könnyen ellenőrizhetően művelettartó, tehát izomorfizmus.

6.4.10 Állítás: G csoport K komplexusa pontosan akkor normálosztó, ha előáll egy G-n értelmezett homomorfizmus magjaként. Ez az előző két pont triviális következménye.

6.4.11 Állítás: ha $H_1, H_2\le G$, akkor $H_1H_2\le G \Leftrightarrow H_1H_2=H_2H_1$.

Bizonyítás: felhasználva **6.1.16.3**-at: $H_1,H_2,H_1H_2\leq G \Rightarrow H_1H_2=(H_1H_2)^{-1}=H_2^{-1}H_1^{-1}=H_2H_1$. Ha pedig a két komplexusszorzat megegyezik, akkor $(H_1H_2)(H_1H_2)^{-1}=H_1(H_2H_2^{-1})H_1^{-1}=H_1(H_2H_1)=(H_1H_1)H_2=H_1H_2$, azaz **6.1.16.5** szerint H_1H_2 valóban részcsoport.

6.4.12 Állítás: $H\leq G,N\triangleleft G \Rightarrow \langle H,N\rangle=H\cdot N$.

Bizonyítás: $H\cdot N\subseteq\langle H,N\rangle$ nyilvánvaló. A normálosztó definíciója alapján $H\cdot N=N\cdot H$, tehát **6.4.11** szerint $H\cdot N$ részcsoport. Ez tehát maga a legszűkebb $H\cup N$-t fedő részcsoport.

6.4.13 Izomorfizmus-tétel I.: ha $H\leq G,N\triangleleft G$, akkor **(1)** $N\triangleleft HN$, **(2)** $(H\cap N)\triangleleft H$ és **(3)** $HN/N\simeq H/H\cap N$.

Bizonyítás: ha a és b konjugáltak H-ban, akkor konjugáltak G-ben is, mert egy olyan H-beli x, mellyel a-t konjugálva b-t kapjuk, nyilván benne van G-ben is. Eszerint a H-beli teljes konjugált osztályok egyszerűen egy továbbparticionálását adják a G-beli konjugált osztályok H-beli részeinek. N teljes G-beli konjugált osztályok uniója, azaz $H\cap N$ előáll H-ban teljes H-beli konjugált osztályok uniójaként, azaz normálosztó H-ban. Ugyanez mondható el $N\triangleleft HN$ esetében, hiszen HN is részcsoport **6.4.12** szerint. A HN-beli N szerinti mellékosztályok mindegyikében van H-beli elem, mert HN minden eleme előáll $h\cdot n$ alakban, ekkor azonos N szerinti mellékosztályban van ezzel a h-val.

Feleltesse meg a $\varphi: HN/N\to H/H\cap N$ leképezés az (aN) HN-beli N szerinti mellékosztálynak az $(aN)\cap H$ H-beli $H\cap N$ szerinti mellékosztályt (az előbb beláttuk, hogy ezt mindig fel tudjuk úgy írni, hogy $a\in H$ legyen). Könnyen ellenőrizhetően $(aN)\cap H=a(N\cap H)$, ezért $(aNbN)\varphi=(ab)(N\cap H)=a(N\cap H)\cdot b(N\cap H)=(aN)\varphi\cdot(bN)\varphi \Rightarrow \varphi$ homomorfizmus. Invertálható az egész $H/H\cap N$-en, mert minden H-beli $H\cap N$ szerinti mellékosztály benne van egy HN-beli N szerinti mellékosztályban, azaz előáll egy HN-beli N szerinti mellékosztály és H metszeteként, másrészt nyilván nincs benne kettőben, mert ezek diszjunktak. φ tehát izomorfizmus.

6.4.14 Izomorfizmus-tétel II.: $M,N\triangleleft G$ és $M\leq N \Rightarrow$ **(1)** $M\triangleleft N$, **(2)** $N/M\triangleleft G/M$ és **(3)** $G/N\simeq (G/M)\big/(N/M)$.

Bizonyítás: a fenti meggondolás alapján M teljes G-beli konjugált osztályok uniója, tehát teljes N-beli konjugált osztályok uniója is egyben. Ha valamely $a,b\in G$ elemekre $ab^{-1}\in M$, akkor $ab^{-1}\in N$, tehát **6.3.1.6** szerint N mellékosztályai előállnak teljes M szerinti mellékosztályok uniójaként. Legyen ψ az a leképezés, amely az aM mellékosztálynak az aN mellékosztályt felelteti meg. (Ez nem függ a reprezentáló elemtől, hiszen mindig azt az N szerinti mellékosztályt kapjuk, amelyik tartalmazza az adott M szerinti mellékosztályt.) ψ homomorfizmus, mert $(aMbM)\psi=(abM)\psi=(abN)=(aN)(bN)=(aM)\psi\cdot(bM)\psi$. Azon M szerinti mellékosztályok vannak ψ magjában, melyek N részei; ezek épp N/M elemei. ψ képe nyilván G/N (minden N szerinti mellékosztály tartalmaz M szerinti mellékosztályt, így előáll képként). Beírva $Im\,\psi=G/N, Ker\,\psi=N/M$-et az $Im\,\psi\simeq (G/M)\big/Ker\,\psi$ homomorfizmus-tételbe éppen a bizonyítandó állítást kapjuk.

6.5 Karakterisztikus részcsoport; centralizátor, normalizátor, kommutátor

6.5.1 Definíció: G csoport automorfizmus-csoportja $Aut(G)=\{\varphi\,|\,\varphi: G\xrightarrow{\sim} G\}$. Belső automorfizmusainak csoportja $Inn(G)=\{\varphi_a\,|\,a\in G,\varphi_a: x\mapsto a^{-1}xa\}$.

6.5.2 Állítás: $Inn(G)\triangleleft Aut(G)$.

Bizonyítás: $Inn(G)\leq Aut(G)$ triviális. **6.4.6** szerint elég tehát belátni, hogy egy $\varphi_a\in Inn(G)$ elem $\psi\in Aut(G)$-vel vett konjugáltja benne van $Inn(G)$-ben. $\forall x\in G: x(\psi^{-1}\varphi_a\psi)=(a^{-1}(x\psi^{-1})a)\psi=(a^{-1}\psi)(x\psi^{-1}\psi)(a\psi)=(a\psi)^{-1}x(a\psi)=x\varphi_{a\psi}$. Eszerint $\psi^{-1}\varphi_a\psi=\varphi_{a\psi}\in Inn(G)$, az állítást beláttuk.

6.5.3 Definíció: $H\leq G$ karakterisztikus részcsoportja G-nek, ha G minden automorfizmusa H-ra megszorítva is automorfizmus, azaz $\forall\varphi\in Aut(G): H\varphi=H$. (Elég $\forall\varphi\in Aut(G): H\varphi\subseteq H$ is, mert akkor $\forall\varphi^{-1}\in Aut(G): H=H\varphi^{-1}$.) Jelölése $H\underset{char}{\triangleleft} G$. Teljesen karakterisztikus részcsoport, ha G minden endomorfizmusa (minden $G\to G$ homomorfizmus) önmagába viszi. Nyilván minden automorfizmus endomorfizmus, tehát minden teljesen karakterisztikus részcsoport karakterisztikus is egyben és minden karakterisztikus részcsoport normálosztó, hiszen N pontosan akkor normálosztó, G minden belső automorfizmusa önmagába viszi.

6.5.4 Állítás: $H\underset{char}{\triangleleft} N\triangleleft G \Rightarrow H\triangleleft G$. ($H\triangleleft N\triangleleft G$ még kevés lenne, mert $A_4\triangleright\langle(12)(34),(13)(24)\rangle\triangleright\langle(12)(34)\rangle$, de $\langle(12)(34)\rangle$ nem normálosztó A_4-ben.)

Bizonyítás: feltételeink szerint $\forall \varphi_a \in Inn(G): N\varphi_a = N$, tehát $\varphi_a\big|_N \in Aut(N)$. Eszerint $H\varphi_a = H(\varphi_a\big|_N) = H$, mert $H \underset{char}{\lhd} N$. Összefoglalva $\forall \varphi_a \in Inn(G): H\varphi_a = H$, H tehát normálosztó G-ben.

6.5.5 Állítás: $H \underset{char}{\lhd} N \underset{char}{\lhd} G \Rightarrow H \underset{char}{\lhd} G$, hiszen $\forall \psi \in Aut(G): \psi\big|_N \in Aut(N) \Rightarrow \psi\big|_H = (\psi\big|_N)\big|_H \in Aut(H)$.

6.5.6 Definíció: G csoport centruma $Z(G) = \{a \in G \,|\, \forall x \in G: ax = xa\}$.

6.5.7 Definíció: $K \subseteq G$ normalizátora $N_G(K) = \{a \in G \,|\, aK = Ka\}$, centralizátora $C_G(K) = \{a \in G \,|\, \forall k \in K: ak = ka\}$. Ekkor $Z(G) = C_G(G)$. Könnyen ellenőrizhetően $Z(G) \le C_G(K) \le N_G(K) \le G$.

6.5.8 Állítás: ha $H \le M \le G$, akkor $H \lhd M \Leftrightarrow M \le N_G(H)$, ezért a normalizátor a legbővebb részcsoport, amiben H normálosztó. Ugyanis $H \lhd M \Leftrightarrow \forall x \in M, \forall a \in H: x^{-1}ax \in H \Leftrightarrow \forall x \in M: x \in N_G(H) \Leftrightarrow M \le N_G(H)$.

Megjegyzés: $K \subseteq H \le G$ esetén $N_H(K) = H \cap N_G(K)$ és $C_H(K) = H \cap C_G(K)$ a definíció alapján.

6.5.9 Állítás: $\big|[a]\big| = \big|G: C_G(a)\big|$.

Bizonyítás: $x^{-1}ax = y^{-1}ay \Leftrightarrow yx^{-1}a = ayx^{-1} \Leftrightarrow yx^{-1} \in C_G(a) \Leftrightarrow C_G(a)\cdot x = C_G(a)\cdot y$, tehát a két konjugáltja pontosan akkor egyezik meg, ha a konjugáló elemek $C_G(a)$ azonos jobb oldali mellékosztályában vannak. A konjugáltak szám(osság)a tehát megegyezik a mellékosztályok szám(osság)ával, $\big|G: C_G(a)\big|$-val.

6.5.10 Következmény: véges csoportban $\big|[a]\big|$ osztja $\big|G\big|$-t (pedig $a \ne 1$-re $[a]$ nem részcsoport $1 \notin [a]$ miatt).

6.5.11 Következmény: $a \in Z(G) \Leftrightarrow \big|[a]\big| = 1$. Ugyanis $\big|[a]\big| = 1 \Leftrightarrow C_G(a) = G \Leftrightarrow \forall x \in G: ax = xa \Leftrightarrow a \in Z(G)$. Tehát a centrum nem más, mint az egyelemű konjugált osztályok uniója.

6.5.12 Állítás: ha $H \le G$, akkor H konjugáltjainak száma $\big|G: N_G(H)\big|$.

Bizonyítás: $x^{-1}Hx = y^{-1}Hy \Leftrightarrow yx^{-1}H = Hyx^{-1} \Leftrightarrow yx^{-1} \in N_G(H) \Leftrightarrow N_G(H)\cdot y = N_G(H)\cdot x$, tehát ha x és y ugyanabban az $N_G(H)$ szerinti jobb oldali mellékosztályban vannak. A konjugáltak szám(osság)a tehát megegyezik a mellékosztályok szám(osság)ával, $\big|G: N_G(H)\big|$ $\big|G: C_G(a)\big|$-val.

6.5.13 Állítás: $Z(G) \underset{char}{\lhd} G$.

Bizonyítás: automorfizmus konjugált osztályt konjugált osztályba visz, mert $(x^{-1}ax)\varphi = (x\varphi)^{-1}(a\varphi)(x\varphi)$ és $x^{-1}(a\varphi)x = ((x\varphi^{-1})^{-1}a(x\varphi^{-1}))\varphi$, azaz egy tetszőleges a elem bármely konjugáltjának képe előáll a képének konjugáltjaként és a képének tetszőleges konjugáltja előáll valamely konjugáltja képeként. Mivel bijekció, minden konjugált osztályt egy vele azonos méretűbe visz át, különbözőket különbözőkbe, tehát az egyelemű konjugált osztályok halmazán bijekciót létesít. Ez **6.5.11** alapján éppen azt jelenti, hogy $Z(G)$ képe önmaga. ($Z(G)$ általában nem teljesen karakterisztikus részcsoport, a legkisebb ellenpélda 16 elemű.)

6.5.14 Állítás: $Inn(G) \simeq G/Z(G)$.

Bizonyítás: tekintsük a $\Phi: a \mapsto \varphi_a$ leképezést. $\varphi_{ab} = \varphi_a\varphi_b$ miatt ez homomorfizmus. Képe nyilván $Inn(G)$, magja pedig $Ker\Phi = \{a \in G \,|\, \forall x \in G: x\varphi_a = x\} = \{a \in G \,|\, \forall x \in G: xa = ax\} = Z(G)$. Ezeket beírva a homomorfizmus-tételbe éppen a bizonyítandó állítást kapjuk.

6.5.15 Megjegyzés: $n \ge 3$ esetén $Z(S_n) = \{1\}$, tehát $\big|Aut(S_n)\big| \ge \big|Inn(S_n)\big| = \big|S_n: Z(S_n)\big| = n!$; $n \ne 6$-ra egyenlőség áll fenn, de $n = 6$-ra nem, ami azért érdekes, mert eszerint S_6-nak van külső automorfizmusa. (Ez okozza, hogy S_6-nak van nem triviális módon beágyazott S_5 részcsoportja.)

6.5.16 Definíció: az $a, b \in G$ elemek kommutátora $[a,b] = a^{-1}b^{-1}ab$. Ekkor $ba\cdot[a,b] = ab$ és $[b,a] = [a,b]^{-1}$. Az a és b elemek pontosan akkor felcserélhetőek, ha $[a,b] = 1$ G derivált csoportja avagy kommutátor-részcsoportja $G' = \langle [a,b] \,|\, a,b \in G \rangle$.

6.5.17 Állítás: a kommutátorok halmazát $\forall \varphi: G \to G$ endomorfizmus önmagába képezi, speciálisan a kommutátorok halmaza teljes konjugált osztályok uniója. (Viszont általában nem részcsoport.)

Bizonyítás: $[a,b]\varphi = (a^{-1}b^{-1}ab)\varphi = (a\varphi)^{-1}(b\varphi)^{-1}(a\varphi)(b\varphi) = [a\varphi, b\varphi]$, azaz kommutátor képe valóban kommutátor.

6.5.18 Következmény: G' teljesen karakterisztikus részcsoport G-ben, mert az előző állítás szerint minden endomorfizmus önmagába képezi a kommutátorok halmazát, így az általa generált részcsoportot, G'-t is (ld. **6.5.22**).

6.5.19 Megjegyzés: G Abel-csoport $\Leftrightarrow Z(G)=G \Leftrightarrow G'=\{1\}$.

6.5.20 Állítás: ha a G csoportban minden 1-től különböző elem másodrendű, akkor G kommutatív.

Bizonyítás: minden elem inverze önmaga, így $[a,b]=a^{-1}b^{-1}ab=(ab)(ab)=1$, azaz minden kommutátor 1.

6.5.21 Tétel: ha a G/N faktorcsoport kommutatív, akkor $G'\leq N$, ha pedig $G'\leq N\leq G$, akkor $N\triangleleft G$ és G/N Abel-csoport.

Bizonyítás: G/N kommutatív $\Rightarrow \forall a,b\in G: (aN)(bN)=(bN)(aN) \Rightarrow (ab)N=(ba)N \Rightarrow (a^{-1}b^{-1}ab)N=N \Rightarrow [a,b]\in N$, tehát minden kommutátor benne van N-ben, következésképp a generált részcsoport, G' is.

Ha $G'\leq N$, akkor $\forall a,b\in G: a^{-1}b^{-1}ab\in N$, azaz $b^{-1}ab\in aN$, speciálisan $\forall a\in N, b\in G: b^{-1}ab\in N$, tehát **6.4.6** szerint N normálosztó. Ekkor $\forall aN, bN\in G/N$-re $[a,b]\in N \Rightarrow (bN)(aN)=(ba)N=(ba)\cdot[a,b]N=(ab)N=(aN)(bN)$, tehát G/N valóban kommutatív.

6.5.22 Állítás: legyen Ψ G endomorfizmusainak egy részhalmaza, K pedig egy olyan komplexus, amely zárt Ψ elemeire, azaz $\forall\psi\in\Psi: K\psi\subseteq K$ és jelölje $\langle K\rangle$-t H. Ekkor $H\psi\subseteq H$, azaz a generált részcsoport is zárt Ψ elemeire. Speciálisan $\Psi=Inn(G)$ választással **(1)** normálosztók vagy teljes konjugált osztályok által generált részcsoport normálosztó, $\Psi=Aut(G)$-vel **(2)** karakterisztikus részcsoportok által generált részcsoport karakterisztikus részcsoport.

Bizonyítás: azt kell belátnunk, hogy egy tetszőlegesen választott $a\in H$ elemre és $\psi\in\Psi$ transzformációra $a\psi\in H$. **6.1.19** szerint a előáll $a=a_1a_2a_3\ldots a_m$ alakban, ahol minden a_i vagy eleme K-nak, vagy valamelyik K-beli elem inverze. Ekkor $a\psi=(a_1\psi)(a_2\psi)(a_3\psi)\ldots(a_m\psi)$. Ha $a_i\in K$, akkor $a_i\psi\in K\psi\subseteq K$, ha pedig $a_i^{-1}\in K$, akkor $(a_i\psi)^{-1}=(a_i^{-1})\psi\in K$, tehát $a\psi$ felírásában is minden tényező előáll valamely K-beli elem hatványaként, ezért $a\psi$ **6.1.19** szerint benne van H-ban.

6.5.23 Következmény: $H\leq G$ esetén $H^G\triangleleft G$, hiszen H összes konjugáltjának halmaza invariáns $Inn(G)$ elemeire.

6.5.24 Definíció: a $H\leq G$ által generált normálosztó a legszűkebb H-t tartalmazó normálosztó. Mivel ennek H minden konjugáltját tartalmaznia kell, tartalmazza H^G-t is. $H^G\triangleleft G$, tehát a generált normálosztó $H^G=\langle H^g \mid g\in G\rangle$.

6.6 Belső és külső direkt szorzat

6.6.1 Állítás: ha az N,M normálosztók metszete $\{1\}$, akkor $\langle N,M\rangle$ bármely x eleme egyértelműen áll elő $x=n\cdot m$: $n\in N, m\in M$ alakban és N minden eleme felcserélhető M minden elemével, azaz $\forall n\in N, m\in M: n\cdot m=m\cdot n$.

Bizonyítás: **6.4.12** szerint $\langle N,M\rangle=N\cdot M$, tehát minden eleme előáll $n\cdot m$ alakban. A felírás egyértelmű, mert $n_1m_1=n_2m_2 \Rightarrow n_1^{-1}n_2=m_1m_2^{-1}\in M \Rightarrow n_1^{-1}n_2\in N\cap M=\{1\} \Rightarrow n_1=n_2 \Rightarrow m_1=m_2$. Már csak a felcserélhetőség van hátra, ehhez elég belátni, hogy a n és m kommutátora 1. Márpedig ez $n^{-1}(m^{-1}nm)$ alakban írva egy N-beli elem konjugáltjának és egy másik N-beli elemnek a szorzata, tehát benne van N-ben. Hasonlóan M-ben, azaz a metszetben is, így hát tényleg 1. Ezzel az állítást beláttuk.

6.6.2 Állítás: **(1)** legyenek $\{N_i \mid 1\leq i\leq n\}$ normálosztók G-ben. Jelölje $\langle N_i \mid 1\leq i\leq n, i\neq k\rangle$-t N_k^*. Ha $\forall k: N_k\cap N_k^*=\{1\}$, akkor $\langle N_i \mid 1\leq i\leq n\rangle$ tetszőleges eleme egyértelműen áll elő $\prod_{i=1}^n n_i$: $n_i\in N_i$ alakban, továbbá ebben a szorzatban a tényezők felcserélhetőek. (Ha nem lennének felcserélhetőek, akkor nem is nagyon lenne értelme a $\prod$ jelnek.)

(2) legyenek $\{N_\alpha \mid \alpha\in\mathbf{I}\}$ olyan normálosztók G-ben, melyekre $N_\beta^*=\langle N_\alpha \mid \alpha\in\mathbf{I}\setminus\{\beta\}\rangle$ jelöléssel $\forall\beta\in\mathbf{I}: N_\beta\cap N_\beta^*=\{1\}$. Ekkor bármely $a\in\langle N_\alpha \mid \alpha\in\mathbf{I}\rangle$ elem a sorrendtől egyértelműen áll elő $\prod_{i=1}^k n_i$: $k\in\mathbb{N}, n_i\in N_{\alpha(i)}\setminus\{1\}$ alakban úgy, hogy az $\alpha(i)$ indexek pedig páronként különbözőek. (Az üres szorzat értéke definíció szerint 1.) Ráadásul egy ilyen szorzat tényezői tetszőlegesen felcserélhetőek.

Bizonyítás: **(1)** teljes indukció n-re. $n=2$ esetén az állítás **6.6.1** szerint igaz. Ha $n\geq 2$, akkor alkalmazzuk **6.6.1**-et az N_1, N_1^* normálosztókra (**6.5.22** szerint ezek tényleg normálosztók), majd az indukciós feltevést az N_1^* csoportban az $\{N_i \mid 2\leq i\leq n\}$ normálosztókra. Az egyértelmű előállítást rögtön megkapjuk, továbbá azt, hogy a $\prod_{i=2}^n n_i$: $n_i\in N_i$ szorzat tényezői felcserélhetőek és maga a szorzat felcserélhető n_1-el. Felhasználva **6.6.1**-et az N_1, N_j normálosztókra minden $1\leq j\leq n$-re megkapjuk a teljes felcserélhetőséget. Ezzel az állítást beláttuk.

(2): tudjuk, hogy a felírható $a=a_1a_2a_3\ldots a_m$: $a_i\in N_{\alpha(i)}$ alakban. Alkalmazva **(1)**-et az $\{N_{\alpha(i)} \mid 1\leq i\leq m\}$ normálosztókra kapjuk, hogy ezen szorzat különböző normálosztókból származó tényezői felcserélhetőek, tehát

össze tudjuk csoportosítani az azonos N_α-ból származóakat. Az asszociativitás miatt ezeket a részeket külön-külön összeszorozhatjuk, a keletkező 1-eket elhagyhatjuk; így a feltételeknek megfelelő felírást kapunk. Tudjuk **(1)**-ből, hogy ennek valóban felcserélhetőek a tényezői; már csak a felírás egyértelműségét kell belátnunk. Tegyük fel, hogy $a_1a_2a_3\dots a_k=b_1b_2b_3\dots b_m$, ahol $a_i\in N_{\alpha(i)}, b_j\in N_{\beta(j)}$. Alkalmazva **(1)**-et a $\{N_{\alpha(i)}\,|\,1\le i\le k\}\cup\{N_{\beta(j)}\,|\,1\le j\le m\}$ normálosztókra kapjuk, hogy a két felírás azonos.

6.6.3 Definíció: G az N,M normálosztók belső direkt szorzata, ha $N\cap M=\{1\}$ és $\langle N,M\rangle=G$. Jelölése $G=N\times M$. Nyilván $G=N\times M, G_1=N_1\times M_1, N\simeq N_1, M\simeq M_1$ esetén $G\simeq G_1$. Véve ugyanis $\varphi: N\xrightarrow{\sim} N_1, \psi: M\xrightarrow{\sim} M_1$-t a $\Psi_{[G\to G_1]}: n\cdot m_{[n\in N,\,m\in M]}\mapsto n\varphi\cdot m\psi$ leképezés **6.6.1** szerint jóldefiniált, bijektív és szemmel láthatóan művelettartó, azaz izomorfizmus.

6.6.4 Definíció: az N,M csoportok $N\times M$ külső direkt szorzatának alaphalmaza $\{(n,m)\,|\,n\in N, m\in M\}$, a művelet pedig $(n_1,m_1)\cdot(n_2,m_2)=(n_1n_2,m_1m_2)$. Ez könnyen láthatóan szintén csoport lesz, egysége $(1,1)$, rendje $|N\times M|=|N|\cdot|M|$. Az is triviális, hogy $N\simeq N_0=\{(n,1)\,|\,n\in N\}$ és $M\simeq M_0=\{(1,m)\,|\,m\in M\}$. Szintén nyilvánvaló $N_0\cap M_0=\{1\}$. Ráadásul $N_0\lhd N\times M$, hiszen $(n,1)\in N_0$-t konjugálva $(x,m)\in N\times M$-el $(x^{-1}nx, m^{-1}\cdot 1\cdot m)=(x^{-1}nx,1)\in N_0$. Ugyanígy $M_0\lhd N\times M$. A fentieket összevetve és a direkt szorzatot G-vel jelölve teljesülnek **6.6.3** feltételei, tehát G belső direkt szorzata az N-el ill. M-el izomorf N_0, M_0 normálosztóknak.

6.6.5 Definíció: G az $\{N_i\,|\,1\le i\le n\}$ normálosztók belső direkt szorzata, ha **6.6.2** jelöléseivel $\forall k: N_k\cap N_k^*=\{1\}$ és $\langle N_i\,|\,1\le i\le n\rangle=G$. Jelölése $G=\prod_{i=1}^n N_i$ vagy $G=\mathop{\times}_{i=1}^{n} N_i$. Ekkor nyilván $G=(\dots((N_1\times N_2)\times N_3)\times\dots\times N_{n-1})\times N_n$.

6.6.6 Definíció: a $\{G_i\,|\,1\le i\le n\}$ csoportok külső direkt szorzata az $(g_1,g_2,g_3,\dots,g_k)$: $g_i\in G_i$ elemek halmaza a koordinátánkénti művelettel. Jelölése ugyanaz, mint a belső direkt szorzaté. Ha két külső direkt szorzat megfelelő tényezői izomorfak, akkor a szorzatok is izomorfak. $\{G_i\,|\,1\le i\le n\}$ külső direkt szorzat belső direkt szorzata lesz a G_i-vel izomorf $N_i=\{(1,\dots,1,g_i,1,\dots,1)\}$ normálosztóknak, sőt G pontosan akkor állhat elő G_i-vel rendre izomorf N_i normálosztók belső direkt szorzataként, ha izomorf $\{G_i\,|\,1\le i\le n\}$ külső direkt szorzatával.

6.6.7 Definíció: G csoport (diszkrét) belső direkt szorzata az $\{N_\alpha\,|\,\alpha\in\mathbf{I}\}$ normálosztóknak, ha $\langle N_\alpha\,|\,\alpha\in\mathbf{I}\rangle=G$ és $\forall\beta\in\mathbf{I}: N_\beta\cap N_\beta^*=\{1\}$ a szokásos jelölésekkel. (Ennek speciális esete **6.6.3** és **6.6.5**.)

6.6.8 Definíció: a $\{G_\alpha\,|\,\alpha\in\mathbf{I}\}$ csoportok G (diszkrét) külső direkt szorzatának alaphalmaza azon $\gamma:\mathbf{I}\to\bigcup_{\alpha\in\mathbf{I}}G_\alpha$ függvények halmaza, melyekre $\forall\alpha\in\mathbf{I}$: $\gamma(\alpha)\in G_\alpha$ és az $\{\alpha\in\mathbf{I}\,|\,\gamma(\alpha)\ne 1\}$ halmaz véges. („Szemléletesen" ezek olyan $|\mathbf{I}|$ dimenziós vektorok, melyek α-dik koordinátája G_α egy eleme és véges sok kivétellel mindegyik koordináta a megfelelő csoport egységeleme.) A művelet az, ami logikus, azaz $\gamma_1,\gamma_2\in G$-re $\gamma_1\gamma_2:\alpha\mapsto\gamma_1(\alpha)\cdot\gamma_2(\alpha)$; itt a szorzás a G_α-beli szorzást jelöli (ez egyszerűen azt jelenti, hogy koordinátánként szorzunk). Könnyen ellenőrizhető, hogy G valóban csoport lesz. (Ennek a direktszorzásnak speciális esete **6.6.4** és **6.6.6**.)

Legyen $\beta\in\mathbf{I}$-re $N_\beta=\{\chi_{\beta,g}\,|\,g\in G_\beta\}$, ahol $\chi_{\beta,g}$ β-hoz g-t rendel, $\mathbf{I}$ többi eleméhez 1-et. (Ez az a vektor, aminek β-dik koordinátája g, a többi 1.) Ekkor $G_\beta\simeq N_\beta$ és

$$\forall\gamma\in G, \chi_{\beta,g}\in N_\beta, \alpha\in\mathbf{I}\setminus\{\beta\}: (\gamma^{-1}\chi_{\beta,g}\gamma)(\alpha)=\gamma^{-1}(\alpha)\chi_{\beta,g}(\alpha)\gamma(\alpha)=(\gamma(\alpha))^{-1}\cdot 1\cdot\gamma(\alpha)=1.$$

Eszerint $\forall\gamma\in G, \chi_{\beta,g}\in N_\beta$: $\gamma^{-1}\chi_{\beta,g}\gamma\in N_\beta$, azaz $N_\beta\lhd G$. Az is látszik, hogy $\langle N_\alpha\,|\,\alpha\in\mathbf{I}\rangle=G$ és $\forall\beta\in\mathbf{I}: N_\beta\cap\langle N_\alpha\,|\,\alpha\in\mathbf{I}\setminus\{\beta\}\rangle=\{1\}$, tehát G előáll az $\{N_\alpha\,|\,\alpha\in\mathbf{I}\}$ normálosztók (diszkrét) belső direkt szorzataként.

Mind a hat esetben látható, hogy ha két direkt szorzat megfelelő tényezői izomorfak, akkor a kapott szorzatok is izomorfak lesznek. Mindhárom esetben beláttuk, hogy a $\prod_{\alpha\in\mathbf{I}}G_\alpha$ külső direkt szorzat előáll $\{N_\alpha\,|\,\alpha\in\mathbf{I}\}$ normálosztóinak belső direkt szorzataként, ahol $\forall\alpha\in\mathbf{I}: G_\alpha\simeq N_\alpha$. Ezek alapján G pontosan akkor bontható G_α-val rendre izomorf N_α normálosztók belső direkt szorzatára, ha izomorf a $\prod_{\alpha\in\mathbf{I}}G_\alpha$ külső direkt szorzattal.

Mivel a belső direkt szorzat definícióján nem változtat a tényezők tetszőleges permutációja, a külső direkt szorzat tényezőinek permutálása csak izomorfia erejéig változtathatja meg a szorzatcsoportot. Megfelelő mennyiségű index és homomorfizmus bevezetésével be lehetne látni, hogy ha a $G\simeq\prod_{\alpha\in\mathbf{I}}G_\alpha$ külső direkt szorzat tényezői rendre a $G_\alpha\simeq\prod_{\beta\in\mathbf{I}_\alpha}H_\beta$ külső direkt szorzatok, akkor $G\simeq\prod_{\alpha\in\mathbf{I},\,\beta\in\mathbf{I}_\alpha}H_\beta$; ezt most nem teszem meg. Ez lehetővé teszi, hogy kissé absztraktabb módon definiáljuk a direkt szorzatot:

6.6.9 Definíció: a direkt szorzás (a belső és külső direktszorzást összevonva) olyan művelet a csoportok izomorfia-osztályai felett (ez más néven egy függvény, amely csoportok izomorfia-osztályainak rendezett

halmazaihoz egy izomorfia-osztályt rendel), amely teljesíti, hogy a $\prod_{\alpha\in\mathbf{I}}\Gamma_\alpha$ művelet eredménye olyan Γ izomorfia-osztály, melyben egy (tetszőleges) G elemnek találhatóak olyan $\{N_\alpha \mid \alpha\in\mathbf{I}\}$ komplexusai, melyekre

(1) $\forall\alpha\in\mathbf{I}: N_\alpha\in\Gamma_\alpha$
(2) $\forall\alpha\in\mathbf{I}: N_\alpha\lhd G$
(3) $\langle N_\alpha \mid \alpha\in\mathbf{I}\rangle = G$
(4) $\forall\alpha\in\mathbf{I}: N_\alpha\cap\langle N_\beta \mid \beta\in\mathbf{I}\setminus\{\alpha\}\rangle=\{1\}$

Mindezidáig azt láttuk be (vagy hittük el), hogy ilyen művelet létezik (ezt neveztük külső direkt szorzatnak) és hogy csak egy lehet (mert az eredmény belső direkt szorzata lesz a tényezőknek, ami csak akkor lehetséges, ha izomorf az általunk megadott külső direkt szorzattal). Eszerint ez egy jóldefiniált művelet. A definíció szimmetriájából következik, hogy kommutatív (a tényezők permutációja nem változtatja) és asszociatív (ez az, amit egyáltalán nem láttunk be). Egységeleme nyilván az egyelemű csoport. **6.6.2.2** szerint a szorzat minden eleme egyértelműen előáll $\prod_{\alpha\in\mathbf{J}} n_\alpha \;:\; \mathbf{J}\subset\mathbf{I}, |\mathbf{J}|<\infty, n_\alpha\in N_\alpha\setminus\{1\}$ alakban, továbbá a szorzat tényezői felcserélhetőek. Ezeket a tényezőket a jövőben koordinátáknak hívom.

6.6.10 Megjegyzés: létezik $\prod^*_{\alpha\in\mathbf{I}} G_\alpha$ ún. komplett direkt szorzat is; itt az alaphalmazba belevesszük azokat az elemeket is, melyeknek végtelen sok 1-től különböző koordinátájuk is van. Erre persze nem teljesül **6.6.9.3**.

6.6.11 Állítás: ha a $G=\prod_{\alpha\in\mathbf{I}} G_\alpha$ csoportban a (1-től különböző) koordinátái $\{a_i\in G_{\alpha(i)} \mid 1\le i\le n\}$, akkor $o(a)$ az o_i számok legkisebb közös többszöröse, ahol o_i az a_i elem rendje a $G_{\alpha(i)}$ csoportban; ha ezek valamelyike végtelen, akkor $o(a)$ is végtelen. (Komplett direkt szorzatban az is megeshet, hogy minden koordináta rendje véges, de ezek nem korlátos halmazt alkotnak – az elem rendje ekkor is végtelen lesz.)

Bizonyítás: a k-adik hatványa pontosan akkor 1, ha minden koordinátája 1. Mivel a direkt szorzatban koordinátánként szorzunk, ez pontosan akkor teljesül, ha a minden koordinátájának k-adik hatványa 1, azaz ha k többszöröse az összes o_i-nek. A legkisebb ilyen k tehát a legkisebb közös többszörös, illetve nincs ilyen k, ha valamelyik koordináta rendje végtelen.

6.6.12 Jelölés: $(\prod_{\alpha\in\mathbf{I}} G)$-t $G^{|\mathbf{I}|}$-vel jelöljük. Z_2^2 például a Klein-féle csoport.

6.7 Cauchy-tétel

6.7.1 Definíció: G elemi Abel-csoport, ha véges sok Z_p direkt szorzata, azaz $G\simeq Z_p^n$. Ekkor **6.6.11** szerint minden 1-től különböző elemének rendje p. Ez mellesleg izomorf az $\mathbb{F}_p$ feletti n dimenziós vektortér additív csoportjával.

6.7.2 Definíció: G p-csoport, ha $\forall a\in G\setminus\{1\}: o(a)<\infty, p\mid o(a)$ és $G\neq\{1\}$. Ilyen pl. Z_{p^k}, Z_{p^∞} és **6.3.5** szerint minden p^n rendű csoport.

6.7.3 „Majdhogynem tétel": ha $|G|=p^n$, akkor $p\,\big|\,|Z(G)|$.

Bizonyítás: osszuk fel G-t konjugált osztályokra. **6.5.10** alapján minden konjugált osztály mérete osztja a csoport rendjét, tehát p hatványa, speciálisan vagy p többszöröse, vagy 1. A $Z(G)$-n kívüli konjugált osztályok mérete tehát mindig p többszöröse, akárcsak a teljes csoport mérete. Eszerint a kimaradó rész, $Z(G)$ elemszáma is p többszöröse és épp ezt akartuk belátni. Rövidesen (**6.7.5**) be fogjuk látni, hogy minden véges p-csoport rendje p-hatvány, tehát minden véges p-csoport centrumának rendje p többszöröse.

6.7.4 Cauchy-tétel: ha a G véges csoport rendjét osztja a p prím, akkor $\exists a\in G: o(a)=p$.

Bizonyítás: tekintsük az $x_1x_2x_3\ldots x_p=1$ egyenlet összes megoldásainak M halmazát. Az első $p-1$ elem tetszőleges választásához pontosan egy x_p ad megoldást, tehát $|M|=|G|^{p-1}$. Tekintsük azt a $\vartheta: G^p\to G^p$ transzformációt, ami $v=(g_1,g_2,\ldots,g_p)$-hez $v\vartheta=(g_p,g_1,g_2,\ldots,g_{p-1})$-et rendeli. Könnyen ellenőrizhetően $v\in M\Rightarrow v\vartheta\in M$. Vegyük észre, hogy $v_1\sim v_2\Leftrightarrow\exists n\in\mathbb{Z}: v_1\vartheta^n=v_2$ ekvivalencia-reláció. Ez M-et ekvivalencia-osztályokra bontja. Ha $v\in M$ minden koordinátája azonos, akkor egyelemű ekvivalencia -osztályban van. Különben p eleműben, hiszen ϑ^p az identitás. Mivel $|M|$ osztható p-vel, a nem p elemű ekvivalencia-osztályok uniójának mérete is osztható p-vel. Ez éppen az olyan megoldások száma, ahol minden x_i megegyezik, azaz $p\,\big|\,|\{x\in G\mid x^p=1\}|=1+|\{x\in G\mid o(x)=p\}|$. Tehát legalább $(p-1)$ p-edrendű elem van G-ben.

6.7.5 Következmény: véges p-csoport rendje nem lehet osztható p-től különböző q prímmel, mert nincs q-adrendű eleme. Tehát minden véges p-csoport rendje p-hatvány.

6.8 Kettős mellékosztályok. Sylow tételei

6.8.1 Definíció: legyen $H,K\leq G$. Ekkor a H,K szerinti kettős mellékosztályok a $\{HxK\,|\,x\in G\}$ komplexusszorzatok. Az alábbiak teljesülnek rájuk:

(1) $x\in HxK$

(2) a HxK, HyK kettős mellékosztályok vagy azonosak, vagy diszjunktak.

Bizonyítás: ha diszjunktak, akkor az állítás igaz. Ha nem, akkor valamely $h_1,h_2\in H;k_1,k_2\in K$ elemekre $h_1xk_1=h_2yk_2$. Ekkor $\forall h_3\in H,k_3\in K: h_3xk_3=h_3h_1^{-1}(h_1xk_1)k_1^{-1}k_3=(h_3h_1^{-1}h_2)y(k_2k_1^{-1}k_3)\in HyK$ tehát $HxK\subseteq HyK$. Hasonlóan $HyK\subseteq HxK$, ezzel az állítást beláttuk. Következmény:

(3) a kettős mellékosztályok a csoport egy partícióját adják. Egy kettős mellékosztály egyrészt H szerinti jobb oldali mellékosztályok uniója, másrészt K szerinti bal oldali mellékosztályok uniója.

6.8.2 Állítás: a HxK kettős mellékosztály **(1)** $|K:(H^x\cap K)|$ H szerinti jobb oldali, illetve **(2)** $|H^x:(H^x\cap K)|$ K szerinti bal oldali mellékosztályból áll.

Bizonyítás: az állítás első feléhez legyen Hxa és Hxb két HxK-beli H szerinti jobb oldali mellékosztály, $a,b\in K$. Nézzük meg, mikor egyeznek ezek meg: $Hxa=Hxb \Leftrightarrow Hxab^{-1}x^{-1}=H \Leftrightarrow xab^{-1}x^{-1}\in H \Leftrightarrow ab^{-1}\in x^{-1}Hx$. Mivel $a,b\in K$, ez ekvivalens $ab^{-1}\in H^x\cap K$-val, ami **6.3.1.6** alapján pontosan akkor teljesül, ha a és b ugyanabban a $H^x\cap K$ szerinti jobb oldali mellékosztályban vannak. A különböző HxK-beli H szerinti jobb oldali mellékosztályok szám(osság)a tehát megegyezik a különböző K-beli $H^x\cap K$ szerinti jobb oldali mellékosztályok szám(osság)ával, ami éppen $|K:(H^x\cap K)|$.

Lássuk a második részt: legyen $a,b\in H$. Ekkor $axK=bxK \Leftrightarrow x^{-1}b^{-1}axK=K \Leftrightarrow x^{-1}b^{-1}xx^{-1}ax\in K \Leftrightarrow (x^{-1}bx)^{-1}(x^{-1}ax)\in(x^{-1}Hx\cap K)$, ami pontosan akkor teljesül, ha az $a^x,b^x\in H^x$ elemek ugyanabban a $H^x\cap K$ szerinti bal oldali mellékosztályban vannak. Ezért a különböző HxK-beli K szerinti bal oldali mellékosztályok szám(osság)a megegyezik a H^x-beli $H^x\cap K$ szerinti bal oldali mellékosztályok szám(osság)ával, ami $|H^x:(H^x\cap K)|$.

6.8.3 Sylow I. tétele: legyen G véges csoport rendje $p^k\cdot m$, ahol p prím, $k\geq 1$ és $p\nmid m$. Ekkor $0\leq i\leq k-1, P\leq G$, $|P|=p^i \Rightarrow \exists P^*\leq G: (|P^*|=p^{i+1}$ és $P\lhd P^*)$, azaz minden p^k-nál kisebb rendű p-részcsoport normálosztóként belerakható egy éppencsak nagyobb p-részcsoportba. Mivel van egyelemű részcsoport, ebből mellesleg következik, hogy $1\leq i\leq k$-ra van p^i rendű részcsoport.

Bizonyítás: teljes indukció i-re. $i=0$-ra az állítás éppen a Cauchy-tétel, amit már beláttunk. Legyen most $1\leq i\leq k-1$. Az indukciós feltevés szerint létezik p^i rendű részcsoport G-ben. Legyen P ilyen. Vegyük a P,P kettős mellékosztályokat, legyenek ezek $\{P\cdot x_i\cdot P\,|\,1\leq i\leq n, x_1=1\}$. A Px_iP kettős mellékosztály éppen $|P:(P^{x_i}\cap P)|$ P szerinti jobb oldali mellékosztály uniója; jelölje ezt a_i. A Lagrange-tétel szerint $a_i\,||P|=p^i$, azaz a_i vagy 1, vagy p-hatvány. Másrészt $\sum a_i$ éppen az összes P szerinti jobb oldali mellékosztály száma, azaz $|G:P|=p^{k-i}$, osztható p-vel. A p-hatvány a_i-k összege osztható p-vel, így a maradék, a p-vel nem osztható a_i-k összege is. Mivel minden a_i vagy 1, vagy p-hatvány, $\sum_{i=1,p\nmid a_i}^{n} a_i=\sum_{a_i=1} a_i=|\{i: a_i=1\}|$.

Tudjuk, hogy $|P:(P^{x_i}\cap P)|=1 \Leftrightarrow P^{x_i}=P \Leftrightarrow x_i\in N_G(P)$. Ez alapján $|\{i: a_i=1\}|=|\{i: x_i\in N_G(P)|$. Márpedig $x_i\in N_G(P)$ esetén $(Px_i)P=x_iP=Px_i\subseteq N_G(P)$, ami azt jelenti, hogy az ilyen kettős mellékosztályok éppen az $N_G(P)$-beli P szerinti mezei mellékosztályok, ezekből kétségkívül $|N_G(P):P|$ van. Így hát $|\{i: a_i=1\}|=|N_G(P):P|$.

Mindezt összevetve $|N_G(P):P|$ osztható p-vel, azaz az $N_G(P)/P$ faktorcsoport rendje is. Ekkor a Cauchy-tétel szerint van benne egy p-edrendű elem, ami generál egy H p-edrendű ciklikus részcsoportot. Legyen ψ az $N_G(P)\to N_G(P)/P$ természetes homomorfizmus. Ekkor H ψ szerinti teljes inverz képe egy P^* részcsoport, melynek rendje p^{i+1}. $P^*\leq N_G(P)$ miatt $P\lhd P^*$, már kész is vagyunk.

6.8.4 Definíció: a G $p^k\cdot m$ rendű csoport p-Sylow-részcsoportjai avagy röviden p-Sylowjai a p^k rendű részcsoportok, ezek halmazát $Syl_p(G)$-vel jelöljük.

6.8.5 Sylow II. tétele: $P,R\in Syl_p(G) \Rightarrow \exists x\in G: P^x=R$, azaz G-nek minden p-Sylowja izomorf, ezért van értelme „a" p-Sylowról beszélni.

Bizonyítás: legyenek a P,R szerinti kettős mellékosztályok $\{Px_iR \mid 1\le i\le n\}$. Legyen $a_i=\left|P^{x_i}:(P^{x_i}\cap R)\right|$, ennyi R szerinti bal oldali mellékosztályból áll Px_iR. Eszerint $\sum_{i=1}^{n}a_i=\left|G:R\right|=m$, ez nem osztható p-vel. a_i ismét csak 1 vagy p-hatvány lehet, mert egy p^k rendű csoport egy részcsoportjának indexe. Csupa p-hatvány nem lehet, mert az összeg nem osztható p-vel. Eszerint $\exists i:\left|P^{x_i}:(P^{x_i}\cap R)\right|=1$, azaz $P^{x_i}=P^{x_i}\cap R$. Mivel P^{x_i} és R azonos méretű véges csoportok, ebből következik $P^{x_i}=R$, a bizonyítandó állítás.

6.8.6 Következmény: $P\in Syl_p(G)\Rightarrow \left|Syl_p(G)\right|=\left|\{P \text{ konjugáltjai}\}\right|$, ami **6.5.12** szerint $\left|G:N_G(P)\right|$. Ez mellesleg osztja P indexét (lévén $P\le N_G(P)$), ami a Lagrange-tétel szerint m. Összefoglalva $\left|Syl_p(G)\right|\Big|m$.

6.8.7 Sylow III. tétele: $\left|Syl_p(G)\right|\equiv 1 \pmod p$.

Bizonyítás: legyen $Syl_p(G)=P\cup\{P_i \mid 1\le i\le n\}$. Definiáljuk a következő relációt $Syl_p(G)\setminus\{P\}$ felett: $P_i\approx P_j$, ha $\exists x\in P:(P_i)^x=P_j$. Ez ekvivalencia-reláció lesz. Nézzük meg, mikor lesz azonos valamely p-Sylow két P-beli elemmel vett konjugáltja: $x,y\in P, 1\le i\le n$-re $(P_i)^x=(P_i)^y \Leftrightarrow P_i\cdot xy^{-1}=xy^{-1}\cdot P_i \Leftrightarrow xy^{-1}\in P\cap N_G(P_i)$. Pontosan akkor, ha ugyanabban az $N=P\cap N_G(P_i)$ szerinti jobb oldali mellékosztályban vannak. P_i konjugáltjainak száma tehát ezen mellékosztályok száma, azaz $\left|P:N\right|$. Ez a változatosság kedvéért vagy 1, vagy p-hatvány. Ha 1 lenne, akkor $N=P$, azaz $P\le N_G(P_i)$. Ekkor $N_G(P_i)$-nek részcsoportja lenne P és P_i is, utóbbi normálosztó. Mivel P és P_i rendje p^k, ennél magasabb p-hatvány pedig nem oszthatja $N_G(P_i)\le G$ rendjét, P és P_i egyaránt $p-$Sylow lenne $N_G(P_i)$-ben, így **6.8.5** szerint egymás konjugáltjai lennének $N_G(P_i)$-ben. Ez lehetetlen, mert $P_i\lhd N_G(P_i)$, tehát egyetlen konjugáltja önmaga, P pedig ettől különbözik.

Tehát $\left|P:N\right|$ sohasem 1, azaz mindig p-hatvány. Eszerint a fent megadott ekvivalencia-osztályok mindegyikének mérete osztható p-vel. Ezek lefedik $Syl_p(G)\setminus\{P\}$-t, azaz $\left|Syl_p(G)\setminus\{P\}\right|=\left|Syl_p(G)\right|-1$ osztható p-vel. Ezzel az állítást beláttuk.

6.8.8 Tétel: ha G rendje $p^k\cdot s$ (ahol s esetleg osztható p-vel), akkor a G-beli p^k rendű részcsoportok száma p-vel osztva 1 maradékot ad. Ennek speciális esete Sylow III. tétele.

6.8.9 Megjegyzés: ha G rendje osztható p-vel, akkor egy P p-részcsoport pontosan akkor p-Sylow, ha $p\nmid\left|G:P\right|$.

6.9 Szemidirekt szorzat

6.9.1 Definíció: legyenek A,B csoportok, $\vartheta:A\to Aut(B)$ homomorfizmus ($\vartheta:a\mapsto\vartheta_a$). Ekkor az $A\leftthreetimes_{\vartheta}B$ szemidirekt szorzat alaphalmaza $\{(a,b)\mid a\in A,b\in B\}$, a művelet pedig $(a,b)\cdot(a',b')=(a\cdot a',b\vartheta_{a'}\cdot b')$. Némi számolással ellenőrizhető, hogy $A\leftthreetimes_{\vartheta}B$ erre a műveletre csoportot alkot. Ennek speciális esete a (kétényezős) direkt szorzat, ahol is ϑ A minden elemét a B feletti identitásba képezi, így $b\vartheta_{a'}=b$.

Vegyük észre, hogy $(a,1)\cdot(a',1)=(a\cdot a',1)$, $(a,1)^{-1}=(a^{-1},1)$, $(1,b)\cdot(1,b')=(1,b\cdot b')$ és $(a,1)\cdot(1,b)=(a,b)$. (Felhasználtuk, hogy ϑ_1 az identitás, hiszen ϑ homomorfizmus.)

6.9.2 Állítás: a $G=A\leftthreetimes_{\vartheta}B$ szemidirekt szorzatban $A_0=\{(a,1)\mid a\in A\}, B_0\{(1,b)\mid b\in B\}$ választással $A\simeq A_0\le A\leftthreetimes_{\vartheta}B$, $B\simeq B_0\lhd A\leftthreetimes_{\vartheta}B$, $A_0\cap B_0=\{1\}$ és $A_0B_0=G$.

Bizonyítás: ebből csak az nem triviális, hogy B_0 minden konjugáltja önmaga. Vegyük egy B_0-beli elem egy A_0-belivel vett konjugáltját: $(a,1)^{-1}(1,b)(a,1)=(a^{-1},1)(a,b\vartheta_a)=(a^{-1}a,1\vartheta_{a^{-1}}\cdot b\vartheta_a)=(1,b\vartheta_a)\in B_0$. Eszerint $A_0\le N_G(B_0)$. Mivel $B_0\le N_G(B_0)$ a definícióból következik, $G=A_0B_0\le N_G(B_0)\Rightarrow B_0\lhd G$.

6.9.3 Állítás: legyen $A\le B, B\lhd G, AB=G$ és $A\cap B=\{1\}$. Ekkor $\forall x\in G$ egyértelműen írható fel $x=ab$: $a\in A,b\in B$ alakban.

Bizonyítás: hogy felírható, az a feltételek része volt. Ha pedig $x=a_1b_1=a_2b_2$, akkor $A\ni a_2^{-1}a_1=b_1b_2^{-1}\in B$, így ez az elem benne van $A\cap B=\{1\}$-ben, tehát $a_1=a_2, b_1=b_2$, a két felírás azonos.

6.9.4 Definíció: legyen $A\le G, B\lhd G, AB=G$ és $A\cap B=\{1\}$. Ekkor $x_1,x_2\in G$ egyértelműen áll elő $x_1=a_1b_1, x_2=a_2b_2$ alakban. Továbbá $x_1x_2=a_1b_1a_2b_2=(a_1a_2)(a_2^{-1}b_1a_2b_2)=(a_1a_2)(b\varphi_{a_2}\cdot b_2)$. Az első tényező szemmel láthatóan A-ban van, a második pedig $b_1\in B\lhd G$ egy konjugáltjának és $b_2\in B$-nek a szorzata, ez benne van B-ben. Vegyük észre, hogy a $\vartheta:A\to Inn(G), a\mapsto\varphi_a$ homomorfizmus $B\lhd G$ miatt tekinthető $\vartheta:A\to Aut(B)$ leképezésnek is, továbbá $\forall a,a'\in A; b,b'\in B$ esetén $(ab)(a'b')=(aa')(b\vartheta_{a'}\cdot b')$. Ennek örömére G-t elnevezzük A és B belső szemidirekt szorzatának.

Látható, hogy **6.9.2** jelöléseivel a $G=A\leftthreetimes_{\vartheta}B$ szemidirekt szorzatban $\varphi_{(a,1)}$-t B_0-ra megszorítva $a\vartheta$-t kapjuk (bár nem $Aut(B)$, hanem $Aut(B_0)$ elemeként, de ez lényegtelen), tehát G belső szemidirekt szorzata A,B-nek.

6.10 Maximális részcsoport, maximális *p*-normálosztó. Frattini-részcsoport

6.10.1 Definíció: az M részcsoport maximális részcsoportja a G csoportnak, ha $M<G$ és nincsen $M<H<G$ részcsoport. Ez ekvivalens azzal, hogy $x\in G\setminus M \Rightarrow \langle M,x\rangle=G$.

Véges csoportban ilyen mindig van (kivéve az egyelemű csoportot). A kváziciklikus csoportban például nincs, a végtelen ciklikus csoportban pedig a $Z_\infty\to Z_p$ faktorleképezés magja minden p prímre maximális részcsoport.

6.10.2 Megjegyzés: a maximális részcsoport nem feltétlenül nagy, például S_p-ben van $Aff(p)$-vel izomorf maximális részcsoport (bár ezt elég nehéz belátni, most csak úgy megemlítjük), pedig $|S_p|=p!$ és $|Aff(p)|=p(p-1)$. Véges p-csoportban **6.8.3**-ból tudjuk, hogy minden maximális részcsoport normálosztó és indexe p.

6.10.3 Állítás: ha G-nek nincs nem triviális részcsoportja, akkor $G\simeq Z_p$ vagy $G\simeq 1$.

Bizonyítás: ha van végtelen rendű eleme, akkor az generál egy $Z_\infty\simeq\langle a\rangle\le G$-t. Ekkor $Z_\infty\simeq\langle a^2\rangle<\langle a\rangle\le G$, tehát találtunk egy $Z_\infty<G$-t. Ha van $a\neq 1$ véges rendű elem, akkor $Z_{o(a)}\simeq\langle a\rangle\le G$. Ha $G\neq\langle a\rangle$, akkor $\langle a\rangle<G$ és kész vagyunk. Ha $G=\langle a\rangle$ és $\exists k\in\mathbb{N}$: $(1<k<a$ és $k\,|\,o(a))$, akkor $1<\langle a^k\rangle<G$. Ha nincs ilyen k, akkor $o(a)=p$ prím és $G\simeq Z_p$. Ha sem végtelen rendű, sem 1-től különböző véges rendű elemet nem találunk, akkor $G\simeq 1$.

6.10.4 Állítás: ha $N\lhd G$ maximális részcsoport, akkor $G/N\simeq Z_p$. Ugyanis ha G/N-ben lenne nem triviális részcsoport, akkor annak a $G\to G/N$ természetes homomorfizmus szerinti M teljes inverz képére $N<M<G$ lenne, ami ellentmond N maximalitásának. Ha pedig G/N-nek nincs nem triviális részcsoportja, akkor **6.10.3** szerint prím rendű ciklikus csoport. (Az egyelemű csoport nem lehet, mert $N<G$.)

6.10.5 Definíció: G Frattini-részcsoportja $\Phi(G)=\bigcap_{\substack{M\text{ maximális}\\ \text{részcsoport }G\text{-ben}}} M$; az üres metszet definíció szerint a teljes G. Maximális részcsoport képe nyilván minden automorfizmusnál maximális részcsoport, tehát $\Phi(G)\underset{char}{\lhd}G$.

Megjegyzés: könnyen látható, hogy egy direkt szorzat centruma a tényezők centrumainak direkt szorzata és a szorzat kommutátor-részcsoportja is a kommutátor-részcsoportok szorzata. A maximális részcsoportok sajnos nem ilyen szépek – már a kéttényezős direkt szorzat Frattini-részcsoportjáról sem lehet bebizonyítani, hogy a tényezők Frattini-részcsoportjainak direkt szorzata (vagy mert nem igaz, vagy mert eldönthetetlen).

6.10.6 Definíció: G véges csoport p-normálosztója egy $P\lhd G$ p-részcsoport. G maximális p-normálosztója a legbővebb p-normálosztó (ld. **6.10.7**). Ezt $o_p(G)$ jelöli. Ha π prímszámok egy halmaza, akkor $o_\pi(G)$ a legbővebb olyan normálosztó, amelynek rendjének prímtényezői π-ben vannak. Ez könnyen ellenőrizhetően $\langle o_p(G)\,|\,p\in\pi\rangle$. Megjegyzendő, hogy p' általában a p-től különböző prímek halmazát jelöli, például $o_{2'}(G)$ (néha egyszerűen $o(G)$) a maximális páratlan normálosztó.

6.10.7 Állítás: véges csoportban van maximális (sőt legnagyobb) p-normálosztó, mert a p-normálosztók által generált részcsoport is p-normálosztó.

Bizonyítás: elég bebizonyítani, hogy ha P_1 és P_2 p-normálosztó G-ben, akkor P_1P_2 is. (Véges csoportban csak véges sok p-normálosztó kerülhet elő, így a generált részcsoportot fel tudjuk építeni úgy, hogy egyszerre mindig csak egy új normálosztót veszünk be.) **6.4.13** szerint $P_1P_2/P_1\simeq P_2/P_1\cap P_2$, azaz $|P_1P_2:P_1|=|P_2:P_1\cap P_2|$. A Lagrange-tétel felhasználásával $|P_1P_2|\cdot|P_1\cap P_2|=|P_1|\cdot|P_2|$. A jobb oldal p-hatvány, ezért a bal is, így $|P_1P_2|$ is. Eszerint P_1P_2 p-csoport és **6.5.22** szerint normálosztó, kész vagyunk. A bizonyítás lényegében ugyanez $o_\pi(G)$ létezésére is.

6.10.8 Állítás: $o_p(G)=\bigcap_{P\in Syl_p(G)}P$.

Bizonyítás: ha N egy p-normálosztó, akkor **6.8.3** szerint része valamelyik P p-Sylownak. Ekkor minden konjugáltja része P megfelelő konjugáltjának. N minden konjugáltja önmaga, P összes konjugáltja az összes p-Sylow, tehát N része az összes p-Sylownak, így a metszetüknek is. Az összes p-Sylow metszete például a Lagrange-tétel szerint p-csoport és normálosztó, mert bármely konjugáltja csak a metszet tényezőit permutálja, magukat a p-Sylowokat nem változtatja. Ezzel az állítást beláttuk.

6.10.9 Állítás: $H\le G$ esetén a legbővebb $N\lhd G$ normálosztó, ami része H-nak, $\bigcap_{g\in G}H^g$.

Bizonyítás: $N \leq H$ miatt N csak olyan elemeket tartalmazhat, melyeknek minden konjugáltja H-ban van, azaz olyanokat, melyek H minden konjugáltjában benne vannak. Már csak azt kell belátnunk, hogy a fenti metszet valóban normálosztó. Akárcsak **6.10.7**-ben, $\bigcap_{g \in G} H^g$-t konjugálva csak a tényezőket permutáljuk, ami a végeredményen nem változtat, így a metszet minden konjugáltja önmaga. Ehhez hasonlóan a H által tartalmazott legnagyobb karakterisztikus részcsoport $\bigcap_{\varphi \in Aut(G)} H\varphi$.

6.11 Normállánc. Jordan-Hölder tétel

6.11.1 Definíció: G csoport normállánca egy olyan $L=(G_i)_{i=0}^r$ sorozat, melyre $G=G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_r=\{1\}$. Az L normállánc hossza r. Az L_1 normállánc finomítása az L normálláncnak, ha L minden elemét tartalmazza és hosszabb nála. A tovább nem finomítható normálláncot kompozícióláncnak hívjuk (végtelen csoportban ilyen nem mindig van). A normállánc faktorai a $\{G_i/G_{i+1} \mid 0 \leq i < r\}$ faktorcsoportok. Két normállánc izomorf, ha a faktoraik között található olyan bijekció, melyben minden izomorf a képével; azaz ha a faktorok csak sorrendjükben különböznek. A $Z_6 \triangleright Z_2 \triangleright 1$ és $Z_6 \triangleright Z_3 \triangleright 1$ láncok például izomorfak, hiszen faktoraik Z_3, Z_2 ill. Z_2, Z_3. Ez nyilván ekvivalencia-reláció.

6.11.2 Állítás: az $L=(G_i)_{i=0}^r$ normállánc pontosan akkor kompozíciólánc, ha minden faktora egyszerű.

Bizonyítás: ha G_i/G_{i+1} nem lenne egyszerű, azaz lenne egy $G_i/G_{i+1} \trianglerighteq N > 1$ normálosztó, akkor N inverz képe a $\psi: G_i \to G_i/G_{i+1}$ természetes homomorfizmusban egy $G_i \trianglerighteq N\psi^{-1} \trianglerighteq G_{i+1}$ részcsoport lenne, amivel finomíthatnánk L-t. Ha pedig L finomítható a $G_i \trianglerighteq M \trianglerighteq G_{i+1}$ részcsoporttal, akkor $G_i/G_{i+1} \trianglerighteq M\psi > 1$ lenne.

6.11.3 Állítás: véges csoportnak van kompozíciólánca, mert ha a $G \triangleleft 1$ normálláncból kiindulva mindaddig finomítunk, amíg lehet, véges sok lépés után nem tudjuk folytatni, hiszen a normállánc elemeinek rendjei páronként különböző osztói a csoport rendjének, ezért nem lehet belőlük tetszőlegesen sok. Amikor az algoritmus véget ér, definíció szerint kompozícióláncot kapunk.

6.11.4 Definíció: a G csoport $L=(G_i)_{i=0}^r$ normálláncának G_k-ra való megszorítása az $L\big|_{G_k}=(G_i)_{i=k}^r$ G_k-beli normállánc. Kompozíciólánc megszorítása **6.11.2** szerint kompozíciólánc.

6.11.5 Jordan-Hölder-tétel: G véges csoport bármely két kompozíciólánca izomorf.

Bizonyítás: azt látjuk be, hogy ha G-nek $L=(G_i)_{i=1}^r$ kompozíciólánca, akkor minden más L_0 kompozíciólánca is pontosan r hosszú és izomorf L-el. Ezt r szerinti indukcióval bizonyítjuk. $r=0$-ra az állítás triviális, hiszen 0 hosszú kompozíciólánca csak az egyelemű csoportnak van, annak pedig ez az egyetlen normállánca. Ha $r=1$, akkor $L=(G,1)$ és nem finomítható. Eszerint G egyszerű és így nem lehet más normállánca. $r=1$-re tehát igaz az állítás.

Tegyük most fel, hogy $2 \leq r_0$ és $0 \leq r < r_0$ esetén igaz az állítás, majd lássuk be $r=r_0$-ra is. Legyen L_0 a $G=H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \ldots \trianglerighteq H_s=\{1\}$ kompozíciólánc, majd lássuk be, hogy $s=r$ és $L_0 \simeq L$. Ha $G_1=H_1$, akkor az indukciós feltevést alkalmazva a K-beli (r_0-1) hosszú $L\big|_{G_1}$ és az $(s-1)$ hosszú $L_0\big|_{G_1}$kompozícióláncra megkapjuk a bizonyítandó állítás mindkét részét. Legyen tehát $G_1 \neq H_1$.

Ekkor $G_1 \trianglelefteq G_1H_1$, ez utóbbi normálosztó G-ben. Ez csak úgy lehetséges, ha $G_1H_1=G$, hiszen L nem finomítható G_1H_1-el. Jelöljük $G_1 \cap H_1$-t M-el. Ekkor az I. izomorfizmus-tétel szerint $G_1H_1/G_1 \simeq H_1/G_1 \cap H_1$, azaz $G/G_1 \simeq H_1/M$ és hasonlóan $G/H_1 \simeq G_1/M$.

M-nek **6.11.3** szerint létezik egy L_M kompozíciólánca. Legyen L_1 az a kompozíciólánc, melynek első három eleme $G_0 \trianglerighteq G_1 \trianglerighteq M$ és $L_1\big|_M=L_M$. Ez valóban kompozíciólánc **6.11.2** szerint, ugyanis a H_1/M faktor izomorf G/G_1-el, ami egyszerű, hiszen L_0 egy faktora, a többi faktor pedig faktora L és L_M valamelyikének. Hasonló módon kezdődjön L_2 $G_0 \trianglerighteq H_1 \trianglerighteq M$-el és legyen $L_2\big|_M=L_M$. Ekkor L_1 és L_2 izomorfak, hiszen első két faktora mindkettőnek G/G_1 és G/H_1 – csak más sorrendben –, a többi faktoruk pedig megegyezik.

Az indukciós feltevést alkalmazva G_1-ben az (r_0-1) hosszúságú $L\big|_{G_1}$ és a tetszőleges $L_1\big|_{G_1}$ normálláncokra kapjuk, hogy izomorfak. L és L_1 első faktora is azonos, ezért L izomorf L_1-el és L_1 hossza r. Mivel L_2 izomorf L_1-el, L_2 hossza is r. Így alkalmazhatjuk az indukciós feltevést az $L_2\big|_{H_1}$ és az $L_0\big|_{H_1}$ kompozícióláncokra, ezek is izomorfak. Ezért L_2 is izomorf L_0-al. Az izomorfia tranzitivitását kihasználva L izomorf L_0-al.

6.11.6 Definíció: G invariáns lánca egy olyan normállánc, melynek minden eleme normálosztó G-ben.

6.11.7 Definíció: ha a $H \leq G$-hez találhatóak olyan $G_1, G_2, \ldots, G_k$ részcsoportok, hogy $G \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_k \triangleright H$, akkor H-t G szubnormális részcsoportjának hívjuk, ennek jelölése $H \lhd\lhd G$. (Ennek megfelelően hívhatnának a normálláncot szubnormális láncnak, az invariáns láncot pedig normálláncnak; nem hívjuk.)

6.12 Feloldható csoport, feloldható hossz

6.12.1 Definíció: G csoport feloldható, ha van olyan normállánca, melyben minden faktor Abel -csoport. (Ez véges csoportra ekvivalens azzal, hogy van olyan normállánca, melynek faktorai prím rendű ciklikus csoportok; ez következni fog a véges Abel-csoportok alaptételéből.)

6.12.2 Definíció: G csoportra G k-adik derivált csoportja $k=0$-ra G, $k \geq 1$-re pedig a $(k-1)$-edik derivált kommutátor-részcsoportja. Jelölése $G^{(k)}$.

6.12.3 Állítás: G pontosan akkor feloldható, ha $\exists r \in \mathbb{N}: G^{(r)} = \{1\}$.

Bizonyítás: **6.5.19**-ből tudjuk, hogy G/N pontosan akkor kommutatív, ha $G' \leq N$. Eszerint ha a $G = N_0 \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \ldots \trianglerighteq N_r = \{1\}$ lánc faktorai kommutatívak, akkor $G' \leq N_1$. Ekkor persze $(G')' \leq N_1'$ is teljesül. Hasonlóan $N_1' \leq N_2$, összevetve $G'' \leq N_2$. Ezt a gondolatmenetet folytatva $G^{(k)} \leq N_k$, speciálisan $G^{(r)} \leq N_r = \{1\}$. Tehát ha G feloldható egy r hosszú normállánccal, akkor $G^{(r)} = \{1\}$.

Ha $G^{(r)} = \{1\}$ valamely $r \in \mathbb{N}$-re, akkor legyen s a legkisebb ilyen r. Ekkor $0 \leq k \leq s \Rightarrow G^{(k+1)} < G^{(k)}$, hiszen ha $G^{(k+1)} = G^{(k)}$ lenne, akkor az összes további derivált csoport is ez lenne. Mivel $G^{(s)}$ egy k-nál nagyobb sorszámú derivált, $\{1\} = G^{(s)} = G^{(k)}$ állna fenn, ami ellentmond s minimalitásának. Eszerint $G = G^{(0)} > G^{(1)} > G^{(2)} > \ldots > G^{(s)} = \{1\}$. Tudjuk, hogy $G^{(k+1)} \underset{char}{\lhd} G^{(k)}$, ez tehát normállánc (sőt invariáns lánc) és előbbi állításunk szerint a legrövidebb lehetséges normállánc, amelynek faktorai kommutatívak. Ennek örömére:

6.12.4 Definíció: G csoport feloldható hossza $d(G) = \mathbf{min}\{r \in \mathbb{N} \mid G^{(r)} = \{1\}\}$. Nem feloldható csoportra nem értelmezzük. Mindemellett $d(G) < \infty$ jelöli azt, hogy G feloldható.

6.12.5 Állítás: $d(G) < \infty$, $H \leq G \Rightarrow d(H) \leq d(G)$, speciálisan egy feloldható csoport minden részcsoportja is feloldható.

Bizonyítás: ha $H \leq G$, akkor $H' \leq G'$. Indukcióval $\forall k \in \mathbb{N}: H^{(k)} \leq G^{(k)}$, tehát $G^{(k)} = \{1\} \Rightarrow H^{(k)} = \{1\}$. Ekkor persze $d(H) = \mathbf{min}\{k \in \mathbb{N}: H^{(k)} = \{1\}\} \leq \mathbf{min}\{k \in \mathbb{N}: G^{(k)} = \{1\}\} = d(G)$.

6.12.6 Állítás: ha $N \lhd G$, akkor $(G/N)^{(k)} = (G^{(k)} \cdot N)/N$.

Bizonyítás: azt látjuk be, hogy tetszőleges G-n értelmezett φ homomorfizmusra $(G\varphi)^{(k)} = (G^{(k)})\varphi$. Ezt alkalmazva a $G \to G/N$ természetes homomorfizmusra megkapjuk az állítást.

$\forall a, b \in G: [a,b]\varphi = [a\varphi, b\varphi]$ miatt az a G-beli kommutátorok képei $G\varphi$-beli kommutátorok, azaz $(G')\varphi \leq (G\varphi)'$. Ha pedig $x, y \in G\varphi$, akkor előállnak $x = c\varphi, y = d\varphi$ alakban, azaz $[x,y] = [c\varphi, d\varphi] = [c,d]\varphi \in (G')\varphi$. Tehát $G\varphi$ minden kommutátora $(G')\varphi$-beli, ezért $(G\varphi)' \leq (G')\varphi$ is teljesül. Összevetve $\underline{\odot}$ $(G\varphi)' = (G')\varphi$, ez bizonyítja az állítást $k=1$ esetére.

Alkalmazzunk teljes indukciót. Tegyük fel, hogy $k \geq 1$, $(G\varphi)^{(k)} = (G^{(k)})\varphi$ és lássuk be, hogy $(G\varphi)^{(k+1)} = (G^{(k+1)})\varphi$. Először az indukciós feltevést, majd $\odot$-et alkalmazva $(G\varphi)^{(k+1)} = ((G\varphi)^{(k)})' = ((G^{(k)})\varphi)' = ((G^{(k)})')\varphi = (G^{(k+1)})\varphi$, ezzel az állítást beláttuk.

(A fenti bizonyítás tulajdonképpen azt használja ki, hogy mind a kommutátorok képzése, mind a generált részcsoport tekintése átvihető a φ homomorfizmuson, a derivált részcsoportok pedig ilyen lépésekkel állíthatóak elő.)

6.12.7 Következmény: ha $N \lhd G$ és $d(G) < \infty$, akkor $d(G/N) \leq d(G)$, azaz feloldható csoport faktorcsoportja – más néven (ld. homomorfizmus-tétel) homomorf képe – is feloldható.

Bizonyítás: ha $G^{(k)} = \{1\}$, akkor $(G/N)^{(k)} = (G^{(k)} \cdot N)/N = \{1\}$.

6.12.8 Tétel: ha $N \lhd G$ és $d(N), d(G/N) < \infty$, akkor $d(G) \leq d(N) + d(G/N)$.

Bizonyítás: $(G^{(d(G/N))} \cdot N)/N = (G/N)^{(d(G/N))} = \{1\}$, tehát $G^{(d(G/N))} \subseteq N$. Eszerint $(G^{(d(G/N))})^{(d(N))} \subseteq N^{(d(N))} = \{1\}$, azaz G $d(N) + d(G/N)$-edik derivált csoportja már $\{1\}$, így az állítás a definíció szerint igaz.

6.12.9 Következmény: G csoport egy L normálláncának faktorai feloldhatóak $\Leftrightarrow$ G feloldható.

6.13 Permutációcsoportok. Reguláris reprezentáció, Cayley-tétel

6.13.1 Definíció: G_0 permutációcsoport az Ω alaphalmazon, ha G_0 elemei $\Omega\to\Omega$ bijekciók és csoportot alkotnak a függvénykompozícióra. Ha $|\Omega|=n$, azaz $G_0\le S_n$, akkor G_0-t n-edfokú permutációcsoportnak nevezzük.

Jelöljön a következő néhány pontban G egy Ω feletti permutációcsoportot.

6.13.2 Jelölés: legyen $\alpha\in\Omega, g\in G$. Ekkor α^g jelöli α képét a g leképezésben. $K\subseteq G, \omega\subseteq\Omega$ esetén $\omega^K=\{\alpha^g\,|\,\alpha\in\omega, g\in K\}$.

6.13.3 Definíció: G tranzitív, ha $\forall\alpha,\beta\in\Omega\,\exists g\in G\colon \alpha^g=\beta$, azaz ha Ω bármely elemét bármely elemébe át tudjuk vinni G-beli leképezéssel.

6.13.4 Definíció: Ω egy α elemének stabilizátora $G_\alpha=\{g\in G\,|\,\alpha^g=\alpha\}$. Ez könnyen ellenőrizhetően részcsoportja lesz G-nek.

6.13.5 Definíció: definiáljuk a ~ relációt Ω-n az alábbi módon: $\alpha\sim\beta\Leftrightarrow\exists g\in G\colon\alpha^g=\beta$, azaz ha $\beta\in\alpha^G$. Ez ekvivalencia-reláció lesz. (Reflexív, mert $1\in G$; szimmetrikus, mert $G^{-1}=G$ és tranzitív, mert $G\cdot G=G$.) Ekkor ~ ekvivalencia-osztályokra bontja Ω-t; az α elem ekvivalencia-osztálya α^G. Ezt α orbitjának hívjuk.

6.13.6 Állítás: $|G\colon G_\alpha|=|\alpha^G|$.

Bizonyítás: $\alpha^g=\alpha^h\Leftrightarrow\alpha^{gh^{-1}}=\alpha\Leftrightarrow gh^{-1}\in G_\alpha$, azaz ha g és h ugyanabban a G_α szerinti jobb oldali mellékosztályban vannak. Eszerint α különböző képeinek száma éppen a mellékosztályok száma. Ez volt bizonyítandó.

6.13.7 Következmény: ha $G\le S_n$ tranzitív permutációcsoport, akkor $|\alpha^G|=|\Omega|=n$, tehát $\forall\alpha\in G\colon|G\colon G_\alpha|=n$. A Lagrange-tétel szerint tehát $|G|$ osztható n-el.

6.13.8 Definíció: G reguláris, ha minden 1-től különböző eleme fixpontmentes, azaz $\alpha^g=\alpha\Rightarrow g=1$. Ez ekvivalens azzal, hogy minden elemének stabilizátora $\{1\}$.

Megjegyzés: ha $G\le S_n$ tranzitív és reguláris, akkor $|G|=n$, hiszen G_α egyelemű, n indexű részcsoportja.

6.13.9 Állítás: ha G permutációcsoportban $\beta=\alpha^g$, akkor $G_\beta=g^{-1}G_\alpha g$. Speciálisan egy tranzitív permutációcsoportban minden stabilizátor izomorf.

Bizonyítás: $x\in G_\alpha\Leftrightarrow\alpha^x=\alpha\Leftrightarrow(\beta^{g^{-1}})^x=\beta^{g^{-1}}\Leftrightarrow\beta^{(g^{-1}xg)}=\beta\Leftrightarrow g^{-1}xg\in G_\beta$.

6.13.10 Cayley-tétel: minden G csoport izomorf egy G_0 tranzitív, reguláris permutációcsoporttal.

Bizonyítás: legyen $\Omega=G$ és rendelje a ψ leképezés $g\in G$-hez Ω azon permutációját, ami az $\alpha\in\Omega$ elemhez $\alpha\cdot g$-t rendeli. (Ez valóban permutáció lesz az egyszerűsítési szabály szerint.) Különböző G-beli elemeknek különböző permutációk felelnek meg, hiszen az egység képe $g\psi$-ben g. Ekkor $\forall\alpha\in\Omega\colon\alpha^{(gh)\psi}=\alpha\cdot gh=(\alpha\cdot g)\cdot h=(\alpha^{g\psi})^{h\psi}$, azaz $(gh)\psi=(g\psi)(h\psi)$. Eszerint ψ művelettartó bijekció G és egy Ω feletti G_0 permutációcsoport között, így $G\simeq G_0$.

6.13.11 Megjegyzés: a fenti G_0 permutációcsoportot hívjuk G reguláris reprezentációjának.

6.13.12 Definíció: $G(\Omega)$ és $G'(\Omega')$ permutációcsoportok izomorfak a $\psi\colon\Omega\to\Omega'$ bijekcióra nézve, ha $\exists\varphi\colon G\xrightarrow{\sim}G'$, hogy $\forall\alpha\in\Omega, g\in G\colon(\alpha^g)\psi=(\alpha\psi)^{g\varphi}$. (Azaz ha az a φ_ψ leképezés, ami $g\in G$-hez az Ω' feletti $g\varphi_\psi\colon\alpha'\mapsto(\alpha')^{\psi^{-1}g\psi}$ permutációt rendeli, véletlenül épp egy $G(\Omega)\to G'(\Omega')$ izomorfizmus. Más szóval ha $G'(\Omega')$ éppen $G(\Omega)$ konjugáltja ψ-vel.) Jelölése $G(\Omega)\overset{\psi}{\simeq}G'(\Omega')$. Ha $\exists\psi\colon G(\Omega)\overset{\psi}{\simeq}G'(\Omega')$, akkor $G(\Omega)\simeq G'(\Omega')$.

6.13.13 Megjegyzés: ha $G(\Omega)\simeq G'(\Omega')$, akkor nyilván $G\simeq G'$. A megfordítás nem igaz, mert pl. $\Omega=\Omega'=\{1,2,3,4\}$ felett $G=\{Id,(12)(34),(13)(24),(14)(23)\}$ és $G'=\{Id,(12),(34),(12)(34)\}$ egyaránt a Klein-féle csoport, de permutációcsoportként nem izomorfak, hiszen $G(\Omega)$ tranzitív, $G'(\Omega')$ pedig nem. (Mellesleg $G(\Omega)$ a Klein-csoport Cayley-tétel szerinti reprezentációja.)

6.13.14 Definíció: $G(\Omega)$ k-szorosan tranzitív, ha $|\Omega|\ge k$ és tetszőleges $\{\alpha_i,\beta_i\in\Omega\,|\,1\le i\le k\}$-ra $\exists g\in G\,\forall i\colon\alpha_i^g=\beta_i$, azaz ha G elemeivel Ω bármely két rendezett k-asa egymásba vihető. Könnyen ellenőrizhető, hogy $G(\Omega)$ k-szorosan tranzitív $\Leftrightarrow$ $G(\Omega)$ tranzitív és $G_\alpha(\Omega\setminus\{\alpha\})$ pedig $(k-1)$-szeresen tranzitív (α tetszőleges Ω-beli elem).

6.13.15 Állítás: ha $|\Omega|=n$ és $G(\Omega)$ k-szorosan tranzitív, akkor $\frac{n!}{(n-k)!}\Big||G|$.

Bizonyítás: teljes indukció k szerint, rögzített $(n-k)=m$ mellett. (A definíció alapján $m\geq 0$.) $k=1, m\geq 0$ esetén az állítás igaz, ld. **6.13.7**. Tegyük fel, hogy az adott m értékkel $k=(k_0-1)$ esetén teljesül az állítás és lássuk be, hogy $k=k_0$ esetén is. Legyen tehát $|\Omega|=k_0+m$ és $G(\Omega)$ k_0-szorosan tranzitív. Ekkor $G(\Omega)$ tranzitív, tehát $|G:G_\alpha|=n$ és G_α (k_0-1)-szeresen tranzitív a (k_0-1+m) elemű $\Omega\setminus\{\alpha\}$ halmazon. Alkalmazva az indukciós feltevést $G_\alpha(\Omega\setminus\{\alpha\})$ -ra $\frac{(n-1)!}{m!}\Big||G_\alpha|$. A Lagrange-tétel szerint $|G|=|G_\alpha|\cdot n$, tehát osztja $n\cdot\frac{(n-1)!}{m!}=\frac{n!}{m!}$ és éppen ezt akartuk bizonyítani.

Jelölés: $S(\Omega)$ jelölje az Ω halmaz összes permutációinak csoportját. $|\Omega|=n$-re persze $S(\Omega)=S_n$.

Megjegyzés: érdekes kérdés, hogy k különböző értékeire hány k-szorosan tranzitív véges permutációcsoport létezik. $|\Omega|\geq k$ esetén $S(\Omega)$, $n\geq(k+2)$ esetén A_n nyilván k-szorosan tranzitív, de ez nem valami izgalmas. Inkább arra vagyunk kíváncsiak, hogy hány ezektől különböző k-szorosan tranzitív véges permutációcsoport van. Egyszeresen tranzitív minden n-re van, például Z_n reguláris reprezentációja, ez máris végtelen sok. Kétszeresen tranzitív lesz minden K testre az $\Omega=K, G(\Omega)=Aff(K)$ permutációcsoport ($|K|=n$ esetén ennek a lehető legkevesebb, $n(n-1)$ eleme van); ez megint végtelen sok eset, hiszen végtelen sok $\mathbb{F}_p$ test van. Háromszorosan tranzitív még mindig végtelen sok van, ezt elhisszük. Négyszeresen tranzitív viszont már összesen négy darab van; ebből az M_{12} és M_{24} nevű csoportok ötszörösen is tranzitívak, stabilizátoraik – M_{11} és M_{23} – csak négyszeresen (ezeket Matthieu-csoportoknak hívják). Hatszorosan tranzitív véges permutációcsoport – A_n, S_n-től eltekintve – nincs.

6.13.16 Definíció: legyen $G(\Omega)$ tranzitív. $\Delta\subseteq\Omega$ imprimitivitási tartomány (IPT), ha $\forall g\in G: (\Delta^g=\Delta$ vagy $\Delta^g\cap\Delta=\emptyset)$, azaz ha Δ képei Ω egy partícióját adják. Nyilván $\{\alpha\}$ IPT és IPT képe is IPT.

6.13.17 Definíció: a $G(\Omega)$ tranzitív permutációcsoport imprimitív, ha $\exists\Delta$ nem triviális $(1\neq\Delta\neq\Omega)$ IPT $G(\Omega)$-ban. Primitív, ha nincs ilyen. Primitív például minden kétszeresen tranzitív permutációcsoport. Imprimitív a kocka mozgás- és transzformáció-csoportja (S_8 részcsoportjaként tekintve), mert minden testátló és minden olyan négy csúcs, amely szabályos tetraédert határoz meg, IPT-t alkot benne.

6.13.18 Definíció: a Δ IPT stabilizátora $G_\Delta=\{g\in G\,|\,\Delta^g=\Delta\}\leq G$.

Megjegyzés: $\Delta^g=\Delta^h\Leftrightarrow\Delta^{gh^{-1}}=\Delta\Leftrightarrow gh^{-1}\in G_\Delta$. Eszerint g és h pontosan akkor viszi ugyanoda Δ-t, ha ugyanabban a G_Δ szerinti jobb oldali mellékosztályban vannak. Ezért Δ képeinek szám(osság)a $|G:G_\Delta|$. Eszerint $|\Omega|=|G:G_\Delta|\cdot|\Delta|$. G-t G_Δ mellékosztályai szerint reprezentálva (ld. később) tehát G-t egy $\frac{|\Omega|}{|\Delta|}$ fokú permutációcsoportba tudjuk leképezni. Ha $\Delta\subseteq\Delta'$ IPT-k, akkor $G_\Delta\leq G_{\Delta'}$.

6.13.19 Következmény: ha a $G(\Omega)$ tranzitív permutációcsoport foka ($|\Omega|$) prím, akkor primitív, mert minden IPT elemszáma osztja G fokát, így vagy $|\Omega|$, vagy 1.

6.13.20 Lemma: legyen $G(\Omega)$ tranzitív permutációcsoport, $\alpha\in\Omega, G_\alpha\leq H\leq G$. Ekkor α^H IPT.

Bizonyítás: legyen $\beta\in(\alpha^H)^x\cap\alpha^H$ és lássuk be, hogy $(\alpha^H)^x=\alpha^H$. Tudjuk, hogy alkalmas $h_1, h_2\in H$ elemekre $\alpha^{h_1x}=\beta=\alpha^{h_2}$, ekkor $\alpha^{h_1xh_2^{-1}}=\alpha$, azaz $h_1xh_2^{-1}\in G_\alpha\leq H$. Így hát $x\in h_1^{-1}Hh_2=H$. Következésképp $(\alpha^H)^x=\alpha^{Hx}=\alpha^H$.

6.13.21 Tétel: a $G(\Omega)$ tranzitív permutációcsoport pontosan akkor primitív, ha G_α maximális részcsoport G-ben.

Bizonyítás: ha G imprimitív, akkor α belerakható egy Δ IPT-be, ahol $\{\alpha\}\neq\Delta\neq\Omega$. Nyilván $G_\alpha\leq G_\Delta\leq G$. A tranzitivitás miatt $\exists g\in G: \alpha^g\in\Delta\setminus\{\alpha\}$, ekkor $g\in G_\Delta\setminus G_\alpha$-ban van. Hasonlóan $\exists h\in G: \alpha^h\in\Omega\setminus\Delta$ és erre $h\in G_\Delta\setminus G_\alpha$. Ezért egyik helyen sem áll fenn egyenlőség: $G_\alpha<G_\Delta<G$ és G_α valóban nem maximális részcsoport. Tegyük most fel, hogy G_α nem maximális részcsoport, azaz $G_\alpha<H<G$. Ha véletlenül $\alpha^H=\Omega$ lenne, akkor $g\in G\setminus H$ választással $\exists h\in H: \alpha^g=\alpha^h$, azaz $gh^{-1}\in G_\alpha<H$ ellentmondana g választásának. Tehát $\alpha^H\neq\Omega$. $\alpha^H=\{\alpha\}$ sem lehet, mert $G_\alpha<H$. α^H tehát olyan IPT, amelynek van α-n kívül eleme, de nem a teljes Ω. Ekkor G imprimitív.

6.14 Az alternáló csoport

6.14.1 Tétel: $n\geq 5$ esetén A_n egyszerű.

Bizonyítás: tegyük fel indirekt módon, hogy $\exists N: 1<N\trianglelefteq A_n$, ahol $n\geq 5$. Legyen g olyan N-beli elem, amelynek – az egységtől eltekintve – a lehető legtöbb fixpontja van N-ben. Ha g ciklikus felírásában lenne két különböző (k és l, $k<l$) hosszú ciklus, akkor g^k-nak fixpontja lenne g minden fixpontja, továbbá g k elemű ciklusának elemei is,

emellett $g^k \neq 1$ lenne, mert g l hosszú ciklusának elemeit g^k nem hagyná helyben. Eszerint $g^k \neq 1$-nek több fixpontja lenne g-nél, ami ellentmond g választásának. Így g ciklusai mind egyenlő hosszúak. Feltehetjük, hogy ez a hossz prím, hiszen ha minden ciklushossz $p \cdot k$, akkor g^k azonos fixpontok mellett p hosszú ciklusokból áll. Az alábbi esetek lehetségesek:

(i) $p=2$, ekkor g legalább 2 ciklusból áll, mert páros permutáció. Megtehetjük, hogy két ciklusának elemeit elkereszteljük $1,2,3,4$-nek, ekkor g ciklikus alakja $(12)(34)\ldots$

(ii) $p=3$ és g egyetlen ciklusból áll, ekkor $g=(123)$

(iii) $p=3$ és g több ciklusból áll, ekkor $g=(123)(456)\ldots$

(iv) $p \geq 5$, ekkor $g=(123\ldots p)\ldots$

Mivel $n \geq 5$, minden esetben vehetjük az $x=(345) \in A_n$ elemet. A **(iii)** és **(iv)** esetekben $y=gxg^{-1}x^{-1}$ csak olyan elemeket mozgat, amelyeket már g is, továbbá könnyen ellenőrizhetően helybenhagyja az 1-el jelölt elemet is. Ráadásul $y=g(xg^{-1}x^{-1}) \in N \cdot N^{x^{-1}}=N$, mert N normálosztó. y tehát egy olyan N-beli elem, amelynek x-nél több fixpontja van, ami ellentmond x választásának. Lássuk most az **(i)** esetet.

Legyen $x=(123) \in A_n, y=gxg^{-1}x^{-1}$. Ekkor $y \in N$, akárcsak az előbb. y-nak fixpontja minden $\{1,2,3,4\}$-en kívüli elem, mert ezekre megszorítva x identitás, g pedig ezek halmazát helybenhagyja. Könnyen ellenőrizhető, hogy $y: 1 \mapsto 4, 4 \mapsto 1, 2 \mapsto 3$ és $3 \mapsto 2$. Eszerint $y=(14)(23)$. A **(ii)** esetben $x=(345) \in A_n, y=x^{-1}gxg$ választással $y \in N$. Az $\{1,2,3,4,5\}$-ön kívüli elemeket x és g egyaránt helybenhagyja, tehát y is. Kiszámolható, hogy $y: 1 \mapsto 3, 3 \mapsto 1, 2 \mapsto 4, 4 \mapsto 2$ és $5 \mapsto 5$, tehát $y=(13)(24)$. Eszerint az **(i)** és **(ii)** esetekben $\exists y \in N$, amely két diszjunkt transzpozíció szorzata. Az alaphalmaz átszámozásával tehát $n=(12)(34) \in N$.

Azt állítjuk, hogy tetszőleges $a=(\alpha\beta)(\gamma\delta) \in A_n$ elem benne van N-ben, ha $\alpha, \beta, \gamma, \delta$ különbözőek. Vegyük azt az $x \in S_n$ permutációt, ami felcseréli az $\langle 1,2,3,4 \rangle$ és a $\langle \alpha, \beta, \gamma, \delta \rangle$ rendezett négyeseket. Ekkor az $x^{-1}nx$ elem $\langle \alpha, \beta, \gamma, \delta \rangle$-t elviszi $\langle 1,2,3,4 \rangle$-be, ott felcseréli α-t β-val, γ-t pedig δ-val, majd az egészet visszaviszi $\langle \beta, \alpha, \delta, \gamma \rangle$-ba. A többi elemmel az x^{-1} utáni n nem csinál semmit, x meg visszaviszi a helyére. Tehát $x^{-1}nx=a$. Sajnos $x \in A_n$ esetén nem mondhatjuk azt, hogy n konjugáltja x-el benne van N-ben, hiszen normálosztó. Viszont vehetjük azt az $x^*=x \cdot (12) \in A_n$ elemet, ami $\langle 1,2,3,4 \rangle$-t és $\langle \beta, \alpha, \gamma, \delta \rangle$-t cseréli fel; ez páros, ha x páratlan és $x^{*-1}nx^*=a$ itt is fennáll. Így $\forall \alpha, \beta, \gamma, \delta$ különböző elemekre $(\alpha\beta)(\gamma\delta) \in N$. Ha $\alpha, \beta, \gamma, \delta$ nem mind különbözőek, akkor feltehetjük, hogy pl. $\beta=\delta$. Mivel $n \geq 5$, vehetünk további két, minden eddigitől különböző ε, η elemeket. Ekkor $(\alpha\beta)(\gamma\delta)=(\alpha\beta)(\varepsilon\eta) \cdot (\varepsilon\eta)(\beta\gamma)$. Ez két olyan elem szorzata, melyek az előbbiek szerint benne vannak N-ben, így $(\alpha\beta)(\gamma\delta)$ is. Tehát bármely két transzpozíció szorzata benne kell legyen N-ben.

Tekintsünk egy tetszőleges A_n-beli elemet és írjuk fel páros sok transzpozíció szorzataként. A szorzat tényezőit kettesével csoportosítva minden rész benne lesz N-ben, tehát maga a szorzat is. Eszerint $A_n \subseteq N$, ami ellentmond indirekt feltevésünknek. Minden esetben ellentmondásra jutottunk, az indirekt feltevés tehát hamis, a bizonyítandó állítás pedig igaz.

6.14.2 Következmény: S_n nem feloldható, ha $n \geq 5$.

Bizonyítás: az előbb beláttuk, hogy $1 \triangleleft A_n \triangleleft S_n$ kompozíciólánc. Az A_n faktor nem kommutatív, tehát S_n-nek nincs olyan normállánca, melynek minden faktora kommutatív.

6.14.3 Következmény: A_n karakterisztikus részcsoport S_n-ben.

Bizonyítás: S_n-ben könnyen ellenőrizhetően nincs A_n-től különböző nem triviális normálosztó. Így A_n képe S_n bármely automorfizmusánál csak A_n lehet.

6.14.4 Megjegyzés: $n \leq 3$ esetén A_n érdektelen, mert $A_1 \simeq A_2 \simeq \{1\}$, $A_3 \simeq Z_3$; A_4 pedig nem egyszerű. (Vegyük $Z_2^2 \simeq H = \{Id, (12)(34), (13)(24), (14)(23)\} \leq A_4$-et. Ebben benne van A_4 minden 1 vagy 2 rendű eleme és semmi más. Így H-t A_4 minden automorfizmusa önmagába viszi, tehát $H \underset{char}{\triangleleft} A_4$. Mivel H és $A_4/H \simeq Z_3$ kommutatív, A_4 feloldható.

6.15 Néhány feloldható csoport. A Sylow-tételek alkalmazásai

Mivel most sokat fogjuk (külön hivatkozás nélkül) használni, megismételjük a **6.12.9** állítást: G csoport L normálláncának faktorai pontosan akkor feloldhatóak, ha G feloldható.

6.15.1 Állítás: ha G rendje p prím, akkor $G\simeq Z_p$, hiszen a Cauchy-tétel miatt van p rendű eleme és az nyilván generálja. Z_p kommutatív, tehát prím rendű csoport feloldható.

6.15.2 Állítás: ha G véges p-csoport, akkor G feloldható.

Bizonyítás: **6.7.5** szerint G rendje p^n. Sylow I. tétele miatt találhatóak olyan $1\triangleleft P_1\triangleleft P_2\triangleleft\ldots\triangleleft P_{k-1}\triangleleft G$ részcsoportok, melyekre $|P_i|=p^i$. Ezen normállánc minden faktora p-edrendű, tehát **6.15.1** szerint feloldható.

6.15.3 Állítás: ha $m,n\in\mathbb{Z}^+$ relatív prímek, akkor $Z_m\times Z_n\simeq Z_{mn}$.

Bizonyítás: legyen G az $\langle x\rangle\simeq Z_m$ és az $\langle y\rangle\simeq Z_n$ csoportok direkt szorzata. **6.6.11** szerint $o((x,y))=mn=|G|$, azaz $Z_m\times Z_n\simeq G=\langle(x,y)\rangle\simeq Z_{mn}$.

6.15.4 Állítás: ha $p<q$ különböző prímek és $|G|=pq$, akkor G feloldható.

Bizonyítás: ha $p<q$, akkor $p\not\equiv 1\ (mod\ q)$. Jelölje $|Syl_q(G)|$-t a. **6.8.6** és **6.8.7** szerint $a|p$, azaz $a\in\{1,p\}$ és $a\equiv 1\ (mod\ q)\Rightarrow a\neq p\Rightarrow a=1$. Eszerint $Q\in Syl_q(G)$-re Q konjugáltjainak száma 1, azaz $Q\triangleleft G$. A $G\triangleright Q\triangleright 1$ normállánc faktorainak rendje p és q, ezek tehát ciklikus, speciálisan kommutatív csoportok. Ekkor G feloldható.

6.15.5 Állítás: ha $p<q$ prímek, $q\not\equiv 1\ (mod\ p)$ és $|G|=pq$, akkor $G\simeq Z_{pq}$.

Bizonyítás: az előbbi módon $P\in Syl_p(G)$ és $Q\in Syl_q(G)$ is normálosztó. $\forall x\in P\cap Q$-ra $o(x)$ osztja $|P|$-t és $|Q|$-t is, tehát $o(x)=1$. Ezért $\{1\}\subseteq P\cap Q\subseteq\{x\in G\,|\,o(x)=1\}=\{1\}$. Az első izomorfizmus-tételből $|PQ:P|=|Q:P\cap Q|=q$. Ebből $|PQ|=pq=|G|\Rightarrow PQ=G$. Ekkor **6.6.3** szerint $G=P\times Q$. Felhasználva **6.15.1**-t $P\simeq Z_p$ és $Q\simeq Z_q$, így **6.15.3** szerint $G\simeq Z_{pq}$.

6.15.6 Megjegyzés: ha $p<q$ és $q\equiv 1\ (mod\ p)$, akkor a fentiek közül $P\triangleleft G$ nem feltétlenül teljesül. $Q\triangleleft P, P\cap Q=\{1\}, PQ=G, P\simeq Z_p$ és $Q\simeq Z_q$ ugyanígy belátható, tehát a szemidirekt szorzat definíciójából $G\simeq Z_q\rtimes_{\vartheta} Z_p$ valamely $\vartheta: Z_p\to Aut(Z_p)$ homomorfizmusra. Szeretnénk megtalálni az összes ilyen ϑ-t, hogy ismerjük az összes pq rendű csoportot. Ehhez először is $Aut(Z_n)$-t kell megvizsgálni.

6.15.7 Definíció: U_n az n-hez relatív prím $mod\ n$ maradékosztályok multiplikatív csoportja. $|U_n|=\varphi(n)$. (Ennek elemei az $\mathbb{F}_n$ gyűrűk egységei.)

6.15.8 Állítás: Z_n endomorfizmusainak félcsoportja a $mod\ n$ maradékosztályok multiplikatív félcsoportja.

Bizonyítás: legyen $G=\langle a\rangle\simeq Z_n, \varphi: G\to G$ homomorfizmus. Jelölje $k\in\mathbb{Z}$-re $\underline{k}$ a k szám $mod\ n$ maradékosztályát. Mivel $a^k=a^{k^*}\Leftrightarrow\underline{k}=\underline{k}^*$, G minden eleme egyértelműen írható fel $a^{\underline{k}}$ alakban. Legyen $a\varphi=a^{\underline{r}}$. Ebből $(a^{\underline{k}})\varphi=(a\varphi)^{\underline{k}}=a^{\underline{k}\cdot\underline{r}}$ már következik, tehát minden $\varphi: G\to G$ homomorfizmus előáll $\varphi_r: a^{\underline{k}}\mapsto a^{\underline{k}\cdot\underline{r}}\ :\ r\in\{0,1,\ldots,n-1\}$ alakban. Látható, hogy $\{\varphi_r\,|\,0\le r\le n-1\}$ elemei valóban páronként különböző homomorfizmusok, ez tehát éppen G endomorfizmusainak halmaza. Az is látható, hogy $a^{\underline{k}}(\varphi_r\cdot\varphi_{r^*})=((a^{\underline{k}})^{\underline{r}})^{\underline{r}^*}=a^{\underline{k}}\varphi_{\underline{r}\cdot\underline{r}^*}$, tehát ezek a homomorfizmusok valóban úgy viselkednek, mint a $mod\ n$ maradékosztályok a szorzásra nézve.

6.15.9 Állítás: $Aut(Z_n)\simeq U_n$.

Bizonyítás: a fenti jelölésekkel a $\varphi_r: G\to G$ homomorfizmus pontosan akkor automorfizmus, ha $G\varphi_r=G$, ami pontosan akkor teljesül, ha $a\varphi_r$ generálja G-t, hiszen $G\varphi_r=\langle a\rangle\varphi_r=\langle a\varphi_r\rangle$. Ez ekvivalens azzal, hogy $o(a^r)=n$, azaz hogy r és n relatív prímek. Ez éppen a bizonyítandó állítást adja.

6.15.10 Tétel: ha p prím, akkor $U_p\simeq Z_{\varphi(p)}\simeq Z_{p-1}$, azaz U_p-nek van generálóeleme. Ezt úgy is mondják, hogy $mod\ p$ létezik primitív gyök.

Bizonyítás: rendelje a ψ függvény $d\in\mathbb{N}$-hez az U_p-beli, d-edrendű elemek számát. Ha $\psi(d)$ nem 0, akkor $d\,\big|\,|U_p|$, tehát elég d-t $(p-1)$ osztóin vizsgálni. Ha $(p-1)=d\cdot t$, akkor tekintsük az alábbi, $\mathbb{F}_p$ feletti polinomokat: $(x^{p-1}-1)=(x^d-1)=\left((x^d)^{t-1}+(x^d)^{t-2}+\ldots+x^d+1\right)$. A baloldali polinomnak pontosan $(p-1)$ gyöke van, mert U_p minden eleme gyöke. Egy d-edfokú és egy $(p-d-1)$-edfokú polinom szorzata áll. Ennek csak úgy lehet $(p-1)$ gyöke, ha mindkettőnek pontosan annyi gyöke van, amennyi a foka. Eszerint pontosan d darab $x\in\mathbb{F}_p$-re teljesül $x^d\equiv 1$, tehát pontosan d darab U_p-beli elem rendje osztja d-t. Ezek száma éppen $\sum_{a|d}\psi(a)$. Tehát ψ összegzési függvénye $d\,|\,(p-1)$ esetén a d helyen éppen d, így $\psi|_{\{d:\,d|(p-1)\}}=\varphi$, speciálisan $\psi(p-1)=\varphi(p-1)\ge 1$, ezért létezik $(p-1)$-edrendű elem. Ezt akartuk belátni.

6.15.11 Állítás: ha $o(a)<\infty$ és az a elem képe a φ homomorfizmusban b, akkor $o(b)\,|\,o(a)$. Ugyanis $b^{o(a)}=(a\varphi)^{o(a)}=(a^{o(a)})\varphi=1\varphi=1$.

6.15.12 Állítás: ha $p<q$ prímek és $q\equiv 1\ (mod\ p)$, akkor kétféle pq rendű csoport van; az egyik Z_{pq}, a másik nem kommutatív.

Bizonyítás: használjuk fel az előző kb. tíz állítást. Tudjuk, hogy minden pq rendű csoport előáll $Z_q \leftthreetimes Z_p$ alakban valamely $\vartheta: Z_p \to Aut(Z_q)$ homomorfizmusra. Legyen $Z_p=\langle a\rangle$ és $Z_q=\langle b\rangle$ továbbá $(q-1)=p\cdot t$. ϑ-t meghatározza a képe, mert ekkor $a^i\in\langle a\rangle$-ra $(a^i)\vartheta=(a\vartheta)^i$ már egyértelmű. Tudjuk, hogy $Aut(Z_q)\simeq Z_{q-1}=Z_{p\cdot t}$. A ϑ homomorfizmus a-t csak 1 vagy p rendű elembe viheti. Ezért $a\vartheta: b\mapsto b^k$-ra $(a\vartheta)^p: b\to b^{k^p}$ már az identitás, tehát $k^p\equiv 1\ (mod\ q)$. Tudjuk, hogy pontosan p darab ilyen k elem van $Z_{p\cdot t}$-ben. $k=1$ esetén $a\vartheta: b\mapsto b$ az identitás, ekkor $Z_q \leftthreetimes Z_p \simeq Z_q\times Z_p \simeq Z_{pq}$, ez mint szemidirekt szorzat érdektelen. Foglalkozzunk most a $k\neq 1$ esettel.

Legyen r p-edrendű $Z_{p\cdot t}$-ben. Ekkor $R=\{r, r^2, r^3, \dots, r^{p-1}\}$ az összes p-edrendű elem. Legyen $o(a\vartheta)=p$, ekkor $a\vartheta: b\mapsto b^k$ valamely $k=r^m\in R$-re. Azt akarjuk belátni, hogy izomorfia erejéig ugyanazt a csoportot kapjuk $\forall k\in R$ esetén. Jelölje $Z_q \overset{m}{\leftthreetimes} Z_p$ az $a\vartheta_m: b\to b^{r^m}$-el kapott szemidirekt szorzatot $(1\le m<p)$. Azt kell bebizonyítanunk, hogy $Z_q \overset{m}{\leftthreetimes} Z_p$ csoportok mind izomorfak, amihez elég $Z_q \overset{1}{\leftthreetimes} Z_p \simeq Z_q \overset{m}{\leftthreetimes} Z_p$. Mivel ϑ_1 homomorfizmus, $a^m\vartheta_1=(a\vartheta_1)^m$. Ebben b képe $b^{(a\vartheta_1)^m}=(\dots((b^{a\vartheta_1})^{a\vartheta_1})\dots)^{a\vartheta_1)}=(\dots((b^r)^r)\dots)^r=b^{r^m}=b^{a\vartheta_m}$. Eszerint $a^m\vartheta_1=a\vartheta_m$, azaz $\langle a^m\rangle \overset{1}{\leftthreetimes} \langle b\rangle=\langle a^m, b\rangle=\langle a, b\rangle=\langle a\rangle \overset{m}{\leftthreetimes} \langle b\rangle$. A bal oldalon $Z_q \overset{1}{\leftthreetimes} Z_p$, a jobb oldalon $Z_q \overset{m}{\leftthreetimes} Z_p$ áll, ezek tehát izomorfak.

Így $Z_q \leftthreetimes Z_p$ értelmes jelölés a Z_{pq}-val nem izomorf pq rendű csoportra, mert pontosan egy ilyen van. Mivel $a\vartheta$ nem az identitás Z_q-ban, az $(a,1)$ elemmel való konjugálás nem az identitás a szemidirekt szorzatban, tehát $Z_q \leftthreetimes Z_p$ nem kommutatív.

6.15.13 Tétel: pontosan azokra az n-ekre izomorf minden n elemű csoport Z_n-el, melyekre n és $\varphi(n)$ legnagyobb közös osztója 1, azaz $\left(\,|G|=n \Rightarrow G\simeq Z_n\right) \Leftrightarrow (n,\varphi(n))=1$.

Definíció: a G véges csoport Frobenius-csoport, ha $\exists H\le G, H\neq\{1\}: \forall x\in G\setminus H: (H\cap H^x)=\{1\}$.

1. *Lemma*: legyenek $H,K\le G$ $\{1\}$-től különböző részcsoportok, melyekre $\forall x\in G\setminus H: (H\cap H^x)=\{1\}$ és $\forall y\in G\setminus K: (K\cap K^x)=\{1\}$. Ekkor $\exists u\in G: (H\cap K^u)\neq\{1\}$.

Bizonyítás: legyen $\bar{H}=\bigcup_{x\in G} H^x, \bar{K}=\bigcup_{x\in G} K^x$ és jelölje $|G|$-t n. H választása miatt $N_G(H)=H$, azaz H konjugáltjainak száma $|G: N_G(H)|=\frac{n}{|H|}$. H különböző konjugáltjai $\{1\}$-től eltekintve páronként diszjunktak, ugyanis ha $H^x\cap H^y\neq\{1\}$, akkor $(H\cap H^{yx^{-1}})=(H^x\cap H^y)^{x^{-1}}\neq\{1\}$, így feltételeink szerint $yx^{-1}\in H$, amiből $H^x=H^y$. Tehát $|\bar{H}|=1+(|H|-1)\cdot\frac{n}{|H|}\ge 1+n-\frac{n}{|H|}\ge 1+n-\frac{n}{2}=1+\frac{n}{2}$ és ugyanígy $|\bar{K}|\ge 1+\frac{n}{2}$. Ezeket összeadva $|\bar{H}|+|\bar{K}|\ge|G|+2$. Így hát $\bar{H}\cap\bar{K}\neq\{1\}$, azaz alkalmas $x,y\in G$-re $H^x\cap K^y\neq\{1\}$. Ekkor $u=yx^{-1}$ választással $H\cap K^u=(H^x\cap K^y)^{x^{-1}}\neq\{1\}$.

2. *Lemma*: legyen G véges, nem kommutatív csoport, melynek minden maximális részcsoportja Abel. Ekkor G nem egyszerű.

Bizonyítás: $\nexists$ G egyszerű. Mivel nem kommutatív, $Z(G)\not\trianglelefteq G$, azaz $Z(G)=\{1\}$. Először is azt állítjuk, hogy ha M, M' G két különböző maximális részcsoportja, akkor $M\cap M'=\{1\}$. M és M' Abel, azaz $M\cap M'$ elemei mind M, mind M' elemeivel felcserélhetőek. Ekkor $\langle M, M'\rangle=G$ elemeivel is, azaz $M\cap M'\le Z(G)=\{1\}$, mint állítottuk.

Legyen M maximális részcsoport G-ben. $G\neq Z_p$ miatt $M\neq\{1\}$, tehát M nem lehet normálosztó, azaz $N_G(M)<G$. Persze $M\le N_G(M)$, így a maximalitásból $M=N_G(M)$. Azaz $\forall x\in G\setminus M: M^x\neq M$. Mivel M^x is maximális részcsoport, $M^x\cap M=\{1\}$ az előző bekezdés szerint minden $x\in G\setminus M$ esetén. M konjugáltjai nem fedhetik le az egész G-t, hiszen ez semmilyen csoport semmilyen nem teljes részcsoportjával nem fordulhat elő. Legyen g egy M konjugáltjain kívüli elem, M' egy g-t fedő maximális részcsoport. Ekkor a fenti módon $\forall y\in G\setminus M'$-re $M'\cap M'^y=\{1\}$. Alkalmazva az első lemmát M, M'-re kapjuk, hogy alkalmas u-ra $M^u\cap M'\neq\{1\}$. $M^u\neq M'$, mert $g\in M'\setminus M^u$. Így $M^u\cap M'$ valóban két különböző maximális részcsoport metszete, az előző bekezdés szerint mégis $\{1\}$, $\lightning$.

Bizonyítás: $(n,\varphi(n))=1 \Leftrightarrow n$ négyzetmentes és ha p,q különböző prímosztói n-nek, akkor $q\not\equiv 1\ (mod\ p)$, ez $\varphi(n)$ képletéből nyilvánvaló. A bizonyításkor ez utóbbi feltételt fogjuk alkalmazni.

$\Rightarrow$: ha n nem négyzetmentes, akkor alkalmas p prímre $n=p^k\cdot m, k\ge 2, p\nmid m$. Ekkor a véges Abel-csoportok alaptétele (**6.17.4**) szerint $G=Z_p\times Z_{p^{k-1}}\times Z_m$ és $Z_n=Z_{p^k}\times Z_m$ nem izomorfak, így G nem ciklikus n-edrendű csoport. Ha az n-t osztó p,q prímekre $p\,|\,q-1$, akkor $n=pqm$ jelöléssel $(Z_p \leftthreetimes Z_q)\times Z_m$ nemkommutatív n-edrendű csoport. A feltétel tehát szükséges.

$\Leftarrow$: legyen n prímtényezőkre bontása $n=\prod_{k=1}^{s}p_k$, ahol $p_k\nmid(p_{k'}-1)$ és lássuk be, hogy minden n-edrendű csoport ciklikus. $s=0,1$ esetére az állítás triviális, $s=2$-re éppen **6.15.5**. Legyen most $s\geq 3$ és tegyük fel, hogy kevesebb prímosztóval rendelkező n-ek esetén az állítás igaz. Speciálisan n minden d valódi osztójára teljesül, hogy minden d-edrendű csoport ciklikus.

Legyen G tetszőleges n-edrendű csoport. Ha kommutatív, akkor van nem triviális normálosztója, pl. a p_1-Sylow. Ha nem kommutatív, akkor az indukciós feltevés szerint minden maximális részcsoportja kommutatív, azaz a második lemma szerint G nem egyszerű. Mindkét esetben vehetünk tehát egy $1<N<G$ normálosztót. Tegyük meg; legyen $d=|G/N|, m=|N|$.

Az indukciós feltevés szerint N és G/N ciklikus: $\exists g\in G: G/N=\langle gN\rangle$. Most olyan $a\in gN$ elemet keresünk, melyre $o(a)=d$. Tekintsük az $1,(d+1),(d^2+d+1),\dots,(d^m+d^{m-1}+\dots+d+1)$ számokat. Ezek összesen már $m+1$-en vannak, így valamely kettő különbsége osztható m-el. Ez a különbség $(1+\dots+d^{l+r})-(1+\dots+d^{r-1})=d^l(1+d+\dots+d^r)=d^l\cdot d^*$ alakba írható, ahol $d^*\equiv 1\ (mod\ d)$. $md=n$ és az n-re tett feltevések szerint $(m,d)=1$, így $m\mid d^l\cdot d^* \Rightarrow m\mid d^* \Rightarrow n\mid d^*\cdot d$.

Legyen $a=g^{d^*}$. Ekkor $d^*\equiv 1\ (mod\ d)$ és $o(gN)=d$ következtében $aN=gN \Rightarrow aN$ generálja G/N-t, így $d=|G/N|$ osztja $o(a)$-t. $a^d=g^{d^*\cdot d}=1$, hiszen a kitevő osztható $n=|G|$-vel. Ebből $o(a)\mid d$, amit az előzővel összevetve $o(a)=d$-re jutunk.

$\langle a\rangle\cdot N$ részcsoport G-ben, mert $N\lhd G$. Rendjét osztja $d=|\langle a\rangle|$ és $m=|N|$, azaz n is $\Rightarrow G=\langle a\rangle\cdot N$. Ekkor alkalmas $\vartheta:\langle a\rangle\to Aut(N)$ homomorfizmusra G előáll $G=\langle a\rangle\underset{\vartheta}{\ltimes}N$ alakban. Az n-re tett feltevések szerint d és $\varphi(m)$, azaz $|\langle a\rangle|$ és $|Aut(N)|$ relatív prímek, azaz ϑ csak a triviális homomorfizmus lehet, így $G=\langle a\rangle\times N\simeq Z_d\times Z_m$, ez pedig **6.15.3** szerint éppen Z_n.

6.15.14 Állítás: ha G rendje p^2, akkor $G\simeq Z_{p^2}$ vagy $G\simeq Z_p\times Z_p$.

Bizonyítás: az egységen kívül G-nek csak p és p^2 rendű eleme lehet. Ha van p^2 rendű eleme, akkor $G\simeq Z_{p^2}$. Ha nincs, akkor legyenek a és $b\notin\langle a\rangle$ p-edrendűek. Sylow I. tétele szerint az $\langle a\rangle$ és $\langle b\rangle$ részcsoportok normálosztók. $\langle a\rangle\cap\langle b\rangle=\{1\}$ kell legyen, mert egy $c\in\langle a\rangle\cap\langle b\rangle\setminus\{1\}$ elem generálná $\langle b\rangle$-t is, ami ellentmond $b\notin\langle a\rangle$-nak. Ekkor persze $|\langle\langle a\rangle,\langle b\rangle\rangle|=|\langle a\rangle|\cdot|\langle b\rangle|=p^2$, azaz $\langle\langle a\rangle\rangle=G$. Így G belső direkt szorzata $\langle a\rangle,\langle b\rangle$-nek, azaz $G\simeq Z_p\times Z_p$.

6.15.15 Burnside-tétel: ha $|G|=p^k\cdot q^l$, ahol p és q különböző prímek, akkor G feloldható. Ezt csak az $l=1$ speciális esetben látjuk be.

Bizonyítás: legyen $P\in Syl_p(G)$. Ha $P\lhd G$, akkor a $G\rhd P\rhd 1$ normállánc faktorai feloldhatóak, ezért G is. Marad az az eset, amikor P-nek egynél több – **6.8.6** szerint éppen q – konjugáltja van. Legyen D maximális azon részcsoportok között, melyek előállnak $H=P_1\cap P_2 : P_1,P_2\in Syl_p(G); P_1\neq P_2$ alakban. Ha $D=\{1\}$, akkor a p-Sylowok egyetlen $G\setminus\{1\}$-beli elemet sem fednek kétszer, tehát $K=\bigcup_{P\in Syl_p(G)}(P\setminus\{1\})$ tagjai diszjunktak, ezért $|G\setminus K|=p^kq-(p^k-1)q=q$. $\forall x\in K$ rendje p-hatvány, hiszen x eleme egy p-Sylownak. Ezért $Q\in Syl_q(G)$-re $K\cap Q=\emptyset$. Ekkor Q csak $G\setminus K$ lehet, tehát $|Syl_q(G)|=|\{G\setminus K\}|=1$, a q-Sylow normálosztó. A $G\rhd Q\rhd 1$ normállánc faktorai feloldhatóak és ismét készen vagyunk. Marad tehát az az eset, amikor $D>1$.

Legyen $D=P_1\cap P_2$. Mivel $P_1\neq P_2$, $D<P_1$. Legyen $L_1=N_{P_1}(D)$. Mivel D egy p-részcsoport P_1-ben és nem azonos vele, Sylow I. tétele szerint D normálosztóként berakható egy $D<D'\leq P_1$ részcsoportba, tehát P_1-beli normalizátora bővebb nála. Ezért $D\trianglelefteq L_1\leq P_1$. Hasonlóan definiálva L_2-t $D\trianglelefteq L_2\leq P_2$. Mivel L_1 és L_2 egyaránt normalizálja D-t és bővebb nála, $D\trianglelefteq T=\langle L_1,L_2\rangle$. T rendje $p^t\cdot q$ és p^t lehet. Ez utóbbit mindjárt kizárjuk.

Ha T rendje p-hatvány lenne, akkor belefoglalható lenne egy P_3 p-Sylowba. Ekkor $(P_1\cap P_3)\geq(P_1\cap T)\geq L_1>D$ és ugyanígy $(P_2\cap P_3)>D$ teljesülne. D maximalitásának $P_1\neq P_3$ és $P_2\neq P_3$ egyaránt ellentmond, tehát $P_1=P_3=P_2$, ami P_1 és P_2 választásának mond ellent. T rendje valóban nem lehet p-hatvány, azaz $|T|=p^t\cdot q$.

Legyen $Q\in Syl_q(T)$. Ekkor az I. izomorfizmus-tétel és $Q\cap P_1=\{1\}$ miatt $|Q\cdot P_1|=|Q\cdot P_1|\cdot|Q\cap P_1|=|Q|\cdot|P_1|=p^k\cdot q$, azaz $Q\cdot P_1=G$. Legyen $N=\langle D^g|g\in G\rangle$, azaz a D által generált normálosztó. Legyen $g\in G$ tetszőleges. Ez az előbbiek szerint felírható $g=rs : s\in P_1, r\in Q\leq T\leq N_G(D)$. Ekkor $D^g=D^{r\cdot s}=(D^r)^s$. Itt $r\in N_G(D)$ miatt $D^r=D$, azaz $D^g=D^s$. $D\leq P_1$ és $s\in P_1$ miatt tehát $\forall g\in G: D^g\leq P_1$, azaz $N\leq P_1$, N rendje p-hatvány. $1<D\leq N$ miatt tehát a $G\rhd N\rhd 1$ lánc első faktora $p^m\cdot q$ rendű valamely $m<k$-ra és az indukciós feltevés szerint feloldható, második faktorának r endje p^{k-m}, ez is feloldható. Eszerint G is feloldható.

6.15.16 Tétel: ha $|G|<\infty$ négyzetmentes, akkor G feloldható.

6.15.17 Definíció: a G véges csoport H részcsoportja Hall-részcsoport, ha rendje és indexe relatív prím. Ha π prímszámok egy halmaza, akkor π-Hall egy olyan részcsoport, amelynek rendjében vannak $|G|$ π-beli prímtényezői, indexében a nem π-beliek.

6.15.18 Tétel (Philip Hall): ha a G véges csoport feloldható, akkor minden π-re van G-ben π-Hall részcsoport. Sőt, ha mindenféle p'-Hall van G-ben, akkor G feloldható. (Ezt nem bizonyítjuk be; például azért, mert a második felének triviális speciális esete a Burnside-tétel.)

6.15.19 Feit-Thompson tétel: ha $|G|$ páratlan, akkor G feloldható.

6.15.20 Következmény: ha $|G|=n=4k+2$, akkor G feloldható.

Bizonyítás: legyen G reguláris reprezentációja $G_0(\Omega)\leq S_n$. Ebben a Cauchy-tétel szerint van egy g_0 másodrendű elem. Ez csak úgy lehetséges, ha diszjunkt transzpozíciók szorzata. Ezek le is fedik a teljes Ω-t, mert reguláris permutációcsoportban az egységen kívül semelyik elemnek nincs fixpontja. Ekkor g_0 $2k+1$ transzpozíció szorzata, így G_0 nem részcsoportja A_n-nek, azaz $G_0A_n=S_n$. $A_n\lhd S_n$-ből az I. izomorfizmus-tétel felhasználásával $G_0/(G_0\cap A_n)\simeq G_0A_n/A_n=S_n/A_n\simeq Z_2$. A $G_0\rhd(G_0\cap A_n)\rhd 1$ normállánc első faktora Z_2, feloldható, a második páratlan rendű, így a Feit-Thompson tétel szerint feloldható. Eszerint G_0 és persze G is feloldható.

6.16 Mellékosztály szerinti reprezentáció

6.16.1 Definíció: reprezentációnak hívunk egy G csoportból egy $G_0(\Omega)$ permutációcsoportra képező homomorfizmust, illetve G képét egy ilyen homomorfizmusban.

6.16.2 Definíció: legyen $H\leq G$. Ekkor G csoport H mellékosztályai szerinti reprezentációja az a $\pi: G\to S(\Omega)$ homomorfizmus, ahol $\Omega\backsim\{H$ jobb oldali mellékosztályai$\}=\{Hx\,|\,x\in G\}$, $g\in G$ képe pedig a $\pi_g: Hx\mapsto Hxg$ permutáció.

Azt állítjuk, hogy ez egy értelmes definíció, azaz π_g permutáció Ω-n, π pedig homomorfizmus. $(Hx)^{\pi_g}=(Hy)^{\pi_g}$ $\Rightarrow Hxg=Hyg\Rightarrow Hxgg^{-1}=Hygg^{-1}\Rightarrow Hx=Hy$, tehát π_g injektív. $\forall Hx\in\Omega$ előáll $(Hxg^{-1})^{\pi_g}$ alakban, így szürjektív is. Eszerint π_g egy $\Omega\to\Omega$ bijekció, közismert nevén permutáció. $\forall Hx\in\Omega; a,b\in G$-re $(Hx)^{\pi_a\pi_b}=(Hxa)^{\pi_b}=Hxab=(Hx)^{\pi_{ab}}$, azaz $\pi_a\pi_b=\pi_{ab}$.

$G\pi$ tranzitív lesz, mert $\forall Hx,Hy\in\Omega: Hy=(Hx)^{\pi_{x^{-1}y}}$.

6.16.3 Állítás: ha π a G csoport H részcsoportjának mellékosztályai szerinti reprezentáció, akkor $Ker\,\pi=\bigcap_{x\in G}H^x$, azaz a legbővebb H-beli normálosztó.

Bizonyítás: $g\in Ker\,\pi\Leftrightarrow\forall Hx\in\Omega: Hxg=Hx\Leftrightarrow\forall Hx\in\Omega: x^{-1}Hxg=x^{-1}Hx$. Mivel H^x részcsoport, ez pontosan akkor teljesül, ha $\forall Hx\in\Omega: g\in H^x\Leftrightarrow g\in\bigcap_{x\in G}H^x$.

6.16.4 Következmény: ha π a G egyszerű csoport H-mellékosztályok szerinti reprezentációja, akkor vagy $H=G$ és $G\pi=\{1\}$, vagy $Ker\,\pi=\{1\}$ és φ izomorfizmus.

6.16.5 Megjegyzés: a mellékosztály szerinti reprezentációt azért kedveljük, mert sokkal kisebb alaphalmaz feletti permutációcsoportra képez, mint a reguláris reprezentáció. Pl. $n\geq 5$ esetén A_n reguláris reprezentációjában $|\Omega|=\frac{n!}{2}$, míg $A_{n-1}\leq A_n$ szerint reprezentálva $|\Omega|=|A_n:A_{n-1}|=n$. Ráadásul izomorfizmust kapunk, mert A_n egyszerű. Mellesleg A_n képe ebben a leképezésben éppen $A_n\leq S_n$ lesz.

6.16.6 Állítás: minden $\pi: G\to S(\Omega)$ tranzitív reprezentáció előáll mellékosztály szerinti reprezentációként.

Bizonyítás: legyen $G\pi=G_0, \alpha\in\Omega$. Legyen $\beta\in\Omega$-ra $H_\beta=\{g\in G\,|\,\alpha^{\pi_g}=\beta\}$. Mivel $G\pi$ tranzitív, H_β nem üres. H_α-t jelölje H. Ez éppen α stabilizátorának π szerinti teljes inverz képe, tehát részcsoport G-ben. Ekkor $\forall x\in G$-re:

$$\boxdot\ Hx=\{gx\in G\,|\,\alpha^{\pi_g}=\alpha\}=\{y\in G\,|\,\alpha^{\pi_y}=\alpha^{\pi_x}\}=H_{\alpha^{\pi_x}}$$

Azt akarjuk belátni, hogy π izomorf a H mellékosztályai szerinti reprezentációval. Jelölje ennek alaphalmazát $\Omega^*=\{Hx\,|\,x\in G\}$. Először is vegyük észre, hogy $\boxdot$ szerint $Hx=Hy\Leftrightarrow\alpha^{\pi_x}=\alpha^{\pi_y}$, azaz a $\beta=\alpha^{\pi_x}\in\Omega$ elemhez kölcsönösen egyértelműen hozzárendelhetjük a $Hx=H_{\alpha^{\pi_x}}$ mellékosztályt. Legyen tehát $\psi:\Omega\to\Omega^*$ a $\alpha^{\pi_x}\mapsto Hx$ bijekció.

Válasszuk az Ω^* feletti π^* reprezentációt úgy, hogy ψ szerint izomorf legyen π-vel, azaz rendelje π^* a $g\in G$ elemhez $\pi_g^*: Hx\mapsto(Hx)^{\psi^{-1}\cdot\pi_g\cdot\psi}$-t és ellenőrizzük, hogy π^* épp a H mellékosztályai szerinti reprezentáció, azaz $(Hx)^{\pi_g^*}=Hxg$. Valóban, $(Hx)^{\pi_g^*}=(Hx)^{\psi^{-1}\cdot\pi_g\cdot\psi}=(\alpha^{\pi_x})^{\pi_g\cdot\psi}=(\alpha^{\pi_{xg}})^{\psi}=Hxg$.

6.16.7 Állítás: ha G rendje $p^2\cdot q^2$, ahol $p<q$ prímek, akkor G feloldható.

Bizonyítás: **6.8.6** szerint a q-Sylowok száma $1, p$ vagy p^2 lehet és $\equiv 1 \pmod q$. Ha 1, akkor $Q\in Syl_q(G)$ normálosztó és a $G\triangleright Q\triangleright 1$ normállánc faktorai p^2 ill. q^2 rendű, azaz feloldható csoportok. p nem lehet, mert $p<q$ miatt $p\not\equiv 1 \pmod q$. Ha p^2, akkor $p^2\equiv 1 \pmod q \Rightarrow q\mid p^2-1=(p-1)(p+1)$. Ez csak úgy lehet, ha $q\mid(p-1)$ vagy $q\mid(p+1)$. $p<q$ miatt csak a második eset lehetséges és az is csak $q=p+1$-nél, amikor is $|G|=2^2\cdot 3^2=36$. Elég tehát belátnunk, hogy nincs 36 rendű egyszerű csoport, hiszen ha lenne N nem triviális normálosztója G-nek, akkor $G\triangleright N\triangleright 1$ faktorai korábbi állítások felhasználásával feloldhatóak lennének. $\nexists G$ egy 36-odrendű egyszerű csoport. Reprezentáljuk $Q\in Syl_3(G)$ mellékosztályai szerint. Ennek indexe 4, G egyszerű, tehát egy $G\to G_0\le S_4$ izomorfizmust kell kapnunk. Ilyen viszont nincs, mert $|G|>24=|S_4|$, $\lightning$.

6.16.8 Állítás: ha $p<q<r$ prímek és $|G|=pqr$, akkor G feloldható.

Bizonyítás: az r-Sylowok száma **6.8.6** szerint csak $1, p, q, pq$ lehet, ebből **6.8.7** szerint csak $1, pq$ lehetséges. Ha 1 van, akkor kész vagyunk. Legyen tehát $|Syl_r(G)|=pq$. Minden r-Sylow minden 1-től különböző eleme r-edrendű és két különböző r-Sylowban nem lehet benne ugyanaz az r-edrendű elem. Eszerint $(\bigcup_{R\in Syl_r(G)} R\setminus\{1\})$-ban $pq(r-1)$ darab r-edrendű elem van. A q-Sylowok száma tehát nem lehet p-nél több, hiszen akkor több, mint $p(q-1)$ darab q-adrendű, legalább $p-1$ p-edrendű elem és egy egységelem lenne G-ben, ami összesen több, mint pqr elem. Ha viszont legfeljebb $p\ (<q+1)$ q-Sylow van, akkor csak egy lehet **6.8.7** miatt, az tehát normálosztó. $G\triangleright Q\triangleright 1$ faktorai feloldhatóak, így G is feloldható.

Megjegyzés: tudjuk, hogy a $p^n, p^n\cdot q, p^2\cdot q^2, pqr$ rendű csoportok feloldhatóak. Ebből megállapíthatjuk, hogy minden 60-nál kisebb rendű csoport feloldható. Ennél többet furcsa is lenne tudni, hiszen A_5 rendje 60.

6.16.9 Állítás: ha G rendje $4\cdot p^k$, akkor feloldható. A p-Sylow indexe ugyanis 4, azaz a mellékosztályai szerinti reprezentáció egy $\pi: G\to S_4$ homomorfizmus. Ennek a magja nem lehet $\{1\}$, mert $|G|\ge 4\cdot 3^2>24=S_4$. $G\triangleright Ker\,\pi\triangleright 1$ faktorai feloldhatóak, így G is.

6.16.10 Állítás: ha G rendje 120, akkor G nem egyszerű.

Bizonyítás: tegyük fel indirekt módon, hogy G egyszerű. **6.8.6** és **6.8.7** miatt $|Syl_5(G)|$ csak 1 vagy 6 lehet, az első eset ellentmond az indirekt feltevésnek. Tehát $S\in Syl_5(G)$-re $|G:N_G(S)|=6$. Reprezentáljuk G-t $N_G(S)$ mellékosztályai szerint. $G\to G_0\le S_6$ izomorfizmust kapunk, mert G egyszerű. Ha $G_0\not\subseteq A_6$, akkor $G_0\cap A_6\triangleleft G_0$, ami ellentmond az indirekt feltevésnek (S_n egy legalább háromelemű részcsoportjában mindig van nem identikus páros permutáció, így $G_0\cap A_6>\{1\}$). Eszerint találtunk a 360 elemű A_6-ban egy 3 indexű részcsoportot, G_0-t. Reprezentálva A_6-ot G_0 szerint egy $A_6\rightarrowtail A\le S_3$ izomorfizmust kapunk, csak sajnos $|A_6|=|S_3|\cdot 60$, $\lightning$. G tehát nem lehet egyszerű.

6.17 Véges Abel-csoportok alaptétele

6.17.1 Tétel: ha G véges Abel p-csoport, akkor ciklikus csoportok direkt szorzata.

(A bizonyításnál az additív jelölésmódot fogom használni, azaz a művelet az összeadás, a neutrális elem a 0, hatványozás helyett egészekkel szorzunk és a direkt szorzatot a direkt összeg – jelölése $\oplus$ – helyettesíti.)

Bizonyítás: legyen G rendje p^n, a legnagyobb A-beli elemrend p^k és $o(a)=p^k$. Legyen B egy olyan részcsoport G-ben, amelynek $A=\langle a\rangle$-val vett metszete $\{0\}$ és erre a tulajdonságra nézve maximális, azaz bármely $b\in G\setminus B$-re $\langle B,b\rangle\cap A>\{0\}$. (Ilyen van, mert $\{0\}$ rendelkezik ezzel a tulajdonsággal, tehát a megfelelő részcsoportok egy nem üres véges halmazt alkotnak.) Azt állítjuk, hogy $G=A\oplus B$. Mivel minden részcsoport normálosztó, ehhez elég $G=A+B$.

$\nexists \exists x\in G\setminus(A+B)$. Ekkor $x\psi=(A+B)+x$ rendje $G/(A+B)$-ben p-hatvány, mert a faktorcsoport is p-csoport. $1<o(x\psi)\le o(x)\le o(a)$ miatt $o(x\psi)=p^r : 1<r\le k$. Ekkor $y=p^{r-1}\cdot x$-re $y\notin(A+B), p\cdot y\in(A+B)$. Legyen $p\cdot y=l\cdot a+b : l\in\mathbb{Z}, b\in B$, így $0=p^k y=p^{k-1}l\cdot a+p^{k-1}b\Rightarrow A\ni p^{k-1}l\cdot a=(-p^{k-1})b\in B$. Mindkét oldal 0 kell legyen, azaz $p^k\mid p^{k-1}l$ és $p^{k-1}\cdot b=0$. Írjuk fel l-t $l=pm : m\in\mathbb{Z}$ alakba, ekkor $p\cdot y=pm\cdot a+b$. Legyen $z=y-m\cdot a$, így $z\notin(A+B)$ és $pz=py-pm\cdot a=b$. B maximalitása miatt $\exists b^*+r\cdot z\in(\langle B,z\rangle\cap A\setminus\{0\}) : b^*\in B, r\in\mathbb{Z}$. Írjuk fel ezt az elemet $b^*+r\cdot z=t\cdot a : t\in\mathbb{Z}$ alakban is. $t\cdot a\notin B\Rightarrow rz\notin B\Rightarrow p\nmid r$. Tehát p és r relatív prímek, azaz $\exists u,v\in\mathbb{Z}: pu+rv=1$. Eszerint $z=(pu+rv)z=u\cdot b+v(t\cdot a-b^*)\in(A+B)$, ami $z\notin AB$ miatt $\lightning$, tehát $G=A\oplus B\simeq Z_{p^k}\oplus B$. Alkalmazva az indukciós feltevést a

G-nél kisebb p-hatvány rendű B Abel-csoportra az előáll ciklikus csoportok direkt összegeként, így persze $G\simeq Z_{p^k}\oplus B$ is.

6.17.2 Tétel: ha az A véges Abel-csoport rendje $|A|=n=\prod_{i=1}^{s}p_i^{\alpha_i}$, akkor $A=\prod_{i=1}^{s}P_i$, ahol P_i egy $p_i^{\alpha_i}$ rendű Abel-csoport.

Bizonyítás: legyen $P_i\in Syl_{p_i}(A)$. Azt akarjuk belátni, hogy $P_i^*=\langle P_j \mid j\neq i\rangle$ jelöléssel $P_i\cap P_i^*=\{1\}$. Ehhez elég, hogy P_i^*-ban nincsen p_i rendű elem. Tudjuk, hogy $P_i^*=P_1P_2\dots P_{i-1}P_{i+1}\dots P_s$. Az I. izomorfizmus-tételből tetszőleges M,N normálosztókra $|MN|\cdot|M\cap N|=|M|\cdot|N|$, azaz $|MN|$ osztja $|M|\cdot|N|$-t. Ezt $(s-2)$-szer alkalmazva $|P_i^*|$ osztja $\prod_{j\neq i}|P_j|=(\prod_{j\neq i}p_j^{\alpha_j})$-t, így nem osztható p_i-vel. Ezért nem is lehet p_i-edrendű eleme, ezzel $P_i\cap P_i^*=\{1\}$-t beláttuk. (Másképp: $P_i^*=P_1P_2\dots P_{i-1}P_{i+1}\dots P_s$ egy tetszőleges eleme $x=\prod_{i\neq j}x_j : x_j\in P_j$. Ezt az $m=\prod_{i\neq j}p_j^{\alpha_j}$-edik hatványra emelve 1-et kapunk, hiszen $o(x_j)\,|\,|P_j|=p_j^{\alpha_j}\Rightarrow o(x_j)\,|\,m\Rightarrow x_j^m=1$ miatt $x^m=\prod_{i\neq j}x_j^m=\prod_{i\neq j}1=1$. Azaz P_i^* minden x elemének rendje osztja m-et, így relatív prím p_i-hez. Speciálisan x nem lehet eleme $P_i\setminus\{1\}$-nek.)

Ekkor a $P_1P_2\dots P_s$ komplexusszorzat egyben a P_i-k direkt szorzata is. Akkor pedig $\prod_{i=1}^{s}p_i^{\alpha_i}$ eleme van, tehát lefedi A-t. Ezzel az állítást beláttuk.

6.17.3 Lemma: legyen **I** véges indexhalmaz. Jelölje $f_n(G)$ tetszőleges G csoportra és $n\in\mathbb{N}$-re azon G-beli elemek számát, melyek rendje osztja n-t, azaz $|\{g\in G\,|\,g^n=1\}|$. Ekkor $f_n(\prod_{i\in\mathbf{I}}G_i)=\prod_{i\in\mathbf{I}}f_n(G_i)$.

Bizonyítás: jelölje a direkt szorzatot D. $f_n(D)=|\{d\in D\,|\,d^n=1\}|=|\{d\in D\,|\,d$ minden x_i koordinátájára $x_i^n=1\}|$. Ez éppen $|\prod_{i\in\mathbf{I}}\{x_i\in G_i : x_i^n=1\}|$ ($\prod$ itt a halmazok direkt szorzatát jelöli). Tudjuk, hogy halmazok direkt szorzatának elemszáma az elemszámok szorzata, tehát $f_n(D)=\prod_{i\in\mathbf{I}}|\{x_i\in G_i : x_i^n=1\}|=\prod_{i\in\mathbf{I}}f_n(G_i)$.

6.17.4 Véges Abel-csoportok alaptétele: minden A véges Abel-csoport előáll prímhatvány rendű ciklikus csoportok direkt szorzataként és ez a felírás a tényezők sorrendjétől eltekintve egyértelmű.

Bizonyítás: alkalmazzuk **6.17.2**-t A-ra, majd **6.17.1**-t a kapott P_i tényezőkre. Így megkapjuk az állítás első felét. Legyen most $\prod_{i\in\mathbf{I}}A_i=A$ olyan direkt szorzat, ahol a tényezők prímhatvány rendű ciklikus csoportok. A lemma szerint tetszőleges p prímre és $k\in\mathbb{N}$ kitevőre $f_{p^k}(A)=\prod_{i\in\mathbf{I}}f_{p^k}(A_i)$. Látható, hogy $f_{p^k}(A_i)=\mathbf{min}(p^k,p^m)$ ha A_i egy p^m rendű ciklikus csoport és 1, ha q^l rendű valamely $q\neq p$ prímre.

Legyen $q_{p,k}=\frac{f_{p^k}(A)}{f_{p^{k-1}}(A)}=\prod_{i\in\mathbf{I}}\frac{f_{p^k}(A_i)}{f_{p^{k-1}}(A_i)}$. Ha $|A_i|$ nem osztható p^k-al, akkor $f_{p^k}(A_i)=f_{p^{k-1}}(A_i)$ és az i-edik tényező 1. Ha osztható vele, akkor $\frac{f_{p^k}(A_i)}{f_{p^{k-1}}(A_i)}=\frac{p^k}{p^{k-1}}=p$. Tehát $q_{p,k}=p^{s_{p,k}}$, ahol $s_{p,k}$ éppen az olyan A_i tényezők száma, melyek rendjét osztja p^k-al. Az p^k rendű tényezők száma, $s_{p,k}-s_{p,k-1}$, egyértelműen meghatározható A-ból. Tehát A minden – a feltételeknek megfelelő – direkt szorzat előállításában minden p prímre és $k\in\mathbb{N}$ kitevőre $s_{p,k}-s_{p,k-1}$ darab Z_{p^k} tényező van. A felírás tehát egyértelmű.

6.17.5 Következmény: G pontosan akkor p^n rendű Abel-csoport, ha $G\simeq Z_{p^{k_1}}\times Z_{p^{k_2}}\times\dots\times Z_{p^{k_t}}$, ahol $\sum_{i=1}^{t}k_t=n$. Az ilyen csoportok száma tehát n partícióinak száma, ezt szokás $p(n)$-el jelölni.

6.18 Végtelen Abel-csoportok. Osztható csoport

6.18.1 Definíció: a G végtelen csoport torziómentes, ha minden 1-től különböző eleme végtelen rendű. Torziócsoport, ha minden eleme véges rendű.

6.18.2 Definíció: legyen A végtelen Abel-csoport. A torziórészcsoportja $T=\{a\in A\,|\,o(a)<\infty\}$. Ez valóban részcsoport, mert ha $a,b\in T$, akkor $a^n=1$ és $b^m=1$. Ekkor $(ab^{-1})^{nm}=(a^n)^m(b^m)^{-n}=1$, azaz $TT^{-1}\subseteq T$.

6.18.3 Állítás: ha A torziórészcsoportja T, akkor A/T torziómentes.

Bizonyítás: ha valamely Tx mellékosztály rendje véges, azaz $Tx^n=T$, tehát $x^n\in T\Rightarrow(x^n)^m=1\Rightarrow x\in T\Rightarrow Tx=T$.

Az Abel-csoportokra a jövőben az additív jelölést használjuk, azaz a művelet $+:(a,b)\mapsto a+b$; a neutrális elem 0; a inverze $-a$. Az a csoportelemre és $k\in\mathbb{Z}$-re értelmezzük $k\cdot a$-t, ez $k=0$-ra 0, $k\in\mathbb{Z}^+$-ra $(k-1)\cdot a+a$, $k\in\mathbb{Z}^-$ esetén $(k+1)a+(-a)$. A direkt szorzatot direkt összegnek mondjuk és $A_1\oplus A_2$-vel illetve $\oplus_{\alpha\in\mathbf{I}}A_\alpha$-val jelöljük.

6.18.4 Jelölés: az A végtelen Abel-csoportra $A_p=\{x\in A\,|\,\exists k\in\mathbb{N}: p^k\cdot x=0\}$.

6.18.5 Állítás: ha A torziócsoport, akkor előáll $A=\oplus_{p\text{ prím}}A_p$ alakban.

Bizonyítás: nyilván $x\in A_p \Leftrightarrow o(x)$ p-hatvány ($1=p^0$-t is beleértve). Ha $x\in\langle A_q \mid q\in p'\rangle$, akkor előáll $\sum_{i=1}^t n_i x_i$ alakban, ahol $x_i\in A_{q_i}$, azaz $q_i^{k_i}x_i=0$. Legyen $m=\prod_{j=1}^t q_j^{k_j}$. Ekkor $mx_i=(\prod_{j\neq i} q_j^{k_j})\cdot(q_i^{k_i}\cdot x_i)=0$, azaz $mx=\sum_{i=1}^t n_i m x_i=0$. Tehát $o(x)$ osztja m-et. Mivel m minden q prímtényezőjére $q\in p'$, $p\nmid m \Rightarrow p\mid o(x)$. Tehát $\langle A_q \mid q\in p'\rangle$-ben nincs valódi p-hatvány rendű elem, azaz $A_p\cap\langle A_q \mid q\in p'\rangle=\{0\}$. Így $\langle A_p \mid p \text{ prím}\rangle=\oplus_{p \text{ prím}} A_p$. Már csak azt kell belátnunk, hogy $a\in A$ előáll $\sum_{i=1}^t n_i x_i$ alakban, ahol $x_i\in A_{p_i}$. Legyen $o(a)=n=\sum_{i=1}^s p_j^{k_j}$ és $n_i=\prod_{j\neq i} p_j^{k_j}$. Az $\{n_i \mid 1\le i\le s\}$ számok legnagyobb közös osztója 1, tehát megfelelő $\{v_i\in\mathbb{Z} \mid 1\le i\le s\}$ együtthatókkal $\sum_{i=1}^s v_i n_i=1$. Ekkor $x=\sum_{i=1}^s v_i(n_i a)$. Azt állítjuk, hogy $n_i a\in A_{p_i}$. Valóban, $p_i^{k_i}(n_i a)=na=0$. Ez tehát éppen a keresett felírás.

Következmény: $(\mathbb{Q},+)/\mathbb{Z}\simeq\oplus_{p \text{ prím}}(\mathbb{Q}/\mathbb{Z})_p\simeq\oplus_{p \text{ prím}} Z_{p^\infty}$.

6.18.6 Definíció: legyen A Abel-csoport, $a\in A, n\in\mathbb{Z}^+$. Ha $\exists x\in A: nx=a$, akkor a osztható n-el, jelölése $n\mid a$.

6.18.7 Definíció: $(D,+)$ osztható csoport, ha $\forall x\in D, n\in\mathbb{Z}^+: n\mid x$. Ilyen pl. $(\mathbb{Q},+)$ és $(\mathbb{R},+)$.

6.18.8 Állítás: ha A Abel-csoport, $a\in A, o(a)=n<\infty$ és p egy n-t nem osztó prím, akkor $p\mid a$. Valóban, feltételeink szerint a $px\equiv 1 \pmod n$ lineáris kongruencia megoldható, ekkor $p\cdot(xa)=(1+tn)\cdot a=a$.

6.18.9 Állítás: ha A Abel-csoportban $\forall a\in A$ elemre és p prímre $p\mid a$, akkor A osztható csoport.

Bizonyítás: legyen $n=\prod_{i=1}^k p_i$, ahol ezek nem feltétlenül különböző prímek. Legyen $a_0=a$ és a_{i+1} egy megoldása a $p_{i+1}x=a_i$ egyenletnek, ha $0\le i<k$. Feltételeink szerint a_k létezik, ekkor $n\cdot a_k=a$.

6.18.10 Következmény: Z_{p^∞} minden p prímre osztható, hiszen tetszőleges $a\in Z_{p^\infty}$-re $p\mid a$ ($\langle a\rangle\simeq Z_{p^k}<Z_{p^\infty}$ belefoglalható egy $Z_{p^{k+1}}<Z_{p^\infty}$-be és ott $xp=a$ megoldható), $q\in p'$-re pedig **6.18.8** szerint $q\mid a$.

6.18.11 Megjegyzés: osztható csoportok direkt összege osztható, hiszen $xn=a$-t megoldhatjuk koordinátánként.

6.18.12 Tétel: minden D osztható csoport előáll $\mathbb{Q}$-val és Z_{p^∞}-el izomorf csoportok direkt összegeként. Ebből csak annyit látunk be, hogy minden ilyen alakú csoport osztható, mert ez a fenti megjegyzés triviális következménye.

6.18.13 Tétel: ha D osztható részcsoport az A Abel-csoportban, akkor $\exists M\le A: A=D\oplus M$.

Bizonyítás: legyen $\chi\subseteq\mathcal{P}(A)$ azon H részcsoportok halmaza, melyekre $D\cap H=\{1\}$. Minden χ-beli $\mathcal{L}$ lánc uniója is részcsoport. Ugyanis $x,y\in U=\bigcup\mathcal{L}$ esetén $\exists H', H''\in\mathcal{L}: (x\in H' \text{ és } y\in H'')$. H-nak a bővebbet választva $xy^{-1}\in HH^{-1}=H\subseteq U$, azaz $UU^{-1}\subseteq U$, U valóban részcsoport és $(\bigcup\mathcal{L})\cap D=\bigcup_{H\in\mathcal{L}}(H\cap D)=\{1\}$. A Zorn-lemma szerint $\mathcal{L}$-ben van maximális elem – legyen M ilyen. Azt akarjuk belátni, hogy $A=D\oplus M$.

↯ $x_1\in A\setminus(D+M)$. M maximalitása miatt $\exists d_1\in D\cap\langle M,x_1\rangle\setminus\{0\}$. Ekkor d_1 előáll $d_1=m_1+k_1x_1 : m_1\in M, k_1\in\mathbb{Z}$ alakban. Persze $k_1\neq 0$, hiszen $d_1\notin D\cap M$, amiből $d_1\neq m_1$. Mivel D osztható és $d_1\in D$, alkalmas $d_1'\in D$ elemre $d_1=k_1d_1'$, azaz $m_1=k_1\cdot(d_1'-x_1)$.

Jelölje $(d_1'-x_1)$-et x_2. Mivel $d_1'\in D$ és $x\notin(D+M)$, $x_2\notin(D+M)$. Ismét M maximalitása $\exists d_2\in D\cap\langle M,x_2\rangle\setminus\{0\}$. Ez előáll $d_2=m_2+k_2x_2 : m_2\in M, k_2\in\mathbb{Z}$ alakban. Ez a felírás választható úgy, hogy $0<k_2<|k_1|$ legyen, mert $k_1x_2=m_1\in M$. Legyen ismét $d_2'\in D$ olyan, hogy $d_2=k_2d_2'$ és jelölje $(d_2'-x_2)$-t x_3. Ekkor $k_2x_3=m_2\in M, x_3\notin(D+M)$ lesz. Folytassuk ezt az algoritmust. Ekkor a $(k_i)_{i=2}^\infty$ pozitív egész számok szigorúan monoton csökkenő sorozatot alkotnak, ↯.

Így hát $A=D+M$. M választása szerint $D\cap M=\{0\}$, azaz $A=D\oplus M$, mint azt bizonyítani akartuk.

6.18.14 Definíció: legyen A Abel-csoport. Ekkor $exp(A)$ az A-ban előforduló elemrendek legkisebb közös többszöröse, amennyiben ez létezik és ∞, ha nem. Nyilván $exp(A)<\infty \Leftrightarrow \{o(a) \mid a\in A\}$ korlátos.

6.18.15 Tétel: $exp(A)<\infty \Leftrightarrow (A\simeq\oplus_{\alpha\in\mathbf{I}} Z_{n_\alpha}$ és $\{n_\alpha \mid \alpha\in\mathbf{I}\}$ korlátos$)$. Ebből $\Leftarrow$ triviális, $\Rightarrow$ meg nem.

6.19 Szabadcsoport, Dyck-tétel

6.19.1 Definíció: szabad Abel-csoportnak hívunk egy olyan csoportot, amely előáll $\oplus_{\alpha\in\mathbf{I}} Z_\infty$ alakban. Speciálisan $FA_n=\oplus_{i=1}^n Z_\infty$. $\oplus_{n\in\mathbb{N}} Z_\infty$-t FA_∞, $\oplus_{\alpha\in\mathbf{I}} Z_\infty$-t pedig $FA_{|\mathbf{I}|}$ jelöli.

6.19.2 Állítás: ha κ,χ különböző számosságok, akkor $FA_\kappa\not\simeq FA_\chi$.

Bizonyítás: azt állítjuk, hogy FA_κ minden generátorrendszere legalább κ számosságú. Tekintsük FA_κ-t mint a $V=\oplus_{\iota\in\kappa}(\mathbb{R},+)$ (diszkrét) direkt összeg egész koordinátájú elemeinek additív csoportját. Legyen χ ennek egy generátorrendszere. Vegyük észre, hogy V κ dimenziós valós vektortér, amelyet (lineáris kombinációval) generál FA_κ. Feltevésünk szerint FA_κ-t (összeadással, azaz lineáris kombinációval is) generálja χ. Tehát V-t generálja χ, következésképp $|\chi|\geq\mathbf{dim}(V)=\kappa$.

Másrészt FA_κ-nak nyilván van κ elemű generátorrendszere, tehát κ éppen a legkisebb olyan számosság, amekkora komplexussal már generálható. Ez FA_χ-ra $\chi\neq\kappa$, tehát a két csoport nem lehet izomorf.

6.19.3 Definíció: vegyünk n darab betűt, legyenek ezek $a_1,a_2,\ldots,a_n$. Legyen F_n az ezekből és $a_1^{-1},a_2^{-1},\ldots,a_n^{-1}$-ből alkotott olyan véges (legalább 0) hosszú szavak halmaza melyekben nem szerepel egymás mellett a_i és a_i^{-1}. A művelet legyen a következő: két szót úgy szorzunk össze, hogy egymás után írjuk őket és mindaddig, amíg van szomszédos a_i és a_i^{-1}, egy ilyen párt letörlünk. Ez idővel véget ér, legfeljebb elfogynak a betűk és 0 hosszú szót kapunk. Könnyen látható, hogy F_n zárt a szorzásra, egysége a 0 hosszú szó – jelölése 1 – és minden elemének van inverze (megfordítjuk és minden betűjét invertáljuk). Tetszőleges $\mathbf{H}$ halmazra $F\langle\mathbf{H}\rangle$ betűi $\mathbf{H}$ elemei (és formális inverzeik), innen a definíció ugyanaz. Ha csak izomorfia erejéig akarjuk megadni, akkor használhatjuk az $F_{|\mathbf{H}|}$ jelölést, hiszen ha $\mathbf{H}\tilde{\psi}\mathbf{H}'$, akkor ψ izomorfizmust indukál $F\langle\mathbf{H}\rangle$ és $F\langle\mathbf{H}'\rangle$ között. F_∞ alatt $F_{\aleph_0}$-t értjük. Ha $\psi:\mathbf{H}\to\mathbf{H}'$ injekció, akkor nyilván $F\langle\mathbf{H}\rangle\simeq F\langle\mathbf{H}\psi\rangle\leq F\langle\mathbf{H}'\rangle$, azaz $|\mathbf{H}|\leq|\mathbf{H}'|\Rightarrow F_{|\mathbf{H}|}\leq F_{|\mathbf{H}'|}$.

6.19.4 Nielsen-Freier tétel: szabadcsoport minden részcsoportja is szabadcsoport.

Megjegyzés: könnyen ellenőrizhetően $|F_1|=|F_\infty|=\aleph_0$. (Nagyobb számosságokra $|F_\kappa|=\kappa$).

6.19.5 Állítás: $F_\kappa/F_\kappa'\simeq FA_\kappa$ (bizonyítás a Dyck-tétel után).

6.19.6 Következmény: ha κ,χ különböző számosságok, akkor $F_\kappa\not\simeq F_\chi$, hiszen $F_\kappa/F_\kappa'\simeq FA_\kappa\not\simeq FA_\chi\simeq F_\chi/F_\chi'$.

Megjegyzés: $F_{n+1}\simeq\langle a^n,b,a^{-1}ba,a^{-2}ba^2,\ldots,a^{1-n}b^{n-1}\rangle\lhd\langle a,b\rangle\simeq F_2$ és $F_\infty\simeq\langle\{a^{-n}ba^n|n\in\mathbb{Z}\}\rangle\lhd\langle a,b\rangle\simeq F_2$.

Tegyük fel, hogy szeretnénk a szabadcsoportokban további egyszerűsítési lehetőségeket megengedni a triviális $a_i\cdot a_i^{-1}=1$ mellett. Például valami miatt szimpatikus lenne, ha az $F_2=\langle a,b\rangle$ csoportban $a^n=1,b^2=1$ és $b^{-1}ab=a^{-1}$ lenne. Általánosabban: szeretnénk ha a $K=\{\omega_\alpha(a,b)|\alpha\in\mathbf{I}\}$ szavak mind 1-el lennének egyenlőek valamilyen $\mathbf{I}$ indexhalmazra. Persze 1-ek szorzata és minden konjugáltja is 1 kell legyen. Az tehát elvárható, hogy a K által generált normálosztó elemeit a jövőben 1-nek tekintsük. Ez gyakorlatilag azt jelenti, hogy vesszük az $F_2|_K=F_2/\langle K\rangle^{F_2}$ faktorcsoportot. Ha meg tudtuk volna pontosan fogalmazni, mit akarunk, akkor láthatnánk, hogy tényleg azt kaptuk: mindazon szavakat, melyeket 1-nek akartunk nevezni, a faktorcsoport egységébe képeztük le és azok az elemek, melyeknek a legcsekélyebb esélyük is megvolt arra, hogy ne az egységbe menjenek, nem tették. Így hát

6.19.7 Definíció: ha $\{\omega_\alpha|\alpha\in\mathbf{I}\}$ olyan kifejezések, melyek rendre az $F\langle\mathbf{H}\rangle$-beli x_α és y_α elemek egyenlőségét mondják ki (pl. $b^{-1}ab=a^{-1}$), akkor $\langle\mathbf{H}|\{\omega_\alpha|\alpha\in\mathbf{I}\}\rangle$ az $F\langle\mathbf{H}\rangle/N$ faktorcsoportot jelöli, ahol $N=\langle\{x_\alpha\cdot y_\alpha^{-1}|\alpha\in\mathbf{I}\}\rangle^{F\langle\mathbf{H}\rangle}$, azaz az $x_\alpha\cdot y_\alpha^{-1}$ elemek által generált normálosztó. (Ebben az $a\in\mathbf{H}$-hoz tartozó mellékosztályt kényelmi okokból továbbra is a-val fogjuk jelölni.) Például $\langle a,b|a^2=1,b^2=1,b^{-1}ab=a\rangle\simeq Z_2^2$.

6.19.8 Dyck-tétel: tegyük fel, hogy G csoportot generálja a K komplexus és G-ben teljesülnek a K elemeire vonatkozó $\omega_\alpha:x_\alpha=y_\alpha$ egyenlőségek, azaz $\varepsilon_\alpha=y_\alpha^{-1}x_\alpha$ jelöléssel $\forall\alpha\in\mathbf{I}:\varepsilon_\alpha=1$. Ekkor G homomorf képe $G^*=\langle K|\{\omega_\alpha|\alpha\in\mathbf{I}\}\rangle$-nek. Speciálisan ha $G=\langle g_1,g_2,\ldots,g_n\rangle$ és G-ben teljesül $\omega_1(g_1,\ldots,g_n),\omega_2(g_1,\ldots),\ldots,\omega_k(g_1,\ldots)$, akkor G homomorf képe $\langle g_1,\ldots,g_n|\omega_1,\ldots,\omega_k\rangle$-nak.

Bizonyítás: legyen az $\{\omega_\alpha|\alpha\in\mathbf{I}\}$ egyenlőségek által $F=F\langle K\rangle$-ban megadott – azaz $\langle\varepsilon_\alpha|\alpha\in\mathbf{I}\rangle$ által generált – normálosztó N. Rendelje $\varphi:F\to G$ az F-et generáló K elemeihez a G-t generáló K megfelelő elemeit, inverzeikhez a megfelelő inverzeket. Ezután F egy tetszőleges x elemét írjuk fel betűnként és minden β betű helyére írjuk be $\beta\varphi$-t. A kapott G-beli elem legyen $x\varphi$. Ekkor φ triviálisan homomorfizmus lesz. Legyen ennek a magja N'. (Ez bizonyos értelemben az összes $y^{-1}x\in F$ szavak halmaza, amelyekre G-ben $\omega:x=y$ teljesül.) Az F/N' faktorcsoportban minden ω_α teljesül, hiszen a homomorfizmus-tétel szerint $G\simeq F/N'$. Ezért az $\{\omega_\alpha|\alpha\in\mathbf{I}\}$ által megadott normálosztó részhalmaza N'-nek, mert $\{\varepsilon_\alpha|\alpha\in\mathbf{I}\}\subseteq N'\lhd F$. Tehát $N\subseteq N'$ és $N,N'\lhd F$. A II. izomorfizmus-tétel szerint $F/N'\simeq(F/N)/(N'/N)$, tehát F/N' éppen F/N képe a $\psi:F/N'\to(F/N)/(N'/N)$ természetes homomorfizmusban.

Megjegyzés: ez a fajta felírás igen praktikus, de messze nem tökéletes. Könnyű vele megadni csoportokat, csak nehéz észrevenni, hogy mit adtunk meg. Például nem valami feltűnő, hogy $\langle a,b|ab^2=b^3a,ba^2=a^3b\rangle=\{1\}$.

Lássuk most **6.19.5** bizonyítását:

Bizonyítás: legyen $|\mathbf{X}|=\kappa$, $G=F\langle\mathbf{X}\rangle$ és $H=FA\langle\mathbf{X}\rangle$ (ez az $\mathbf{X}$ elemei által generált Z_∞-ek direkt szorzata). Tekintsük az $A=\langle\mathbf{X}\,|\,\forall a,b\in G\colon ab=ba\rangle$ csoportot. Itt a definíció jelöléseivel $\{\varepsilon\}=\{\varepsilon_{a,b}\,|\,a,b\in G\}=\{[a,b]\,|\,a,b\in G\}$. Ez tehát a G-beli kommutátorok halmaza, azaz a generált normálosztó éppen G', így definíció szerint $A=G/G'$; legyen a faktorleképezés ψ (ez a generátorokat ($\mathbf{X}$ elemeit) önmagukba képezi). Másrészt H-ban bármely két szó felcserélhető, tehát az összes felsorolt reláció teljesül benne, így a Dyck-tétel szerint homomorf képe A-nak. Sőt, a bizonyítás olyan $\varphi\colon A\to H$ homomorfizmust ad, amely a generátorokat önmagukba képezi.

Azt állítjuk, hogy A az $\langle x\psi\rangle$: $x\in\mathbf{X}$ normálosztók belső direkt szorzata és ezek mind Z_∞-el izomorfak. Mivel $x\psi\varphi\in H$ végtelen rendű, $x\psi$ is az kell legyen, tehát $\langle x\psi\rangle\simeq Z_\infty$ valóban fennáll. $A=G/G'$ miatt A kommutatív, így $\langle x\psi\rangle\triangleleft A$. Hogy együtt generálják A-t, az nyilvánvaló, hisz már $\mathbf{X}$ is generálja. Csak az van hátra, hogy $\langle x\psi\rangle\cap\langle y\psi\,|\,y\in\mathbf{X}\setminus\{x\}\rangle=\{1\}$. Legyen $(x\psi)^n\in\langle y\psi\,|\,y\in\mathbf{X}\setminus\{x\}\rangle$ tetszőleges. Ekkor $(x\psi\varphi)^n\in\langle y\psi\varphi\,|\,y\in\mathbf{X}\setminus\{x\}\rangle\le H$. Viszont a $H=FA\langle\mathbf{X}\rangle=\oplus_{y\in\mathbf{X}}\langle y\psi\varphi\rangle$ csoportban $\langle x\psi\varphi\rangle\cap\langle y\psi\varphi\,|\,y\in\mathbf{X}\setminus\{x\}\rangle=\{1\}$, tehát ez csak $(x\psi\varphi)^n=1$ esetén fordulhat elő. Mivel $\mathbf{X}$-en $\psi\varphi$ az identitás, $x\psi\varphi=x\neq1$. H torziómentes, így $(x\psi\varphi)^n=1\Rightarrow n=0$, ebből $(x\psi)^n=1$. A vizsgált metszet tehát $\{1\}$. Így A az $\mathbf{X}\psi=\mathbf{X}$ elemei által generált szabad Abel-csoport, mint azt bizonyítani akartuk; φ természetesen az identitás.

6.20 Az általánosított kvaterniócsoport és társai

6.20.1 Definíció: az általánosított kvaterniócsoport $Q_{2^n}=\langle a,b\,|\,a^{2^{n-1}}=1,b^2=a^{2^{n-2}},b^{-1}ab=a^{-1}\rangle$, ha $n\ge3$. Így $Q=Q_8$.

6.20.2 Állítás: Q_{2^n} rendje 2^n.

Bizonyítás: jelölje Q_{2^n}-t G. $a^kb=ba^{-k}$ és $a^kb^{-1}=b^{-1}a^{-k}$ miatt G bármely eleme felírásában megtehetjük, hogy b hatványait kivisszük a balszélre és az átlépett a-hatványok helyére néha az inverzüket írjuk. Ily módon minden elem felírható $b^i\cdot a^j$ alakban. Persze feltehetjük, hogy $0\le i<2$ és $0\le j<2^{n-1}$, hiszen b^{2m} helyére $a^{m\cdot2^{n-2}}$, $a^{2^{n-1}}$ helyére 1 írható. Így legfeljebb 2^n-féle különböző szót kaphatunk, tehát legfeljebb ennyi eleme van G-nek. Másrészt legyen ε egy primitív 2^{n-1}-edik egységgyök, $a=\left(\begin{smallmatrix}\varepsilon&0\\0&\varepsilon^{-1}\end{smallmatrix}\right)\in SL_2(\mathbb{C})$ és $b=\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)\in SL_2(\mathbb{C})$. a rendje 2^{n-1} és $b\notin\langle a\rangle$, azaz $|\langle a,b\rangle|\ge2^n$. Ellenőrizhető, hogy $\langle a,b\rangle$-ben teljesül $a^{2^{n-1}}=1,b^2=a^{2^{n-2}}$ és $b^{-1}ab=a^{-1}$, tehát homomorf képe G-nek. Így mindkettő köteles pontosan 2^n elemű lenni és persze izomorfak is, mert a $G\to\langle a,b\rangle$ homomorfizmus magja $\{1\}$ az elemszám miatt.

6.20.3 Állítás: pontosan két nyolcadrendű nem kommutatív csoport van, mégpedig D_4 és Q.

Bizonyítás: legyen $|G|=8$. Ha van nyolcadrendű eleme, akkor $G\simeq Z_8$ kommutatív, érdektelen. Ha $G\setminus\{1\}$ minden eleme másodrendű, akkor is kommutatív. Van tehát egy negyedrendű elem, a. $\langle a\rangle$ egy 2 indexű részcsoport, tehát normálosztó. Legyen $b\in G\setminus\langle a\rangle$. Mivel $\langle a\rangle$ 2 indexű, $b^2\in\langle a\rangle$. $b^2\in\{a,a^{-1}\}$ esetén $o(b)=8$ lenne, amit már kizártunk, azaz $b^2\in\{1,a^2\}$. $b^{-1}ab\in\langle a\rangle$ rendje azonos kell legyen a rendjével, mert φ_b automorfizmusa G-nek. Így hát csak a vagy a^{-1} lehetne. Az első esetben $ab=ba$, ekkor G Abel, érdektelen. Ha $b^{-1}ab=a^{-1}$, akkor $G\simeq\langle a,b\,|\,a^4=1,b^2=1,b^{-1}ab=a^{-1}\rangle=D_4$ vagy $G\simeq\langle a,b\,|\,a^4=1,b^2=a^2,b^{-1}ab=a^{-1}\rangle=Q$. Ezt akartuk belátni.

6.20.4 Állítás: $G/Z(G)$ nem lehet ciklikus csoport.

Bizonyítás: jelölje $Z(G)$-t C. Tegyük fel, hogy $G/C=\langle Ca\rangle$. Ekkor $\langle C,a\rangle$. Itt a felcserélhető a generátorrendszer minden elemével, mert azok vagy a-hatványok, vagy centrumelemek. C elemei szintén felcserélhetőek a generátorrendszer minden elemével, mert C a centrum. Tehát G-t felcserélhető elemek generálják, így kommutatív. Akkor viszont $G/Z(G)=1$ és nem ciklikus.

6.20.5 Állítás: ha $p>2$ prím, akkor pontosan két p^3 rendű nem kommutatív csoport van.

Bizonyítás: legyen G egy p^3 rendű, nem kommutatív csoport. Mivel nem ciklikus, nincs p^3 rendű eleme. Ha van p^2 rendű, akkor később be fogjuk látni, hogy $G\simeq\langle a,b\,|\,a^{p^2}=b^p=1,b^{-1}ab=a^{1+p}\rangle$, ez más néven $Z_p\ltimes Z_{p^2}$. Ha minden elem p-edrendű, akkor legyen $C=Z(G)$ és nézzük meg, mi lehet G/C rendje. 1 nem lehet, mert G nem Abel. p nem lehet, mert nem ciklikus. p^3 nem lehet, mert véges p-csoport centruma nem $\{1\}$. Tehát $|G/C|=p^2$ és mivel nem ciklikus, csak $Z_p\times Z_p$ lehet. Legyen $G/C=\langle Ca,Cb\rangle$. Ekkor $a^{-1}b^{-1}ab=c\in C$, mert G/C Abel, azaz $G'\le C$. Tehát G homomorf képe a $H=\langle a,b\,|\,a^p=b^p=1,a^{-1}b^{-1}ab=c,c^p=1,ac=ca,bc=cb\rangle$ csoportnak. Kiszámolható, hogy $H\simeq Z_p\ltimes(Z_p\times Z_p)$ (és hogy ebből csak egyféle van).

6.20.6 Tétel: ha $n\geq 4$, $|G|=2^n$, G nem kommutatív és van 2^{n-1} rendű eleme, akkor az alábbi négy csoport egyike

(1) $D_{2^{n-1}}=\langle a,b\,|\,a^{2^{n-1}}=b^2=1, b^{-1}ab=a^{-1}\rangle\simeq Z_{2^{n-1}}\rtimes_{\vartheta} Z_2$, ahol $b\vartheta: a\mapsto a^{-1}$ (diédercsoport),
(2) $Q_{2^n}=\langle a,b\,|\,a^{2^{n-1}}=1, b^2=a^{2^{n-2}}, b^{-1}ab=a^{-1}\rangle$ (általánosított kvaterniócsoport),
(3) $M_n(2)=\langle a,b\,|\,a^{2^{n-1}}=b^2=1, b^{-1}ab=a^{1+2^{n-2}}\rangle\simeq Z_{2^{n-1}}\rtimes_{\vartheta} Z_2$, ahol $b\vartheta: a\mapsto a^{1+2^{n-2}}$,
(4) $SD_n=\langle a,b\,|\,a^{2^{n-1}}=b^2=1, b^{-1}ab=a^{-1+2^{n-2}}\rangle\simeq Z_{2^{n-1}}\rtimes_{\vartheta} Z_2$, ahol $b\vartheta: a\mapsto a^{-1+2^{n-2}}$ (szemidiéder-csoport)

és ezek páronként nem-izomorf 2^n rendű csoportok.

Bizonyítás: mint **6.20.1**-nél, az **(1)**, **(2)**, **(3)** és **(4)** csoportok tetszőleges eleme felírható $b^s\cdot a^t$ alakban, ahol $s\in\{0,1\}$ és $0\leq t\leq 2^{n-1}$, tehát legfeljebb 2^n eleműek. A megadott szemidirekt szorzatokban teljesülnek a megfelelő feltételek és mindegyik 2^n elemű. A felírt izomorfiák tehát jogosak és a négy csoport rendje valóban 2^n. Ha tehát G-ben teljesül valamelyik feltételcsoport, akkor izomorf a megfelelő csoporttal, mert homomorf képe és azonos az elemszámuk. A szemidirekt szorzatos felírásokból látszik, hogy **(1)**, **(3)** és **(4)** páronként nem-izomorfak, **(2)**-ben pedig könnyen ellenőrizhetően csak egy másodrendű elem van, tehát nem állhat elő szemidirekt szorzatként.

Legyen a egy 2^{n-1} rendű elem. Legyen $b\in G\setminus\langle a\rangle$, továbbá $b^{-1}ab=a^r$. (Ez valóban a-hatvány lesz, mert $A=\langle a\rangle$ indexe $2\Rightarrow$ normálosztó.) $r\not\equiv 1\ (mod\ 2^{n-1})$, mert különben az $\{a,b\}$ generátorrendszer elemei felcserélhetőek, G pedig kommutatív lenne. $G/A\simeq Z_2$ miatt $b^2\in A\Rightarrow a=b^{-2}ab^2=b^{-1}(b^{-1}ab)b=b^{-1}(a^r)b=a^{r^2}\Rightarrow r^2\equiv 1\ (mod\ 2^{n-1})$. Eszerint $2^{n-1}\,|\,(r-1)(r+1)$. E két tényező egyike legfeljebb az első hatványon osztható 2-vel, a másik tehát legalább 2^{n-2}-vel osztható. Az $r\not\equiv 1$ megkötés figyelembevételével az $r\equiv -1, r\equiv 1+2^{n-2}, r\equiv -1+2^{n-2}\ (mod\ 2^{n-1})$ esetek lehetségesek.

Legyen $b^2=a^m$. Ekkor $a^m=b^2=b^{-1}b^2b=b^{-1}a^mb=a^{mr}$, azaz $\underline{\odot}\ (r-1)\cdot m\equiv 0\ (mod\ 2^{n-1})$.

(1) és (2) eset: $r\equiv -1$. Ezt beírva $\odot$-be $-2m\equiv 0\ (mod\ 2^{n-1})$, ez a $b^2=a^0=1$ és $b^2=a^{2^{n-2}}$ eseteket teszi lehetővé; ezek épp az **(1)**, **(2)** feltételeket adják.

(3) eset: $r\equiv 1+2^{n-2}$. Ezt beírva $\odot$-be $2^{n-2}\cdot m\equiv 0\ (mod\ 2^{n-1})$, azaz $m\equiv 0\ (mod\ 2)$. Legyen $m=2m'$, ekkor $n\geq 4$ miatt $(1+2^{n-3})$ páratlan, ezért $j(1+2^{n-3})+m'\equiv 0\ (mod\ 2^{n-2})$-nek pontosan egy megoldása van. $c=b\cdot a^j$ választással $c\notin A$, $c^{-1}ac=a^{-j}b^{-1}aba^j=a^{-j}\cdot a^{1+2^{n-2}}\cdot a^j=a^{1+2^{n-2}}$ és $c^2=b^2(b^{-1}a^jb)a^j=a^m\cdot a^{j\cdot(1+2^{n-2})}\cdot a^j=a^{2\cdot[m'+j\cdot(1+2^{n-3})]}=1$ mert a szögletes zárójelben lévő kifejezés j választása miatt osztható 2^{n-2}-vel. Tehát $G=\langle a,c\rangle\simeq M_n(2)$.

(4) eset: $r\equiv -1+2^{n-2}$. $\odot$ szerint $(2^{n-2}-2)\cdot m\equiv 0\ (mod\ 2^{n-1})$. $n\geq 4\Rightarrow 4\,|\,2^{n-2}\Rightarrow 4\nmid(2^{n-2}-2)\Rightarrow 2^{n-2}\,|\,m$, azaz $b^2=a^0=1$ vagy $b^2=a^{2^{n-2}}$. Az első esetben rögtön SD_n-t kapjuk, a másodikban b helyett inkább vegyük $c=ba$-t, ekkor $c^{-1}ac=a^{-1}b^{-1}aba=a^{-1+2^{n-2}}$ és $c^2=baba=b^2b^{-1}aba=a^{2^{n-2}}\cdot a^{-1+2^{n-2}}\cdot a=1$, tehát $G=\langle a,c\rangle\simeq SD_n$.

6.20.7 Tétel: ha $p>2$ prím, $n\geq 3$, G rendje p^n, van egy p^{n-1} rendű a eleme és G nem kommutatív, akkor $G\simeq M_n(p)=\langle a,b\,|\,a^{p^{n-1}}=b^p=1, b^{-1}ab=a^{1+p^{n-2}}\rangle$. (Ez mellesleg $Z_{p^{n-1}}\rtimes_{\vartheta} Z_p$, ahol $b\vartheta: a\mapsto a^{1+p^{n-2}}$. Ez valóban nem Abel-csoport, mert $n\geq 3$ miatt $b\vartheta$ nem az identitás.)

Bizonyítás: legyen $A=\langle a\rangle, b\in G\setminus A$. Sylow I. tétele szerint $A\lhd G$, azaz $b^{-1}ab=a^r$: $0\leq r<p^{n-1}$. Ha $r=1$ lenne, akkor az $A\cup\{b\}$ generátorrendszer elemei felcserélhetőek lennének, tehát G kommutatív lenne. $r=0$ szintén lehetetlen, mert $a^0=1$ nem áll elő más elem konjugáltjaként. Eszerint $1<r<p^{n-1}$.

$b^{-1}a^jb=(b^{-1}ab)^j=a^{rj}$, azaz teljes indukcióval $b^{-i}ab^i=b^{-1}(b^{1-i}ab^{i-1})b=b^{-1}a^{r^{i-1}}b=a^{r^i}$. Mivel $G/A\simeq Z_p$, $\forall x\in G: x^p\in A$, speciálisan $b^p\in A$. A ciklikus $\Rightarrow$ kommutatív $\Rightarrow$ $a^{r^p}=b^{-p}ab^p=ab^{-p}b^p=a\Rightarrow r^p\equiv 1\ (mod\ o(a))$, behelyettesítve $r^p\equiv 1\ (mod\ p^{n-1})$. Felhasználjuk, hogy ez csak akkor lehetséges, ha $r=1+kp^{n-2}$, ahol $p\nmid k$.

Ekkor j megadható úgy, hogy $jk\equiv 1\ (mod\ p)$ teljesüljön. $c=b^j$ választással $c^{-1}ac=b^{-j}ab^j=a^{rj}$ lesz. A kitevő $r^j=(1+kp^{n-2})^j\equiv 1+jk\cdot p^{n-2}+\ldots\equiv 1+p^{n-2}\ (mod\ p^{n-1})$, tehát $c^{-1}ac=a^{1+p^{n-2}}$. Jelölje $(1+p^{n-2})$-t h. Tekintsük most a (ca^i) alakú elemeket. a-t egy ilyennel konjugálva $(ca^i)^{-1}a(ca^i)=a^{-i}a^ha^i=a^h$-t kapunk; (ca^i) hatványai a következők:

$$(ca^i)^2=c^2(c^{-1}a^ic)a^i=c^2(c^{-1}ac)^ia^i=c^2a^{i\cdot(1+h)}.$$

A $(ca^i)^m=c^ma^{i\cdot(\sum_{j=0}^{m-1}h^j)}$ indukciós feltevésből a következő hatvány:

$$(ca^i)^{m+1}=(ca^i)\cdot(ca^i)^m=(c^{m+1}c^{-m}a^i)\cdot c^ma^{i\cdot(\sum_{j=0}^{m-1}h^j)}=c^{m+1}(c^{-m}ac^m)^i\cdot a^{i\cdot(\sum_{j=0}^{m-1}h^j)}=c^{m+1}\cdot a^{i\cdot h^m}\cdot a^{i\cdot(\sum_{j=0}^{m-1}h^j)}=c^{m+1}\cdot a^{i\cdot(\sum_{j=0}^{m}h^j)}.$$

Eszerint $S=1+h+h^2+\ldots+h^{p-1}$ jelöléssel $(ca^i)^p=c^p\cdot a^{i\cdot S}$. Felhasználva, hogy $h^j=(1+p^{n-2})^j\equiv 1+j\cdot p^{n-2}\ (mod\ p^{n-1})$, $S\equiv p+p^{n-2}\cdot(0+1+2+\ldots+(p-1))\equiv p+p^{n-2}\cdot\frac{p(p-1)}{2}\equiv p\ (mod\ p^{n-1})\Rightarrow a^S=a^p\Rightarrow (ca^i)^p=c^p\cdot a^{p\cdot i}$. Mivel $c^p\in A$, felírható $c^p=a^t$ alakban. $G\neq Z_{p^n}\Rightarrow G\neq\langle c\rangle\Rightarrow\langle c^p\rangle\neq A\Rightarrow\langle a^t\rangle\neq A\Rightarrow$ t osztható p-vel. Eszerint található olyan i, amelyre

$t+i\cdot p\equiv 0\ (mod\ p^{n-1})$. Erre az i-re $(ca^i)^p=c^p\cdot a^{ip}=a^t\cdot a^{ip}=a^{t+ip}=1$. Összefoglalva $d=ca^i$ választással $a^{p^{n-1}}=1, d^{-1}ad=a^{1+p^{n-2}}$ és $d^p=1$. A Dyck-tétel szerint tehát $G=\langle a,d\rangle$ homomorf képe a nemrég definiált $M_n(p)$ csoportnak. Elemszámuk azonos, tehát izomorfak.

6.20.8 Lemma: az általánosított kvaterniócsoportban a szokásos jelölésekkel minden $Q_{2^n}\setminus\langle a\rangle$-beli elem negyedrendű. Valóban, minden ilyen elem előáll $b\cdot a^m$ alakban és $(b\cdot a^m)^2=b^2(b^{-1}a^mb)a^m=b^2a^{-m}a^m=b^2=a^{2^{n-2}}$. Ismét négyzetre emelve 1-et kapunk és ezt akartuk belátni. Ebből következik, hogy Q_{2^n} nem áll elő szemidirekt szorzatként, hiszen minden nem triviális részcsoportjában van másodrendű elem, ez pedig csak $a^{2^{n-2}}$ lehet, tehát nincs két olyan nem triviális részcsoportja, melyek metszete $\{1\}$.

6.20.9 Lemma: ha p prím, $|G|=p^n$ és G-nek pontosan egy p rendű részcsoportja van, akkor vagy $p=2$ és G általánosított kvaterniócsoport, vagy G ciklikus.

Bizonyítás: teljes indukció n szerint. $n=1$ és $n=2$ esetén az állítás triviális. Tegyük fel, hogy $n\geq 3$ és kisebb n esetén már tudjuk az állítást. Sylow tétele miatt G-ben található p^{n-1} rendű P részcsoport. Ebben is pontosan egy p-edrendű részcsoport van, mert Cauchy tétele szerint legalább egy van, több meg G-re tett feltevésünk szerint nem lehet. G nem állhat elő valódi szemidirekt szorzatként (ahol egyik tényező sem 1), mert bármely 1-nél nagyobb részcsoportjában benne van az egyetlen Z_p részcsoport, tehát bármely kettő metszetében is.

Az indukciós feltevésből P vagy ciklikus, vagy általánosított kvaterniócsoport. Ha tehát $p>2$, akkor G-ben van p^{n-1} rendű ciklikus részcsoport, ekkor **6.20.7** szerint G vagy Abel, vagy $M_n(p)$. Mivel G nem szemidirekt szorzat, $M_n(p)$-t kizárhatjuk, az pedig a véges Abel-csoportok alaptételéből következik, hogy ha egy véges Abel-csoport nem áll elő nem triviális direktszorzatként, akkor ciklikus.

Ha $p=2$ és G nem ciklikus, de szerencsés módon találtunk egy 2^{n-1} rendű ciklikus részcsoportot G-ben, akkor **6.20.6** szerint G a $D_{2^{n-1}}, Q_{2^n}, M_n(2), SD_n$ csoportok egyike és nem szemidirekt szorzat. Tehát csak Q_{2^n} lehet, ebben valóban pontosan egy másodrendű elem van, $a^{2^{n-2}}$. Ha G-nek nincs $Z_{2^{n-1}}$-el izomorf részcsoportja, akkor az indukciós feltétel szerint minden 2 indexű részcsoportja $Q_{2^{n-1}}$. Ha ez lehetetlen, akkor kész vagyunk.

↯ G minden 2 indexű részcsoportja általánosított kvaterniócsoport.

Vegyük először az $n=4$ esetet. Ekkor $Q=\langle a,b\,|\,a^4=1, b^2=a^2, b^{-1}ab=a^{-1}\rangle \lhd G$ és $|G:Q|=2$, azaz $G=Q\cup Qc$ és $c^{-1}Qc=Q$. Q-ban könnyen ellenőrizhetően három negyedrendű részcsoport van: $\langle a\rangle, \langle b\rangle$ és $\langle ab\rangle$. A c-vel való konjugálás automorfizmus Q-ban, rendje pedig 2-hatvány, mert c rendje 2-hatvány. φ_c egy permutációt indukál Q negyedrendű részcsoportjain, ezen permutáció rendje osztja φ_c rendjét, tehát továbbra is 2-hatvány. Így hát nem egy hármas ciklus, azaz van fixpontja. Szimmetriaokokból feltehetjük, hogy például $c^{-1}\langle a\rangle c=\langle a\rangle$. Ekkor φ_c a-t $\langle a\rangle$ egy generátorelemébe kell vigye $\Rightarrow$ vagy $c^{-1}ac=a$, vagy $c^{-1}ac=a^{-1}$. Az első esetben $\langle a,c\rangle$ egy nyolcadrendű Abel-részcsoport G-ben, ami ellentmond azon feltételezésünknek, hogy G minden 2 indexű részcsoportja Q-val izomorf. A második esetben $\langle a,cb\rangle$ lesz kommutatív. Így hát nincsen olyan 16-odrendű csoport, amelynek minden 8-adrendű részcsoportja Q.

Legyen most $n\geq 5$ és tegyük fel, hogy a 2^n rendű G csoport minden 2 indexű G_1 részcsoportja izomorf $Q_{2^{n-1}}=\langle a,b\,|\,a^{2^{n-2}}=1, b^2=a^{2^{n-3}}, b^{-1}ab=a^{-1}\rangle$-el. Legyen $G=G_1\cup G_1c$. Ekkor $c^{-1}G_1c=G_1$, sőt $c^{-1}\langle a\rangle c=\langle a\rangle$, mert **6.20.8** szerint $\langle a\rangle$ az egyetlen ilyen rendű ciklikus részcsoport G_1-ben. Eszerint $c^{-1}ac=a^r$, ahol r páratlan, hiszen $c^{-1}\langle a\rangle c=\langle a\rangle$. $|G:G_1|=2$ miatt $c^2\in G_1$. Ha $c^2\in\langle a\rangle$, akkor $c^{-2}ac^2=a\Rightarrow r^2\equiv 1\ (mod\ 2^{n-2})$, ha pedig $c^2\in G_1\setminus\langle a\rangle$, akkor előáll $c^2=a^m\cdot b$ alakban, azaz $c^{-2}ac^2=b^{-1}a^{-m}aa^mb=b^{-1}ab=a^{-1}\Rightarrow r^2\equiv -1\ (mod\ 2^{n-2})\Rightarrow r^2\equiv -1\ (mod\ 8)$, ami lehetetlen. Marad a $c^2\in\langle a\rangle, r^2\equiv 1\ (mod\ 2^{n-2})$ eset.

Ekkor $|\langle a,c\rangle|=2\cdot|\langle a\rangle|=2^{n-1}$, feltevéseink szerint ebből következik $G_2=\langle a,c\rangle\simeq Q_{2^{n-1}}$. Sőt, $o(a)=\frac{1}{2}|G_2|$ miatt alkalmas $d\in G_2\setminus\langle c\rangle$ elemre $\langle a,c\rangle=G_2=\langle a,d\,|\,a^{2^{n-2}}=1, d^2=a^{2^{n-3}}, d^{-1}ad=a^{-1}\rangle$ és $c\in G_2\setminus\langle a\rangle$. Ekkor c előáll $c=a^kd$ alakban és $c^{-1}ac=d^{-1}a^{-k}aa^kd=d^{-1}ad=a^{-1}$. Akkor viszont $(bc)^{-1}a(bc)=a$, tehát $G_3=\langle a,bc\rangle$ kommutatív. $bc\notin\langle a\rangle$, mert $bc\in G_1c\Rightarrow bc\in G_1\supseteq\langle a\rangle$. Tehát G-nek van egy legalább 2^{n-1} rendű Abel-részcsoportja. Ebben van $Q_{2^{n-1}}$-el nem izomorf 2^{n-1} rendű, ↯.

6.20.10 Tétel: ha p prím, $|G|=p^n$ és valamely $1\leq k<n$-re G-nek pontosan egy p^k rendű részcsoportja van, akkor vagy $p=2, k=1$ és G általánosított kvaterniócsoport, vagy G ciklikus.

Bizonyítás: n szerinti indukció rögzített k mellett. Kezdőlépésként lássuk be az $n=k+1$ esetre. Legyen $P\leq G$ az egyetlen p^k rendű részcsoport G-ben és $x\in G\setminus P$. Ha $\langle x\rangle<G$ lenne, akkor Sylow első tétele szerint x lefedhető lenne

egy $p^{n-1}=p^k$ rendű P' részcsoporttal. $x\in P'\setminus P$ miatt $P\neq P'$, ami ellentmondás, tehát tetszőleges ilyen x-re $G=\langle x\rangle$, G ciklikus.

Legyen most $n\geq k+2$, P pedig az egyetlen p^k rendű részcsoport. Legyen M maximális $P\leq M<G$ részcsoport. Véges csoportban ilyen mindig van, továbbá Sylow I. tétele és $n>k+1$ szerint $P<M$. Az indukciós feltevés szerint M vagy ciklikus, vagy általánosított kvaterniócsoport. Ekkor M-ben pontosan egy p-edrendű részcsoport van. Ha lenne egy másik Z_p G-ben, az belefoglalható lenne egy P-től különböző P' p^k rendű részcsoportba, pedig ilyen nincs a G-re tett feltevés szerint. Tehát az egész G-ben is csak egy p-edrendű részcsoport van, így **6.20.9** szerint ciklikus vagy általánosított kvaterniócsoport.

Már csak azt kell belátnunk, hogy ha G általánosított kvaterniócsoport és pontosan egy 2^k rendű részcsoportja van, akkor $k=1$. Vegyük észre, hogy a $Q_{2^{n+1}}=\langle a,b\,|\ldots\rangle$ csoportban $\langle a^2,b\rangle\simeq Q_{2^n}$, azaz $n>k\geq 3$ esetén $Q_{2^n}>Q_{2^k}$ és persze $Q_{2^n}>Z_{2^k}$, tehát Q_{2^n}-nek egynél több 2^k rendű részcsoportja van. Negyedrendű részcsoport $Q=Q_8$-ban már három van (ld. **6.20.8**), azaz Q_{2^n}-ben is legalább három van, lévén $Q_{2^n}>Q_8$. Ezzel az állítást beláttuk.

6.21 Transzfer. Schur- és Schur-Zassenhaus tételek

6.21.1 Definíció: legyen $H\leq G$ egy n indexű részcsoport, A Abel-csoport, $\vartheta: H\to A$ homomorfizmus. Legyenek H mellékosztályai $Ht_1, Ht_2, \ldots, Ht_n$. Megtehetjük, hogy $g\in G$-vel való jobbról szorzást a mellékosztályok, speciálisan azok indexei feletti $g: Ht_i\mapsto Ht_{i(g)}\ (=Ht_i\cdot g)$ permutációjaként kezeljük. Ily módon $g\in G$-nek egy S_n-beli permutációt feleltetünk meg (ld. mellékosztály szerinti reprezentáció). Legyen a $\vartheta^*: G\to A$ homomorfizmus a következő: $x\vartheta^*=\prod_{i=1}^n (t_i\cdot x\cdot t_{(i)x}^{-1})\vartheta$. (A $\prod$ szimbólum használata megengedett, mert a tényezők az A Abel-csoport elemei.) Ezt nevezzük transzfernek.

6.21.2 Állítás: ez egy értelmes definíció, azaz nem függ a t_i elemek választásától és tényleg homomorfizmus.

Bizonyítás: legyen $Ht_i=Ht_i'$, azaz $t_i'=h_it_i$. Ekkor $x\vartheta^{*\prime}=\prod_{i=1}^n (t_i'\cdot x\cdot t_{(i)x}'^{-1})\vartheta=\prod_{i=1}^n h_i\vartheta\cdot(t_i\cdot x\cdot t_{(i)x}^{-1})\vartheta\cdot h_{(i)x}^{-1}\vartheta$. Mivel A Abel, ezt szabadon átrendezhetjük. Tehát $x\vartheta^{*\prime}=(\prod_{i=1}^n h_i\vartheta)\cdot(\prod_{(i)x=1}^n h_{(i)x}\vartheta)^{-1}\cdot\prod_{i=1}^n (t_i\cdot x\cdot t_{(i)x}^{-1})\vartheta$. A második szorzatban az első szorzat tényezőinek inverzei szerepelnek, ez a két szorzat tehát kiejti egymást. A harmadik szorzat éppen $x\vartheta^*$, azaz $x\vartheta^{*\prime}=x\vartheta^*\ \Rightarrow\ \vartheta^*$ valóban nem függ a t_i-k választásától. Lássuk be, hogy $(xy)\vartheta^*=x\vartheta^*\cdot y\vartheta^*$:

$$(xy)\vartheta^*=\prod_{i=1}^n (t_i\cdot xy\cdot t_{(i)(xy)}^{-1})\vartheta=\prod_{i=1}^n (t_ixt_{(i)x}^{-1}\cdot t_{(i)x}yt_{(i)(xy)}^{-1})\vartheta=\prod_{i=1}^n (t_ixt_{(i)x}^{-1})\vartheta\cdot\prod_{(i)x=1}^n (t_{(i)x}yt_{((i)x)y}^{-1})\vartheta,$$

hiszen a szorzatok még mindig átrendezhetőek. Az első szorzat láthatóan $x\vartheta^*$. A második $j=(i)x$ szerint indexelve éppen $y\vartheta^*$. Szép csendben felhasználtuk, hogy $(i)(xy)=((i)x)y$; ez azért igaz, mert a mellékosztály szerint reprezentáció is homomorfizmus.

Ha már így beláttuk, hogy t_i bárhogyan választható a megfelelő mellékosztályból, akkor megpróbálunk praktikus reprezentálóelemeket találni. Mint tudjuk, az $x\in G$-vel való jobbról szorzás egy permutáció a mellékosztályokon. Bontsuk ezt diszjunkt ciklusokra. Legyen belőlük k darab, az m-edik hossza legyen l_m, maga a ciklus $Hs_m, Hs_mx, Hs_mx^2, \ldots, Hs_mx^{l_m-1}$. Persze $\sum_{m=1}^k l_m=n$.

Rögzítsük most m-et és legyen $t_i=s_mx^{i-1}\ :\ 1\leq i\leq l_m$. Ekkor $(i)x=i+1$ ha $1\leq i<l_m$ és $(l_m)x=1$. Tekintsük most a ϑ^*-ot definiáló szorzat azon tényezőit, melyek az m-edik ciklusból származnak:

$$\prod_{i=1}^{l_m} (t_ixt_{(i)x}^{-1})\vartheta=\left(\prod_{i=1}^{l_m}\left((s_mx^i)x(s_mx^{i+1})^{-1}\right)\vartheta\right)\cdot(s_mx^{l_m-1}\cdot x\cdot s_m^{-1})\vartheta=\left(\prod_{i=1}^{l_m}(s_ms_m^{-1})\vartheta\right)\cdot(s_mx^{l_m}s_m^{-1})\vartheta=(s_mx^{l_m}s_m^{-1})\vartheta.$$

Az $x\vartheta^*$-ot definiáló szorzatban a ciklusok szerint csoportosítva a tényezőket és beírva, amit az imént kiszámoltunk, $x\vartheta^*=\prod_{m=1}^k (s_mx_m^ls_m^{-1})\vartheta$. Ezt a felírást nevezzük ϑ^* „jó felírásának”.

6.21.3 Definíció: ha ϑ a $H\to H/H'$ természetes homomorfizmus, azaz a lehető legnagyobb Abel-csoportba megy, amely előáll H homomorf képeként akkor a kapott ϑ^* transzfert $\tau_{G,H}$-val jelöljük és a „transzfer H-ba” névvel illetjük. Ha H Abel-csoport, akkor ϑ az identitás.

6.21.4 Lemma: legyen $H\leq Z(G)$ és $|G:H|=n$. Ekkor $\varphi: x\mapsto x^n$ homomorfizmus.

Bizonyítás: azt állítjuk, hogy $\varphi=\tau_{G,H}$. Tekintsük τ jó felírását. $(s_mx^{l_m}s_m^{-1})\vartheta=s_mx^{l_m}s_m^{-1}$, mert H Abel, így $H/H'=H$. $s_mx^{l_m}s_m^{-1}\in H\subseteq Z(G)$ tehát konjugálva s_m-el önmagába megy, azaz $s_mx^{l_m}s_m^{-1}=s_m^{-1}(s_mx^{l_m}s_m^{-1})s_m=x^{l_m}$. Eszerint $x\tau=\prod_{m=1}^k x_m^l=x^{\sum_{m=1}^k l_m}=x^n$, ezt akartuk belátni.

6.21.5 Lemma: ha $H\le G, |G:H|=n<\infty$ és G végesen generált, akkor H is. ($|G:H|<\infty$ szükséges, mert $F_\infty<F_2$ és F_∞ nem végesen generált.)

Bizonyítás: legyen $G=\langle X\rangle, k=|X|$. Legyenek H mellékosztályai $Ht_1, Ht_2, \dots, Ht_n$ ahol $t_1=1$. Legyen $(i)g$ olyan, hogy $Ht_i\cdot g=Ht_{(i)g}$. Ekkor $t_i\cdot g=h_i(g)\cdot t_{(i)g}$, ahol $h_i(g)\in H$. Azt állítjuk, hogy $\{h_i(x)\,|\,1\le i\le n, x\in X\cup X^{-1}\}$ generálja H-t. Legyen $a\in H$ tetszőleges. Ez előáll $a=a_1a_2a_3\dots a_s\ :\ X\cup X^{-1}$ alakban, ahol.

$$a=t_1\cdot a_1a_2a_3\dots a_s=h_1(a_1)\cdot t_{(1)a_1}\cdot a_2a_3\dots a_s=h_1(a_1)\cdot h_{(1)a_1}(a_2)t_{(1)a_1a_2}\cdot a_3\dots a_s=\dots$$
$$\dots=h_1(a_1)\cdot h_{(1)a_1}(a_2)\cdot h_{(1)a_1a_2}(a_3)\cdot\dots h_{(1)a_1a_2\dots a_{s-2}a_{s-1}}(a_s)\cdot t_{(1)a}$$

Mivel $a\in H$, $t_{(1)a}=t_1=1$, sikerült a-t előállítanunk $h_i(x)\in H\ :\ 1\le i\le n, x\in X\cup X^{-1}$ alakú számok szorzataként.

6.21.6 Schur tétele: ha $|G:Z(G)|=n<\infty$, akkor $|G'|<\infty$.

Bizonyítás: jelölje $Z(G)$-t C. Legyenek C mellékosztályai $Cg_1, Cg_2, \dots, Cg_n$. Ha $c,c'\in C$, akkor $[cg_i, c'g_j]=[g_i, g_j]$, tehát legfeljebb n^2 különböző kommutátor van G-ben, így G' végesen generált. Az I. izomorfizmus-tételből $G'/(G'\cap C)\simeq CG'/C\le G/C$. Eszerint $k=|G':G'\cap C|\le|G:C|=n$, azaz G'-ben $M=G'\cap C$ véges indexű részcsoport. A lemma szerint M végesen generált, legyen $M=\langle A\rangle=\langle a_i\,|\,1\le i\le m\rangle$. A másik lemma szerint $\varphi: x\mapsto x^n$ homomorfizmus G-ben és C-be képez, mert $\varphi=\tau_{G,C}$. Másrészt $Im\,\varphi$ kommutativitása miatt $Ker\,\varphi\ge G'\ge M$. Tehát $\forall x\in M: x^n=1$. Tetszőleges $x\in M$ előáll A-beli elemek szorzataként. A kommutativitás miatt ez átrendezhető $x=\prod_{i=1}^m a_i^{\alpha_i}$-vé és a kitevők választhatóak úgy, hogy $0\le\alpha_i<n$ legyen, hiszen $a_i\in M\Rightarrow a_i^m=1$. Ilyen szorzat összesen n^m lehet, tehát $|M|\le n^m$. $|G'|=k\cdot|M|\le n^{m+1}$, ezzel az állítást beláttuk.

6.21.7 Frattini-elv: ha $H\triangleleft G$ és $P\in Syl_p(H)$, akkor $G=N_G(P)\cdot H$.

Bizonyítás: legyen $g\in G$ tetszőleges. $g^{-1}Pg\le H$, mert H normálosztó. Így $g^{-1}Pg$ is p-Sylow H-ban. Sylow II. tétele szerint előáll $h^{-1}Ph\ :\ h\in H$ alakban. Ekkor $g^{-1}Pg=h^{-1}Ph$, amiből $P\cdot(gh^{-1})=(gh^{-1})\cdot P$, azaz $gh^{-1}\in N_G(P)$. Tekintve a $g=gh^{-1}\cdot h$ felírást $gh^{-1}\in N_G(P)$ és $h\in H$, azaz $g\in N_G(P)\cdot H$.

6.21.8 Definíció: K a H részcsoport komplementuma G-ben, ha $K\le G, H\cap K=\{1\}$ és $KH=G$. (Ez utóbbi **6.4.11** szerint ekvivalens $HK=G$-vel, tehát K komplementuma H-nak $\Leftrightarrow$ H komplementuma K-nak.)

6.21.9 Schur-Zassenhaus tétel: **(1)** ha $N\triangleleft G, |N|=n, |G:N|=m$ és m,n relatív prímek, akkor N-nek létezik H komplementuma G-ben. Ekkor $G=N\rtimes H$ és $H\simeq G/N$. **(2)** minden ilyen H egymás konjugáltja.

Bizonyítás: legyen először N Abel.

(1) Jelölje a G/N faktorcsoportot Q. Definiáljuk $a\in N, Ng\in Q$-ra a^{Ng}-t a^g-nek. (Ez nem függ a reprezentáns elemtől, mert $g'\in Ng$ esetén $g'=xg$ $(x\in N)$, ekkor $a^{xg}=(x^{-1}ax)^g=a^g$, mert N kommutatív.) Válasszunk ki minden $x\in Q$-ra egy $t_x\in x$ elemet. Az lenne jó, ha $H_0=\{t_x\,|\,x\in Q\}$ részcsoport lenne G-ben, mert minden mellékosztályban van pontosan egy eleme, azaz $H_0N=G$ és $H_0\cap N=\{1\}$. Mostantól csak azon igyekszünk, hogy a t_x elemeket úgy válasszuk meg, hogy részcsoportot alkossanak.

Legyen $\boxdot\ t_xt_y=t_{xy}\cdot c(x,y)$. Ekkor $c(x,y)\in N$, hiszen $t_xt_y\in xy$. Tudjuk, hogy $(t_xt_y)t_z=t_x(t_yt_z)$. A bal oldalt átalakítva $t_{xy}\cdot c(x,y)\cdot t_z=t_{xy}t_z\cdot c(x,y)^{t_z}$-t kapunk. Mivel $c(x,y)\in N$, definiáltuk $c(x,y)^z$-t és ez egyenlő $c(x,y)^{t_z}$-vel. Tovább folytatva $t_{xy}t_z\cdot c(x,y)^{t_z}=t_{xyz}\cdot c(xy,z)\cdot c(x,y)^z$. A jobb oldal $t_x(t_yt_z)=t_xt_{yz}\cdot c(y,z)=t_{xyz}\cdot c(x,yz)\cdot c(y,z)$. Felhasználva, hogy a két oldal egyenlő $\underline{\boxdot}\ c(xy,z)\cdot c(x,y)^z=c(x,yz)\cdot c(y,z)$.

Legyen $d(y)=\prod_{x\in Q}c(x,y)$. (Ezek mind az N kommutatív csoport elemei és véges sokan vannak, tehát használhatjuk a $\prod$ jelet.) Legyen $y,x\in Q$ rögzített. Tekintsük $\boxdot$-t minden egyes $x\in Q$-ra és szorozzuk össze ezeket:

$$\prod_{x\in Q}\boxdot(x,y,z)\ :\ \prod_{x\in Q}c(xy,z)\cdot\prod_{x\in Q}c(x,y)^z=\prod_{x\in Q}c(x,yz)\cdot\prod_{x\in Q}c(y,z).$$

A z-vel konjugálás felcserélhető a szorzással (hiszen automorfizmus), így a második szorzat $(\prod_{x\in Q}c(x,y))^z$ alakba írható. Vegyük észre továbbá, hogy az első három szorzatban $c(\text{változó}_1, \text{változó}_2)$ első argumentuma befutja Q-t, a másik pedig állandó. Így ez a három szorzat rendre $d(z), d(y)$ és $d(yz)$. Az utolsó szorzat egy konstans $|Q|=m$-edik hatványa. Egyenletünk tehát a következő alakba írható: $d(z)\cdot d(y)^z=d(yz)\cdot c(x,y)^m$, átrendezve

$$\underline{\boxdot}\ d(yz)=d(y)^z\cdot d(z)\cdot c(x,y)^{-m}.$$

Mivel N rendje relatív prím m-hez, a $g\mapsto g^{-m}$ leképezés automorfizmus N-ben, így az inverze, ψ is az. Legyen $e(y)=d(y)\psi$. Ekkor $c(x,y)^{-m}\psi=c(x,y)\psi^{-1}\psi=c(x,y)$ és $(a^z)^{-m}=(a^{-m})^z$, tehát $(d(y)^z)\psi=(d(y)\psi)^z$. (Most épp azt láttuk be,

hogy ψ és $\varphi_z: a\mapsto a^z$ felcserélhető automorfizmusok, ami nyilvánvaló, hiszen φ_z felcserélhető a hatványozással, azaz ψ^{-1}-el is, így persze ψ-vel is.) Alkalmazzuk ψ-t ⚂-ra:

$$\underline{⚂}\ e(yz)=e(y)^z\cdot e(z)\cdot c(y,z)\ .$$

Legyen végül $s_x=t_x\cdot e(x)$. Persze $s_x\in x$, mert $e(x)\in N$. Ha belátjuk, hogy az s_x-ek részcsoportot alkotnak G-ben, akkor $H=\{s_x\,|\,x\in Q\}$ megfelel komplementumnak. Ehhez elég belátni, hogy $s_xs_y=s_{xy}$, hiszen akkor $\varphi: x\to s_x$ izomorfizmus, tehát a képe csoport. ⊡ és ⚂ felhasználásával:

$$s_xs_y=t_x\cdot e(x)\cdot t_y\cdot e(y)=t_xt_y\cdot(t_y^{-1}e(x)t_y)\cdot e(y)=t_{xy}\cdot c(x,y)\cdot e(x)^{t_y}\cdot e(y)==t_{xy}\cdot c(x,y)\cdot e(x)^y\cdot e(y)=t_{xy}\cdot e(xy)=s_{xy},$$

kész vagyunk.

(2) Legyen H és H^* két komplementum, azaz $HN=H^*N=G$ és $H\cap M=H^*\cap M=\{1\}$. Az $x\in Q$ mellékosztály H-beli eleme legyen s_x, H^*-beli eleme t_x. Ekkor $x\mapsto s_x$ és $x\mapsto t_x$ egyaránt izomorfizmus. Legyen $t_x=s_x\cdot a(x)$, ekkor $a(x)\in N$.

Ekkor $s_{xy}\cdot a(xy)=t_{xy}=t_xt_y=s_x\cdot a(x)\cdot s_y\cdot a(y)=s_xs_y\cdot a(x)^{s_y}\cdot a(y)=s_xs_y\cdot a(x)^y\cdot a(y)\ \Rightarrow\ \underline{⚂}\ a(xy)=a(x)^y\cdot a(y)$. Legyen $b=\prod_{x\in Q}a(x)$. ⚂-t rögzített y mellett minden $x\in Q$-ra összeszorozva $\prod_{x\in Q}a(xy)=\prod_{x\in Q}a(x)^y\cdot\prod_{x\in Q}a(y)$, ezt – mint az **(1)** résznél – átírhatjuk $\underline{⚂}\ b=b^y\cdot a(y)^m$ alakba. Megint létezik olyan ψ automorfizmusa N-nek, hogy $(x\psi)^m=x$. c-vel jelölve $b\psi$-t és alkalmazva ψ-t az előbbi egyenletre $\underline{⚂}\ c=(b^y)\psi\cdot a(y)=c^y\cdot a(y)$, mert $(c^y)^m=b^y$ miatt $(b^y)\psi=c^y$. Ekkor ⚂-ből $a(y)=(c^{-1})^y\cdot c$. Vegyük észre, hogy $t_y=s_y\cdot a(y)=s_y\cdot(c^{-1})^y\cdot c=s_y\cdot(c^{-1})^{s_y}\cdot c=s_ys_y^{-1}c^{-1}s_yc=(s_y)^c$. Eszerint $H^*=H^c$; ezt akartuk belátni.

Térjünk rá arra az esetre, amikor N nem Abel. Alkalmazzunk $|G|$ szerinti indukciót; $|G|=1$ esetén az állítás igaz. $n=1$ triviális, úgyhogy inkább találjunk egy $p\,|\,n$ prímet. Ekkor $p\nmid m$, mert n és m relatív prímek. Legyen $P\in Syl_p(N)$. Ekkor persze $P\in Syl_p(G)$, mert $|G:P|$ osztója $|G:N|=m$-nek, tehát nem osztható p-vel. Legyen $C=Z(P), L=N_G(P)$ és $M=N_G(C)$. **6.7.3** alapján C nem egyelemű. $C\overset{\lhd}{_{char}}P\lhd L\Rightarrow C\lhd L\Rightarrow L\le N_G(C)=M$.

$Syl_p(N)\subseteq Syl_p(G)$, hiszen p ugyanazon a hatványon osztja N és G rendjét. Másrészt $Syl_p(N)$ egy elemének minden G-beli konjugáltját is fedi N, mert normálosztó. Így $Syl_p(G)$ minden eleme előáll, következésképp $Syl_p(N)=Syl_p(G)$. A Frattini-elv szerint $N\lhd G, P\in Syl_p(G)=Syl_p(N)$-ből következik $G=N_G(P)\cdot N$, azaz $G=L\cdot N\le M\cdot N$. Legyen $N_1=N\cap M$. Az I. izomorfizmus-tételből $M/_{M\cap N}\simeq MN/_N$, tehát $|M:N_1|=|G:N|=m$.

N_1 rendje osztja N rendjét, tehát relatív prím m-hez. $C\le N_1$, mert $C\le P\le N$ és $C\lhd N_G(C)=M$. Eszerint M, C, N_1-re alkalmazhatjuk a II. izomorfizmus-tételt, mely szerint $N_1/C\lhd M/C$ és $|M/C:N_1/C|=|M/N_1|=m$. $|M/C|\le|G/C|<|G|$, mert C nem egyelemű. Így hát alkalmazhatjuk az indukciós feltevést $N_1/C\lhd M/C$-re. Azt kapjuk, hogy az alkalmas $Y\le M/C$ részcsoportra $Y\cdot(N_1/C)=M/C$ és $Y\cap(N_1/C)=\{1\}$. Véve ezután a $\psi: M\to M/C$ természetes homomorfizmus szerinti teljes inverz képet azt kapjuk, hogy $X=Y^{\psi^{-1}}$-re $X\cdot N_1=(Y\cdot(N_1/C))^{\psi^{-1}}=(M/C)^{\psi^{-1}}=M$ $X\cap N_1=(Y\cap(N_1/C))^{\psi^{-1}}=\{1\}^{\psi^{-1}}=Ker\,\psi=C$. Az I. izomorfizmus-tételből $M/_{N_1}=XN_1/_{N_1}\simeq X/_{X\cap N_1}=X/_C$, azaz $|X:C|=|M:N_1|=m$.

Tehát C egy m indexű, m-hez relatív prím rendű kommutatív részcsoport X-ben. Az előző rész szerint van olyan H részcsoport X-ben, melyre $H\cap C=\{1\}$ és $|H|=m$. $H\subseteq M, X$ és a metszet asszociativitásának felhasználásával:

$H\cap N=(H\cap M)\cap N=H\cap(M\cap N)=(H\cap X)\cap N_1=H\cap(X\cap N_1)=H\cap C=\{1\}$. Az elemszámok miatt $HN=G$. Tehát H komplementuma N-nek. **(2)**-t a második esetben nem látjuk be. (A bizonyítás nagyjából így megy: ha N vagy G/N feloldható, akkor minden komplementum konjugált. Ha $(n,m)=1$, akkor N és G/N valamelyike páratlan rendű és a Feit-Thompson tétel szerint feloldható.)