Permutációcsoport, csoporthatás

Szakdolgozat

Készítette: **Fazekas Fanni**

Matematika BSc, Matematika tanári szakirány

Témavezető: **Hermann Péter** egyetemi docens

Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Budapest

2013

Tartalomjegyzék

Bevezetés

Dolgozatom H. E. Rose *A Course on Finite Groups* című könyve alapján dolgozza fel a véges csoportelmélet egy szeletét. Az első fejezetben található történeti áttekintés után a csoporthatás tárgyalásával kezdődik a második fejezet, amelyben előző ismereteimre építve definiálok néhány új fogalmat, és ezekkel kapcsolatban oldok meg feladatokat. A fejezet végén ismertetem a Burnside-lemmát, aminek segítségével a csoportelmélet egy nem tisztán algebrai alkalmazását igyekszem megmutatni.
A következőkben véges p-csoportokkal kapcsolatos feladatokon keresztül jutok el Sylow tételeihez, melyeket felhasználva kis, vagy speciális elemszámú csoportok tulajdonságait, felépítését vizsgálom.

1. fejezet

A csoportelmélet kezdetei

Csoportokat természetesen már azelőtt is ismertünk, hogy maga a fogalom kialakult volna, példaképpen a valós vagy komplex számokat, szimmetriacsoportokat és maradékosztályokat. Nem létezett azonban precíz definíció erre a rendszerre: nem volt követelmény az egységelem és az inverzek létezése, sem az asszociativitás, még ha utóbbit sokszor feltételezték is hasonló struktúrák tanulmányozása során.

A csoport fogalmának tisztázását a 18. század végén kezdődő geometriai, számelméleti, és Joseph-Louis Lagrange által tanulmányozott harmad- és negyedfokú egyenletekkel kapcsolatos kutatások motiválták. Lagrange feladatának ezen egyenletek algebrai megoldhatóságának mikéntjét tekintette, és bár az ő nevéhez kötjük leginkább a csoportelmélet kialakulásának kezdetét, valójában sosem említ csoportokat munkája során. Megjelenik viszont a Lagrange tevékenységét folytató Paolo Ruffini eredményeiben, aki elsőként vezeti be a permutációcsoport fogalmát.

A következőkben sok matematikus kezdett el az algebra ezen új ágával foglalkozni, köztük Augustin Louis Cauchy, aki 1844-ben publikált művében felépíti a permutációcsoportokat, immár mint saját lábakon álló elméletet, Niels Henrik Abel, aki 1824-ben először látta be, hogy ötödfokú egyenletekre nem lehet megoldóképletet felírni, illetve Évariste Galois, aki elsőként foglalkozott a csoportokon belül normálosztókkal, és aki először bizonyította be, hogy a legkisebb egyszerű, nem Abel-csoport elemszáma hatvan. Galois munkássága azonban addig nem volt ismert, amíg Joseph Liouville nem publikálta 1846-

ban, mivel erre Galois-nak már nem volt lehetősége - 1843. május 30-án ugyanis halálos sérülést szerzett egy párbaj során, amit egy Stephanie nevű hölgyért vívott. Kéziratait végül a testvére és egy barátja másolta le, majd küldte tovább több matematikusnak, így biztosítva életművének fennmaradását. Ezen írásnak eredményeit nevezzük ma Galois-elméletnek.

Galois után rengeteg matematikus következett, aki hozzájárult a mai csoportelmélet alapköveinek letételéhez, a teljesség igénye nélkül Betti, Cayley, Hölder, Jordan, Frobenius és Klein. Az ő életművüket összegezve születik meg William Burnside 1897-ben publikált *The Theory of Groups of Finite Order* és Heinrich Weber 1895-ös *Lehrbuch der Algebra* című műve, ami a következő század matematikusait ösztönözve a csoportelméletet a 20. század egyik legnagyobb eredményévé teszi.

1.1. Peter Ludwig Mejdell Sylow

Az 1832-es születésű norvég matematikus, Peter Ludwig Mejdell Sylow egyetemi tanulmányai után először Abel és Jacobi erdeményein kezdett dolgozni, amit látva tanára Galois-hoz irányította. Ezekben az években ismerkedett meg sok kortársa, például Liouville, Kronecker és Duhamel munkásságával. 1862-től előadást tartott az (University of Christiania), és bár ekkor még nem bizonyította be a "Sylow tételeket", de kérdéseket tett fel róla: érdekelte, hogy Cauchy tétele, miszerint ha egy csoport elemszáma osztható p-vel, akkor a csoportban van p elemszámú részcsoport, általánosítható-e p-hatványokra.

Sylow életműve az 1873 és 1881 között írt *Théorèmes sur les groupes de substitutions* című publikációban jelent meg mindössze tíz oldalon, amit a véges csoportelmélet közel minden eredménye felhasznál.

2. fejezet

Csoporthatás, pálya és stabilizátor

2.1. Csoporthatás

A csoporthatás fogalmának bevezetéséhez tekintsünk először egy példát.
Legyen $G = \mathbb{Z}_5^{\times}$ a nemnulla modulo 5 maradékosztályok által alkotott csoport a szorzásra, továbbá legyen $X = \{\widetilde{1},\ \widetilde{2},\ \widetilde{3},\ \widetilde{4}\}$ alaphalmaz. Látjuk, hogy példánkban az X halmaz és a G csoport elemei ugyanazok, így a könnyebb megkülönböztetés érdekében X elemeit hullámmal jelöljük. Tekintsük egy $\widetilde{x} \in X$ elemnek vett szorzatát egy $g \in G$ elemmel, és jelöljük a következőképpen: $\widetilde{x} * g$. Ekkor

$$\widetilde{x} * e = \widetilde{x},$$

tehát a G egységelemével való szorzás nem módosítja X elemeit, illetve az asszociativitásból következően, ha $g, h \in G$, akkor

$$\widetilde{x} * (gh) = (\widetilde{\widetilde{x} * g}) * h,$$

tehát x-re alkalmazva a gh-t ugyanazt kapjuk, mint ha először g-re alkalmazzuk az x-et, majd az eredményre h-t. Ezt G hatásának nevezzük az X-en.
Válasszunk ki most egy elemet G-ből, és nézzük meg mi történik az egyes X-beli elemekkel, például $3 \in G$ hatására.

$$\widetilde{1} * 3 = \widetilde{3}, \quad \widetilde{2} * 3 = \widetilde{1}, \quad \widetilde{3} * 3 = \widetilde{4}, \quad \widetilde{4} * 3 = \widetilde{2}.$$

Látjuk, hogy X egy permutációját kaptuk, tehát az eljárás egy leképezést ad a G csoportból S_x-be, ahol S_x az X összes permutációja.

2.1.1. Definíció. Adott egy nem üres X halmaz és egy G csoport. Azt mondjuk, hogy a *G csoport hat az X halmazon*, ha minden $g \in G$-re és $x \in X$-re értelmezünk egy $x * g \in X$ elemet úgy, hogy bármely $g, h \in G$ és $x \in X$-re a következő feltételek teljesülnek:

(i) $x * e = x$

(ii) $x * (gh) = (x * g) * h$.

Ezzel tehát egy $X \longrightarrow X$ leképezést definiáltunk, ahol minden $g \in G$-re $x \longrightarrow x * g$.

2.1.2. Tétel. *A fent definiált leképezés X egy permutációja.*

Bizonyítás: A tétel bizonyításához azt kell belátnunk, hogy a leképezés X egy (önmagára képező) bijekciója. Tegyük fel, hogy $x, y \in X$ és $x*g = y*g$. A csoporthatás definíciójából adódóan

$$x = x * e = x * (gg^{-1}) = (x * g) * g^{-1} = (y * g) * g^{-1} = y * (gg^{-}1) = y,$$

tehát a leképezés injektív. Legyen most $z \in X$. Ekkor $g \in G$-re

$$z = z * e = z * (g^{-1}g) = (z * g^{-1}) * g,$$

tehát a leképezés szürjektív is, és így X-nek egy permutációja. $\square$

2.2. A pálya és a stabilizátor közti összefüggés

2.2.1. Állítás. *Tegyük fel, hogy a G csoport hat az X halmazon. Definiáljuk X-en a $\sim$ relációt a következő módon: ha x, $y \in X$, akkor $x \sim y$ akkor és csak akkor, ha $x * g = y$ valamely $g \in G$-re. Ekkor a $\sim$ reláció ekvivalenciareláció.*

Bizonyítás: A reláció reflexív, mivel $x \sim x$ teljesül, ha $x * e = x$. A szimmetria számolással adódik: tegyük fel, hogy $x \sim y$, vagyis $x * g = y$ valamely $g \in G$-re. Ekkor

$$y * g^{-1} = (x * g) * g^{-1} = x * (gg^{-1}) = x * e = x,$$

amiből $y \sim x$. Végül tegyük fel, hogy $y \sim z$, $y * h = z$ valamely $h \in H$-ra. Ekkor

$$x * (gh) = (x * g) * h = y * h = z,$$

amiből $x \sim z$. $\square$

2.2.2. Definíció. Ha G hat X-en, a fent definiált $\sim$ reláció egy ekvivalenciaosztályát a hatás *pályájának*, más néven *orbitjának* nevezzük. Ha a pálya tartalmaz egy $x \in X$ elemet, akkor azt x pályájának nevezzük, és a következőképp jelöljük: $\mathcal{O}_G\{x\}$.

$\mathcal{O}_G\{x\}$ tehát azon $x \in X$ elemek részhalmaza, amelyekbe G hatására el tudunk jutni, vagyis

$$\mathcal{O}_G\{x\} = \{x * g \mid g \in G\}.$$

Az X halmaz előáll pályáinak diszjunkt uniójából, mivel ezeket ekvivalenciaosztályokként definiáltuk.

2.2.3. Definíció. Hasson G csoport az X halmazon. Ekkor $x \in X$-re a

$$stab_G(x) := \{g \in G : x * g = x\}$$

részhalmaz x *stabilizátora* G-ben.

A $stab_G(x)$ tehát olyan részhalmaz G-ben, ami fixen hagyja X elemeit.

2.2.4. Állítás. $stab_G(x) \leq G$.

Bizonyítás: A bizonyításhoz felhasználjuk a részcsoportok következő tulajdonságát: $H \subseteq G$ esetén $H \leq G$ akkor és csak akkor, ha

(i) H nem üres, és

(ii) ha $g,\ h \in H$, akkor $g^{-1}h \in H$.

Az, hogy a két feltétel szükséges, a részcsoport definíciójából következik. Tegyük fel, hogy (i) és (ii) is teljesülnek $H \subseteq G$-re. Legyen $g \in H$, ilyen g van az első feltétel miatt. Ekkor $e = gg^{-1} \in H$ a második feltételből. Ha $g,\ e \in H$, akkor $g^{-1} = g^{-1}e$, így H zárt az inverzképzésre. Legyen most $g,\ h \in H$, így $gh = (g^{-1})^{-1}h \in H$, tehát G zárt a műveletre, ez a művelet pedig asszociatív, hiszen az volt G-n.
Elég tehát, ha $stab_G(x)$ kielégíti a előbbi két feltételt. A hatás definíciójából $e \in stab_G(x)$, hiszen $x * e = x$, valamint ha $g, h \in stab_G(x)$, akkor

$$x * (gh^{-1}) = (x * g) * h^{-1} = (x * h) * h^{-1} = x,$$

mivel $x * g = x = x * h$, tehát $gh^{-1} \in stab_G(x)$, amivel beláttuk az állítást. $\square$

2.2.5. Feladat. *Tekintsük a négyzet szimmetriacsoportját, mint a sík egybevágósági transzformációinak részcsoportját. Írjuk le a sík pontjainak pályáját és stabilizátorát, valamint keressünk összefüggést a pálya és a megfelelő stabilizátor elemszáma között.*

Megoldás. A csoport elemei négy darab tükrözés az átlók illetve az oldalfelező merőlegesek mentén, illetve az $n \cdot 90°$-os forgatások, ahol $n = 1, 2, 3$, vagy 4. Az átlók illetve az oldalfelező merőlegesek a középpontot kivéve négy-négy helyre kerülhetnek a csoport hatására, így pályájuk négy elemű. A középpont pályája egy elemű, hiszen a transzformációk csak önmagába vihetik. Az összes többi pont pályája nyolc elemű, ezek minden csoportelem hatására különböző síkbeli pontokba kerülnek.
Az átlók és oldalfelező merőlegesek pontjait egy megfelelő tükrözés, illetve a $360°$-os forgatás hagyja helyben, kivéve a középpontot, amit minden transzformáció helyben hagy. Minden más pontot csak egy identikus leképezés visz önmagába.
Megfigyelhetjük, hogy egy adott pont stabilizátorának elemszáma a pont képeinek számával megszorozva mindig 8-at ad, ami éppen D_4 elemszáma. ♣

2.2.6. Tétel. *Ha G csoport hat a H halmazon, $x \in X$ és $\mathcal{O}_G\{x\}$ az x elem pályája, akkor*

$$|\mathcal{O}_G\{x\}| = [G : stab_G(x)],$$

vagyis x pályájának hosszát szorozva x stabilizátorának elemszámával megkapjuk G elemszámát.

Bizonyítás: Hasson a G csoport az X halmazon és legyen $x \in X$. Szeretnénk összeszámolni, hányféle különböző elemet kaphatunk $x * g$-re. Világos, hogy erre $|G|$ választási lehetőségünk van, ezek viszont nem feltétlenül különbözők.
Tegyük fel, hogy $x * g = x * h$. Mindkét oldalt megszorozva h^{-1}-gyel kapjuk:

$$x * (gh^{-1}) = (x * h)h^{-1} = x \cdot e = x$$

Tehát gh^{-1} benne van x stabilizátorában, amivel ekvivalens:

$$stab_G(x) \cdot g = stab_G(x) \cdot h.$$

Így tehát, ha $x * g \neq x * h$, akkor ezek $stab_G(x)$ különböző mellékosztályaihoz tartoznak, és így a Lagrange-tétel miatt $|G|/|stab_G(x)|$ különböző darab van belőlük. □

2.3. Példák csoporthatásra

2.3.1. Definíció. Egy G csoportban a és b elemek *konjugáltak*, ha létezik $g \in G$, hogy $g^{-1}ag = b$. A konjugáltság ekvivalenciareláció, aminek osztályait a csoport konjugáltosztályainak nevezzük.

2.3.2. Állítás. *Egy N részcsoport G-ben akkor és csak akkor normálosztó, ha N konjugáltosztályok egyesítése.*

Bizonyítás: Legyen $N \triangleleft G$. A normálosztó definíciójából adódik, hogy minden $g \in G$-re

$$g^{-1}Ng \subseteq N,$$

ami minden $x \in N$-re és minden $g \in G$-re felírva

$$g^{-1}xg \in N.$$

Ez épp azt jelenti, hogy minden $x \in N$-re x konjugáltosztálya része az N-nek, és így a konjugáltosztályok egyesítése éppen az N. Mivel minden lépésünk ekvivalens volt, ezzel beláttuk az állításunkat. $\square$

Hasson a G csoport az $X = G$ halmazon a következő módon: minden $g, x \in G$-re legyen

$$x * g = g^{-1}xg.$$

Ez valóban hatást definiál, hiszen

$$x * e = e^{-1}xe = e$$

és minden $h \in G$-re

$$x * hg = (hg)^{-1}xhg = g^{-1}h^{-1}xhg = g^{-1}(x * h)g = x * h * g.$$

Ezt nevezzük G konjugálással hatásának, aminek segítségével a következőkben további fogalmakat definiálhatunk.

2.3.3. Állítás. *Ha a G csoport az X halmazon konjugálással hat, akkor X pályái éppen G konjugáltosztályai.*

Az állítás abból következik, hogy két elem akkor kerül egy konjugáltosztályba, ha a csoport egy elemével egymásba konjugálhatók.

2.3.4. Definíció. Legyen G csoport, $x \in G$. Azt a részcsoportot, amely az x-szel fölcserélhető elemekből áll, az x elem G-beli *centralizátorának* nevezzük, és $C_G(x)$-szel jelöljük.

A definíciót megfogalmazhatjuk a következőképpen is: tekintsük a konjugálással hatást a G csoporton. Ekkor az $x \in G$ elem stabilizátorát az x centralizátorának nevezzük:

$$C_G(x) = stab_G(x) = \{g \in G : g^{-1}xg = x\} = \{g \in G : xg = gx\}.$$

Az eddigiekre közvetlenül alkalmazhatjuk a pálya és stabilizátor közti összefüggést, erről szól a következő

2.3.5. Állítás. *Egy G csoportban az x elem konjugáltosztályának elemszáma az x centralizátorának indexe.*

A Lagrange-tétel szerint így véges csoportokban a konjugáltosztály elemszáma osztója a csoport elemszámának.

2.3.6. Feladat. *Határozzunk meg minden véges csoportot (izomorfia erejéig), amelynek pontosan két konjugáltosztálya van.*

Megoldás. Tegyük fel, hogy G véges csoportnak pontosan két konjugáltosztálya van, így $|G| \geq 2$. Mivel az egységelem saját maga konjugáltosztálya, a másik konjugáltosztály szükségképpen $G - \{e\} := K$. A centralizátor és a konjugáltosztályok közti összefüggésből következik, hogy

$$|K| = (|G| - 1) \mid |G|,$$

amiből $|G| = 2$. Minden két elemű csoport izomorf a másodrendű ciklikus csoporttal, így az egyetlen csoport aminek két konjugáltosztálya van a $\mathbb{Z}_2$. ♣

2.3.7. Állítás. *A G csoportban azon elemek halmaza, amelyek minden G-beli elemmel felcserélhetők kommutatív normálosztót alkotnak G-ben. Ezt a részcsoportot jelöljük $Z(G)$-vel, és a G csoport centrumának nevezzük.*

Bizonyítás: $Z(G)$ részcsoportja G-nek, mivel $eg = ge$ minden $g \in G$-re, továbbá ha $a, b \in G$, akkor $abg = agb = gab$, erről a tulajdonságról pedig láttuk, hogy ekvivalens a részcsoport definíciójával. A $Z(G)$ részcsoport kommutatív definíció szerint, és mivel minden $g \in G$-re $ag = ga \Leftrightarrow gag^{-1} = a$, a centrum normálosztó a csoportban. $\square$

2.3.8. Feladat. *Adjuk meg D_3 konjugáltosztályait, centralizátorait és centrumát.*

Megoldás. A csoportot generáljuk a háromszög egyik szimmetriatengelyére való tükrözéssel (ez legyen t), és a $120°$-os forgatással (f). A tükrözést a konjugálás 3 elembe viheti: $\{t,\ tf,\ tf^2\}$, tehát a konjugáltosztály három elemű, és csak tükrözésekből áll.

A tükrözés centralizátora, vagyis a tükrözéssel kommutáló elemek csak önmaga és az egységelem, vagyis a t által generált két elemű részcsoport. A forgatást a konjugálás csak forgatásba viheti (és a konjugálással meg is kapok minden forgatást), mivel ha egy másik forgatással konjugálom, a transzformációk kompozíciója irányítástartó marad, ha pedig tükrözéssel konjugálom, a kompozícióban a másodrendű tükrözés mindig páros sokszor szerepel, és így kompozícióként az egységelemet adja.

A forgatás centralizátora az egységelem, az f és az f^2, vagyis az f által generált három elemű részcsoport. A többi tükrözés (szintén a kompozícióban szereplő tükrözések paritásából adódóan) konjugálással ugyancsak tükrözésbe mehet.

Az egységelem a csoportot egy konjugáltosztályra, magára a csoportra osztja, valamint mindennel kommutál, tehát centralizátora szintén az egész csoport.

Vegyük észre, hogy mind a centralizátor, mind a konjugáltosztály elemszámának kiszámításához használhatjuk a stabilizátor és a pálya közti összefüggést, például

$$|C_{D_3}(f)| = 3,\ |D_3| = 6,$$

így a kongjugáltosztályok száma 2.

Végül D_3 centruma az egy elemű csoport, hiszen $C_{D_3}(f) \cap C_{D_3}(t) = < e >$. ♣

2.3.9. Tétel (Osztályegyenlet). *Legyen G véges, $K_1, K_2, \ldots K_m$ az összes egynél nagyobb elemszámú konjugáltosztály G-ben. Ekkor*

(i) $G = Z(G) \cup \bigcup_{i=1}^{k} K_i$, *ahol az uniók diszjunkt uniókat jelölnek, valamint*

(ii) $|G| = |Z(G)| + \sum_{i=1}^{k} |K_i| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)],\ x_i \in G,\ i = 1 \ldots k,$

ahol minden x_i-re x_i konjugáltosztályának elemszáma nagyobb, mint 1.

Bizonyítás: Az, hogy G diszjunkt uniója a konjugáltosztályainak, következik abból, hogy ezek ekvivalenciaosztályok.
A második egyenlőség első része adódik abból, hogy (i)-ben az uniók diszjunktak, a második egyenlőség pedig a konjugáltosztályok és a centralizátor közti összefüggésből következik. □

2.3.10. Állítás. *Ha p prím és $|G| = p^n$, akkor $Z(G) \neq < e >$.*

Bizonyítás: Ha G Abel-csoport, akkor kész vagyunk. Tegyük fel, hogy van G-ben legalább egy olyan x_i elem, amely konjugáltosztályának elemszáma nagyobb, mint egy. A centralizátor és a konjugáltosztályok elemszáma közti összefüggésből, illetve a Lagrange-tételből adódóan

$$p \mid [G : C_G(x_i)]$$

néhány x_i-re, amire teljesül a feltételünk. Az osztályegyenletet felhasználva $p \mid |Z(G)|$, mivel feltettük, hogy $p \mid |G|$.
A centrum elemszáma nagyobb mint 0, hiszen tartalmazza az egységelemet, így $|Z(G)|$-nek legalább p darab eleme van, amiből következik az állítás. □

2.3.11. Definíció. Legyen H részcsoport G-ben. Ekkor azon $g \in G$ elemek, melyekre $gH = Hg$, részcsoportot alkotnak G-ben, amit a H részcsoport G-beli *normalizátorának* nevezünk és $N_G(H)$-val jelölünk.

2.3.12. Feladat. *$N_G(H)$ a G csoport egy alkalmas hatásánál H stabilizátora.*

Megoldás. Legyen H részcsoport G-ben és $g \in G$. Ekkor

$$g^{-1}Hg = \{g^{-1}hg : h \in H\}$$

részcsoportot H *konjugált részcsoportjának* hívjuk G-ben. Ezt a fogalmat felhasználva definiálhatjuk G hatását minden $H \leq G$ részcsoportok halmazán a következőképpen:

$$H * g = g^{-1}Hg, \ g \in G.$$

Ez hatás, mivel

$$H * e = e^{-1}He = H,$$

$$H * gh = (gh)^{-1}Hgh = h^{-1}(g^{-1}Hg)h = H * g * h.$$

H pályája a H-val konjugált részcsoportok halmaza G-ben, a stabilizátora pedig éppen

$$stab_G(H) = \{g \in G : g^{-1}Hg = H\},$$

amit be kellett látnunk. ♣

2.3.13. Megjegyzés. *A pálya elemszáma és a stabilizátor közti összefüggést a normalizátorra is alkalmazhatjuk, tetszőleges H részcsoport konjugáltjainak száma tehát*

$$[G : N_G(H)].$$

2.3.14. Feladat. *Legyen $H \leq G$. Ekkor $N_G(H)$ a legbővebb H-t tartalmazó részcsoport G-ben, ahol $H \lhd N_G(H)$.*

Megoldás. Mivel $H \subseteq N_G(H)$, és $N_G(H)$ csoport, ezért $H \leq N_G(H)$. A H részcsoport pontosan akkor normálosztó egy $J \leq G$ részcsoportban, ha minden $j \in J$-re $jH = Hj$, vagyis ha $J \leq N_G(H)$. ♣

2.4. Burnside-lemma

A következő tétel segítségével leszámlálási problémákat tudunk kezelni. Nevét William Burnside-ról kapta, bár a bizonyítást nem az ő nevéhez kötjük, hanem Georg Frobenius-éhoz, aki 1887-ben látta be az állítást. Széles körben azonban csak Burnside 1911-ben publikált könyvének (*Theory of Groups of Finite Order*) megjelenése után vált ismertté, ami többek között kettejük munkájának összefoglaló műve.

2.4.1. Tétel (Burnside-lemma). *A G véges csoport az X véges halmazon hat. Ekkor G pályáinak száma a G elemei fixpontjainak átlaga, vagyis*

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|,$$

ahol N a pályák száma és $|Fix(g)|$ azon $x \in X$ elemek száma, amiket g fixál, vagyis önmagába visz.

Bizonyítás: Legyen n azon (x, g) párok száma, amire $x * g = x$. Ezeket a párokat számláljuk le kétféleképpen úgy, hogy először g-t, majd x-et rögzítjük.

Ha g rögzített, akkor az ilyen párok száma éppen g fixpontjainak száma. Ezt összeszámlálva minden egyes $g \in G$-re, ha x befutja az X halmazt, n ezen fixpontszámok összege, vagyis

$$n = \sum_{g \in G} |Fix(g)|.$$

Rögzítsük most x-et, a párok száma így pontosan x stabilizátorának elemszáma, összesen tehát

$$n = \sum_{x \in X} |stab_G(x)|.$$

A pálya és a stabilizátor közti összefüggésből

$$\sum_{y \in \mathcal{O}_G(x)} |stab_G(y)| = |\mathcal{O}_G(x)||stab_G(x)| = |\mathcal{O}_G(x)| \frac{|G|}{|\mathcal{O}_G(x)|} = |G|.$$

Az eddigiekből felírható a következő egyenlőség:

$$\sum_{g \in G} |Fix(g)| = \sum_{x \in X} |stab_G(x)| = |G| \cdot N,$$

amivel beláttuk az állítást. $\square$

2.4.2. Feladat. *Egy szabályos háromszög csúcsait szeretnénk három színnel színezni. Hány különböző színezés létezik, ha két színezést akkor különböztetünk meg, hogyha forgatással illetve tükrözéssel nem vihetők egymásba?*

Megoldás. Legyen X az összes színezett háromszögek halmaza, amin a D_3 csoport hat. Két színezés akkor és csak akkor megkülönböztethetetlen, ha egy pályán vannak, így a különböző pályák számát kell meghatároznunk.

Tekintsük először a D_3-beli elemek fixpontjait. Az identitás minden háromszöget fixál, ez $3^3 = 27$ lehetőség. Háromféle tükrözés hagyja helyben a háromszöget, és ezek egyenként $3^2 = 9$ háromszöget fixálnak. Végül a $120°$-os és a $240°$-os forgatás összesen 3 háromszöget visz önmagába. A Burnside-lemma alapján tehát

$$\frac{1}{|G|}\sum_{g\in G}|Fix(g)| = \frac{27+3\cdot 9+2\cdot 3}{6} = 10,$$

azaz 10 különböző színezése létezik a háromszögnek. ♣

2.4.3. Feladat. *Hányféle különböző, vagyis mozgással nem egymásba vihető kockát kaphatunk, ha a kockák csúcsát fekete vagy fehér színekkel színezzük?*

Megoldás. Legyenek az X alaphalmaz elemei a színezett kockák, G pedig csoport, ami forgatásokkal hat X-en. Mivel 8 csúcsa van egy kockának, $|X| = 2^8$. A csoportnak 24 eleme van, mégpedig a következők:

- 90-, 180-, és $270°$-os forgatások két szemben fekvő lap átlóinak metszetét összekötő egyenes körül. Mindegyikből három-három van, hiszen a kockának 6 lapja van, szemben levő lappárokból pedig 3.

- $180°$-os forgatások két átellenes él középpontjait összekötő egyenes körül. Ebből 6 darab van, lévén a kockának 12 éle.

- 120- és $240°$-os forgatások a testátló egyenese körül, ami a 4 testátló miatt 8 különböző forgatást jelent.

- Végül az identitás X mind a 2^8 elemét fixálja.

Az első esetben, ha 180°-kal forgatunk, látható, hogy ha a kockát félbevágjuk az oldalfelezőkön áthaladó tükörsík mentén, az egyik oldalon levő színezés meghatározza a másik oldalon levőt. Mivel egy ilyen oldalon 4 pontunk van, 2^4 színezés lehetséges.

Ha 90- vagy 270°-kal forgatunk, egy-egy lapon egy-egy csúcs kiszínezése már determinálja a többi csúcs színét, ez esetben 2^2 választásunk van.

Két átellenes él középpontjait összekötő egyenes körüli forgatás során ugyanazt kapjuk, mint az első típusú 180°-os forgatásnál: 4 csúcs színezése határozza meg az egész kocka színezését, ami 2^4 különböző eset.

Végül tekintsük a 120- és 240°-kal történő forgatást. Azt a két csúcsot, amin átmegy a forgatás tengelye 2^2-féleképp színezhetjük, hiszen ezeket nyilván helybenhagyja a forgatás. Ha ezeken kívüli csúcsot választunk, ezt a forgatás két másik pontba viheti, amivel együtt olyan háromszöget kapunk, amelynek minden oldala a kocka egyik lapátlója. A kockán, ha a tengely rögzített, két ilyen háromszöget különböztethetünk meg, így két (különböző háromszögön levő) pont színezése meghatározza a további színezést, ami további 2^2 választást jelent.

Alkalmazva a Burnside-lemmát kapjuk:

$$\frac{2^8 + 3 \cdot 2^4 + 6 \cdot 2^2 + 6 \cdot 2^4 + 8 \cdot 2^4}{24} = 23.$$

Tehát 23 különböző kockát kaphatunk a csúcsokat fehérre vagy feketére színezve. ♣

3. fejezet

p-Csoportok, Sylow tételei

3.1. Véges p-csoportok

Legyen p a továbbiakban rögzített prímszám.

3.1.1. Definíció. Egy G csoportot *p-csoportnak* nevezünk, ha benne minden elem rendje p-hatvány.

Véges csoportok esetén a következő tétellel belátható, hogy a fenti definíció ekvivalens azzal, hogy egy G csoport prímhatványrendű.

3.1.2. Tétel (Cauchy-tétel). *Ha G véges csoport és $p \mid |G|$, akkor G-ben van legalább egy p-ed rendű elem.*

3.1.3. Tétel. *G véges p-csoport akkor és csak akkor, ha $|G| = p^k$ valamely nemnegatív k egészre.*

Bizonyítás: $k = 0$ esetén az állítás nyilván teljesül. Tegyük fel, hogy G egy p-csoport, tehát minden elemének rendje p-hatvány, és legyen $|G| = q^t m$, ahol q prím, $q \nmid m$, $q \neq p$ és $t > 0$. A Cauchy-tétel szerint G-ben van q-rendű elem, ami ellentmond a feltevésünkkel. Következésképpen $q = p$ és $m = 1$. Mivel G prímrendű ciklikus csoport, a tétel megfordítása Lagrange tételéből egyenesen következik. □

3.1.4. Feladat. *Ciklikus p-csoportban minden elem, ami nem generálja a csoportot, p-hatvány.*

Megoldás. Legyen $g \in G$, $o(g) = p^n$ generátorelem G-ben és legyen $h \in G$, úgy, hogy $< h > = \; H < G$, valamint $|H| = p^k, \; k < n$. Lagrange tételéből $|H| \mid |G| = p^n$. Tegyük fel, hogy $h = g^j$, lássuk be, hogy $p \mid j$. A hatvány rendjének képlete szerint

$$o(h) = o(g^j) = \frac{o(g)}{(o(g), \; j)} = \frac{p^n}{(p^n, \; j)} = p^k,$$

tehát $p^n = p^k \cdot (p^n, \; j)$, amiből $p \mid j$. Legyen $j = p \cdot j_0$, így $h = g^{p \cdot j_0} = (g^{j_0})^p$. ♣

3.1.5. Feladat. *Határozzuk meg az összes* 8*-adrendű nem kommutatív* G *csoport részcsoportjait, centrumát, és mutassuk meg, mivel izomorf a* $G \backslash Z(G)$ *faktorcsoport. Keressünk normálosztókat és rajzoljunk részcsoporthálót is.*

Megoldás. A nyolcadrendű csoportok a legkisebb nem Abel-féle p-csoportok, ezért foglalkozunk velük külön ebben a fejezetben. A kommutatív nyolcadrendű csoportok a véges Abel-csoportok alaptétele szerint a $\mathbb{Z}_8$, a $\mathbb{Z}_4 \times \mathbb{Z}_2$ és a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, így ezektől különböző csoportokat keresünk.

Legyen tehát G egy nyolc elemű, nem kommutatív csoport. Ha G-ben lenne nyolcadrendű elem, akkor G ciklikus lenne, és így Abel-féle, valamint ha minden eleme másodrendű, izomorf $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$-vel. Tegyük fel tehát, hogy G-ben van egy negyedrendű a elem, így a generátuma normálosztó G-ben, hiszen az általa generált részcsoport indexe 2. Jelöljünk b-vel egy elemet a generált részcsoporton kívül, így

$$G = \{e, \; a, \; a^2, \; a^3, \; b, \; ba, \; ba^2, \; ba^3\}.$$

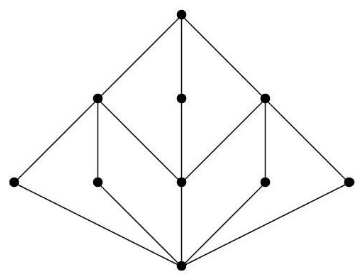
Számolással ellenőrizhetjük, hogy semelyik két elem nem egyenlő egymással, például ha $a = ab$ lenne, akkor igaz a következő: $a = ab \Rightarrow a^{-1}a = a^{-1}ab \Rightarrow e = b$. Hasonlóan juthatunk ellentmondásra a többi esetben is.

Nézzük meg, mivel egyenlő b^2, hiszen ez nem szerepel az elemek között, de része a csoportnak. Ha $b^2 = a^k b$ alakú, akkor $b = a^k$, de feltettük, hogy b nem a generátuma. Ha $b^2 = a$, vagy a^3, akkor b nyolcadrendű, és így G ciklikus, amit már szintén kizártunk. Így két lehetséges esetünk maradt: $b^2 = e$, vagy $b^2 = a^2$.

Mivel az a által generált részcsoport normálosztó, $b^{-1}ab = a^r \in < a >$ amennyiben $r = 0,\ 1,\ 2$, vagy 3. Ha $r = 0$, akkor $a = e$, ha $r = 1$, akkor G kommutatív, és ha $r = 2$, akkor

$$e = a^4 = (b^{-1}ab)^2 = b^{-1}a^2b \Rightarrow a^2 = e.$$

Így csak $r = 3$ valósulhat meg, tehát $b^{-1}ab = a^3$. Ebből kapjuk, hogy legfeljebb két különböző ilyen csoportunk lehet, és ez D_4, illetve Q, vagyis a négyzet szimmetriacsoportja és a kvaterniócsoport.



3.1. ábra. A D_4 csoport részcsoporthálója.

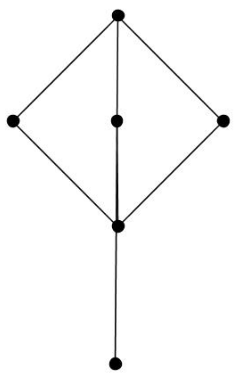
Tekintsük először a diédercsoportot. Ennek két generáló eleme legyen f, a $90°$-os forgatás, illetve t, az egyik szimmetriatengelyre való tökrözés, így

$$D_4 = \{e,\ f,\ f^2,\ f^3,\ t,\ tf,\ tf^2,\ tf^3\}.$$

A két triviális részcsoporton kívül a tükrözésekkel, illetve f^2-tel, mivel ezek másodrendű elemek, tudunk másodrendű részcsoportokat generálni. Van továbbá D_4-ben három negyedrendű részcsoport, ezek az $< f >$ ciklikus csoport, az $\{e, f^2, t, tf^2\}$ és az $\{e, f^3, t, tf^3\}$. Utóbbi három normálosztó is, hiszen 2 indexű részcsoportok D_4-ben, számolással pedig ellenőrizhető, hogy az $< f^2 >$ másodrendű részcsoport szerinti bal- és jobboldali mellékosztályok is megegyeznek. Ez a normálosztó lesz D_4 centruma, a centrum szerinti faktorcsoport pedig

$$D_4/Z(G) = D_4/\{e, f^2\} \cong V,$$

ahol V a téglalap szimmetriacsoportja, aminek az egységelemen kívül 3 darab másodrendű eleme van. A V csoportot Klein-csoportnak nevezzük, és esetenként D_2-vel azonosítjuk.



3.2. ábra. A kvaterniócsoport részcsoporthálója.

A kvaterniócsoport elemei $\{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$. A triviális részcsoportokon kívül másodrendű részcsoportot generál a -1, illetve negyedrendű részcsoportokat kapunk a negyedrendű elemek $(i,\ j,\ k)$ generátumaiból. Minden részcsoport normálosztó, a negyedrendűek ugyanolyan okból mint a D_4 negyedrendű részcsoportjai, $\{1,\ -1\}$ pedig Q centruma. A faktorcsoport ebben az esetben is a Klein-csoporttal izomorf, az egyes mellékosztályok a $\{\pm 1\}$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$.

A két részcsoporthálóban a legalsó pont az id, továbbá ha G és H különböző részcsoportok, valamint $G > H$, akkor G-t feljebb rajzoljuk, mint H-t, és ha nincs olyan csoport ami tartalmazza H-t és benne van G-ben, akkor vonallal kötjük össze őket. ♣

3.2. Sylow tételei

3.2.1. Tétel (Sylow-tételek). *Tegyük fel, hogy $|G| = p^r m$, ahol p prím és $p \nmid m$. Ekkor teljesülnek az alábbi állítások.*

(1) G-ben van p^r rendű részcsoport, amit a csoport p-Sylow részcsoportjának nevezünk.

(2) G-nek bármely két p-Sylow részcsoportja konjugált G-ben.

(3) G egy p-Sylow részcsoportja akkor és csak akkor egyértelmű, ha a p-Sylow részcsoport normálosztó G-ben.

(4) Ha n_p azt a számot jelöli, ahány p-Sylow részcsoport van G-ben adott p prímre, akkor

$$n_p \geq 1,\ n_p \mid m, \quad n_p \equiv 1\ (mod\ p).$$

(5) G minden p-hatványrendű részcsoportja benne van G egy p-Sylow részcsoportjában.

3.3. A Sylow-tételek alkalmazásai

3.3.1. Feladat. *Ha K normális p-részcsoport, P pedig p-Sylow részcsoport a véges G csoportban, akkor $K \leq P$ minden P-re.*

Megoldás. Legyenek G-ben a p-Sylow részcsoportok $P_1, P_2, ..., P_n$. Sylow 2. tételéből tudjuk, hogy $P_1, P_2, ..., P_n$ konjugáltak, tehát minden $g \in G : g^{-1}Kg = K$, illetve Sylow 5. tétele miatt minden p-csoport benne van egy p-Sylow részcsoportban. Ebből következik, hogy $g^{-1}P_ig \supseteq g^{-1}Kg = K$ minden i-re. ♣

3.3.2. Definíció. Egy H részcsoportot G-ben *karakterisztikus részcsoportnak* nevezünk, ha H invariáns G minden automorfizmusára, vagyis $h \in H,\ \phi \in Aut(G) \Rightarrow \phi(h) \in H$. Jelölés: $H\ char\ G$.

3.3.3. Feladat. *Ha P egyetlen p-Sylow részcsoport G-ben, akkor P char G.*

Megoldás. Legyen $\phi \in Aut(G)$. Ekkor $|\phi(P)| = |P|$, hiszen ϕ kölcsönösen egyértelmű. Így tudjuk, hogy $\phi(P)$ is p-Sylow részcsoport, és mivel ez egyértelmű volt, $\phi(P) = P$, amiből következik az állítás. ♣

3.3.4. Feladat. *Minden* 45 *elemű csoport Abel-féle.*

Megoldás. Legyen $|G| = 45 = 3 \cdot 3 \cdot 5$. Sylow 3. tételéből

$$n_3 \mid 5, \quad n_3 \equiv 1 \pmod 3,$$

$$n_5 \mid 9, \quad n_5 \equiv 1 \pmod 5,$$

amiből $n_3 = 1$ és $n_5 = 1$. Ekkor tehát G-nek van egy 3- és egy 5-Sylow részcsoportja, ami normálosztó. Legyenek ezek P_3 és P_5. Mind P_3, mind P_5 Abel-csoport, P_5 azért, mert ciklikus, P_3-ról pedig megmutatjuk, hogy mivel elemszáma p^2 alakú, szükségképpen Abel-féle.

3.3.5. Állítás. *Ha p prím és* $|G| = p^2$*, akkor G Abel-csoport.*

Tegyük fel, hogy G nem kommutatív, így $Z(G)$ valódi részcsoport G-ben, és így elemszáma a Lagrange-tétel miatt 1 vagy p. A (2.3.10) állítás miatt azonban a centrum nem lehet egy elemű, így $|G/Z(G)| = p$, amiből adódóan $G/Z(G)$ ciklikus. Vegyünk egy $e \neq g \in Z(G)$ és egy $h \in G \setminus Z(G)$ elemet. Ezek felcserélhetők, hiszen g centrumbeli, és az általuk generált részcsoport kommutatív részcsoportja G-nek, mivel e két elem által generált részcsoport olyan elemekből áll, amelyek felírhatók g és h, valamint ezek inverzeiből képzett akárhány tényezős szorzatként.

A generált részcsoport tartalmazza G centrumát, sőt a h elemmel vett generátumok miatt bővebb nála, és így elemszáma csak p-nél nagyobb lehetne. Ekkor $Z(G)$ nem valódi részcsoport G-ben, ami ellentmondás.

A két p-Sylow részcsoport metszete tehát triviális, és mindkettő normálosztó G-ben, P_3 és P_5 elemei így kommutálnak egymással. A 45 elemű csoportot felírhatjuk a két p-Sylow részcsoport direkt szorzataként, mivel $[|P_3|, |P_5|] = 1$, ezek kiadják a csoportot. Mivel Abel-csoportok direkt szorzata is Abel-csoport, G szükségképpen kommutatív.

Izomorfia erejéig a véges Abel-csoportok alapatétele szerint két ilyen csoport létezik, ezek $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ és $\mathbb{Z}_9 \times \mathbb{Z}_5$. ♣

3.3.6. Feladat. *Határozzuk meg D_n Sylow részcsoportjainak számát.*

Megoldás. Tekintsük először D_n-ben a 2-Sylow részcsoportokat. Legyen $|D_n| = 2^k t$. Az n-szögben minden t-dik csúcsot véve egy szabályos 2^k-szöget kapunk, amit éppen egy, a $D_{2^k}(\leq D_n)$ diédercsoporttal izomorf csoport hagy helyben. Mivel $|D_{2^k}| = 2 \cdot 2^k$, ez épp egy 2-Sylow részcsoport. Ilyen 2^k szögből éppen t darab van, ami t darab különböző részcsoportot határoz meg. Ennél több nem is lehet, mivel Sylow 5. tétele szerint minden p-hatványrendű részcsoport benne van egy p-Sylow részcsoportban.

Ha $p > 2$, akkor a p-Sylow részcsoportokban nem lehet tükrözés a Lagrange-tétel miatt, hiszen $2 \nmid p^k$, a tükrözések pedig másodrendűek. A részcsoport így csak forgatásokból áll, ezek pedig ciklikus, kommutatív részcsoportokat, vagyis normálosztókat alkotnak D_n-ben, ezekről pedig tudjuk, hogy egyértelműek minden k-ra. ♣

3.3.7. Feladat. *Legyen $H \leq G$, P egy p-Sylow részcsoportja H-nak, Q pedig p-Sylow részcsoportja G-nek úgy, hogy $P \leq Q$. Ekkor $P = Q \cap H$.*

Megoldás. Világos, hogy P része $Q \cap H$-nak, így csak a másik irányú tartalmazást kell belátnunk. Ahhoz, hogy $Q \cap H \subseteq P$, elég azt bizonyítanunk, hogy $Q \cap H$ p-csoport, ami a Lagrange-tételből adódik, hiszen $Q \cap H \subseteq Q \Rightarrow |Q \cap H| \mid |Q|$. ♣

3.3.8. Feladat. *Határozzuk meg A_5 Sylow-részcsoportjait.*

Megoldás. A_5 rendje $5 \cdot 4 \cdot 3 = 60$, tehát feladatunk, hogy 5-, 3- illetve 2-Sylow részcsoportokat keressünk. Tekintsük először az 5-Sylow részcsoportokat. Sylow 4. tételéből adódóan

$$n_5 \mid 12, \quad n_5 \equiv 1 \ (mod\ 5),$$

amiből $n_5 = 1$ vagy 6.

Az alábbiakban felhasználjuk, hogy minden m hosszú ciklus felírható $m - 1$ transzpozíció kompozíciójaként, és így minden páratlan hosszú ciklus páros permutáció. A_5 ötödrendű elemeivel több 5 elemű részcsoportot is tudunk generálni, ilyen például

$$< (12345) > \;=\; \{id, (12345), (13524), (14253), (15432)\},\ \text{valamint}$$
$$< (12354) > \;=\; \{id, (12354), (13425), (15243), (14532)\},$$

így a fenti kongrenciákból adódóan összesen 6 ilyen Sylow részcsoportnak kell lennie.
A 3-Sylow részcsoportok tekintetében hasonlóan járunk el, az előző tételt használva

$$n_3 \mid 20,\ n_3 \equiv 1\ (mod\ 3),$$

amiből $n_3 = 1, 4$ vagy 10.
A 3 elemű részcsoportok generálásához egy harmadrendű elemre van szükségünk, ilyenből a csoporton belül van 20 darab. Mivel minden ilyen részcsoport az egységelemen kívül egy harmadrendű elemből és az inverzéből áll, valamint mivel ezek metszete triviális, a 20 elemmel 10 ilyen részcsoportot tudunk generálni.

A 2-Sylow részcsoportokra az eddig használt tételt alkalmazva kapjuk:

$$n_2 \mid 15,\ n_2 \equiv 1\ (mod\ 2),$$

amiből $n_2 = 1, 3, 5$ vagy 15.
A 2-Sylow részcsoportokat transzpozíciókkal, másodrendű elemekkel generálhatjuk. Tekintsük most egy ilyen H részcsoportját A_5-nek. R_5 jelölje azt a részcsoportot, amely csak olyan ciklusokat tartalmaz, amelyek az 5-öt helyben hagyják:

$$R_5 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Ilyen típusú részcsoportból van 5 darab, be kell látnunk, hogy több nem lehet.
Nézzük meg, mi történik az $a := (12)(34)$ ciklussal, ha konjugáljuk egy tetszőleges σ permutációval.

$$\sigma^{-1}(12)(34)\sigma = \sigma^{-1}(12)\sigma\sigma^{-1}(34)\sigma = (1 * \sigma, 2 * \sigma)(3 * \sigma, 4 * \sigma).$$

Az a elem centralizátora így 8 elemű S_5-ben. Tudjuk, hogy a centralizátor indexe épp a konjugáltak száma, valamint $C_{A_5}(a) = C_{S_5}(a) \cap A_n$. Így, mivel a nem cserélhető fel páratlan permutációval, A_n-ben a centralizátorának elemszáma éppen az S_n-beli centralizátor elemszámának fele lesz, amivel beláttuk, hogy ez az 5 darab 2-Sylow részcsoport van A_5-ben. ♣

A feladatból kiderül, hogy A_5-nek nincs $3, 4$, illetve 5 elemű normálosztója, mivel ha lenne, a megfelelő Sylow-részcsoportok egyértelműek volnának. Ehhez kapcsolódóan most kimondunk egy tételt kis elemszámú, nem Abel-féle csoportok egyszerű voltáról, valamint bebizonyítjuk néhány speciális elemszámú csoportról, hogy van bennük normális részcsoport.

3.3.9. Definíció. Egy G csoport *egyszerű*, ha pontosan két normálosztója van.

3.3.10. Feladat. *Mutassuk meg, hogy A_5 a legkisebb nem Abel-féle egyszerű csoport.*

Megoldás. A bizonyítás a Sylow-tételek alkalmazásával történik, oly módon, hogy megmutatjuk minden 60-nál kisebb elemszámú, nem kommutatív csoportról, hogy nem egyszerű. Ezután bebizonyítjuk, hogy A_5 egyszerű, illetve hogy egy nemkommutatív 60-adrendű egyszerű csoport mindenképpen izomorf A_5-tel.

3.3.11. Állítás. *Ha G nem Abel-féle és $|G| < 60$, akkor G nem egyszerű.*

Tudjuk, hogy prímhatvány elemszámú csoportok centruma nem triviális. Mivel a centrum egy elemű konjugáltosztályok egyesítése, így $Z(G)$ mindig (kommutatív) normálosztó, következésképpen az ilyen típusú csoportok nem egyszerűek.

Tegyük fel, hogy a csoport rendje $p^k m$ alakú tetszőleges $k \geq 0$ kitevőre, ahol p prím, m természetes szám és $m \leq p$. Sylow 4. tételéből következően $n_p \equiv 1 \ (mod\ p)$, valamint $n_p \mid m$, így $n_p \leq m$. Az ilyen típusú csoportok tehát pontosan egy p-Sylow részcsoportot tartalmaznak, ami Sylow 3. tétele szerint normálosztó G-ben.

A következőkben belátjuk, hogy az olyan csoportokban, amelyek elemszáma $2^p(2^p-1)$ alakú, vagy találunk 2-Sylow, vagy (2^p-1)-Sylow részcsoportot, amely normálosztó. Ezzel mutatjuk meg a $12 = 2^2(2^2-1)$, illetve az $56 = 2^3(2^3-1)$ elemszámú csoportokról, hogy nem lehetnek egyszerűek.

Legyen a továbbiakban $2^p - 1 = q$. Az állítás bizonyításához szintén Sylow 4. tételét használjuk. Felírva n_q-ra a tételből következő kongruenciát és oszthatóságot kapjuk: $n_q = 1$ vagy 2^p. Ha az eredmény 1, kész vagyunk, a második esetben legyen $Q_1, Q_2, ..., Q_{2^p}$ az összes q-Sylow részcsoport. Mivel ezek mind prímrendű részcsoportok, metszetük triviális, ebből adódik, hogy a csoportban $2^p(q-1) = 2^pq - 2^p$ elem van az egységelemen kívül. Így pontosan 2^p olyan elem van, amely nincs benne semelyik q-Sylow részcsoportban. A 2-Sylow részcsoport minden eleme eközött a 2^p elem között található, hiszen nem tartalmazhat elemet a q-Sylow részcsoport elemei közül, továbbá, mivel a 2-Sylow részcsoport rendje éppen 2^p, ez az egyetlen 2-Sylow részcsoport van a csoportban.

A 40 és 45 rendű csoportokat ki tudjuk zárni Sylow 4. tétele alapján, hiszen

$$40 = 2^3 \cdot 5 \Rightarrow n_5 = 1,$$

$$45 = 3^2 \cdot 5 \Rightarrow n_5 = 1.$$

A fennmaradó elemszámok így a 24, 30, 36 és a 48.

Tekintsünk most egy $|G| = 36 = 2^2 \cdot 3^2$ elemű csoportot. A Sylow-tételek alapján tudjuk, hogy létezik $P \leq G$ részcsoport, amire $|P| = 9$. Legyen $x \in P,\ g \in G$ és tekintsük G hatását a P szerinti jobb oldali mellékosztályokon a következő módon: $Px * g = Pxg$. Ekkor G egy 4 elemű halmazon hat homomorfizmussal: $G \longrightarrow S_4$. Ennek a leképezésnek a magja nem triviális, hiszen $|S_4| = 24 \leq 36 = |G|$, a homomorfizmus magjáról pedig tudjuk, hogy normálosztó. A $|G| = 24$ és 48 esetét hasonlóképpen zárhatjuk ki.

Legyen végül $|G| = 30 = 2 \cdot 3 \cdot 5$. Tegyük fel, hogy $n_2,\ n_3$ és n_5 is nagyobb 1-nél. Sylow 4. tétele alapján $n_5 \equiv 1\ (mod\ 5)$ és $n_5 \mid 2 \cdot 3$, amiből $n_5 = 6$. Szintén a tétel következményeként $n_3 \equiv 1\ (mod\ 3)$ és $n_3 \mid 2 \cdot 5$, amiből $n_3 \geq 5$ és $n_2 \geq 3$. G-nek $n_2 \cdot (2-1) = n_2$ darab másodrendű, $n_3 \cdot (3-1) = 2 \cdot n_3$ darab harmadrendű és $n_5 \cdot (5-1) = 4 \cdot n_5$ darab ötödrendű eleme van. Számoljuk össze hány eleme van így G-nek!

$$|G| = 30 \geq 1 + n_2 + 2 \cdot n_3 + 4 \cdot n_5 \geq 1 + 3 + 5 \cdot 2 + 4 \cdot 6 = 34,$$

ami ellentmondás. Ebből következik, hogy n_2, n_3 és n_5 közül valamelyiknek szükségképpen egynek kell lennie, így G-nek van egy egyértelmű Sylow részcsoportja, és így normálosztója. A bizonyítás ugyanígy működik tetszőleges $|G| = pqr$, ahol p, q és r prímek és $p < q < r$.

Egy másik érvelést kapunk arra, hogy a csoport rendje nem lehet 30, sőt $2 \cdot (2k-1)$ alakú, ha G önmagán való hatását vizsgáljuk. Minden $g, x \in G$-re legyen $x \to xg$. Ha $g \in G$-re $o(g) = 2$, akkor az ennek megfelelő permutáció páratlan, így $g \neq e$-re a hatás semelyik elemet sem hagyja fixen. Így kapunk a csoportban egy 2 indexű részcsoportot, amely szerint G-nek két baloldali mellékosztálya van, és mivel ez megegyezik a jobboldali mellékosztályaival, a részcsoport normálosztó.

Ezzel beláttuk az első állításunkat.

3.3.12. Állítás. *A_5 egyszerű csoport.*

A_5 Sylow-részcsoportjait már meghatároztuk, innen tudjuk, hogy $n_3 = 10$ és $n_5 = 6$. Tegyük fel, hogy A_5 nem egyszerű, legyen $N \lhd G$.

Négy esetet fogunk megkülönböztetni aszerint, hogy N elemszáma mivel osztható.

Legyen először $5 \mid |N|$. Ekkor, ha H egy 5-Sylow részcsoport N-ben, akkor H az A_5-ben is Sylow-részcsoport. Így tetszőleges K-ra, ha K egy 5-Sylow részcsoport

$$K = \sigma H \sigma^{-1}, \quad \sigma \in A_5.$$

Mivel N zárt a konjugálásra

$$K = \sigma H \sigma^{-1} \subseteq \sigma N \sigma^{-1} = N.$$

Ebből adódóan N-ben minden 5-Sylow részcsoport benne van, és ezek metszete triviális, így az ötödrendű elemek száma $6 \cdot (5-1) = 24$. Mivel $|N| \mid |A_5| = 60$, szükségképpen $|N| = 30$. Így viszont minden 3-Sylow részcsoport is N-beli (mert $3 \mid |N|$), ezzel együtt pedig N-nek több mint 30 eleme lenne.

Ha azt tesszük fel, hogy $3 \mid |N|$, akkor az előző érveléssel analóg módon minden 3-Sylow részcsoport N-beli, és a harmadrendű elemek száma $10 \cdot (3-1) + 1 = 21 \;\Rightarrow |N| = 30$, amiből ellentmondásra jutunk.

Ha $|N| = 4$, akkor ez egyetlen 4-Sylow részcsoport A_5-ben:

$$N = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Ez a részcsoport viszont nem normálosztó, hiszen

$$(345)(12)(34)(345)^{-1} = (12)(45) \notin N.$$

Végül, ha $|N| = 2$, akkor az N normálosztót egy transzpozíció generálja, legyen ez (a, b), ahol a és b különbözők. Válasszunk egy $c = 1,\ 2,\ 3,\ 4,\ 5$ elemet, úgy, hogy $c \neq a$ és $c \neq b$. Ekkor $(abc)(ab)(abc)^{-1} = (bc) \notin N$, ami ellentmondás.

3.3.13. Állítás. *A_5 az egyetlen 60-adrendű nem Abel-féle egyszerű csoport.*

Legyen G egyszerű, $|G| = 60$. Célunk, hogy megmutassuk, G-nek van 5 indexű részcsoportja, hiszen ekkor G izomorf A_5 egy részcsoportjával, és mivel $|G| = 60 = |H|$, ezért $G \cong H$.

A (3.3.8) feladatban láthattuk, hogy a 2-Sylow részcsoportok száma 1, 3, 5, vagy 15. A következőkben belátjuk, hogy egy egyszerű csoportban, ha elemszáma 60, a 2-Sylow részcsoportok száma nem lehet 5-nél kisebb.

Hasson G a 2-Sylow részcsoportokon konjugálással, és tekintsük azt a homomorfizmust $G \to S_n$-be, amit ez meghatároz, és ahol S_n az X halmaz (vagyis a 2-Sylow részcsoportok) önmagára képző bijekcióinak halmazát jelöli. A leképezés nem triviális, így magja nem lehet G-vel egyenlő, mivel G-ben a 2-Sylow részcsoportok egymás konjugáltjai Sylow 2. tétele szerint. Továbbá, mivel G egyszerű, a leképezés magja nem lehet $\{e\}$ -től különböző, mivel ha ennél bővebb lenne, normálosztót alkotna G-ben.

Ha a leképezés magja csak az egységelemből áll, a homomorfizmus injektív, és így $|G| \leq |S_x|$. Ez éppen azt jelenti, hogy $|G| = 60 \leq n!$, amivel ekvivalens, hogy $n_2 \geq 5$.

Ha $n_2 = 5$, tekintsük G konjugálással hatását a részcsoportokon. Tudjuk, hogy bármely részcsoport stabilizátora az ő normalizátora, és hogy a normalizátor indexe egyenlő a vele konjugált részcsoportok számával. Mivel minden p-Sylow részcsoport egymás konjugáltja, $[G : N_G(P)] = n_p$, tehát G-nek van 5 indexű részcsoportja.

Ha $n_2 = 15$, különböztessünk meg két esetet: vagy bármely két 2-Sylow részcsoport triviálisan metszi egymást, vagy van legalább két olyan részcsoport, aminek van közös eleme az egységelemen kívül. Az első esetben $60 - (15 \cdot (4-1) + 1) = 15$ elem nincs benne a 2-Sylow részcsoportok egyikében sem. Mivel $n_3 = 10$ az (3.3.8) feladat miatt, a 3-Sylow részcsoportokban $10 \cdot (3-1) = 20$ elem van. Összesen tehát $45 + 20 = 65 > |G|$ elemet számoltunk össze, ami ellentmondás.

A második esetben legyen P_1 és P_2 két egymást nem triviálisan metsző 2-Sylow részcsoport G-ben. Mivel $|P_1| = |P_2| = 4$, a két részcsoport kommutatív, és így benne vannak a metszetük normalizátorában, jelöljük ezt $N_G(M)$-mel. Az eddigiekből adódóan

$$4 \mid |N_G(M)|, \quad \text{illetve} \quad 4 < |N_G(M)|,$$

tehát

$$N_G(M) = 3 \cdot 4,\ 5 \cdot 4,\ \text{vagy}\ 15 \cdot 4.$$

Ha $N_G(M) = 20$, akkor $[G : N_G(M)] = 3$, amiről beláttuk, hogy nem lehetséges. Ha $N_G(M) = 60$, akkor $M \triangleleft N_G(M) = G$, ami szintén ellentmondás. Így $N_G(M) = 12$ valósulhat csak meg, amiből $[G : N_G(M)] = 5$.

A három állításból azt kaptuk tehát, hogy izomorfia erejéig egyetlen olyan egyszerű, nem kommutatív csoport van, melynek elemszáma legfeljebb 60, nevezetesen az A_5. ♣

Irodalomjegyzék

[1] Keith Conrad: *Consequences of the Sylow Theorems*

http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/sylowapp.pdf

[2] H. E. Rose: *A Course on Finite Groups*, Springer-Verlag

London, 2009.

[3] Kiss Emil: *Bevezetés az algebrába*, Typotex

Budapest, 2007.

[4] Kiss Emil: *Bevezetés az algebrába - A gyakorlatok és a feladatok megoldásai*, Typotex

Budapest, 2007.

[5] http://groupprops.subwiki.org

[6] http://www-history.mcs.st-and.ac.uk

[7] http://sosborne.public.iastate.edu/algqual2012

[8] http://crazyproject.wordpress.com

[9] http://euler.slu.edu/∼ srivastava

Nyilatkozat

Név: Fazekas Fanni

ELTE Természettudományi Kar, szak: Matematika Bsc

NEPTUN azonosító: LCRSEE

Szakdolgozat címe: Permutációcsoport, csoporthatás

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2013. május 29.

____

a hallgató aláírása