Fejezetek a csoportelméletből

Dobos Dániel
matematika-fizika szakos hallgató
ELTE TTK

Témavezető:
Dr. Hermann Péter
egyetemi docens
ELTE TTK Algebra és Számelmélet Tanszék

Budapest, 2009.

Tartalomjegyzék

1 Bevezetés **1**

1.1 A szakdolgozat felépítése 1

1.1.1 Néhány jelölés 2

1.2 Köszönetnyilvánítás 3

2 Elméleti áttekintés **5**

2.1 A csoport fogalma 5

2.2 Rend, részcsoportok, normálosztók 13

2.2.1 Rend 13

2.2.2 Részcsoportok 15

2.2.3 Normálosztók 25

2.3 Homomorfizmusok 31

2.4 Konjugálás 39

2.5 Direkt és szemidirekt szorzat 44

2.5.1 A direkt szorzat 44

2.5.2 A szemidirekt szorzat 50

2.6 A Sylow-tételek 53

2.7 Permutációcsoportok 61

2.7.1 Az n-edfokú szimmetrikus csoport 62

2.7.2 Orbit, stabilizátor 68

2.7.3 Permutációreprezentáció és csoporthatás 70

2.8 Feloldható és nilpotens csoportok 75

2.8.1 Normállánc, kompozíciólánc 76

2.8.2 Feloldható csoportok 79

2.8.3 Kommutátorok 83

2.8.4 Nilpotens csoportok 88

2.8.5 A Frattini-részcsoport 94

2.9 Szabad csoportok és prezentációk 97

2.9.1 Szabad csoportok 97

2.9.2 Prezentációk 103

3 Feladatok **107**

4 Egy középiskolás szakkör **141**
4.1 Tervezés 142
4.1.1 Általános észrevételek 142
4.1.2 A téma vázlata 143
4.1.3 A foglalkozás tervezett anyaga 148
4.2 Kivitelezés - reflexió 163

1. fejezet

Bevezetés

1.1. A szakdolgozat felépítése

A csoportelmélet - nem kifejezetten középiskolás fejezete a tudománynak. Amiért mégis ezt választottam szakdolgozati témának, az az a tény, hogy a sok érdekes és szép matematikából, melyet az egyetemen tanultam, talán ez áll legközelebb hozzám. A szakdolgozat célja, hogy bemutassa e kiterjedt területnek egy kicsiny részét, voltaképpen az alapjait, felépítse az elméletet és annak alkalmazásait néhány tetszetős példával illusztrálja. Az utolsó fejezetben pedig egy „kísérletet” írok le, amelyet egy középiskolai szakköri foglalkozáson tettem arra, hogy megismertessem a tanulókat a csoport fogalmával.

Az előbbieknek megfelelően a szakdolgozat három fő részből áll.

A *második*, terjedelmesre sikerült fejezet az elméleti rész. Ebben azokra a megértési nehézségekre (is) koncentrálva, amelyekkel saját magam is találkoztam az anyag elsajátítása során, tárgyalom azokat a fogalmakat és tételeket, amelyeket később használni fogok. Bár ez a fejezet önálló eredményt nem tartalmaz, úgy

gondolom, ez a szubjektív, „pedagógiai” jelleg elárul valamit arról a megszerzett tudásról, tanári attitűdről, melyről számot kell adnom; ezért is „hagytam” ilyen hosszúra nyúlni. Az elmélet minden egyetemi csoportelmélet tankönyvben hozzáférhető, én leginkább a [1]-et, emellett időnként a [2]-t és [3]-t használtam. Az elméleti tudásom alapját persze az az ismeret képezi, melyet az egyetemi (reguláris és speciál-)előadásokon és gyakorlatokon tanultam meg.

A *harmadik fejezetben* néhány feladaton keresztül mutatom be az elmélet alkalmazásait. A nagyrészt az egyetemi óráimról és az [1] könyvből vett példák kiválasztásánál részben önmagukban, részben elméleti értelemben vett érdekességük vezérelt. Itt is az a törekvés érvényesül, hogy a problémákra általam adott megoldásokat részletekbe menően tárgyaljam azokra a nehézségekre fókuszálva, amelyekkel nekem is meg kellett birkóznom, ill. másoknak is felhívnám a figyelmét rá. A feladatok sorrendje nem pontosan követi az elméleti rész sorrendjét, annál is inkább, mert általában egy-egy feladat megoldásához különböző helyekről származó, apróbb ismeretekre van szükség. A 3. fejezet 17. feladatában egy apró önálló eredményt mutatok be.

Végül a *negyedik fejezet* a fent jelzett szakköri foglalkozásról szól, tartalmazza a tervezés lépéseit, az ezzel kapcsolatos meggondolásokat, valamint a kivitelezés tapasztalatait és értékelését.

1.1.1. Néhány jelölés

A megszokott matematikai jelölések mellett (és részben ezeken belül) a szakdolgozatban az alábbiak érvényesek:

- A p mindig (pozitív) prímet jelöl, hacsak nincs az adott helyen másként definiálva.
- A függvényeket, leképezéseket (az algebrában megszokott módon) jobbra

írom, azaz x képét az f függvénynél $(x)f$ jelöli.

1.2. Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, *Hermann Péternek* a mintegy másfél évig (el)húzódó munkában nyújtott kitartó és önzetlen segítségért és biztatásért.

2. fejezet

Elméleti áttekintés

2.1. A csoport fogalma

2.1.1. Definíció: *Csoportnak nevezünk egy G nemüres halmazt, ha értelmezve van rajta egy $\circ$-rel jelölt kétváltozós művelet, azaz egy $G \times G \to G$ függvény, amely teljesíti a következő ún. csoportaxiómákat:*

i) asszociatív: $\forall x, y, z \in G$ *esetén*

$$x \circ (y \circ z) = (x \circ y) \circ z$$

ii) létezik egy e (kétoldali) egységelemnek nevezett elem, amelyre fennáll:

$$g \circ e = e \circ g = g \quad \forall g \in G$$

iii) a csoport minden g elemének létezik g^{-1}-zel jelölt (kétoldali) inverze, amelyre teljesül:

$$g \circ g^{-1} = g^{-1} \circ g = e$$

Ezt úgy mondjuk, hogy G csoport a $\circ$ műveletre nézve, jelben: (G,$\circ$) csoport. Persze ha nem okoz félreértést, akkor a műveletet nem hangsúlyozzuk ki újra és újra és egyszerűen csak a G csoportról beszélünk.
A későbbiekben belátjuk majd, hogy mind az egységelem, mind az inverz egyértelmű.
Megállapodás: Az egyszerűség kedvéért a műveletre innentől kezdve a szorzás szokásos $\cdot$ jelét használjuk majd, amelyet legtöbbször (szokás szerint) el is hagyunk.

Szembeötlő, hogy a művelet *kommutativitását nem követeljük meg*; azokat a csoportokat, ahol ez is teljesül, kommutatív, vagy (*Niels Abel* után) *Abel-csoportoknak* nevezzük. Egyébként ha a G csoport x és y elemeire $xy = yx$, akkor ezeket (egymással) *felcserélhetőeknek* mondjuk.
A kommutativitás „elengedésének” az az oka, hogy sok „természetes” példa van nem kommutatív csoportokra, amelyeket szintén vizsgálni akarunk. Az asszociativitásra viszont már akkor is szükség van, ha egy elem hatványairól akarunk beszélni: enélkül ui. ha $a \in G$ tetszőleges elem, akkor pl. a^3-nek nem lenne értelme, hiszen nem tudnánk eldönteni, hogy az $(a \cdot a) \cdot a$ vagy $a \cdot (a \cdot a)$! Megmutatható azonban, hogy az asszociativitási szabály $i)$-beli alakjából következik, hogy akárhány (véges sok) tényezős szorzatot lehet tetszőlegesen zárójelezni, az nem változtat az eredményen.
A fenti axiómák megkövetelésével könnyen látható módon teljesülnek a hatványozás szokásos azonosságai is, pl. bármely $a \in G$ esetén $\left(a^k\right)^\ell = a^{k\ell}$ tetszőleges k,ℓ egész számokra; egy elem nulladik hatványát most is célszerűen az egységelemként definiáljuk.

Alapvető észrevétel, hogy csoportban az $xy = xz$ egyenlőségből az x^{-1}-zel bal oldalról való szorzással és az asszociativitást kihasználva $y = z$ következik tetszőleges $x, y, z \in G$ esetén:

$$xy = xz \Leftrightarrow x^{-1}(xy) = x^{-1}(xz) \Leftrightarrow \overbrace{(x^{-1}x)}^{e} y = \overbrace{(x^{-1}x)}^{e} z.$$

Ez persze (mint a nyilak is jelzik) visszafelé is elvégezhető; csoportban tehát **ekvivalens átalakításként szabad „egyszerűsíteni"** (erre időnként *egyszerűsítési szabályként* fogunk hivatkozni).

A G csoport (mint halmaz) számosságát (azaz véges csoport esetén annak elemszámát), melyet szokás a *csoport rendjének* is nevezni, $|G|$-vel jelöljük majd.

Bármiféle részletezés nélkül megjegyezzük, hogy a csoport fenti fogalmához jutunk akkor is, ha csak „egyoldali" (pl. jobb) egységelem és (minden elemhez) ugyanazon oldali inverz létezését követeljük meg (a többi követelmény megtartásával).

Most három egyszerű, de alapvető állítást igazolunk. Először is levezetjük az egységelem és az inverz egyértelműségét.

2.1.2. Tétel: *A G csoportnak egyetlen egységeleme van.*

Bizonyítás: Tegyük fel ui., hogy e_1 és e_2 két egységelem. Vizsgáljuk az $e_1 \cdot e_2$ szorzatot! Mivel e_1 (kétoldali) egységelem, így ezzel e_2-t (balról) szorozva e_2-t kapjuk az egységelem definiáló tulajdonsága miatt. Ugyanígy adódik (ezúttal e_2 egységelem tulajdonságát használva), hogy a szorzat értéke e_1. Tehát $e_1 = e_2$.■

2.1.3. Tétel: *A G csoport minden elemének egyértelműen létezik inverze.*

Bizonyítás: Legyen $g \in G$ és g_1^{-1}, g_2^{-1} g-nek két inverze. Ekkor határozzuk meg a $g_1^{-1}gg_2^{-1}$ szorzat értékét! Az asszociativitási szabály miatt ez a szorzat értelmes, mert bármilyen zárójelezéssel ugyanazt az eredményt adja. Nézzük most a kétféle zárójelezés eredményét:

$$(g_1^{-1}g)g_2^{-1} = eg_2^{-1} = g_2^{-1}$$
$$g_1^{-1}(gg_2^{-1}) = eg_1^{-1} = g_1^{-1}$$

Tehát $g_1^{-1} = g_2^{-1}$. ■

Mivel $(x^{-1})^{-1} = x$, így bármely G csoportban az $x \mapsto x^{-1}$ egy $G \to G$ bijekciót jelent.

2.1.4. Tétel: *Legyenek $x_1, x_2, \ldots, x_n \in G$, ahol G csoport. Ekkor fennáll:*

$$(x_1 x_2 \cdot \ldots \cdot x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \cdot \ldots \cdot x_1^{-1}.$$

Bizonyítás: Az inverz egyértelműsége miatt elég ellenőriznünk, hogy a megadott elemeket összeszorozva (bármely irányból) az egységelemet kapjuk. Pl. „balról jobbra" szorozva és kihasználva az asszociativitást:

$$(x_1 \cdot x_2 \cdot \ldots, \underbrace{(x_{n-1} \underbrace{(x_n \cdot x_n^{-1})}_{e} x_{n-1}^{-1})}_{e} \cdot \ldots \cdot x_1^{-1}) = e$$

Persze kommutatív csoportban ez megegyezik (pl.) a „vizuálisan sejthető" $x_1^{-1} x_2^{-1} \cdot \ldots \cdot x_n^{-1}$-nel is, egyébként azonban nem feltétlenül van így.

Példák csoportokra:

– Az *egész számok* a szokásos összeadásra nézve csoportot alkotnak, melyet $\mathbb{Z}$-vel jelölünk. Az egységelem a 0, k inverze pedig $-k$. Vegyük észre, hogy a csoport minden elemét megkapjuk úgy, hogy az 1-et hatványozzuk (itt a hatványozás persze az ismételt összeadást jelenti): pl. (kivételesen szorzással írva) $-5 = (1^{-1})^5 = 1^{-5}$.
Ilyen tulajdonságú a következő példánk is:

– A *modulo n maradékosztályok* az összeadásra (melyet természetes módon értelmeztünk) nézve Abel-csoportot alkotnak, ezt $\mathbb{Z}_n$ jelöli. A csoport egységeleme a (0) maradékosztály, a (k) inverze pedig egyszerűen $(-k)$. Most minden elem az (1) maradékosztálynak hatványa:

$$G = \{(1), (1)^2 = (2), \ldots, (1)^n = (n) = (0)\}$$

Amint kiderül majd, az (1) helyett tetszőleges redukált maradékosztály hatványaiként előáll a csoport.

Látható, hogy minden n-re létezik n elemű csoport (ellentétben pl. a véges testekkel), ami a definíció alapján még nem volt nyilvánvaló.

Eddigi példáink motiválják egy új fogalom bevezetését:

2.1.5. Definíció: *Ha egy csoport egyetlen elem hatványaiból áll, akkor* ***ciklikus csoportnak*** *nevezzük.*

Minden n-re van n elemű ciklikus csoport, és van (megszámlálhatóan) végtelen ciklikus csoport is. Ezekről a csoportokról lesz még szó.

Természetesen adott halmaz esetén nem értelmezhetjük akárhogyan a műveletet. A fenti listát pl. nem kezdhettük volna úgy, hogy „A természetes számok a szokásos összeadásra nézve ...", ugyanis ekkor csak a 0 lehetne az egységelem, az egységelem egy, még nem bizonyított egyértelműségi tulajdonsága miatt, így a nemnulla elemeknek nem lenne inverze, hiszen nincs a számoknak ellentettje. Emellett sem $\mathbb{Z}$-ben, sem $\mathbb{Z}_n$-ben nem vehettük volna a szokásos szorzást műveletnek, ui. erre nézve sem létezik minden elemnek inverze, nevezetesen pl. a $0 \in \mathbb{Z}$ illetve a $(0) \in \mathbb{Z}_n$ elemek nem invertálhatóak.

Néhány további példa csoportokra:

– Tetszőleges *test és vektortér elemei* a testbeli ill. vektortérbeli összeadásra nézve kommutatív csoportot alkotnak, amint azt megköveteljük a struktúrák axiómáiban. Így pl. $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}_p, +)$, $(\mathbb{R}^n, +)$ Abel-csoportok; a + persze a szokásos (test-, illetve vektortérbeli) összeadást jelenti. Mivel testben minden nemnulla elemnek létezik reciproka, így bármely test nemnulla elemei a testbeli *szorzásra* nézve szintén (a testaxiómák szerint) Abel-csoportot alkotnak. Például $\mathbb{Z}_p$ nemnulla elemei a maradékosztályok közötti szorzásra nézve csoportot alkotnak. Ez ráadásul ciklikus

csoport, hiszen a modulo p primitív gyök létezése éppen azt jelenti, hogy az előbbi csoport egy elem (ez a primitív gyök) hatványaiból áll. Általában is belátható, hogy véges test (amelynek elemszáma bármely prímhatvány lehet, és csak azok) nemnulla elemei a szorzásra nézve ciklikus csoportot alkotnak.

– Ha X egy nemüres halmaz, akkor X *önmagára menő bijekciói* (amelyeket *permutációknak* nevezünk) a (függvény)kompozíció műveletére nézve csoportot alkotnak. Az asszociativitás a kompozícióra mindig teljesül, egységelem a halmaz identikus függvénye, inverz a szokásos függvényinverz. Nagyon fontos példánk lesz az a speciális eset, amikor $|X| = n$ (amit általában $X = \{1,2,\ldots,n\}$-ként képzelünk el); ebben az esetben n-edfokú szimmetrikus csoportról beszélünk, ezt S_n-nel jelöljük majd.

2.1.6. Definíció: *Az $\{1,2,\ldots,n\}$ halmaz önmagára menő bijekciói a függvénykompozícióra nézve csoportot alkotnak, melyet* ***n-edfokú szimmetrikus csoportnak*** *nevezünk és S_n-nel jelölünk.*

Itt a bijekciók a szokásos permutációkat jelölik abban az értelemben, hogy most magát az „átrendezést” mint függvényt értjük az elnevezés alatt. Ez a csoport *nem kommutatív*, amint azt később látni fogjuk; S_n-ről sok szó esik majd a 2. fejezet 7.1 pontjában.

– Az n dimenziós euklideszi tér *egybevágóságai* a kompozíció műveletére nézve csoportot alkotnak, egységelem a tér identikus függvénye, inverz a szokásos függvényinverz. (Ezen csoport fogalma persze általánosítható tetszőleges metrikus térre.) Ezt $\mathrm{Iso}(n)$-nel jelöljük. Ez a csoport sem kommutatív, amint a következő példánk (későbbi) részletes vizsgálatánál kiderül majd.

– Vegyünk a(z euklideszi) síkon egy n oldalú ($n \geq 3$) szabályos sokszöget és tekintsük azokat az egybevágósági transzformációkat, amelyek a sokszöget helyben hagyják. $2n$ transzformációt rögtön tudunk mondani: ezek a sokszög középpontja körüli $\frac{k \cdot 2\pi}{n}$ szögű forgatások ($k = 0,1,\ldots,n-1$) és páros n esetén a szimmetriaátlókra és a szemköztes oldalak felezőmerőlegesére, páratlan n esetén egy csúcsot a szemköztes oldal felezőpontjával összekötő egyenesekre vonatkozó tükrözések; ezekből szintén n darab van.

Gondoljuk meg, hogy nincs több! Egy kiválasztott csúcsot (legfeljebb) n helyre képezhet egy egybevágósági transzformáció, amelyet *egyértelműen meghatároz* a csúcsok képe a távolságtartás miatt; a szomszédos csúcs már csak legfeljebb két helyre kerülhet (az eredeti csúcs képével szomszédos két csúcs valamelyikére). Legfeljebb $2n$ transzformáció lehet tehát és ennyit meg is tudtunk adni. Világos, hogy két ilyen transzformáció kompozíciója, illetve bármely ilyen transzfomáció inverze is helyben hagyja a sokszöget. Az előbbiek alapján tehát egy újabb fontos csoportot definiálhatunk:

2.1.7. Definíció: *A sík azon egybevágósági transzformációi, melyek egy (rögzített) szabályos n-szöget önmagába visznek, a kompozíció műveletére nézve csoportot alkotnak. Ezt a csoportot D_n-nel jelöljük és* ***n-edfokú diédercsoportnak*** *nevezzük.*

Mivel sokszor szükségünk lesz rá a továbbiakban, írjuk le most D_n elemeit kissé „algebraibb” alakban. Jelölje f az n oldalú sokszög középpontja körüli $\frac{2\pi}{n}$ szögű (pozitív irányú) forgatást, t pedig a fent leírt tengelyek valamelyikére vonatkozó (rögzített) tengelyes tükrözést. Azt állítjuk, hogy

$$D_n = \{e, f, f^2, \ldots, f^{n-1}, t, tf, \ldots, tf^{n-1}\}.$$

Ezek az elemek persze mind benne vannak a csoportban és számuk $2n$, tehát elég belátnunk, hogy páronként különböznek:

$i)$ $f^j = f^k, 0 \leq j < k \leq n-1 \Rightarrow f^{k-j} = e$, de ez a nemnulla kitevők közül legelőször n-nél következik be, ami így ellentmondás.
$ii)$ $tf^j = tf^k \Leftrightarrow f^j = f^k$, az egyszerűsítési szabály szerint. Így ezt visszavezettük az előző esetre.
$iii)$ $f^j = tf^k \Leftrightarrow t^{-1} = t = f^{k-j}$ (balról t^{-1}-zel, jobbról $(f^j)^{-1} = f^{-j}$-vel szorozva), ami szintén nem lehet (utóbbi egy - esetleg identikus - forgatás, t pedig egy tükrözés).
Összefoglalva: a sokszög középpontja körüli $\frac{2\pi}{n}$ szögű forgatást f-fel, valamely (rögzített) lehetséges tengelyre vonatkozó tükrözést pedig t-vel jelölve

$$D_n = \{e, f, f^2, \ldots, f^{n-1}, t, tf, ..., tf^{n-1}\}.$$

Itt f hatványai a forgatások, a többi elem pedig tengelyes tükrözés.

A fenti definíciók némelyikében van egy „nyugtalanító” vonás. Például a diédercsoport esetében ha a síkon adott oldalszámmal különböző szabályos n-szögeket nézünk, akkor más és más elemek (azaz más egybevágóságok) fogják alkotni a D_n csoportot (mint halmazt). Eközben persze „érezhető”, hogy „lényegében ugyanarról” van szó. Ugyanez a helyzet akkor, mikor pl. S_5-öt előbb az $\{1, \ldots, 5\}$, majd (mondjuk) a $\{6, \ldots, 10\}$ halmaz bijekcióiként képzeljük el: más elemek alkotják az alaphalmazt, de mégis ugyanarra gondolunk. Egy n elemű ciklikus csoport is sokféle alaphalmazon realizálható, de a struktúra mindig ugyanaz marad. Ezek az észrevételek úgy foglalhatók össze, hogy szeretnénk pontosan megfogalmazni a kapcsolatot külöböző alaphalmazokon értelmezett, de tulajdonképpen azonos csoportok között; miután ez megtörtént, nem tekintenénk különbözőeknek azokat, melyek ilyen kapcsolatban állnak.

A szükséges fogalom persze a vektortereknél megismert *izomorfizmus* lesz, melyet azonban csak a fejezet 3. pontjában tárgyalunk, viszont addig is „titokban” használjuk majd a megfogalmazásainkban.

2.2. Rend, részcsoportok, normálosztók

2.2.1. Rend

Legyen G csoport és $g \in G$. Tekintsük g hatványait! Könnyen adódik, hogy két különböző kitevőjű hatvány, g^n és g^m $(n > m)$ pontosan akkor esik egybe, ha van olyan $k \in \mathbb{N}, k \geq 1$, melyre $g^k = e$:

$$g^m = g^n \Leftrightarrow g^{n-m} = e$$

Eszerint adott g elem esetén két eset lehetséges: vagy a hatványai periodikusan ismétlődnek, vagy minden hatványa különböző (és így végtelen sok különböző hatványa van).

2.2.1. Definíció: *Legyen G csoport és $g \in G$. Ekkor g* ***rendjét****, melyet $o(g)$-vel jelölünk, a következő módon értelmezzük:*

$$o(g) = \begin{cases} k & \text{ha } k \text{ a legkisebb olyan } \geq 1 \text{ természetes szám, melyre } g^k = e \\ \infty & \text{ha nincs olyan } \ell \in \mathbb{N}, \ell \geq 1 \text{ , amire } g^\ell = e \text{ teljesülne} \end{cases}$$

Pl. a komplex p-edik egységgyökök a (szokásos) szorzásra nézve csoportot alkotnak, ahol minden elem rendje 1 vagy p; utóbbiak éppen a primitív p-edik egységgyökök. Ha a modulo 10 *redukált maradékosztályokat* tekintjük, ezek is csoportot alkotnak a szorzásra az (1) egységelemmel, ahol pl. a (3) maradékosztály rendje 4, ui. $(3)^4 = (1)$ és 4-nél kisebb kitevőre ez nem teljesül.

Az egységelem az egyetlen olyan elem (bármely csoportban), melynek 1 a rendje. Véges csoportban persze minden elem rendje véges kell hogy legyen, de könnyű olyan végtelen csoportot találni, ahol szintén minden elem véges rendű (általában az ilyen tulajdonságú csoportot *torziócsoportnak* nevezik): ilyen pl. az összes komplex egységgyökök csoportja a szorzásra. Emellett már olyan csoportot is ismerünk, ahol az egységelemen kívül minden elem rendje végtelen (ezt

torziómentes csoportnak hívják): ilyen pl. az egészek vagy a valós számok (additív) csoportja. Van olyan csoport is, melyben véges és végtelen rendű elemek egyaránt előfordulnak: pl. a sík már említett egybevágóságcsoportjában egy adott pont körüli φ szögű forgatás (pontosan akkor) végtelen rendű, ha φ nem racionális többszöröse 2π-nek; ezenkívül pl. egy tengelyes tükrözés rendje mindig 2 (kétszer egymás után végrehajtva a sík identikus függvényét kapjuk.)

A fenti meggondolások azt is mutatják, hogy bármely $g \in G$ hatványai olyan (persze) ciklikus csoportot alkotnak, melynek elemszáma éppen $o(g)$ (ami esetleg végtelen); pontosan akkor lesz ez végtelen ciklikus csoport, ha g rendje végtelen. Leolvashatjuk azt is, hogy adott $g \in G,\ o(g) = n$ elem k-adik és ℓ-edik hatványa pontosan akkor egyezik meg, ha $k \equiv \ell \,(\mathrm{mod}\, n)$. Mivel $(g^{-1})^k = (g^k)^{-1}$, ezért $o(g^{-1}) = o(g)$.

A $g \in G$ hatványaiból álló (véges vagy végtelen) csoportot $\langle g \rangle$-vel jelöljük, de a definíciót majd egy későbbi, általánosabb fogalom kapcsán rögzítjük. Nyilvánvaló, hogy egy *véges csoport pontosan akkor ciklikus, ha van benne a csoport elemszámával megegyező rendű elem.*

Ha adott a G csoportban egy g véges rendű elem, akkor g minden hatványának a rendjét meg tudjuk adni:

2.2.2. Tétel: *Legyen G csoport és $g \in G$, mely véges rendű: $o(g) = n$. Ekkor*

$$o(g^k) = \tfrac{n}{(n,k)}$$

Bizonyítás: Feltehetjük, hogy $k > 0$, mivel $s > 0$-val $g^{-s} = (g^{-1})^s$ és $o(g^{-1}) = o(g)$. Azt kell belátnunk, hogy a fenti a legkisebb ℓ kitevő, melyre g^k-t emelve az egységelemet kapjuk. Határozzuk meg, hogy melyik a legkisebb $m = k\ell$, melyre $g^m = e$.

Ez az m a rend tulajdonsága szerint többszöröse n-nek, mivel $g^m = e$, másrészt definíciója szerint többszöröse k-nak . Az ilyenek közül a legkisebb $[k, n]$, aminek értéke - mint számelméletből tudjuk - éppen $\frac{nk}{(n,k)}$. Ebből k-val való egyszerűsítés

után az állításban szereplő kifejezést kapjuk g^k rendjére. ∎

A tétel egyszerű következménye (pl.) az a korábban kimondott állítás, hogy a $\mathbb{Z}_n$ ciklikus csoportban éppen $\varphi(n)$ olyan elem van, mely hatványaiként a teljes csoport előáll, hiszen éppen ennyi az n-edrendű elemek száma ($\varphi(n)$ az Euler-féle függvény). Ezek az elemek $+$-szal jelölve a műveletet $\underbrace{(1)+(1)+...(1)}_{k\,\text{db}}$, $k \geq 0,\ (k,n) = 1$ alakúak, azaz pontosan a redukált maradékosztályok.

2.2.2. Részcsoportok

Tekintsük az egész számok csoportjában a páros számok részhalmazát! Látható, hogy ez a szokásos összeadásra nézve csoportot alkot a teljes csoporton belül. Kézenfekvő egy új fogalom bevezetése:

2.2.3. Definíció: *Legyen G csoport. A $\emptyset \neq H \subseteq G$ halmazt a G* ***részcsoportjának*** *nevezzük, ha H csoport a G-beli műveletre nézve.*
Ezt így jelöljük: $H \leq G$

Minden legalább kételemű csoportnak van legalább két részcsoportja: az egységelemből álló egyelemű részcsoport és a teljes csoport. Ezeket *triviális részcsoportoknak* nevezzük, a többit *valódiaknak*. Később pontosan megadjuk majd azokat a csoportokat, melyeknek csak triviális részcsoportjaik vannak.
További példák: részcsoportot alkotnak a már említett páros számok az egészek csoportjában, általában az m-mel osztható számok ugyanebben a csoportban, a racionális számok a valós (vagy komplex) számok csoportjában, az eltolások $\text{Iso}(n)$-ben, forgatások D_n-ben.
Jegyezzük meg, hogy az Abel-csoportok definíciója szerint ezeknek minden részcsoportjuk is kommutatív. (Ha itt csak valódi részcsoportokra gondolunk, akkor

ennek megfordítása nem igaz; erre később látunk majd több példát is.)

Ha a G csoport H részhalmazáról be akarnánk látni, hogy részcsoport G-ben, akkor az eddigiek alapján nem lenne más lehetőségünk, mint ellenőrizni a csoportaxiómák teljesülését. Természetesen itt az első kérdés az, hogy a G-n értelmezett művelet egyáltalán művelet-e H-n is, azaz *nem vezet-e ki* H-ból. Az asszociativitás persze igaz, hiszen az G-ben is teljesült. Önmagában azonban (ellentétben a vektorterek részstruktúráival, az alterekkel) *nem elég*, ha H zárt a műveletre: vegyük pl. a természetes számokat az egészek csoportjában, amire ez teljesül, de nincs a nemnulla elemeknek inverze. A következő könnyen bizonyítható tétel szükséges és elégséges kritériumot ad a „részcsoportságra”:

2.2.4. Tétel: *Legyen G csoport, $\emptyset \neq H \subseteq G$. Ekkor fennáll:*

$$H \leq G \Leftrightarrow \forall x, y \in H \text{ esetén } xy^{-1} \in H$$

Egyszerűen belátható pl. ennek segítségével, hogy *részcsoportok metszete is részcsoport*.

A már említett példákban a részcsoportok egységeleme megegyezett a teljes csoport egységelemével. Ez általában is igaz. Persze nem az a kérdés, hogy G egységeleme minden $H \leq G$-beli elemet fixen hagy-e (hiszen ez az axiómák miatt teljesül), hanem az, hogy G egységeleme *benne van-e H-ban*. Megtörténhetne ugyanis az, hogy H-nak van egy különálló egységeleme, ami G-nek nem minden elemét hagyja fixen. A helyzet azonban, mint mondtuk, nem ez, hiszen e_G-vel és e_H-val jelölve G és H (esetleg két különböző) egységelemét:

$$e_H = e_H e_H = e_H e_G \Rightarrow e_H = e_G$$

Itt az egységelemek definiáló tulajdonságát és a 2.1. pont végén említett egyszerűsítési szabályt használtuk (e_H G-beli inverzével szoroztunk balról).

Ha X és Y a G csoport tetszőleges nemüres *részhalmazai*, akkor természetes módon értelmezhetjük az XY részhalmazt a következőképpen:

$$XY \stackrel{\text{def}}{=} \{xy \mid x \in X, y \in Y\}$$

Látható, hogy a szokásos módon „számolhatunk" az előbbi definíció szerint, azaz pl. $r\,(xY) = (rx)Y = \{rxy \mid y \in Y\}$ (itt Y egy részhalmaz, r és x két elem a csoportban).

Az előbbi definíció mintájára beszélhetünk egy X nemüres részhalmaz inverzéről is:

$$X^{-1} \stackrel{\text{def}}{=} \{x^{-1} \mid x \in X\}.$$

Legyen $H \leq G$ és vezessük be a következő $\sim$ relációt G-n:

$x \sim y$, ha $y = xh$ valamely $h \in H$-val.

Gondoljuk meg, hogy $\sim$ ekvivalenciareláció:

$i)$ *reflexív*, hiszen $\forall x \in G\ x = xe$, ahol e a H G-vel megegyező egységeleme.

$ii)$ *szimmetrikus*, hiszen jobbról való szorzással $y = xh \Rightarrow x = yh^{-1}$, ahol persze $h^{-1} \in H$, mivel H részcsoport.

$iii)$ *tranzitív*, ugyanis $y = xh_1$ és $z = yh_2$ esetén az asszociativitást is kihasználva $z = x(h_1h_2)$, ahol $h_1, h_2 \in H$ miatt $h_1h_2 \in H$.

Eszerint G az előbbi ekvivalenciareláció diszjunkt ekvivalenciaosztályaira bomlik; az $x \in G$-t tartalmazó osztály xH. Az ilyen „alakú" részhalmazoknak külön nevük van:

2.2.5. Definíció: *Legyen $H \leq G$, ahol G tetszőleges csoport. Ekkor az xH, $x \in G$ részhalmazokat G-ben* ***H szerinti bal oldali mellékosztályoknak*** *nevezzük.*

Láttuk: G a H szerinti mellékosztályok diszjunkt uniójára bomlik. Világos, hogy minden xH mellékosztály számossága megegyezik H számosságával, hiszen az egyszerűsítési szabály miatt $h \mapsto xh$ egy bijekció a mellékosztály és H elemei között.

Az előbbi ekvivalenciarelációt persze „fordítva” is csinálhattuk volna, azaz H elemeivel balról való szorzással; így a **jobb oldali mellékosztályokhoz** jutottunk volna. Azt várjuk, hogy „ugyanannyi” jobb és bal oldali mellékosztály van, azaz a két oldali mellékosztályok halmazának számossága ugyanakkora. Ez valóban így van, amint alább belátjuk majd, most csak elnevezzük ezt a számosságot:

2.2.6. Definíció: *Legyen G csoport, $H \leq G$.*
*A H szerinti bal oldali mellékosztályok halmazának számosságát (mely megegyezik a jobb oldali mellékosztályok számosságával) $|G : H|$-val jelöljük és a H (G-beli) **indexének** nevezzük.*

A fenti állítás véges csoportokra közvetlenül adódik, hiszen minden mellékosztály elemszáma ugyanannyi és megegyezik a részcsoport elemszámával. Ebből származik az alábbi, alapvető fontosságú tétel:

2.2.7. Tétel (Lagrange): *Ha G véges csoport és $H \leq G$, akkor $|H|$ osztója $|G|$-nak.*
Természetesen ilyenkor $|G : H| = \frac{|G|}{|H|}$ (ezért az index is osztója a csoport elemszámának).

Ennek egyszerű következménye, hogy prímrendű csoportnak csak triviális részcsoportjai vannak (hamarosan látjuk majd, hogy ez a tulajdonság az egyelemű csoporton kívül pontosan a prímrendűekre igaz).

Felmerül a kérdés, hogy G-nek két eleme, x és y mikor esik ugyanabba a $H \leq G$ szerinti (pl.) baloldali mellékosztályba? Mivel $a \in G$ az aH-ban van, így az előző kérdés azzal egyenértékű, hogy mikor teljesül $xH = yH$. Ehhez először azt válaszoljuk meg, hogy milyen x-ekre teljesül $xH = H$. A válasz:

$$xH = H \Leftrightarrow x \in H.$$

Ugyanis ha $x \in H$, akkor $xH \subseteq H$ a részcsoport tulajdonsága miatt, másrészt ekkor tetszőleges $h \in H$ esetén $h = x(x^{-1}h)$, ahol $x \in H$ miatt $x^{-1} \in H$ és így $x^{-1}h \in H$ is teljesül, tehát $h \in xH$. A $\Leftarrow$ irány ezzel kész.
Megfordítva: $xH = H \Rightarrow$ ha $h \in H$ tetszőleges, akkor $h = xh'$ valamely $h' \in H$ elemmel, amiből $x = hh'^{-1} \in H$ adódik.
Tehát H maga egy mellékosztályt alkot.

Most visszatérünk a korábbi általánosabb kérdéshez tartozó egyenlőséghez, amit a részhalmazok szorzatáról (és inverzéről) mondottak értelmében átalakítunk:

$$xH = yH \Leftrightarrow y^{-1}(xH) = H \Leftrightarrow (y^{-1}x)H = H \Leftrightarrow y^{-1}x \in H$$

Vagyis x és y pontosan akkor esik ugyanabba a H szerinti baloldali mellékosztályba, ha $y^{-1}x \in H$. Persze a fenti sorban x^{-1}-zel is szorozhattunk volna balról, akkor az $x^{-1}y \in H$ feltételt kaptuk volna, ami egyenértékű az előzővel, hiszen $x^{-1}y$ az inverze $y^{-1}x$-nek, tehát egyszerre esnek (vagy nem esnek) H-ba. Az előbbi gondolatmenetet a jobboldali mellékosztályokra alkalmazva ugyanez az eredmény adódik.
Most már be tudjuk látni, hogy a bal és jobb oldali mellékosztályok halmaza ugyanolyan számosságú, nevezetesen vegyük észre, hogy az x-szel képezett bal oldali mellékosztály inverze az x^{-1}-gyel képezett jobboldali mellékosztály:

$$(xH)^{-1} = H^{-1}x^{-1} = Hx^{-1}$$

Eszerint az invertálás bijekciót jelent a jobb és bal oldali mellékosztályok között: a szürjektivitás nyilvánvaló (G minden eleme előáll x^{-1} alakban), az injektivitás pedig az előbbi eredményből adódik:

$$xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow Hx^{-1} = Hy^{-1}$$

Példaként ismét tekintsük $G = \mathbb{Z}$-t és benne a $H = \{7\text{-tel osztható számok}\}$ részcsoportját! Ekkor a bal oldali és a jobb oldali mellékosztályok egybeesnek és pl. a 3-at tartalmazó (jobb és bal oldali) mellékosztály a következő (kivételesen

a szokásos $+$ jelet használva a műveletre): $3 + H = \{\ldots,3,10,13,16,19,\ldots\}$; látjuk, hogy a mellékosztályok éppen a szokásos modulo 7 maradékosztályok.

Általában nem igaz, hogy egy részcsoport szerinti jobb és bal oldali mellékosztályok egybeesnek; jegyezzük meg azonban, hogy Abel-csoportokban ez természetesen minden részcsoportra igaz, hiszen ezeknél $xh = hx\ \forall x \in G$, $h \in H$ is teljesül. Azokkal a részcsoportokkal (tetszőleges csoportban), melyekre teljesül a fenti tulajdonság, a következő fejezetben foglalkozunk majd.

Ha van egy $G \geq H \geq K$ „részcsoport-láncunk", akkor megkérdezhetjük, hogy (van-e és ha igen) mi a kapcsolat az egyes „szóba jövő" indexek között? A válasz a lehető „legtermészetesebb":

2.2.8. Tétel: *Legyen G csoport és $G \geq H \geq K$ részcsoportok. Ekkor fennáll:*

$$|G : K| = |G : H| \cdot |H : K|$$

(Ez persze általánosan a halmazelméletből ismert számosságszorzást jelenti.)

Bizonyítás: A bizonyítást abban az esetben végezzük, mikor mindkét index véges. Tetszőleges számosságra is működik értelemszerű módosítással és felhasználva a *kiválasztási axiómát* (minden baloldali mellékosztályból ki kell választani pontosan egy elemet).

Legyenek G-ben a H szerinti mellékosztályok $\{x_i H,\ i = 1, \ldots, m\}$, H-ban pedig a K szerinti mellékosztályok $\{y_j K,\ j = 1, \ldots, n\}$. Ekkor, mivel G az előbbiek, H az utóbbiak uniója, így fennáll: $G = \bigcup_{i,j} x_i y_j K$. Azt kell még belátnunk, hogy a felírt $x_i y_j K$ (G-beli) mellékosztályok páronként diszjunktak, így az összes K szerinti bal oldali mellékosztály G-ben pontosan egyszer szerepel a felsorolásban.

Valóban, tegyük fel, hogy valamelyik kettő (mondjuk $x_1 y_1 K$ és $x_2 y_2 K$) nem diszjunkt; ekkor azonban egybeesnek:

$$x_1 \underbrace{y_1 K}_{\subseteq H} = x_2 \underbrace{y_2 K}_{\subseteq H} \Rightarrow x_1 H \text{ és } x_2 H \text{ nem diszjunkt} \Rightarrow x_1 H = x_2 H$$

$$\Rightarrow x_1 = x_2 \Rightarrow y_1K = y_2K \Rightarrow y_1 = y_2.$$

Tehát két mellékosztály pontosan akkor nem diszjunkt, ha ugyanazzal az x_i-vel és y_j-vel képződtek, vagyis mn db K szerinti mellékosztály van; ezt kellett igazolnunk. ∎

Ha G csoport, $\emptyset \neq X \subseteq G$, akkor H „kifeszít” egy részcsoportot ahhoz hasonlóan, ahogy egy vektortér valamely nemüres részhalmaza kifeszít egy alteret. Ezt azzal analóg módon értelmezzük:

2.2.9. Definíció: *Legyen G csoport, $X \subseteq G, X \neq \emptyset$. Ekkor azt a legszűkebb részcsoportját G-nek, mely X-et tartalmazza, az **X által generált részcsoportnak** nevezzük és $\langle X \rangle$-vel jelöljük. X elemeit **generátorelemeknek** hívjuk.*

Bizonyos csoportok előállnak valamely véges részhalmazuk generált részcsoportjaként, mint pl. a véges csoportok (mondjuk a teljes csoport generátumaként; más példa: $D_n = \langle t, f \rangle$), vagy a végtelen ciklikus csoportok (egyetlen elem generálásával).

2.2.10. Definíció: *A G csoport **végesen generált**, ha*

$$G = \langle X \rangle, \text{ ahol } \emptyset \neq X \subseteq G \text{ és } |X| < \infty$$

A 2.2.9. -ban szereplő „legszűkebbség” persze azt jelenti, hogy $H \leq G$, $X \subseteq H$ esetén $\langle X \rangle \leq H$.

A generált részcsoport biztosan létezik, mert $X \subseteq G$ miatt az alábbi metszet értelmes és teljesíti a követelményeket:

$$\langle X \rangle = \bigcap_{X \subseteq K \leq G} K$$

$\langle X \rangle$-nak természetesen tartalmaznia kell minden olyan szorzatot, mely X-beli elemek (egész kitevős) hatványaiból áll. Ennél „tovább” azonban nem is kell mennünk, hiszen (pl.) a 2.2.4. tétel alapján könnyű igazolni, hogy az említett elemek részcsoportot alkotnak, így a legszűkebbségi tulajdonság miatt a generált

részcsoport ennek része; ezek tehát a mindkét irányú tartalmazás miatt egybeesnek.

2.2.11. Tétel: *A G csoport $X \neq \emptyset$ részhalmaza által generált részcsoport a következő elemek halmaza:*

$$\langle X \rangle = \{x_1^{n_1} x_2^{n_2} \cdot \ldots \cdot x_k^{n_k} \mid x_i \in X, n_i \in \mathbb{Z}, 0 < k \in \mathbb{N}\}$$

Az előbbi tétel értelmében véges sok elem által generált részcsoport mindig *megszámlálható* (azaz véges, vagy megszámlálhatóan végtelen) sok elemből áll; ez mutatja, hogy pl. $(\mathbb{R}, +)$ nem végesen generált. A megszámlálhatóság feltétele - mint az sejthető - nem elégséges, ugyanis bár a számosság engedné, de $(\mathbb{Q}, +)$ sem végesen generált, hiszen véges sok racionális szám által generált részcsoportjában csak véges sok nevező fordul elő.

Az $|X| = 1$ speciális esetben a korábban már tárgyalt egy elem hatványaiból álló ciklikus részcsoportot kapjuk. Vegyük észre, hogy ekkor a 2.2.7. tétel azt mondja, hogy véges csoport bármely g elemére $o(g) \mid |G|$. Ha ezt p elemű csoportokra alkalmazzuk, ahol prím, akkor azt látjuk, hogy ilyen csoportokban az egységelemen kívül minden elem rendje p (mivel, amint mondtuk, csak az egységelem rendje 1). De ebből az következik, hogy egy ilyen csoport biztosan ciklikus, hiszen van benne olyan elem (igazából $\forall \neq e$ elem ilyen), melynek rendje megegyezik a csoport elemszámával! Ez azt mutatja, hogy „tulajdonképpen csak egyféle" p elemű csoport van: a $\mathbb{Z}_p$ „típusú" ciklikus csoport. Más szóval csak annyi „szabadságunk" van, hogy máshogy nevezzük az alaphalmaz elemeit, de ettől eltekintve nem lehet definiálni két „lényegesen" különböző csoportot egy p elemű halmazon.

Az idézőjeles szavak pontos jelentését a már említett *izomorfia* fogalmának meghatározása adja majd a következő pontban.

Az elhangzottak alkalmazásaként először teljesen leírjuk a ciklikus csoportok részcsoportjait, majd meghatározzuk, hogy pontosan melyek azok a csoportok, melyeknek csak triviális részcsoportjaik vannak.

2.2.12. Tétel: *Legyen G ciklikus csoport. Ekkor a következők teljesülnek:*
G minden részcsoportja ciklikus.
Ha G végtelen, $G = \langle a \rangle$, akkor minden részcsoportja $\langle a^k \rangle$, $k \in \mathbb{N}$ alakú végtelen (ciklikus) csoport.
Ha G véges, akkor minden $k \mid |G|$-re pontosan egy k elemű részcsoport létezik G-ben.

Bizonyítás: Legyen $G = \langle a \rangle$ ciklikus, $e \neq H \leq G$. Jelölje k a legkisebb olyan pozitív egész kitevőt, melyre $a^k \in H$ (ilyen persze létezik, hiszen H (is) a valamely hatványaiból áll). Belátjuk, hogy valójában $H = \langle a^k \rangle$.
Nyilván $a^k \subseteq H$, mert H részcsoport. Másrészt indirekt tegyük fel, hogy van olyan h elem H-ban, mely nem a generált részcsoportban van. Ekkor valamely $r, s \in N$ számokra $h = a^{kr+s} \in H, 0 \neq s < k$ (a kitevőjét k-val maradékosan osztva), ami ellentmond k minimalitásának, ui. ekkor a^s is H-ba esne (mivel a^{kr} is H-beli).

Ebből rögtön következik az állítás második része is, csak annyit kell megjegyeznünk, hogy $\left|\langle a^k \rangle\right| = o(a^k)$ persze végtelen kell hogy legyen, különben a rendje is véges volna. Emellett vegyük észre, hogy $H = \langle a^k \rangle$ indexe éppen k, ugyanis az $eH, aH, a^2H, \ldots, a^{k-1}H$ az összes mellékosztály.

Rátérve a harmadik részre legyen $|G| = n$ és $k \mid n$. Ekkor $\left|\langle a^{\frac{n}{k}} \rangle\right|$ éppen k, ui. a 2.2.2. tétel szerint ennyi a rendje a generátorelemnek. Ha $\langle a^d \rangle$ egy másik k elemű részcsoport, akkor $o(a^d) = \frac{n}{(n,d)} = k$, amiből $\frac{n}{k} = (n, d)$, így $\frac{n}{k} \mid d$, tehát $\langle a^d \rangle \subseteq \langle a^{\frac{n}{k}} \rangle$ és mivel mindkettő véges, így egybeesnek.
Ezzel a bizonyítás teljes. ∎

2.2.13. Tétel: *A G csoportnak pontosan akkor nincs nemtriviális részcsoportja, ha $|G| = 1$ vagy p.*

Bizonyítás: Először is az egyelemű (azaz csak az egységelemből álló csoportnak és a 2.2.7. Lagrange-tétel miatt a p elemű csoportoknak csak triviális részcsoportjaik lehetnek.
A megfordításhoz legyen G legalább kételemű csoport, melynek csak triviális részcsoportjai vannak és vegyünk egy $e \neq g \in G$ elemet. Ekkor $\langle g \rangle = G$, hiszen a generált részcsoport triviális részcsoport, de nem lehet egyelemű. Eszerint G ciklikus. De a nem egyelemű ciklikus csoportok közül pontosan a prímrendűek azok, melyeknek csak triviális részcsoportjaik vannak az előző tétel alapján, így $|G| = p$ és ezzel az állítást beláttuk. ∎

Végül még két állítás a részcsoportokkal kapcsolatban, melyet később használni fogunk.

2.2.14. Tétel: *Legyen G csoport, $H, K \leq G$.*
i) $HK \leq G \Leftrightarrow HK = KH$
ii) $|H| \cdot |K| = |HK| \cdot |H \cap K|$ *(tetszőleges $H,\ K$ részcsoportok esetén).*

Bizonyítás: *i)* Ha $HK \leq G$, akkor $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$, tehát ezzel az iránnyal készen vagyunk.
A másik irányhoz az 2.2.4. tételre hivatkozunk majd: legyen h_1k_1 és h_2k_2 a HK két eleme. Ekkor írhatjuk:

$$h_1k_1(h_2k_2)^{-1} = h_1 \overbrace{(\underbrace{k_1k_2^{-1}}_{=k' \in K} h_2^{-1})}^{=h'k'' \in HK} = \underbrace{h_1h'}_{\in H} k'' \in HK$$

ii) Legyen $D = H \times K$ a (halmazelméleti) direkt szorzata H-nak és K-nak. Vezessünk be egy $\sim$ relációt D-n:

$$(h, k) \sim (h', k') \Leftrightarrow hk = h'k'$$

Rögtön látható, hogy $\sim$ ekvivalenciareláció; a $[(h,k)]$ ekvivalenciaosztályban éppen azok a (h',k') (rendezett) párok vannak, melyekre $h'k' = hk$. Eszerint az ekvivalenciaosztályok halmazának számossága $|HK|$.

Másrészt hány elem van egy osztályban?

$$hk = h'k' \Leftrightarrow \underbrace{h'^{-1}h}_{\in H} = \underbrace{k'k^{-1}}_{\in K} \Leftrightarrow (h',k') = (hx^{-1}, xk), \text{ ahol } x \in H \cap K.$$

A második nyílnál az átalakítás csak a $\Rightarrow$ irányt adja, de a $\Leftarrow$ irány nyilvánvaló. Mivel különböző $x \in H \cap K$-k különböző (h',k') párokat jelentenek, így azt kaptuk, hogy egy ekvivalenciaosztály számossága $|H \cap K|$.

Ebből és az előző eredményből adódik, hogy a diszjunkt ekvivalenciaosztályok uniójának, azaz $H \times K$-nak számossága:

$$|H| \cdot |K| = |HK| \cdot |H \cap K| \qquad \blacksquare$$

2.2.3. Normálosztók

Mint már jeleztük, a részcsoportok közül kitüntetett szerepet játszanak azok, melyek szerinti jobb és baloldali mellékosztályok megegyeznek:

2.2.15. Definíció: *Legyen G csoport. Az $N \leq G$ részcsoportot (G-beli)* ***normálosztónak*** *nevezzük, ha az N szerinti jobb és baloldali mellékosztályok egybeesnek, azaz jelben $Ng = gN \ \forall g \in G$.*

Azt, hogy N normálosztója G-nek, így jelöljük: $N \triangleleft G$, vagy $G \triangleright N$.

Használatos még a normális részcsoport és az invariáns részcsoport elnevezés is.

Minden legalább kételemű G csoportban van legalább két normálosztó: a két triviális részcsoport G és e. Ezeket *triviális normálosztóknak* nevezzük. Bizonyos csoportoknak nincs is ennél több normálosztójuk, egy (nemtriviális) példát már ismerünk is: a $\mathbb{Z}_p$ csoportnak csak triviális részcsoportjai, így csak triviális normálosztói vannak. Mint később kiderül majd, vannak más, bonyolultabb szer-

kezetű és nemkommutatív csoportok is, melyek ilyen tulajdonságúak.

2.2.16. Definíció: *A G csoportot **egyszerűnek** nevezzük, ha csak triviális normálosztói vannak.*

A másik végletként már említettük, hogy Abel-csoportban minden részcsoport normálosztó. Érdekes tény azonban, hogy ez a tulajdonság *nem jellemzi* a kommutatív csoportokat (de pontosan tudjuk, hogy melyek azok a csoportok, melyek ilyen tulajdonságúak). Kommutatív egyszerű csoportok az egyelemű csoporton kívül pontosan a $\mathbb{Z}_p$ típusúak, hiszen mivel ebben az esetben minden részcsoport normálosztó, így csak triviális részcsoportok lehetnek, az ilyen csoportokat pedig leírtuk a 2.2.13. tételben.

Eddigi nemkommutatív példáinkat nézve pl. D_n-ben a forgatások (melyekből n darab van) egy 2 indexű normálosztót alkotnak. Általában igaz ugyanis, hogy egy 2 indexű N részcsoport normálosztó, hiszen az egyik szerinte vett jobb és bal oldali mellékosztály saját maga, „ezek” tehát megegyeznek, de ezenkívül már csak egy bal és jobb oldali mellékosztály van, tehát mindkettőnek $G\backslash N$-nel kell megegyeznie.

Később általánosítjuk majd ezt az állítást a G véges csoport olyan H részcsoportjára, melyre $|G:H|$ a $|G|$ legkisebb prímosztója (annak bizonyítása azonban már nem ilyen „kombinatorikus” úton fog történni).
A „normálosztóság” *nem tranzitív*, pl. gyorsan meggondolható, hogy D_4-ben az $\{e, f^2, t, tf^2\}$ elemek (részcsoportot és így a 2 index miatt) normálosztót alkotnak, ebben pedig $H = \{e, tf^2\}$ szintén egy 2 indexű normálosztó, ami *nem normálosztó* D_4-ben, mert $fH = \{f, ftf^2\} = \{f, tf\} \neq Hf = \{f, tf^3\}$.

A definícióból rögtön látszik, hogy $N \leq M \leq G$ és $N \lhd G$ esetén $N \lhd M$ is teljesül (de ennek fordítottja nem igaz). Vegyük észre továbbá, hogy a 2.2.14. tétel $i)$ része alapján $N \lhd G$, $H \leq G$ esetén $\langle N, H\rangle = NH = HN$. Sőt, ha $N, H \lhd G$,

akkor $NH \triangleleft G$ is igaz, ui. egy később még szerepet játszó egyszerű trükkel:

$$g^{-1}(nh)g = \underbrace{g^{-1}ng}_{\in N}\underbrace{g^{-1}hg}_{\in H} \ \forall g \in G, n \in N, h \in H.$$

A következő tétel a „normálosztóság” három ekvivalens jellemzését adja:

2.2.17. Tétel: *Legyen G csoport, $N \leq G$. A következő állítások ekvivalensek:*
i) $N \triangleleft G$
ii) $\forall g \in G$*-re* $g^{-1}Ng = N$
iii) $\forall g \in G, n \in N$*-re* $g^{-1}ng \in N$

Bizonyítás: A bizonyítást „kényelmesebb” (a szokásos „ciklikus bizonyítás” helyett) úgy végeznünk, hogy először az első két állítás, majd a második kettő egyenértékűségét látjuk be.
$i) \Leftrightarrow ii)$: Egyszerű szorzással adódik (a részhalmazok szorzatáról mondottak szerint).
$ii) \Rightarrow iii)$: Ez közvetlen következménye $g^{-1}Ng$ definíciójának.
$iii) \Rightarrow ii)$: Rögzített $g \in G$ esetén tekintsük az $N^* = g^{-1}Ng$ halmazt! Be kell látnunk, hogy ez megegyezik N-nel. N^* minden eleme N-ben van a feltevés szerint, így $N^* \subseteq N$. Másrészt ha $n \in N$, akkor az $n = g^{-1}\underbrace{(gng^{-1})}_{\in N}g$ azonosságot használva $n \in N^*$, hiszen az $iii)$ feltevést $g' = g^{-1}$-re alkalmazva adódik a kapcsos zárójeles tartalmazás. Tehát $N = N^*$, amit igazolnunk kellett. ∎

Megjegyzendő, hogy az $N \leq G$ feltétel nem hagyható el, pl. tetszőleges sok elemből álló részhalmaza egy kommutatív csoportnak teljesíti a részcsoportságon kívüli feltételeket, de nem is szükségképpen részcsoport.

Az előbbi tételben felbukkanó, G-n értelmezett és G-be képező $\varphi : \ x \mapsto g^{-1}xg$ ($g \in G$ rögzített) függvény szerepet játszik majd a későbbiekben. Vegyük észre, hogy φ injektív és szürjektív G-n:

$g^{-1}xg = g^{-1}yg \Rightarrow x = y$ (balszorzás g-vel, jobbszorzás g^{-1}-zel);

$x \in G \Rightarrow x = g^{-1}(gxg^{-1})g$ („megoldottuk az egyenletet”).

A fejezet következő pontjában látni fogjuk, hogy φ-nek még egy fontos tulajdonsága van. Most csak az elnevezését adjuk meg:

2.2.18. Definíció: *Legyen G csoport, $g \in G$ egy rögzített elem.*
Az $x \mapsto g^{-1}xg$ függvényt, mely egy $G \to G$ bijekció, ***g-vel való konjugálásnak*** *nevezzük és φ_g-vel jelöljük.*

Ez a magyarázat arra, miért hívják a normálosztót *invariáns* részcsoportnak: ui.

$N \triangleleft G \Leftrightarrow N$ minden $g \in G$-vel való konjugálásnál fixen marad,

azaz N *invariáns* φ_g-re $\forall g \in G$ esetén.

Ha adott a G csoport X nemüres részhalmaza, akkor a(z X által) generált részcsoport fogalmához hasonlóan definiálhatjuk az X *által generált normálosztó* fogalmát: ez a legszűkebb olyan normálosztó G-ben, mely tartalmazza X-et. A keresett normálosztó előáll úgy, mint az *összes X-et tartalmazó normálosztó metszete*. Nyilván tartalmazza valamennyi konjugáltját X-nek és az ezek elemeiből álló tetszőleges szorzatokat, így az ezek által generált részcsoportot is. Könnyű meggondolni, hogy ennél tovább nem is kell mennünk, mert a kapott részcsoport már normálosztó G-ben, ami a generált részcsoport legszűkebbségi tulajdonsága miatt megegyezik az $\langle X \rangle$ által generált normálosztóval.
Az elmondottakat az alábbi definícióban foglaljuk össze:

2.2.19. Definíció: *Legyen G csoport, $\emptyset \neq X \subseteq G$.*
Ekkor az ***X által generált normálosztónak****, vagy X normális lezártjának nevezzük és X^G-vel jelöljük a legszűkebb olyan normálosztót G-ben, mely X-et tartalmaza.*
Egyszerűen adódik, hogy $X^G = \bigcap_{X \subseteq N \triangleleft G} N = \langle g^{-1}Xg \mid g \in G \rangle = \langle X \rangle^G$.

A normális lezárt fogalma mellett $H \leq G$ esetén értelmezhetjük az ún. *normális belső* fogalmát is: ez a legbővebb H-ban lévő G-beli normálosztó. Ez persze azt jelenti, hogy ha N a H-ban lévő G-beli normálosztó, akkor N benne van H normális belsejében; ezzel megadhatjuk a normális belsőt mint az ilyen normálosztók által generált részcsoportot.
Megjegyzendő: bármely $H \leq G$ esetén az egységelem biztosan egy H-ban lévő G-beli normálosztó és látható, hogy ezúttal nem értelmezhető a fogalom tetszőleges részhalmaz esetén (mert semmi sem garantálja pl., hogy akár egyetlen elemének konjugáltját is tartalmazza). H normális belseje H-nak minden konjugáltjában benne van (mert invariáns a konjugálásra) és utóbbiak metszete egyszerűen meggondolható módon normálosztó G-ben, tehát ez a normális belső.

2.2.20. Definíció: *Legyen G csoport, $H \leq G$.*
*H **normális belsejének** hívjuk és H_G-vel jelöljük a legbővebb olyan G-beli normálosztót, mely H-ban van. Könnyű belátni a következőket:*

$$H_G = \langle N \mid N \leq H,\ N \triangleleft G \rangle = \bigcap_{g \in G} g^{-1} H g$$

Két további részcsoportot is rendelhetünk természetes módon a G csoport tetszőleges nemüres részhalmazához. Az egyik G azon elemeiből áll, melyekkel való konjugálás X-et *mint halmazt* fixen hagyja; G egységeleme például ilyen tulajdonságú. Tegyük fel, hogy g és h ilyen tulajdonságú. Ekkor nyilvánvalóan gh is ilyen, másrészt g^{-1} is, hiszen $gXg^{-1} = g(g^{-1}Xg)g^{-1} = X$.
Eszerint a $g^{-1}h$-val való konjugálás is fixen hagyja X-et, tehát valóban részcsoportot alkotnak a megfelelő elemek (2.2.4. miatt).
Az előzőhöz hasonlóan azok az elemek is részcsoportot alkotnak G-ben, melyekkel való konjugálás a nemüres $X \subseteq G$ *minden elemét* fixen hagyja. Vegyük észre, hogy adott $x \in X$ esetén $g^{-1}xg = x \Leftrightarrow gx = xg$ alapján ez pontosan az x-szel *felcserélhető* elemeket jelenti.

Az így kapott csoport persze részcsoportja lesz az előbb definiált (rész)csoportnak, sőt nem nehéz meggondolni, hogy normálosztó is abban.
Íme az előbbiekben „tárgyalt" két részcsoport elnevezése:

2.2.21. Definíció: *Legyen G csoport, $\emptyset \neq X \subseteq G$.*
Azok a $g \in G$ elemek, melyekre $(X)\varphi_g = X$ teljesül, azaz X-szel felcserélhetők, részcsoportot alkotnak G-ben, melyet X (G-beli) ***normalizátorának*** *nevezünk és $N_G(X)$-szel jelölünk.*
Azok a $g \in G$ elemek, melyekre $\forall x \in X$-re $(x)\varphi_g = x$ teljesül, azaz X minden elemével felcserélhetők, részcsoportot alkotnak G-ben, melyet X (G-beli) ***centralizátorának*** *nevezünk és $C_G(X)$-szel jelölünk.*
Fennáll: $C_G(X) \triangleleft N_G(X)$, és a definícióból világos, hogy ha $H \leq G$, akkor $H \triangleleft N_G(H)$ is teljesül.

Nem nehéz meggondolni, hogy *véges* csoport esetén a normalizátor definíciójában $(X)\varphi_g \subseteq X$-et is írhattunk volna (mivel a konjugálás mint bijekció ilyenkor egy véges halmazon hat), azonban végtelen csoportoknál ez nem feltétlenül van így.

A következőkben kiderül, miért kitüntetett részcsoport a normálosztó.
Legyen $N \triangleleft G$ és tekintsük az N szerinti (pl.) bal oldali mellékosztályokat (tudjuk: a megfelelő bal és jobb oldali mellékosztályok egybeesnek). Értelmezni szeretnénk egy $\circ$ műveletet ezeken úgy, hogy csoportot kapjunk. Kézenfekvőnek tűnik a következő definíció:

$$(aN) \circ (bN) \stackrel{\text{def}}{=} (ab)N$$

Ez a definíció, bármennyire is „szemléletes", *nem jó* akkor, ha egy *„nemnormálosztó"* részcsoportot veszünk N helyett. A problémát az okozza, hogy itt halmazokat akarunk összeszorozni úgy, hogy a szorzást egy-egy elemmel végzett műveletre vezetjük vissza. De ezeket az elemeket többféleképpen is választhatjuk; ha tehát különböző választás esetén más eredményt kapunk, akkor a definíció nem

használható. Azonban ez az akadály nem áll fenn akkor, ha (mint most) egy normálosztó szerinti mellékosztályokról beszélünk, ugyanis ilyenkor a fenti szorzás éppen *a két mellékosztály részhalmazszorzatát* adja, ami persze nem függ attól, hogy mely elemekkel írtuk fel az elején azokat:

$$(aN)(bN) = (Na)(bN) = N(ab)N = (Nab)N = abNN = abN$$

Itt persze a sor elején jelölt szorzás a részhalmazszorzást jelenti és a két oldali mellékosztályok egyezését használjuk ki többször is.

A művelet tehát értelmes, nyilvánvalóan asszociatív (hiszen a G-beli szorzás az), egységelem az N (mellékosztály) és aN inverze $a^{-1}N$.
Eszerint (szándékunknak megfelelően) csoportot kaptunk:

2.2.22. Definíció: *Legyen G csoport, $N \triangleleft G$.*
*Az N szerinti mellékosztályok az $aN \circ bN \stackrel{def}{=} (ab)N$ szorzásra nézve csoportot alkotnak, melyet G-nek N szerinti **faktorcsoportjának** hívunk és G/N-nel jelölünk.*

A továbbiakban (némi pongyolasággal) a faktorcsoportbeli műveletet is a (legtöbbször ki sem írt) $\cdot$-tal jelöljük majd.

A korábbi $G = \mathbb{Z}$, $N = \{n\text{-nel osztható számok}\}$ példáinkat véve a G/N faktorcsoport éppen a szokásos $\mathbb{Z}_n$ (a szokásos maradékosztályösszeadással mint művelettel).
A következő pontból kiderül, hogy a faktorcsoport fogalma egy természetesebb fogalomhoz kapcsolódik.

2.3. Homomorfizmusok

Ebben a részben csoportok közötti leképezéseket fogunk vizsgálni.
Természetesen (ahogy pl. a vektorterek közötti függvényeknél is) most is csak

olyan leképezések érdekesek számunkra, amelyek megőrzik a struktúrát, azaz *tartják a műveletet*.

2.3.1. Definíció: *Legyen G és H csoport rendre a $\circ$ és $\bullet$ műveletekkel.*
*A $\varphi : G \to H$ függvényt G-ből H-ba menő **homomorfizmusnak** hívjuk, ha műveletartó, azaz $\forall g_1, g_2 \in G$ esetén $(g_1 \circ g_2)\varphi = (g_1)\varphi \bullet (g_2)\varphi$.*

Ha G tetszőleges csoport, akkor G identikus függvénye egy $G \to G$ homomorfizmus, másrészt ha H is tetszőleges csoport, akkor a $\varphi : G \to H,\ (g)\varphi \equiv e_H$ szintén egy homomorfizmus bármely G és H csoportok között. Kevésbé triviális példa az a $\mathbb{Z} \to 2\mathbb{Z} = \{\text{páros számok}\}$ függvény, melynél $z \mapsto 2z$.
A homomorfizmusok néhány elemi tulajdonságát foglaljuk össze a következő tételben:

2.3.2. Tétel: *Legyen G és H csoport, φ egy $G \to H$ homomorfizmus.*
Ekkor a következők teljesülnek:
*i) Ha $K \leq G$, akkor $(K)\varphi \leq H$. Speciálisan $(G)\varphi \leq H$, ez a (H-beli) részcsoport G **képe** (φ-nél), jele: $\operatorname{Im}\varphi$;*
ii) $(e_G)\varphi = e_H$ (ezek persze a megfelelő egységelemek);
iii) $(g^{-1})\varphi = \big((g)\varphi\big)^{-1}$;
*iv) Azok a $k \in G$ elemek, melyekre $(k)\varphi = e_H$, normálosztót alkotnak G-ben, melyet a homomorfizmus **mag**jának hívunk és $\operatorname{Ker}\varphi$-vel jelölünk.*
v) $N \triangleleft G$ esetén $(N)\varphi \triangleleft \operatorname{Im}\varphi$
és $M \triangleleft \operatorname{Im}\varphi$ esetén M teljes inverz képe normálosztó G-ben, azaz

$$(M)\varphi^{-1} = \{g \in G :\ (g)\varphi \in M\} \triangleleft G \quad .$$

Bizonyítás: i) Egyszerűen ellenőrizhetjük a csoportaxiómák teljesülését.
ii) $(e_G)\varphi$-vel való szorzás a művelettartás miatt minden elemet fixen hagy $\operatorname{Im}\varphi$-ben, így megegyezik annak H-val is egyező egységelemével.
iii) Hasonlóan érvelünk mint az előbb.

$iv)$ A „részcsoportság” azonnal adódik a művelettartásból. Legyen $n \in G$ olyan, hogy $(n)\varphi = e_H$ és $g \in G$ tetszőleges. Ekkor a művelettartás és $iii)$ miatt:

$$(g^{-1}ng)\varphi = (g^{-1})\varphi \cdot e_H \cdot (g)\varphi = e_H$$

így az 2.2.17. $iii)$ pontja szerint készen is vagyunk.

$v)$ Ugyanúgy igazolható, mint az előbbi állítás. ∎

Az $iv)$ pont szerint tehát ha „találunk” valamilyen $G \to H$ homomorfizmust, akkor annak magja egy G-beli normálosztó lesz.

Valójában a fordított állítás is igaz: *bármely normálosztó G-ben alkalmas G-ről menő homomorfizmus magja*. Legyen ugyanis $N \triangleleft G$ és tekintsük azt a

$\varphi : G \to G/N$ függvényt, melyre $(g)\varphi = gN \ \forall g \in G$. Ez a faktorcsoportbeli művelet definíciója miatt művelettartó, tehát egy homomorfizmus, másrészt a magja éppen N:

$gN = e_{G/N} = N \Leftrightarrow g \in N$, amint azt a mellékosztályoknál meggondoltuk.

Az előbb leírt homomorfizmust *természetes homomorfizmusnak* hívják.

Néhány speciális tulajdonsággal bíró homomorfizmusnak külön neve van:

2.3.3. Definíció: *Legyen G és H csoport.*

A $\varphi : G \to H$ homomorfizmust

$i)$ ***monomorfizmusnak** nevezzük, ha injektív;*

$ii)$ ***epimorfizmusnak** nevezzük, ha szürjektív;*

$iii)$ ***izomorfizmusnak** nevezzük, ha injektív és szürjektív.*

*Egy $G \to G$ homomorfizmust **endomorfizmusnak**, egy G-ről G-re menő izomorfizmust pedig **automorfizmusnak** nevezünk.*

Monomorfizmus pl. az egész számokat identikusan a valós számok additív csoportjába képező függvény (de ez nem epimorfizmus), epimorfizmus a természetes homomorfizmus bármely G és $N \triangleleft G$ esetén (de ez nem feltétlenül monomorfizmus). Izomorfizmus pl. az a $\mathbb{Z}_n$-ből az n-edik komplex egységgyökök halmazá-

ba menő φ függvény, melynél a (k) maradékosztály képe $\big((k)\big)\varphi = \cos\frac{2k\pi}{n} + + i\sin\frac{2k\pi}{n}$.
Endomorfizmusra példa a fentebb már említett $\mathbb{Z} \to 2\mathbb{Z}$ leképezés (ráadásul ez izomorfizmus), általában tetszőleges Abel-csoportban a *k-adik hatványozás*: $x \mapsto x^k$. Végül azokban az Abel-csoportokban, melyek nem ún. elemi kommutatív 2-csoportok (ezekről később lesz szó), nemtriviális automorfizmus az invertálás: $g \mapsto g^{-1}$. Megjegyzendő, hogy nem kommutatív csoportban ez a függvény (és általában a hatványozás) *nem feltétlenül műveletartó*.

Egyszerű észrevétel, hogy a G csoport *automorfizmusai a kompozícióra nézve* szintén csoportot alkotnak (melynek egységeleme G identikus függvénye), ezt G **automorfizmuscsoportjának** nevezzük és $\operatorname{Aut} G$-vel jelöljük.

A G és H csoportokat egymással **izomorfnak** mondjuk, ha van $G \to H$ izomorfizmus. Ezt így jelöljük: $G \cong H$.
Az elnevezés jogos, mert ha φ egy $G \to H$ izomorfizmus, akkor nyilvánvalóan φ^{-1} egy $H \to G$ izomorfizmus lesz. Természetesen $G \cong G$ és az is látható, hogy $G \cong H,\ H \cong K \Rightarrow G \cong K$ (az identikus függvény, illetve a megfelelő izomorfizmusok kompozíciója alkalmas izomorfizmusok lesznek). Pongyolán tehát úgy is fogalmazhatunk, hogy az „izomorfnak lenni” ekvivalenciareláció; ez azért nem helyes, mert (mint látni fogjuk) az *összes csoportok nem alkotnak halmazt*, így nem beszélhetünk ekvivalenciarelációról ezek halmazán.

Egy $\varphi : G \to H$ izomorfizmus jellemezhető a maggal és a képpel is. Nyilván $\operatorname{Im}\varphi = H$, hiszen definíció szerint φ szürjektív. Másrészt könnyű meggondolni, hogy φ pontosan akkor injektív, ha $\operatorname{Ker}\varphi = e$:
$\exists g_1 \neq g_2 \in G,\ (g_1)\varphi = (g_2)\varphi \Rightarrow e \neq g_1^{-1}g_2 \in \operatorname{Ker}\varphi$; azt már láttuk, hogy $e \in \operatorname{Ker}\varphi$, így ha más elemek is vannak a magban, akkor φ több helyen veszi fel e_H-t, tehát nem injektív. A következő tételt igazoltuk:

2.3.4. Tétel: *Legyen G és H csoport.*
A $\varphi : G \to H$ homomorfizmus pontosan akkor monomorfizmus, ha Ker $\varphi = e$ és pontosan akkor izomorfizmus, ha emellett Im $\varphi = H$ is teljesül.

Amint arra már többször is utaltunk, a most definiált izomorfizmus fogalmával lehet precízzé tenni a korábban csak a szemléletre alapozott azonosításokat a különböző alaphalmazokon értelmezett „lényegében azonos" csoportok között. Tehát pl. azt mondhatjuk, hogy az előbbi példában szereplő $\mathbb{Z}_n$ és $\left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 1,2,\ldots,n\right\}$ (a szokásos műveletekkel) „tulajdonképpen azonos" csoportok *izomorfia erejéig egyeznek.* Általában n elemű ciklikus csoportból és végtelen ciklikus csoportból is *izomorfia erejéig* egyféle van, ugyanis egy olyan függvény, amely a fenti példa szerint egy generátorelem megfelelő hatványait a másik csoport egy generátorelemének ugyanazon hatványaiba viszi, izomorfizmust jelent a két csoport között.
Ugyanígy, az a korábbi állításunk, hogy egy p elemű halmazon lényegében csak egyféleképpen lehet úgy műveletet értelmezni, hogy csoportot kapjunk, azt jelenti, hogy tetszőleges p elemű halmazokon értelmezett csoportok (páronként) izomorfak lesznek egymással. (Érdekességként, bizonyítás nélkül megjegyezzük, hogy az „n elemű halmazon izomorfia erejéig egyféle csoport van" állítás nem csak $n = p$-re igaz, hanem *Burnside* (egy) tétele szerint pontosan azon n-ekre, melyekre $\big(n, \varphi(n)\big) = 1$).
Természetesen amikor pl. azt mondjuk, hogy az összes p^2 elemű csoport szerkezetét ismerjük (ami, mint látni fogjuk, igaz), akkor ezt úgy értjük, hogy izomorfia erejéig ismerjük azokat.

Egy $V \to W$ vektortérhomomorfizmusnál (azaz lineáris leképezésnél) a képtér szerkezetét meghatározza V és a leképezés magtere; ezzel analóg módon egy $\varphi : G \to H$ csoporthomomorfizmusnál is G és Ker φ határozza meg a kép szer-

kezetét:

2.3.5. Tétel (Homomorfizmustétel): *Legyen G és H csoport, $\varphi : G \to H$ homomorfizmus. Ekkor*

$$G/Ker\,\varphi \cong Im\,\varphi.$$

Bizonyítás: Definiálunk egy α homomorfizmust $G/\mathrm{Ker}\,\varphi$-ről $(G)\varphi = \mathrm{Im}\,\varphi$-re, amiről belátjuk, hogy izomorfizmus. α legyen a következő:

$$g\mathrm{Ker}\,\varphi \mapsto (g)\varphi$$

Először is (mivel ismét halmazokon értelmeztünk műveletet az elemeik segítségével) be kell látnunk, hogy α jól definiált, azaz nem függ a reprezentáns választásától. Ez tényleg így van:

$$g\mathrm{Ker}\,\varphi = h\mathrm{Ker}\,\varphi \Leftrightarrow g^{-1}h \in \mathrm{Ker}\,\varphi \Leftrightarrow (g^{-1}h)\varphi = \big((g)\varphi\big)^{-1}(h)\varphi = e_H \Leftrightarrow$$
$$\Leftrightarrow (g)\varphi = (h)\varphi \Rightarrow (g\mathrm{Ker}\,\varphi)\alpha = (h\mathrm{Ker}\,\varphi)\alpha.$$

Tehát α jól definiált. A művelettartás nyilvánvalóan teljesül a faktorcsoportbeli művelet definíciója és φ művelettartása miatt. Így α epimorfizmus.
Másrészt $\mathrm{Ker}\,\alpha$ azokból a $g\mathrm{Ker}\,\varphi$ mellékosztályokból áll, melyekre $(g)\varphi = e_H$; de ezek éppen $\mathrm{Ker}\,\varphi = e_{G/\mathrm{Ker}\,\varphi}$-t alkotják, azaz α monomorfizmus (hiszen a magja csak az egységelemből áll). Az állítást ezzel igazoltuk. ∎

A homomorfizmustétel szerint egy csoport homomorf képei leírhatók, ha ismerjük az összes normálosztóját. Például ha G egyszerű csoport, akkor csak önmagával izomorf, vagy triviális homomorf képe lehet (hiszen bármely $G \to H$ homomorfizmus magja az egyszerűség miatt vagy e_G, vagy G).
Azt is látjuk, hogy ha G és H véges csoportok, melyekre $(|G|, |H|) = 1$, akkor csak triviális homomorfizmus mehet G-ből H-ba, hiszen $|G/\mathrm{Ker}\,\varphi|$ közös osztója $|G|$-nek és $|H|$-nak.

Most jöjjön egy példa arra, hogyan kereshetünk normálosztót úgy, mint egy

$G \to H$ homomorfizmus magját. $H \leq G$ esetén definiálhatjuk azt az $N_G(H) \to \operatorname{Aut} H$ homomorfizmust, amely $N_G(H) \ni n \mapsto \varphi_n \mid_H$ (azaz a normalizátor egy eleméhez a vele való konjugálás H-ra való megszorítását rendeljük); a következő pontban gondoljuk majd meg, hogy a konjugálás izomorfizmus (amihez még a művelettartás hiányzik), ezért jelen esetben egy $H \to H$ automorfizmus, továbbá azt, hogy az előbbi hozzárendelés tényleg művelettartó. Ennek a homomorfizmusnak a magját azok az $N_G(H)$-beli elemek alkotják, melyekkel való konjugálás H identikus függvénye, azaz annak minden elemét fixen hagyja; de ezek éppen a $C_G(H)$ centralizátor elemei. Tehát $H \leq G$ esetén a $C_G(H) \lhd N_G(H)$ összefüggésre egy újabb, „elegánsabb" bizonyítást nyertünk, sőt $H \lhd G$ esetén az adódik (számolásmentesen), hogy *normálosztó centralizátora is normálosztó*.

Most két alapvető tételt bizonyítunk a homomorfizmusokkal kapcsolatban.

2.3.6. Tétel:

1. **(Első izomorfizmus tétel)** Legyen G csoport, $N \lhd G$, $H \leq G$. Ekkor

$$H \cap N \lhd H \quad \text{és} \quad H/H \cap N \cong HN/N$$

2. **(Második izomorfizmus tétel)** Legyen G csoport, $M, N \lhd G$, $M \leq N$. Ekkor

$$G/N \cong {}^{G/M}\!/_{N/M}$$

Bizonyítás: **1.** Tekintsük a $\varphi : G \to G/N$ természetes homomorfizmus $\varphi \mid_H$ megszorítását H-ra! Ez egy $H \to G/N$ homomorfizmus, melynek magja természetesen $H \cap N$, amely eszerint (mint 2.3.2. iv)-ből tudjuk) normális részcsoportja H-nak.

Másrészt a homomorfizmustétel alapján $H/H \cap N \cong \operatorname{Im} \varphi_H$. Vegyük észre, hogy

H képe megegyezik az N-et tartalmazó HN részcsoport képével, hiszen mindkettő a $hN,\ h \in H$ alakú mellékosztályokból áll (mindkettő a G/N csoportban), amiről persze tudjuk, hogy HN/N (az $N \triangleleft NH$ észrevételt alkalmazzuk a $\varphi \mid_{HN}$ megszorítással).

Ezt összevetve a homomorfizmustétellel éppen a bizonyítandó állítást nyerjük.

2. Vizsgáljuk a következő $\varphi : G/M \to G/N$ leképezést:

$$(gM)\varphi = gN$$

Azt várjuk, hogy φ izomorfizmus.

Ennek belátásához megint azt kell meggondolnunk először, hogy a definíció értelmes: $gM = hM \Leftrightarrow g^{-1}h \in M \Rightarrow g^{-1}h \in N$ (mivel $M \leq N$) $\Leftrightarrow gN = hN$.

Világos, hogy φ művelettartó (mert a faktorcsoportokban „éppen jól” vannak definiálva a műveletek), és a szürjektivitás adódik a definícióból (gN előáll mint gM képe). Tehát már csak Ker φ meghatározása maradt hátra:

$gN = e_{G/N} \Leftrightarrow g \in N$; eszerint a mag a $gM,\ g \in N$ mellékosztályokból áll, melyek pontosan N/M-et alkotják.

A homomorfizmustételt felírva a bizonyítással készen vagyunk. ∎

Külön tételként mondjuk ki egy olyan következményét az előbbieknek, amelyet számos alkalommal fogunk használni a későbbiekben.

2.3.7. Tétel: *Legyen G csoport, $N \triangleleft G$.*

Ekkor a természetes homomorfizmus kölcsönösen egyértelmű megfeleltetést létesít G-nek N-et tartalmazó részcsoportjai és a G/N faktorcsoport részcsoportjai között.

A 2.3.2. v) pontja szerint normálosztók egymásnak felelnek meg.

Bizonyítás: Ha $N \leq M \leq G$, akkor (mint láttuk) M képe részcsoport G/N-ben, ami éppen $MN/N = \{mN \mid m \in M\}$, azaz M-nek N szerinti mellékosztályai alkotják a képet. Amennyiben M_1 és M_2 két különböző N-et tartalmazó

részcsoportja G-nek, akkor különböző N szerinti mellékosztályokból kell állniuk, így tehát más (G/N-beli részcsoport) lesz a képük.
Másrészt (2.3.2. iv) miatt) ha $M^* \leq G/N$, akkor M^* teljes inverz képe részcsoport G-ben, ami biztosan tartalmazza $e_{G/N}$ teljes inverz képét, azaz N-et.
Ezzel beláttuk, hogy a természetes homomorfizmus injektív és szürjektív kapcsolatot jelent a tételben szereplő részcsoportok között. ∎

Ebből következik például, hogy pontosan akkor nincs G-ben olyan M normálosztó, mely tartalmazza N-et, ha G/N *egyszerű csoport*; ennek később lesz még jelentősége.

Végül a homomorfizmusokkal kapcsolatban emeljünk ki még egy tulajdonságot. Ha $G \triangleright N$, és adott egy φ G-ről menő homomorfizmus, akkor a 2.3.2. tétel szerint $(G)\varphi \triangleright (N)\varphi$. Az említett fontos tulajdonság az, hogy $(G)\varphi/(N)\varphi$ *éppen a* G/N *faktorcsoport „képe* φ*-nél”*, ugyanis a természetes módon definiált $(gN)\varphi \overset{\text{def}}{=} (g)\varphi(N)\varphi$ egy homomorfizmusa G/N-nek, amelynél az a fenti csoportba megy át.

2.4. Konjugálás

A 2.2. pontban láttuk, hogy a G csoport g elemével való φ_g konjugálás egy $G \to G$ bijekciót jelent. Ott már jeleztük, hogy még egy fontos tulajdonsága van: ez éppen a *művelettartás*, azaz $(xy)\varphi_g = (x)\varphi_g(y)\varphi_g$ tetszőleges $g, x, y \in G$ esetén:

$$(xy)\varphi_g = g^{-1}xyg = \overbrace{g^{-1}xg}^{(x)\varphi_g}\overbrace{g^{-1}yg}^{(y)\varphi_g}.$$

Eszerint φ_g automorfizmusa G-nek; az ilyen automorfizmusokat (tehát a konjugálásokat) *belső automorfizmusoknak* is hívják (a nem belső automorfizmusok pedig a *külső* jelzőt kapják).

Nem nehéz meggondolni, hogy a G csoport belső automorfizmusai csoportot alkotnak a kompozíció műveletére nézve, mely természetesen részcsoport, sőt normálosztó $\operatorname{Aut} G$-ben; teljesül továbbá, hogy $(\varphi_g)^{-1} = \varphi_{g^{-1}}$. A „normálosztóság" igazolásához legyen $\alpha \in \operatorname{Aut} G$, vizsgáljuk meg, hogyan hat az $(\alpha)^{-1}\varphi_g\alpha$ szorzat (mely $\operatorname{Aut} G$ egy eleme) az $x \in G$ elemen:

$$(x)\big(\alpha^{-1}\varphi_g\alpha\big) = \Big(g^{-1}\big((x)\alpha^{-1}\big)g\Big)\alpha = \underbrace{\big((g^{-1})\alpha\big)}_{((g)\alpha)^{-1}}\underbrace{\big((x)\alpha^{-1}\big)\alpha}_{x}\big((g)\alpha\big) = (x)\varphi_{(g)\alpha}.$$

Tehát a φ_g belső automorfizmus tetszőleges automorfizmussal való konjugáltja is belső automorfizmus, így az 2.2.17. $iii)$ tétel szerint valóban normálosztó a konjugálásokból álló részcsoport.

2.4.1. Definíció: *Legyen G csoport.*
A $\varphi_g \ : \ g \in G$ konjugálások normálosztót alkotnak $\operatorname{Aut} G$-ben, melyet G ***belső automorfizmuscsoportjának*** *hívunk és $\operatorname{Inn} G$-vel jelölünk.*

Az elnevezésben a „belső" szó arra utal, hogy ezek az automorfizmusok természetes módon adódnak „magából a csoportból". Emellett pl. $\mathbb{Z}$-ben az $x \mapsto -x$ invertálás egy természetes módon adódó *külső* automorfizmus, ugyanis itt minden konjugálás identikus (sőt, az előbbi példa tetszőleges Abel-csoporttal elmondható, egyetlen (típusú) kivételtől eltekintve: $(\mathbb{Z}_2)^k$ esetén az invertálás egybeesik az identitással, ami persze konjugálás - hogy nincs más ellenpélda, az kiderül a 3.5. feladatból).

Tekintsük most azt a $\beta : \ G \to \operatorname{Inn} G$ függvényt, mely $g \mapsto \varphi_g$! Valójában β egy epimorfizmus, hiszen a definíciójából adódó szürjektivitás mellett művelettartó is:

$$(x)(\varphi_g\varphi_h) = h^{-1}g^{-1}xgh = (x)\varphi_{gh}.$$

Ebből következik, hogy $G/\operatorname{Ker}\beta \cong \operatorname{Inn} G$ a homomorfizmustétel szerint. $\operatorname{Ker}\beta$ azokból a G-beli elemekből áll, melyekkel való konjugálás G identikus függvénye, azaz minden elemet fixen hagy. Az előbbi $\forall x \in G \ g^{-1}xg = x$ feltételből a

már látott ekvivalens átalakítással a $\forall x \in G\ xg = gx$ feltételt nyerjük. Tehát azok az elemek alkotják β magját, melyek G minden elemével felcserélhetők (erről persze egyébként is rögtön látszik, hogy normális részcsoport G-ben). Ez nagyon fontos részcsoport:

2.4.2. Definíció: *A G csoport azon elemeinek halmazát, melyek minden $g \in G$-vel felcserélhetők, a csoport **centrumának** nevezzük és $Z(G)$-vel jelöljük.*
Azonnal látszik, hogy $Z(G) \triangleleft G$ és a fenti meggondolások szerint a centrum szerinti faktorcsoport a belső automorfizmuscsoporttal izomorf:

$$G/Z(G) \cong \mathit{Inn}\, G$$

A centrum definíciójából adódik, hogy $Z(G) = \bigcap_{x \in G} C_G(x) = C_G(G)$. Világos, hogy G pontosan akkor kommutatív, ha $Z(G) = G$. A „másik végletként" később azt is látni fogjuk, hogy pl. S_n centruma triviális (azaz csak az egységelemből áll), ha $n \geq 3$. Jegyezzük meg, hogy $Z(G)$ minden részcsoportja normálosztó G-ben, hiszen a centrumelemek tetszőleges részhalmaza zárt a konjugálásra.

Vizsgáljuk most a konjugálást más szemszögből. Vezessünk be egy relációt G-n:

$$g \sim k \text{ , ha } \exists\, x \in G,\ k = (g)\varphi_x \text{ (azaz } g\text{-nek konjugáltja } k)$$

A konjugálásról már elmondottakból egyszerűen adódik, hogy $\sim$ ekvivalenciareláció, így G ennek diszjunkt ekvivalenciaosztályaira bomlik; utóbbiakat **konjugáltosztályoknak** nevezzük. Az $[x]$ konjugáltosztályt ($x \in G$) x konjugáltjai alkotják. Látható, hogy az egyelemű konjugáltosztályokban *pontosan a centrum elemei* találhatók (melyeknek minden konjugáltjuk önmaga). Egy csoport konjugáltosztályainak szám(osság)át a csoport **osztályszámának** nevezzük és h-val jelöljük. Ha például G véges Abel-csoport, $|G| = n$, akkor $h = n$, hiszen minden konjugáltosztály egyelemű; eddigi meggondolásaink alapján ez a tulajdonság jellemzi is a véges kommutatív csoportokat.

Számoljuk meg, hány elem van az $[x]$ konjugáltosztályban (azaz mekkora a számossága); ehhez azt vizsgáljuk meg, hogy mikor konjugálja két elem (g és h ugyanoda x-et:

$$g^{-1}xg = h^{-1}xh \Leftrightarrow hg^{-1}xgh^{-1} = x \Leftrightarrow gh^{-1} \in C_G(x) \Leftrightarrow gC_G(x) = hC_G(x).$$

Azaz pontosan akkor konjugálják ugyanabba az elembe, ha ugyanabba az x centralizátora szerinti (mondjuk) baloldali mellékosztályba esnek. Eszerint $|[x]| = |G : C_G(x)|$ (mert a mellékosztályok halmazának számossága a részcsoport indexe).

Az előbbi gondolatmenetet egy $\emptyset \neq X \subseteq G$-re is alkalmazhatjuk, tehát kérdezhetjük, hogy egy nemüres X részhalmaznak hány konjugáltja van G-beli elemekkel. Valójában ezek a konjugáltak is egy ekvivalenciaosztály elemei, ugyanis figyeljük meg, hogy a *G csoport nemüres részhalmazaiból álló halmazon is ekvivalenciareláció a konjugáltság*. A fenti levezetés most a $|G : N_G(X)|$ eredményt adja. (Látjuk: ennek speciális esete az előző eredmény, hiszen egyetlen elem esetén a centralizátor és a normalizátor egybeesik).
Egy tételben összefoglaljuk ezeket a fontos összefüggéseket:

2.4.3. Tétel: *Legyen G csoport, $G \supseteq X \neq \emptyset$.*
Ekkor X-nek annyi konjugáltja van G-beli elemekkel, amennyi $|G : N_G(X)|$.
Speciálisan, ha $X = \{x\}$ egyelemű halmaz, akkor $N_G(x) = C_G(x)$ miatt ez $|G : C_G(x)|$-szel megegyezik.

Fenti eredményünk szerint tehát egy *G véges csoport minden konjugáltosztályának elemszáma osztója a csoport elemszámának* (hiszen az egy részcsoport indexe). Ebből azonnal levezethetünk egy nevezetes tételt, abból pedig egy másikat.

2.4.4. Tétel: *Legyen G olyan véges csoport, melynek elemszáma p^k, $k \geq 1$.*
Ekkor $|Z(G)| > 1$, azaz a centrum nem állhat csak az egységelemből.

Bizonyítás: Írjuk fel G elemszámát a diszjunkt konjugáltosztályok c_i $(i = 1, \ldots, n)$ elemszámainak összegeként, ahol feltehető, hogy $c_j : j = 1,2, \ldots, m$-mel a centrum elemeiből álló egyelemű konjugáltosztályok elemszámait (azaz 1-et) indexeltük:

$$|G| = p^k = \overbrace{c_1}^{=1} + \overbrace{c_2}^{=1} + \ldots + \overbrace{c_m}^{=1} + c_{m+1} + \ldots + c_n \ (*)$$

Itt p osztja az $(m+1)$-ediktől kezdve valamennyi tagot, hiszen innentől a nem centrumbeli elemek konjugáltosztályait soroltuk fel, amelyek egyrészt nem egyetlen elemből állnak, másrészt elemszámuk p^k osztója. Emiatt p osztja $\sum_{i=1}^{m} c_i =$ $= \sum_{i=1}^{m} 1 = m = |Z(G)|$-et is, hiszen osztja a bal oldalon lévő $|G|$-t. Ha egyetlen elemből (az egységelemből) állna a centrum, akkor $m = 1$, ami ellentmondás. ∎

A bizonyításban szereplő (*) összefüggést **osztályegyenletnek** hívják.
Most jöjjön a már jelzett nevezetes következmény:

2.4.5. Tétel: *Legyen G olyan csoport, melyre $|G| = p^2$.*
Ekkor G kommutatív.

Bizonyítás: G centruma az előbbi tétel szerint nem állhat egyetlen elemből, tehát vagy p elemű, vagy p^2 elemű, utóbbi esetben persze $G = Z(G)$, így készen vagyunk. Indirekt tegyük fel tehát, hogy $|Z(G)| = p$ és az egyszerűbb jelölés miatt legyen $Z = Z(G)$.
G/Z ciklikus (hiszen p elemű), azaz $G/Z = \{Z, aZ, a^2Z, \ldots, a^{p-1}Z\}$ valamely (bármely) $a \in G, a \notin Z$ elemmel. Mivel az összes Z szerinti mellékosztály uniója G, ezért G minden eleme felírható $a^k z$ alakban, ahol $z \in Z$.
Vegyük G két tetszőleges $g_1 = a^{k_1} z_1$ és $g_2 = a^{k_2} z_2$ elemét és szorozzuk őket össze a két lehetséges módon:

$$g_1 g_2 = a^{k_1} \underbrace{z_1 a^{k_2}}_{=a^{k_2} z_1} z_2 = a^{k_1+k_2} z_1 z_2$$
$$g_2 g_1 = a^{k_2} \underbrace{z_2 a^{k_1}}_{=a^{k_1} z_2} z_1 = a^{k_1+k_2} z_1 z_2.$$

Itt azt használtuk ki, hogy a z_i elemek a centrumban voltak, egy elem hatványai pedig egymással mindig felcserélhetők.
Előbbi eredményünk szerint azonban G kommutatív, hiszen bármely két eleme felcserélhető, ez ellentmondás, mert feltettük, hogy $Z(G) \neq G$. ∎

A fejezet következő pontjában kiderül majd, hogy ennek segítségével a p^2 rendű csoportok szerkezetét teljesen le tudjuk írni.
Érdemes észrevenni, hogy az előbb valójában a következő meglepő állítást is beláttuk:

Ha $G/Z(G)$ ciklikus, akkor G kommutatív.

(azaz a centrum szerinti faktor csak akkor lehet ciklikus, ha triviális, mert $G = Z(G)$ miatt egyetlen elemből áll).

2.5. Direkt és szemidirekt szorzat

2.5.1. A direkt szorzat

Ha adott két csoport, A és B, akkor könnyen „készíthetünk” egy újabbat úgy, hogy (halmazelméleti értelemben vett) direkt szorzatukat természetes módon felruházzuk egy művelettel. Végezzük ugyanis az $(a_1, b_1),\ (a_2, b_2) \in A \times B$ elemekkel a műveletet *komponensenként*, azaz a megfelelő csoportbeli művelettel összeszorozva a megfelelő komponenseket:

$$(a_1, b_1) \cdot_{A\times B} (a_2, b_2) \overset{\text{def}}{=} (\underbrace{a_1 a_2}_{A\text{-beli}\ \cdot}, \underbrace{b_1 b_2}_{B\text{-beli}\ \cdot})$$

Az így definiált műveletre nézve $A \times B$ csoportot alkot, melynek egységeleme (e_A, e_B) és $(a, b)^{-1} = (a^{-1}, b^{-1})$; ezek közvetlenül adódnak a definícióból. A kapott csoportot (is) $A \times B$-vel jelöljük, A-t és B-t *direkt faktoroknak* hívjuk.

Világos, hogy az $A^* = \{(a, e_B) \mid a \in A\}$, illetve $B^* = \{(e_A, b) \mid b \in B\}$ részcsoportok $A \times B$-ben, melyek rendre A-val illetve B-vel izomorfak, $A^*B^* = = A \times B$ és metszetük csak az ($A \times B$-beli) egységelemből áll.
Valójában ezek *normálosztók* is a direkt szorzatban, pl. lássuk be A^*-ről:

$$(a', b')^{-1}(a, e_B)(a', b') = (a'^{-1}aa', b'^{-1}e_Bb') = (a^*, e_B)$$

Előbbi definíciónk és meggondolásunk ugyanúgy végigvihető akkor, ha tetszőlegesen sok, de véges sok csoport direkt szorzatát definiáljuk. Tehát az A_i $(i = 1, \ldots, n)$ csoportok direkt szorzata az $(a_1, a_2, \ldots, a_n)$ „n komponensű vektorokból" áll, ahol a vektorokat komponensenként „szorozzuk össze".
Egységelem az $(e_{A_1}, e_{A_2}, \ldots, e_{A_n})$ lesz, az $A_i^* = \left\{(e_{A_1}, \ldots, e_{A_{i-1}}, a_i, e_{A_{i+1}}, \ldots, e_{A_n})\right\}$ $(a_i \in A_i)$ elemek egy A_i-vel izomorf normálosztót alkotnak, továbbá fennállnak a következők:

$$A_i^* \cap \langle A_j \mid j \neq i \rangle = e_{A_1 \times \ldots \times A_n} \quad \text{és} \quad A_1^*A_2^* \ldots A_n^* = A_1 \times A_2 \times \ldots \times A_n.$$

Ha *tetszőlegesen sok* csoport direkt szorzatáról akarunk beszélni, azaz adott a Λ indexhalmaz és a $\{G_\lambda : \lambda \in \Lambda\}$ csoportok, akkor a korábbi definíciónkat kétféle irányban is kiterjeszthetjük „természetes módon".

Egyrészt a szokásos (halmazelméleti) direkt szorzatnál maradva értelmezhetjük a $(g_\lambda) : g_\lambda \in G_\lambda$ esetleg „végtelen sok komponensű vektorokból" álló csoportot, ahol a vektorok λ-komponense a G_λ csoportból van és a műveletet a korábbiak szerint komponensenként végezzük. Itt értelemszerű módosításokkal igaz marad az egységelemről, inverzről, a (megfelelően definiált) G_λ^*-okról szóló észrevétel. Emellett azonban ha Λ végtelen halmaz, akkor sem a G_λ^* normálosztók szorzataként (amely a végtelen sok tényező miatt nem értelmes), sem azok generátumaként (amely végtelen sok tényező esetén is értelmes, de nem a most definiált csoportot adja) *nem áll elő* a csoport.
Az így értelmezett csoportot a G_λ csoportok **Descartes-szorzatának** nevezzük

majd (megkülönböztetve a most következő definíciótól).

Az előbbi „hiányosságon” úgy segíthetünk, hogy azt a részcsoportot tekintjük a G_λ-k Descartes-szorzatában, amelyben a vektoroknak *véges sok kivétellel minden komponense a megfelelő csopotbeli egységelem* („csak véges sok nemnulla elem van a sorozatban”). Ezt a G_λ-k **külső direkt szorzatának** hívjuk.
Könnyű belátni (a külső direkt szorzat „csoportságán” túlmenően), hogy ez normálosztó a Descartes-szorzatban. Persze a korábban már szereplő G_λ^* csoportok mind benne vannak a külső direkt szorzatban is (tehát normálosztók is benne) és ezúttal igaz lesz, hogy *ezek generátumaként a külső direkt szorzat előáll*.

Nyilvánvaló, hogy ha (amint a pont elején) csak véges sok csoportunk van, azaz Λ véges, akkor akkor *a két fogalom egybeesik*. Ezzel szemben pl. $\Lambda = \mathbb{N}$-et és $G_\lambda \equiv \mathbb{Z}_2$-t tekintve már a számosságok is eltérnek: a Descartes-szorzat számossága $2^{\aleph_0} = c$, míg a külső direkt szorzaté „csak” $\aleph_0$.
Az eddigieket az alábbi definícióban összegezzük:

2.5.1. Definíció: *Legyenek adva a $\{G_\lambda : \lambda \in \Lambda\}$ csoportok ($\Lambda \neq \emptyset$).*
*A G_λ csoportok **Descartes-szorzatának** nevezzük és $Cr_{\lambda\in\Lambda}G_\lambda$-val jelöljük azt a csoportot, mely a (g_λ) „vektorokból” áll, ahol a λ-komponens G_λ-ból való és a műveleteket komponensenként végezzük.*
*A G_λ csoportok **külső direkt szorzatának** nevezzük és $Dr_{\lambda\in\Lambda}G_\lambda$-val jelöljük azokat a (g_λ)-vektorokat, melyeknek λ-komponense G_λ-ból való és véges sok kivétellel minden komponens e_λ (a G_λ egységeleme); a műveleteket itt is komponensenként végezzük.*
G_λ^*-gal jelölve azon vektorokat, melyeknek a λ komponensén kívül minden komponense (a megfelelő) egységelem, teljesül, hogy

$$G_\lambda^* \lhd Cr_{\lambda\in\Lambda}G_\lambda \text{ és } G_\lambda^* \cap \left\langle G_\mu^* : \lambda \neq \mu \right\rangle = e_{Cr_{\lambda\in\Lambda}G_\lambda}.$$

Fennállnak ezenkívül a következők:
$Dr_{\lambda\in\Lambda}G_\lambda \lhd Cr_{\lambda\in\Lambda}G_\lambda$;

$Dr_{\lambda\in\Lambda}G_\lambda = \langle G_\lambda^* \mid \lambda \in \Lambda\rangle$;
Ha $|\Lambda| < \infty$, *akkor* $Dr_{\lambda\in\Lambda}G_\lambda = Cr_{\lambda\in\Lambda}G_\lambda$.

A fentiekben csoportokból mint építőkövekből hoztunk létre újabb csoportokat a direkt szorzat segítségével. Természetesen ennek fordítottja is ésszerű célkitűzés: adott G csoportot szeretnénk „felbontani" (pl.) $G = A \times B$ alakban; így a direkt faktorokkal már külön-külön lehetne műveleteket végezni és G szerkezetét jobban megértenénk. Az előbbit *direkt felbontásnak* hívják.
Ehhez persze először meg kell fogalmaznunk, hogy mit is értünk ezen a felbontáson, hiszen a csoport nem elempárokból/„vektorokból" áll, ellentétben a direkt szorzattal. Láttuk, hogy a külső direkt faktorok normálosztók, amelyek „lényegében diszjunktak" (az egységelemtől mint metszettől eltekintve) és generálják a külső direkt szorzatot; amint az alábbiakból kiderül, ez a három tulajdonság elég is ahhoz, hogy megragadjuk a direkt szorzat lényegét.

2.5.2. Definíció: *Legyen G csoport, $\{N_\lambda : \lambda \in \Lambda\}$ pedig olyan normálosztók G-ben, melyekre teljesülnek az alábbiak:*

$$\langle N_\lambda : \lambda \in \Lambda\rangle = G \text{ és } N_\lambda \cap \langle N_\mu : \mu \neq \lambda\rangle = e_G.$$

Ekkor azt mondjuk, hogy G az N_λ normálosztók ***belső direkt szorzata****.*

Egyszerű észrevétel, hogy az egymást csak az egységelemben metsző N_λ és N_μ normálosztók bármely két eleme felcserélhető egymással, ugyanis tekintsük $n_\lambda \in N_\lambda$, $n_\mu \in N_\mu$ esetén tekintsük a két elem ún. *kommutátorát* (az ilyen elemekről a 8. pontban részletesen lesz majd szó):

$$[n_\lambda, n_\mu] = \underbrace{\underbrace{n_\lambda{}^{-1} n_\mu{}^{-1} n_\lambda}_{\in N_\mu}\, n_\mu}_{\in N_\mu} = \underbrace{n_\lambda{}^{-1}\, \underbrace{n_\mu{}^{-1} n_\lambda n_\mu}_{\in N_\lambda}}_{\in N_\lambda} = e \qquad \text{és így}$$

$$n_\lambda n_\mu = n_\mu n_\lambda$$

Ezt és a definícióban lévő feltevéseket figyelembe véve fennáll, hogy G *minden eleme egyértelműen írható fel* $n_{\lambda_1}n_{\lambda_2}\cdot\ldots\cdot n_{\lambda_k}$ alakban, ahol a tényezők a megfelelő normálosztókból valók és a *sorrendjük nem számít*. Itt már csak az egyértelműséget kell meggondolnunk.

Legyen $g = n_{\lambda_1}n_{\lambda_2}\cdot\ldots\cdot n_{\lambda_k} = n_{\mu_1}n_{\mu_2}\cdot\ldots\cdot n_{\mu_\ell}$ két különböző felírás. A felcserélhetőség miatt feltehetjük, hogy a két oldalon nincsenek azonos indexű tagok (mert őket a tényezők sorrendjének átrendezésével és a szokásos inverzzel való szorzással egy oldalra csoportosíthatjuk) és persze egy-egy oldalon is minden szereplő index különböző (a tényezőket így csoportosítottuk), valamint $n_{\lambda_1} \neq e$ (egyébként le sem írjuk). Fejezzük ki ezután n_{λ_1}-et:

$$n_{\lambda_1} = n_{\mu_1}n_{\mu_2}\cdot\ldots\cdot n_{\mu_\ell}\cdot n_{\lambda_k}^{-1}n_{\lambda_{k-1}}^{-1}\ldots n_{\lambda_2}^{-1}.$$

Ez viszont ellentmond a feltevésnek, hiszen így:

$$e \neq n_{\lambda_1} \in \langle N_{\mu_1},\ldots,N_{\mu_l},N_{\lambda_2},\ldots,N_{\lambda_k}\rangle.$$

Belátható, hogy a direkt szorzat az előbbiekben bizonyított tulajdonságokkal is karakterizálható (ezt nem részletezzük).

Definiáljunk egy $\alpha : G \to Dr_{\lambda\in\Lambda}N_\lambda$ függvényt a következőképpen. Írjuk fel g-t az előbb látott $g = n_{\lambda_1}n_{\lambda_2}\cdot\ldots\cdot n_{\lambda_k}$ alakban és rendeljük ehhez azt az $(n_\lambda) \in Dr_{\lambda\in\Lambda}N_\lambda$ vektort, melynek λ_i komponense n_{λ_i} ($i = 1,2,\ldots,k$), a többi komponense pedig a megfelelő e_λ egységelem. Ekkor α jól definiált az imént látott egyértelműség miatt, másrészt nyilvánvalóan injektív és szürjektív, továbbá az n_λ tényezők felcserélhetősége miatt *művelettartó* is. α tehát izomorfizmus G és az adott normálosztók külső direkt szorzata között: $G \cong Dr_{\lambda\in\Lambda}N_\lambda$. Ez azt jelenti, hogy G-ben úgy számolhatunk, hogy *külön-külön végezzük a műveletet* a megadott normálosztókban; éppen ezt vártuk el a csoport egy direkt felbontásától, tehát a fent megkövetelt tulajdonságokkal azt jól karakterizáltuk.

Hasonlóan meggondolhatjuk, hogy ha az $\{N_\lambda\}$-kból „indulunk ki”, akkor (korábbi jelöléseinkkel) $Dr_{\lambda\in\Lambda}N_\lambda$ az N_λ^*-ok belső direkt szorzatával lesz izomorf.

Az előbbi meggondolások szellemében a későbbiekben ugyanazt a jelet használjuk majd a belső és a külső direkt szorzatra.

Alkalmazzuk most az elmondottakat arra, hogy - amint azt korábban ígértük - leírjuk a p^2 rendű csoportok szerkezetét.

2.5.3. Tétel: *Tegyük fel, hogy* $|G| = p^2$.
Ekkor $G \cong \mathbb{Z}_{p^2}$ *vagy* $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Bizonyítás: Azt már beláttuk 2.4.5.-ben, hogy G kommutatív. Ha G ciklikus (is), akkor persze $G \cong \mathbb{Z}_{p^2}$ és készen vagyunk.
Ha nem ciklikus, akkor az egységelemen kívül minden elem rendje p kell hogy legyen; válasszunk egy tetszőleges $m \neq e$ elemet és legyen $\langle m \rangle = M$. M tehát egy p elemű részcsoport, ami (lévén Abel-csoportban vagyunk) normálosztó is. Legyen $n \in G \backslash M$ és $\langle n \rangle = N$; N is egy p elemű normálosztó és persze
$M \cap N = e$ (prímrendű részcsoportok vagy egybeesnek, vagy csak az egységelemben metszik egymást). Az előbbi két normálosztó metszete tehát egyelemű és teljesül, hogy $NM = G$ (ui. $|NM| = \frac{|N||M|}{|N \cap M|} = p^2$).
Ez éppen azt mutatja, hogy $G \cong N \times M \cong \mathbb{Z}_p \times \mathbb{Z}_p$. ∎

A direkt felbontás hasznosságát illusztrálandó, bizonyítás nélkül álljon itt az egyik legelső struktúratétel a csoportelmélet történetében, amelyből többek között az előbbi állítás is könnyedén adódik:

2.5.4. Tétel (A véges Abel-csoportok alaptétele): *Ha G véges Abel-csoport, akkor G egyértelműen felbontható prímhatványrendű ciklikus csoportok direkt szorzatára, azaz* $G \cong \mathbb{Z}_{p_1}^{k_1} \times \mathbb{Z}_{p_2}^{k_2} \times \ldots \times \mathbb{Z}_{p_s}^{k_s}$ *(p_i nem feltétlenül különböző prímek).*

Végül jegyezzük meg, hogy nem minden csoport bontható fel nemtriviálisan direkt szorzatra (azaz úgy, hogy egyik direkt faktor sem az egyelemű csoport), pl.

az egyszerű csoportok ilyenek, de a fentiek értelmében ilyen $\mathbb{Z}_{p^2}$ is, amely csak $\mathbb{Z}_p \times \mathbb{Z}_p$ alakú lehetne, de utóbbi csoportban minden $\neq e$ elem p-edrendű, míg az előbbiben van p^2 rendű elem is, tehát nem izomorfak (persze az előbb kimondott alaptételre is hivatkozhattunk volna).

2.5.2. A szemidirekt szorzat

Egy másik módszert mutatunk arra, hogyan lehet két csoportból egy újabb csoportot létrehozni. Ezúttal a „belülről kifelé” irány tűnik természetesebbnek, így ennek ismertetésével kezdjük, majd ebből kiindulva megfogalmazzuk a (célként kitűzött) másik irány definícióját is.

2.5.5. Definíció: *Tegyük fel, hogy adott a G csoportban egy N normálosztó és egy H részcsoport, melyekre a következők teljesülnek:*

$$HN = G \quad \text{és} \quad N \cap H = e.$$

*Ekkor G-t H és N **belső szemidirekt szorzatának** hívjuk, amit így jelölünk:*

$$G = N \rtimes H \quad \text{vagy} \quad G = H \ltimes N.$$

*H-t az N **komplementumának** hívjuk.*

Vegyük észre, hogy a feltételek mellett G minden eleme *egyértelműen* írható hn alakban, ahol $h \in H,\ n \in N$:

$$h_1n_1 = h_2n_2 \Leftrightarrow \underbrace{h_2^{-1}h_1}_{\in H} = \underbrace{n_2n_1^{-1}}_{\in N} \Rightarrow h_2^{-1}h_1 = n_2n_1^{-1} = e \Rightarrow h_1 = h_2,\ n_1 = n_2$$

Hogyan tudunk összeszorozni két elemet G-ben a H-beli és az N-beli „komponenseik” segítségével?

$$\big(h_1n_1\big)\big(h_2n_2\big) = h_1h_2\overbrace{h_2^{-1}n_1h_2}^{(n_1)\varphi_{h_2}}n_2 = \overbrace{\big(h_1h_2\big)}^{\in H}\overbrace{\big((n_1)\varphi_{h_2}n_2\big)}^{\in N}.$$

Itt az egyértelmű felírás mellett azt használtuk ki, hogy N normálosztó; ez az *egyetlen felírása* a szorzatnak hn alakban.

Előbbi meggondolásunk azt mutatja, hogy G izomorf azzal a csoporttal, melynek elemei $(h,n) : h \in H,\ n \in N$ párok, és a művelet:

$$\big(h_1, n_1\big)\big(h_2, n_2\big) = \big(h_1 h_2, (n_1)\varphi_{h_2} n_2\big)$$

ami persze úgy értendő, hogy H-nak a konjugálással való hatását N-en „használjuk műveletként". A direkt szorzatnál elmondottakkal összevetve az is látható, hogy az „erősebb" $G \cong H \times K$ állításhoz pontosan az kell, hogy H bármely elemével való konjugálás minden $n \in N$-et fixen hagyjon (ekkor ugyanis H is normálosztóvá válik és persze „továbbra is" $H \cap K = e$).

Ebből kiindulva legyen most adva H és N két csoport és egy $\varphi : H \to \mathrm{Aut}\, N$ homomorfizmus (az előbbi konjugálást „általánosítjuk"). Jelölje φ_h a $h \in H$ képét az előbbi homomorfizmusnál. Definiáljunk egy, a fentivel megegyező „alakú" műveletet a $\{(h,n) :\ h \in H, n \in N\}$ halmazon annyi „vizuális" eltéréssel, hogy *hatványként jelöljük a képet* (alább világossá váló áttekinthetőségi okból):

$$(h_1, n_1)(h_2, n_2) \stackrel{\text{def}}{=} (h_1 h_2, n_1^{\varphi_{h_2}} n_2)$$

Jegyezzük meg, hogy a művelet értelmes a kiinduló feltevések miatt. Azt állítjuk, hogy csoportot kaptunk; ehhez most (mivel nem egy nagyobb struktúra részstruktúrájáról van szó, így nem vizsgálhatunk „részcsoportságot") ellenőrizzük a csoportaxiómákat:

$i)$ *asszociativitás*:

$\big((h_1, n_1)(h_2, n_2)\big)\big(h_3, n_3\big) = \big(h_1 h_2, n_1^{\varphi_{h_2}} n_2\big)\big(h_3, n_3\big) = \big(h_1 h_2 h_3, n_1^{\varphi_{h_2}\varphi_{h_3}} n_2^{\varphi_{h_3}} n_3\big)$;

másrészt

$\big(h_1, n_1\big)\big((h_2, n_2)(h_3, n_3)\big) = \big(h_1, n_1\big)\big(h_2 h_3, n_2^{\varphi_{h_3}} n_3\big) = \big(h_1 h_2 h_3, n_1^{\varphi_{h_2 h_3}} n_2^{\varphi_{h_3}} n_3\big) =$

$= \big(h_1 h_2 h_3, n_1^{\varphi_{h_2}\varphi_{h_3}} n_2^{\varphi_{h_3}} n_3\big)$.

Itt egyrészt azt használtuk ki, hogy φ művelettartó leképezés H-ból $\mathrm{Aut}\, N$-be, másrészt hogy φ_h egy művelettartó leképezés N-ből N-be (bármely $h \in H$-ra); látható, hogy valóban *asszociatív* a fent definiált művelet.

$ii)$ *egységelem* persze az (e_H, e_N) lesz; ez rögtön látszik abból, hogy $\varphi_{e_H} = id_N$ kell hogy legyen a 2.3.2. $ii)$ tulajdonság miatt.
$iii)$ *inverz*: $(h,n)^{-1} = \left(h^{-1}, (n^{\varphi_{h^{-1}}})^{-1}\right)$; ezt csak ki kell számolni.
Így a kapott struktúra tényleg csoport:

2.5.6. Definíció: *Legyenek adva a H és N csoportok és egy $\varphi : H \to Aut\, N$ homomorfizmus.*
*Ekkor a $\{(h,n) : h \in H, n \in N\}$ halmaz a $(h_1,n_1)(h_2,n_2) = (h_1h_2, n_1^{\varphi_{h_2}} n_2)$ műveletre nézve csoportot alkot, melyet H és N **külső szemidirekt szorzatának** hívunk.*
A definíció persze függ a φ függvénytől, így ezt mindig meg kell adnunk.

Természetesen azt várjuk, hogy itt is egy meghatározott értelemben izomorf kapcsolat van a két eltérően definiált „külső” és „belső” fogalom között. Valóban, tekintsük N és H előbbi külső szemidirekt szorzatában az $N^* = \{(e_H, n) : n \in N\}$ és a $H^* = \{(h, e_N) : h \in H\}$ részhalmazokat. Könnyen adódik, hogy ezek részcsoportok, melyek metszete persze az egységelem és a teljes csoportot generálják. Sőt, várakozásainknak megfelelően N^* még *normálosztó* is, ami a művelet definíciójából azonnal következik (egy tetszőleges elemmel való konjugálásnál a „H-beli komponensek egyszerűen kiejtik egymást”).
Ez éppen azt mutatja, hogy a külső szemidirekt szorzat a H^* és N^* belső szemidirekt szorzatával izomorf, ahol a H^* elemeivel való *konjugálás* a φ által meghatározott módon hat N elemein.
Persze itt is tekinthetjük a dolgot fordítva: ekkor azt a (fentebb már szereplő állítást) kapjuk, hogy a $G = HN$ belső szemidirekt szorzat az $N^* = \{(n, e_H) : n \in N\}$ és $H^* = \{(h, e_N) : h \in H\}$ csoportok külső szemidirekt szorzatával izomorf, ahol a definícióban szereplő $\varphi : H^* \to \mathrm{Aut}\, N^*$ függvényt a H-nak N-en való konjugálása adja.

Az előbbi izomorfiára támaszkodva későbbiekben a külső szemidirekt szorzatra is a $\ltimes$ illetve $\rtimes$ jeleket használjuk majd.

Példaként álljon itt D_n, amely a forgatásokból álló $\langle f \rangle$ n-edrendű ciklikus csoportnak (mint normálosztónak) és a $\langle t \rangle$ másodrendű csoportnak szemidirekt szorzata, ahol a t-vel való konjugálás az *invertálás*:

$$D_n = \langle f \rangle \rtimes \langle t \rangle\,;\ t^{-1}f^k t\big(= tf^k t = (t^{-1}ft)^k\big) = f^{-k}$$

2.6. A Sylow-tételek

Ebben a pontban néhány fontos tételt bizonyítunk véges csoportokra, melyeket számos feladatban fogunk majd használni. Némi előkészülettel kezdjük.

2.6.1. Definíció: *Legyen p prím.*
*Egy G csoportot **p-csoportnak** hívunk, ha minden elemének rendje p-nek valamilyen (≥ 0 kitevőjű) hatványa.*

A Lagrange-tételből következik, hogy minden véges p^k elemű csoport p-csoport. Vannak azonban végtelen p-csoportok is, ahogy a következő példánk mutatja. Legyen p prím és C_k a p^k-adik komplex egységgyökök csoportja a szorzásra nézve. Ekkor nyilván $C_k \leq C_\ell$, ha $k \leq \ell$ és így nem nehéz belátni, hogy $\bigcup_k C_k$ szintén csoport, melyet *kváziciklikus p-csoportnak*, vagy p^∞ típusú *Prüfer-csoportnak* hívnak. Ennek tetszőleges eleme benne van valamely C_k-ban, így rendje p-hatvány. A véges p-csoportokról ejtünk még pár szót később.

A Lagrange-tételből természetesen nem következik a fenti állítás megfordítása. Megtörténhetne például, hogy egy 30 elemű csoportban az egységelemen kívül csak 3 és 5 rendű elemek vannak. Azonban mégsem ez a helyzet: bizonyos számok biztosan előfordulnak mint valamely elem rendje, feltéve persze, hogy

osztói a csoport elemszámának; ezek a számok a *prímek.* Következzen *Cauchy* tételének rendkívül szellemes, *James H. McKay*-től származó bizonyítása.[6]

2.6.2. Tétel (Cauchy): *Tegyük fel, hogy a p prím osztója a G véges csoport elemszámának.*
Ekkor van G-ben p-edrendű elem.

Bizonyítás: Legyen $|G| = n$.
Tekintsük azokat a G^p-beli p komponensű $(g_1, g_2, \ldots, g_p)$ „vektorokat", azaz rendezett p-eseket, melyekre $g_1 g_2 \cdot \ldots \cdot g_p = e$, jelölje ezek halmazát H.
(Ilyen pl. a csupa e-ből álló p komponensű vektor, tehát H nemüres.)
Hány eleme van H-nak? A vektorok első $p-1$ elemét bárhogyan választhatjuk, az utolsót ez már egyértelműen meghatározza (az ui. a többiek szorzatának inverze kell hogy legyen). Eszerint $|H| = n^{p-1}$, ami persze p-vel osztható ($p \mid n$ miatt).
Vegyük észre, hogy egy vektorból nagyon „szemléletes módon" kaphatunk egy másik H-beli vektort úgy, hogy „mod p jobbra eltoljuk", azaz

$$(g_1, g_2, \ldots, g_p) \mapsto (g_p, g_1, \ldots, g_{p-1})$$

Ez tényleg H-ban lesz, mert az eltolás annak felel meg, hogy a $g_1 g_2 \ldots g_p = e$ szorzatot jobbról g_p^{-1}-nel, balról g_p-vel megszoroztuk, ami így szintén e lesz.
Jelöljük az előbbi „transzformációt" E-vel, egymás után alkalmazásait pedig E^k-val, ahol persze a „balra tolást" jelentő negatív k értékek is értelmesek.
Most H-n könnyedén értelmezhetünk egy $\sim$ relációt:
Legyen $\underline{u} \sim \underline{v}$, ha $\underline{v} = E^k(\underline{u})$, azaz H elemeit mint vektorokat jelölve $\underline{u}$ és $\underline{v}$ álljanak relációban, ha az E-t valahányszor egymás után alkalmazva $\underline{u}$ a $\underline{v}$-be megy át.
$\sim$-ről rögtön látszik, hogy ekvivalenciareláció, egy ekvivalenciaosztályban egy vektor elforgatottjai vannak. Hány elemet jelent ez? Természetesen E^p mindenkit fixen hagy és így a(z elem)rendnél látott megfontolással ha az r-edik
$(r > 0)$ a legkisebb hatványa E-nek, mely egy adott vektort önmagába visz, akkor

p-nek osztja r és így $r = 1$ vagy p (maradékosan osztjuk r-rel p-t).
Az $r = 1$ pontosan azt jelenti, hogy a *vektor minden komponense azonos*, tehát az vagy a csupa e-ből álló vektor, vagy egy olyan vektor, melynek minden komponense egy $a \in G$ p-edrendű elem. A többi vektort tartalmazó ekvivalenciaosztály az előbbiek szerint p elemű.
Írjuk fel $|H|$-t mint az ekvivalenciaosztályok elemszámainak összegét!

$$|H| = 1 + \underbrace{1 + \ldots + 1}_{k \text{ db}} + \ell \cdot p.$$

Itt az első 1-es a „csupaegy” vektor, a k db 1-es a p-edrendű elemekből álló vektorok (esetleg $k = 0$, azaz egy ilyen sincs), az $\ell \cdot p$ pedig az ℓ db többi p elemű ekvivalenciaosztály. De itt p osztja $|H| = n^{p-1}$-t és persze osztja ℓp-t, ezért osztja $1 + k$-t is, így $k = 0$ nem lehetséges.
Ebből adódik, hogy van p-edrendű elem, amint állítottuk. ∎

Cauchy tétele mutatja, hogy pl. a fenti példánkban szereplő 30 elemű csoportban biztosan lesznek olyan elemek, melyek rendje 2,3 és 5; az is kiderül továbbá belőle, hogy a véges p-csoportok *pontosan* a p-hatvány rendű csoportok. Érdemes hozzátennünk, hogy $p = 2$-re a Cauchy-tétel egy teljesen elemi meggondolással is kijön: az $x \mapsto x^{-1}$ egy olyan „majdnem párosítás”, amely csak az egységelemnél és a másodrendű elemeknél (ui. pontosan ezekre igaz az $x = x^{-1}$ összefüggés) nem működik, eszerint bármely véges csoportban ezeken kívül páros sok elem van, tehát páros elemszámú csoportban kell lennie másodrendű elemnek is.
Látni fogjuk, hogy a Cauchy-tétel megfelelője *semmilyen m összetett számra nem igaz (így a prímhatványokra sem)*, azaz bármely m összetett számra van olyan G véges csoport, hogy m osztja $|G|$-t, de nincs G-ben m-edrendű elem.

Más értelemben azonban, ha nem egy elem, hanem egy *részcsoport rendjét* értjük alattuk, mégis kitüntetett szerepet játszanak bizonyos összetett számok, nevezetesen a *prímhatványok*, a véges csoportoknál.

Erről szólnak a most következő *Sylow-tételek.*

2.6.3. Definíció: *Legyen G véges csoport.*
*A $P \leq G$ részcsoportot G **p-Sylow részcsoportjának** nevezzük, ha $|P| = p^k,\ k \geq$ ≥ 1, ahol $p^k \mid |G|$, de $p^{k+1} \nmid |G|$.*

Egyáltalán nem nyilvánvaló, hogy egyáltalán létezik p-Sylow részcsoport, de ez így van:

2.6.4. Tétel (Sylow I. tétele): *Legyen G véges csoport, $|G| = p^k \ell$, ahol $k \geq$ $\geq 1,\ (\ell, p) = 1$.*
Ekkor G tartalmaz p-Sylow részcsoportot.

Bizonyítás: $|G| = n$-re vonatkozó indukciót használunk; $n = 1$-re persze az állítás igaz. Tegyük fel, hogy n-nél kisebb rendű csoportokra már beláttuk az állítást és vizsgáljuk most G-t. Két esetet különböztetünk meg:

$i)$ *G centrumának elemszáma p-vel osztható.* Ekkor van $Z(G)$-ben p-edrendű elem Cauchy tétele miatt; legyen ez z. A centrum minden részcsoportja normálosztó G-ben, így $\langle z \rangle$ egy p elemű normálosztó. Ekkor a $G/\langle z \rangle$ csoportra alkalmazhatjuk az indukciós feltevést, hiszen ennek $|G/\langle z \rangle| = \frac{n}{p}$ elemszáma kisebb mint n, így ez tartalmaz p^{k-1} elemű részcsoportot. Ennek a teljes inverz képe (a homomorfizmustétel szerint) egy p^k elemű, azaz egy p-Sylow részcsoport lesz G-ben.

$ii)$ *$|Z(G)|$-t nem osztja p.* (Ilyen véges csoportok egyébként léteznek, pl. mint már említettük, S_5 centruma egyelemű.) Ekkor írjuk fel a 2.4.4. tétel bizonyításánál megismert osztályegyenletet:

$$n = |Z(G)| + c_{m+1} + \ldots + c_s.$$

Itt $i = m+1, \ldots, s$-sel a nem centrumbeli elemek konjugáltosztályainak elemszámait indexeltük. Mivel p osztja n-et és nem osztja $|Z(G)|$-t, így valamely c_i-t

sem osztja. Eszerint ha a tetszőleges elem ebből a konjugáltosztályból, akkor $c_i = |G : C_G(a)| = \frac{n}{|C_G(a)|}$ nem osztható p-vel, ezért $|C_G(a)| = p^k \cdot s$, ahol $s < \ell$, mert a nem a centrumban van, ezért centralizátora nem a teljes csoport.
Az indukciós feltevés alapján ez a centralizátor tartalmaz egy p-Sylow részcsoportot, ami jelen esetben (az elemszáma miatt) G-nek is p-Sylowja. A bizonyítással készen vagyunk. ∎

Most már tudjuk, hogy léteznek a p-Sylow részcsoportok, így rögtön felmerül két további kérdés: (izomorfia erejéig) *hányféle* van és összesen *hány db* van belőlük? A második kérdésre adandó válasz biztosan függ az adott csoport szerkezetétől (nem csak az elemszámtól), hiszen pl. $\mathbb{Z}_{10}$-ben a 2.2.12. tétel alapján csak egyetlen ciklikus 2-Sylow van, míg D_5-ben mind az öt tükrözés egy-egy 2 elemű 2-Sylowot generál (amelyek persze mind ciklikusak). Ebben a két példában a 2-Sylowok kételeműek voltak, így persze izomorfak egymással; az alábbiakból kiderül, hogy ez mindig így van, méghozzá egy „jól ismert” izomorfizmus viszi a p-Sylowokat egymásba.
A fenti kérdésekre választ adó II. és a III. Sylow-tételt egyszerre mondjuk ki és bizonyítjuk.

2.6.5. Tétel:

i) **Sylow II. tétele:** Jelölje $\mathrm{Syl}_p(G)$ a G véges csoport p-Sylow részcsoportjaiból álló halmazt.
Ekkor teljesül: $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \ (mod\, p)$.

ii) **Sylow III. tétele:** A G véges csoport p-Sylow részcsoportjai egymás konjugáltjai.

Bizonyítás: Jelölje (a normális lezárttól való megkülönböztetés miatt) ${}^GP$ egy tetszőleges $P \in \mathrm{Syl}_p(G)$ G-beli konjugáltjaiból álló halmazt: ${}^GP = \{g^{-1}Pg \mid g \in G\}$.

Mivel a konjugálás izomorfizmus G-n, így minden részcsoportján is az, tehát ez a halmaz p-Sylow részcsoportokból áll. Azt fogjuk megmutatni, hogy ${}^GP \equiv$ $\equiv 1 \ (mod\, p)$, másrészt ez az összes p-Sylow részcsoportot tartalmazza.

Legyen H egy tetszőleges (rögzített) p-Sylow részcsoport. Ennek elemeivel való konjugálások is persze a p-Sylow részcsoportokat permutálják. Vezessünk be egy ekvivalenciarelációt ${}^GP$-n:

$$K_1 \sim K_2, \text{ ha } K_2 = h^{-1}K_1h \text{ valamely } h \in H\text{-ra } (K_1,\ K_2 \in {}^GP) \quad .$$

Ez ${}^GP$ elemeit diszjunkt ekvivalenciaosztályokba sorolja, mégpedig pontosan a $H \in \mathrm{Syl}_p(G)$ elemeivel való konjugáltság szerint. Hány elemű lesz a $[K]$ ekvivalenciaosztály? Ezt ugyanúgy gondolhatjuk meg, ahogy a konjugáltosztályok elemszámát vizsgáltuk:

$$h_1^{-1}Kh_1 = h_2^{-1}Kh_2 \Leftrightarrow \underbrace{h_2h_1^{-1}}_{\in H}Kh_1h_2^{-1} = K \Leftrightarrow h_2h_1^{-1} \in H \cap N_G(K) \Leftrightarrow$$
$$\Leftrightarrow h_1H \cap N_G(K) = h_2H \cap N_G(K)$$

Azt látjuk tehát, hogy K konjugáltjainak száma éppen annyi, ahány $H \cap N_G(K)$ szerinti bal oldali mellékosztály van H-ban, azaz $|H : H \cap N_G(K)|$. Most meggondoljuk, hogy ez az index „általában” nem 1, tehát általában p-vel osztható (mivel a H p-csoport elemszámának osztója):

(*) Állítás: $H \neq K \Rightarrow |H : H \cap N_G(K)| > 1$. (Később még hivatkozunk majd erre, ezért a (*) megjelölés).

Ugyanis tegyük fel indirekt, hogy az index 1, azaz (ami ugyanezt jelenti) $H = H\cap$ $\cap\, N_G(K)$ és így $H \leq N_G(K)$. Ekkor legyen $x \in H$ olyan elem, melyre $x \notin K$; ilyen elem biztosan létezik, hiszen H és K p-Sylow részcsoportok, így egyik sem lehet része a másiknak. Tekintsük a $L = \langle K, x\rangle$ részcsoportot! Mivel feltevésünk szerint $H \leq N_G(K)$, így $L \leq N_G(K)$, tehát $K \lhd L$, így a normálosztókról szóló pontban lévő meggondolás (és a generált részcsoport legszűkebbségi tulajdonsága) miatt $L = \langle K, x\rangle = \langle K, \langle x\rangle\rangle = K\,\langle x\rangle$. Számoljuk ki L elemszámát! A 2.2.14. tétel szerint $|L| = |K\,\langle x\rangle| = \frac{|K||\langle x\rangle|}{|K\cap\langle x\rangle|}$. Ez p-nek egy hatványa, hiszen a tört-

ben szereplő minden szám ilyen, másrészt szigorúan nagyobb kell hogy legyen, mint $|K|$, ugyanis $x \notin K$ miatt $\langle K, x\rangle > K$. Így ellentmondásra jutottunk, hiszen K egy p-Sylow részcsoport volt G-ben, ezért nem lehet nála nagyobb elemszámú p-részcsoportot találni.

Azt kaptuk tehát, hogy a fenti osztályokba sorolásnál minden olyan ekvivalenciaosztály elemszáma osztható p-vel, mely valamely H-tól különböző K p-Sylow konjugáltjaiból áll.

Legyen most $H = P$. Ekkor persze (fenti jelölésünket értelemszerűen használva) ${}^{H}P = \{P\}$ és a többi ekvivalenciaosztály elemszáma p-vel osztható. Ebből adódik, hogy $\left|{}^{G}P\right| \equiv 1 \,(\mathrm{mod}\, p)$. Tegyük fel, hogy van olyan $H \in \mathrm{Syl}_p(G)$, melyre $H \notin {}^{G}P$! Ez alapján készítve az osztályba sorolást azt kapjuk, hogy $\left|{}^{G}P\right| \equiv$ $\equiv 0 \,(\mathrm{mod}\, p)$ (mert most minden ekvivalenciaosztály elemszáma p-vel osztható), ami ellentmondás.

Ez éppen azt jelenti, hogy $\mathrm{Syl}_p(G) = {}^{G}P$, azaz az összes p-Sylow részcsoport megkapható úgy, mint valamelyik (bármelyik) p-Sylow konjugáltja. Amint kiderült, $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \,(\mathrm{mod}\, p)$. ∎

Előbbi eredményünk szerint a véges G csoport p-*Sylowjai egymással (páronként) izomorfak*. Jegyezzük meg, hogy a normalizátornál elmondottak szerint egy $P \in$ $\in \mathrm{Syl}_p(G)$ részcsoportnak $|G : N_G(P)|$ számú konjugáltja van G-beli elemekkel, amit előbbi eredményünkkel összevetve $\left|\mathrm{Syl}_p(G)\right| = |G : N_G(P)|$, ahol P egy tetszőleges p-Sylow részcsoport G-ben. Azt is látjuk, hogy a p-Sylow(ok) *pontosan akkor normálosztó(k), ha 1 van belőlük,* azaz $|G : N_G(P)| = 1$ (ekkor teljesül ugyanis, hogy a egyetlen p-Sylow minden konjugáltja önmaga, a konjugáltak pedig $\mathrm{Syl}_p(G)$-t alkotják). Egyszerű észrevétel még, hogy egy p-részcsoport pontosan akkor p-Sylow részcsoport, ha az indexe relatív prím p-hez.

Most illusztráljuk a Sylow-tételek alkalmazását egy egyszerű állítással: nem létezik 51 elemű egyszerű csoport. Ugyanis legyen $|G| = 51 = 3 \cdot 17$ és vizsgáljuk a(z I. tétel miatt létező) 17-Sylowokat! Ezek számáról tudjuk, hogy $\equiv 1 \pmod{17}$, másrészt megegyezik $|G : N_G(P)|$-vel, ami az indexek szorzástétele miatt (2.2.8.) osztója $|G : P| = 3$-nak. Az előbbi két feltétel szerint egyetlen 17-Sylow van, ami így (nemtriviális) normálosztó, tehát G nem egyszerű. A 3. fejezet néhány feladatában ezt általánosítjuk majd többféle értelemben is.

Emeljünk ki egy (további) lényeges következményt. Ehhez először figyeljük meg, hogy a II. és III. Sylow-tétel bizonyításában szereplő $(*)$ állítás igazolásához tulajdonképpen csak annyit használtunk ki, hogy $H \leq G$ egy olyan p-(rész)csoport, mely nem része a K-(p-Sylow)nak. A teljes bizonyítás ezt megelőző része pedig tetszőleges $H \leq G$-vel elmondható. Ezek szerint ha H egy tetszőleges p-részcsoportja G-nek, és *feltesszük, hogy H nincs benne egyik p-Sylowban sem* (ami elvileg megtörténhetne), akkor ugyanúgy a $\left|{}^G P\right| \equiv 0 \pmod{p}$ ellentmondásra jutunk, mint ott. Ezzel beláttuk a következőt:

A G véges csoport minden p-részcsoportja benne van egy p-Sylow részcsoportban.

Végül még két állítást igazolunk a Sylow-részcsoportokról, melyekre később szükségünk lesz.

2.6.6. Tétel:

i) Legyen G véges csoport, $P \in \mathrm{Syl}_p(G)$ és $N_G(P) \leq H \leq G$.
Ekkor $H = N_G(H)$.

ii) Ha $N \triangleleft G$, akkor $N \cap P \in \mathrm{Syl}_p(N)$ és $PN/N \in \mathrm{Syl}_p(G/N)$, azaz normálosztót egy p-Sylow a saját p-Sylowjában metsz és egy p-Sylow részcsoport homomorf képe a kép p-Sylowja.

Bizonyítás: $i)$ $H \leq N_G(H)$ $\big($sőt: $H \lhd N_G(H)\big)$ minden részcsoportra igaz, mint láttuk.

Legyen most $n \in N_G(H)$. Ekkor $\varphi_n \mid_H$ egy automorfizmusa H-nak, így P-t valamely $P^* \leq H$ p-Sylowba viszi. Mivel P^* a H-nak is p-Sylowja és bármely két ilyen konjugált egymással, ezért $\exists h \in H,\ h^{-1}P^*h = P$.

Ekkor $hn \in N_G(P) \leq H$, így $n \in H$; ezzel a bizonyítás kész.

$ii)$ Az 1. izomorfizmustételt felírva a $G \to G/N$ természetes homomorfizmusra és annak P-re vett megszorítására az elemszámokra a következő összefüggés adódik:

$$\frac{|P|}{|P \cap N|} = \frac{|PN|}{|N|} \longrightarrow |N : P \cap N| = \frac{|N|}{|P \cap N|} = \frac{|PN|}{|P|}$$

Tehát a normálosztóban a metszet indexe a jobb oldali kifejezés, ami *relatív prím* p-hez, hiszen P egy p-Sylow. Ebből adódik az első tulajdonság.

A második állításhoz számoljuk ki a faktorcsoportban P képének indexét:

$$|G/N : PN/N| = \frac{\frac{|G|}{|N|}}{\frac{|PN|}{|N|}} = \frac{|G|}{|PN|}$$

ami szintén relatív prímhez ugyanúgy, mint az előbb és a számolásból világos, hogy P képe is p-csoport; ezzel a második tulajdonságot is igazoltuk.

Érdemes megjegyezni, hogy (N helyett) $H \leq G$-re az $ii)$-beli első tulajdonság nem feltétlenül igaz, hiszen pl. ha több p-Sylow van (amikor tehát egyik sem normálosztó), akkor egyikük a másikukat nem annak p-Sylowjában metszi. ∎

2.7. Permutációcsoportok

A legtermészetesebb módon adódó permutációkból álló csoport, az S_n *n-edfokú szimmetrikus csoport* ismertetésével kezdjük.

2.7.1. Az n-edfokú szimmetrikus csoport

Amint az 1. pontban definiáltuk, S_n az $\{1,2,\ldots,n\}$ halmaz bijekcióiból (permutációiból) áll, művelet a kompozíció; a halmaz elemeit *pontoknak* hívjuk majd. A definícióból rögtön adódik, hogy $|S_n| = n!$.

Először két (nem teljesen független) kézenfekvő megadását ismertetjük a csoport elemeinek.

$i)$ Azt a permutációt, amely az i-t és a j-t ($1 \leq i \neq j \leq n$) felcseréli, a többi elemet pedig fixen hagyja, (ij)-vel jelöljük és **cserének**, vagy **transzpozíciónak** nevezzük. Egy csere természetesen másodrendű, így saját maga inverze. Gondoljuk meg azt az egyszerű állítást, hogy *minden permutáció cserék szorzata* (azaz kompozíciója). Ugyanis ha $\vartheta \in S_n$, akkor a kiindulási $(1,2,\ldots,n)$ állapotban először cseréljük ki 1-et $(1)\vartheta$-val (a többit változatlanul hagyva), majd 2-t $(2)\vartheta$-val és így tovább; ezek a lépések nem „zavarják" egymást, hiszen ϑ egy bijekció. Persze ha valamely i-re $i = (i)\vartheta$, vagy már egy korábbi lépésben a helyére került, akkor azzal a ponttal semmit sem csinálunk. Végül minden elem a ϑ által meghatározott helyére kerül, azaz (a függvényben szereplő zárójeleket az egyszerűség kedvéért elhagyva) $\vartheta = (1\,1\vartheta)(2\,2\vartheta)\cdot\ldots\cdot(n\,n\vartheta)$.
A cserék szorzataként történő megadás persze nem egyértelmű, hiszen pl. bárhova beilleszthetünk egy $(ij)(ij) = e$ elemet, azonban látni fogjuk, hogy az előállításban szereplő cserék számának *paritását* ϑ egyértelműen meghatározza.

$ii)$ Ha $\vartheta \in S_n$ tetszőleges $\neq e$ permutáció, akkor induljunk el az 1 pontból és képezzük egymás után a megelőző elem képét: $\Big(\ldots\Big(\big((1)\vartheta\big)\vartheta\Big)\vartheta\Big)\vartheta\ldots$. Ennek a sorozatnak persze valamikor záródnia kell, azaz egy korábbi ponthoz kell visszaérkeznünk, ami csak az 1 (a kiindulási) pont lehet, különben ϑ nem lenne injektív. Ha ezen a sorozaton kívül van(nak) még pont(ok), akkor azok közül tetszőlegesen választva egyet ismét bejárhatunk az előbbi módon egy sorozatot és így tovább.

Látható, hogy ezzel tulajdonképpen ϑ-t olyan permutációk szorzataként írtuk fel, amelyek néhány elemet a fenti módon, azaz ciklikusan permutálnak. Ezeket **ciklusoknak**, egy-egy „sorozatban” szereplő pontok számát pedig a *ciklus hosszának* nevezzük és k-ciklusokról beszélünk majd, ahol k a hossz. Egy k-ciklust így jelölünk: $(i_1\, i_2\, \ldots\, i_k)$ és ha $k = 1$, azaz egy fixpontról van szó, akkor azt általában nem írjuk ki. Világos, hogy a ciklus leírását bármelyik pontjából elkezdhetjük, azaz „modulo k eltolhatjuk a vektort”. Pl. az $1 \mapsto 2,\ 2 \mapsto 3, \ldots, n-1 \mapsto 1$ permutáció egy $(n-1)$-ciklus, jele: $(1\,2\,3 \ldots\, n-1) = (2\,3 \ldots\, n-1\ 1)$ stb. Persze a cserék éppen a 2-ciklusok. Könnyű meggondolni azt, hogy egy *k-ciklus rendje éppen k*.

A fentiek szerint S_n minden permutációja (sorrendtől eltekintve - ld. alább) *egyértelműen bontható diszjunkt ciklusok szorzatára*, azaz olyan ciklusokéra, melyeknek nincs közös mozgatott eleme (az egységelem csupa 1-ciklus szorzata, amelyet nem jelölünk). *Két diszjunkt ciklus természetesen egymással felcserélhető*, ezért a szorzatuk tényezőnként hatványozható. Eszerint ha ismerjük ϑ ciklusfelbontását, akkor ϑ^k ciklusfelbontása az egyes ciklusok k-adik hatványainak szorzata. Ebből az is adódik, hogy egy permutáció *rendje* a ciklusfelbontásban szereplő ciklushosszak *legkisebb közös többszöröse* (ez a legkisebb szám, melyre valamennyi szereplő ciklust emelve e-t kapjuk). Pl. S_{10}-ben a $\vartheta = (12)(345)(6\ 7\ 8\ 9\ 10)$ permutáció rendje $o(\vartheta) = [2,3,5] = 30$ és négyzete $\vartheta^2 = \underbrace{(12)^2}_{e}\underbrace{(345)^2}_{(354)}\underbrace{(6\ 7\ 8\ 9\ 10)^2}_{(6\ 8\ 10\ 7\ 9)} =$
$= (354)(6\ 8\ 10\ 7\ 9)$.

Megjegyzendő, hogy $n \geq 3$ esetén S_n *nem kommutatív*, mert pl. $(12)(23) = (132) \neq (23)(12) = (123)$ (persze $S_2 \cong \mathbb{Z}_2$ és $S_1 = e$ kommutatívak).

Most rátérünk S_n egy fontos részcsoportjának ismertetésére.

Ha $\vartheta \in S_n$ egy permutáció, akkor ϑ **inverziószámát** a determináns definíciójában szereplő inverziószámmal egyező módon értelmezzük:

Legyen az inverziószám ℓ, ha ℓ esetben fordul elő, hogy $i < j$, de $(i)\vartheta > (j)\vartheta$ valamely $i, j \in \{1,2,\ldots,n\}$ esetén.
Pl. az e, (12) csere és a „fordított sorrend permutáció” $\big(= (1\ n)(2\ n-1)\ldots(\lfloor \frac{n}{2} \rfloor\ \lceil \frac{n}{2} \rceil)\big)$ inverziószámai rendre 0, 1 illetve $\binom{n}{2}$, utóbbi persze a legnagyobb lehetséges inverziószám.
Most bevezethetünk egy új fogalmat: egy permutáció **páros,** illetve **páratlan** aszerint, hogy az inverziószáma páros vagy páratlan. Vizsgáljuk, hogyan függ össze az inverziószám azzal, hány csere szorzataként írunk fel egy permutációt.
Egy ϑ permutációt balról $(i\ \ i+1)$-vel szorozva az $(i)\vartheta$, $(i+1)\vartheta$ szomszédos helyzetű elemek cserélnek helyet: ilyenkor az inverziószám ± 1-et változik, hiszen ebben az esetben csak a cserében szereplő két pont „inverziós viszonya” módosul. Erre visszavezethetjük két „távolabbi pont”, mondjuk $(i)\vartheta,\ \ (k)\vartheta$ $(i < k)$ cseréjének esetét is, amely az (ik)-val való balszorzásnak felel meg. Ezt ugyanis elvégezhetjük úgy, hogy ϑ-t balról szorozgatva szomszédos cseréket hajtunk végre egymás után:

$$\big((k-1\ k)\ldots(i+1\ i+2)(i+1\ i)\ldots(k-1\ k-2)(k\ k-1)\big)\cdot\vartheta$$

Mint látjuk, ez mindig páratlan sok lépést jelent, így (ik)-val balról szorozva egy permutációt, annak inverziószáma páratlan sokkal változik meg (hiszen minden lépésben ± 1-gyel változik és páratlan sok lépés van).
Már tudjuk, hogy minden permutáció cserék szorzata, és minden egyes cserével való (bal)szorzásnál az inverziószám páratlan sokat változik. Ebből következik, hogy (amint fentebb állítottuk) egy permutáció cserék szorzataként való felírásában a tényezők számának paritása egyértelműen meghatározott, ugyanis az inverziószám természetesen nem a felbontástól függ: *páros permutáció mindig páros sok és páratlan permutáció mindig páratlan sok csere szorzata*.

Még fontosabb következmény, hogy S_n-ben *a páros permutációk részcsoportot alkotnak*. Ennek igazolásához a 2.2.4. tételt használjuk (jegyezzük meg,

hogy az egységelem páros permutáció, így nemüres halmazról beszélünk): ha ϑ_1, ϑ_2 páros permutációk, akkor mindkettőnek vehetjük egy-egy páros sok csere szorzataként történő előállítását, de ekkor ϑ_2^{-1} a megfelelő cserék fordított sorrendű szorzata (a szorzat inverzéről szóló tétel és a cserék másodrendű volta miatt), azaz $\vartheta_1\vartheta_2^{-1}$ is előáll mint páros sok csere szorzata, tehát páros permutáció.

Korábbi meggondolásaink szerint egy páros és egy páratlan permutáció szorzata páratlan permutáció; ez mutatja, hogy $n \geq 2$ esetén *ugyanannyi páros és páratlan permutáció van S_n-ben*, hiszen (pl.) az (12)-vel való (mondjuk) balszorzás egy bijekciót jelent a páros és páratlan permutációk között ($n = 1$ esetén persze $A_1 = S_1 = e$).

2.7.1. Definíció: *S_n páros permutációi részcsoportot alkotnak, amelynek a neve **n-edfokú alternáló csoport**, jele: A_n.*
Ha $n \geq 2$, akkor $|A_n| = \frac{n!}{2}$, így minden n-re $A_n \triangleleft S_n$.

Jegyezzük meg, hogy a normálosztóság az inverziószám-paritások vizsgálatából is látszik.

Például A_4-et a következő elemek alkotják:

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), \text{ 3-ciklusok}\}.$$

Általában igaz, hogy egy *k-ciklus paritása megegyezik $k-1$ paritásával*, ugyanis egy ilyen ciklus előáll $k-1$ db transzpozíció szorzataként:

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_2 i_k) \dots (i_{k-1} i_k)$$

(csak ellenőrizni kell, hogy valóban minden elem a megfelelő helyre kerül). Emiatt az előbbi példánkban szereplő 8 db 3-ciklus mind páros permutáció és így 12 elemet soroltunk fel, ami éppen $|A_4|$, tehát az összes elemet megkaptuk. Az is látható, hogy a 3 db másodrendű elem és e részcsoportot kell hogy alkosson, ugyanis A_4 2-Sylowja 4 elemű, amelyben az egységelemen kívül csak 2-hatványrendű

elemek lehetnek. Kis számolással kiderül, hogy ez a részcsoport normálosztó is A_4-ben, amely $\mathbb{Z}_2 \times \mathbb{Z}_2$-vel izomorf.

Az okra, ami miatt az A_n-ek különösen fontosak számunkra, a következő tétel világít rá, amelyet bizonyítás nélkül közlünk:

2.7.2. Tétel: *Ha $n \geq 5$, akkor A_n egyszerű.*

Tegyük hozzá, hogy $A_1 = A_2 = e$ egyelemű csoportok, $A_3 \cong \mathbb{Z}_3$ (mivel 3 elemű) és A_4-ben az imént „találtunk" egy négyelemű normálosztót. A feladatok egyikében belátjuk majd, hogy 60-nál kisebb elemszámú nemkommutatív egyszerű csoport nincs is, tehát a legkisebb „valódi" egyszerű csoport az 5-ödfokú alternáló csoport.

A most következő meggondolásból kiderül, hogy S_n *konjugáltosztályainak* „összetétele" nagyon szemléletesen leírható és $Z(S_n)$ a lehető legegyszerűbb csoport, ha $n \geq 3$.
Legyen $\vartheta,\ \alpha \in S_n$ és vizsgáljuk az $\alpha^{-1}\vartheta\alpha$ elemet. Mivel ϑ egyértelműen felírható diszjunkt ciklusok szorzataként és a konjugálás művelettartó, így elég meghatároznunk, hogy egy ciklussal mi történik a konjugálás során. Vegyük tehát a $\gamma = (i_2 i_2 \dots i_k)$ ciklus konjugáltját α-val. Ha $(j)\alpha^{-1} \in \{1,2,\dots,n\}$ olyan pont, melyet nem mozgat a ciklus (azaz nincs az $i_1, i_2, \dots, i_k$ pontok között), akkor $\alpha^{-1}\gamma\alpha$ fixen hagyja j-t, mert csak az ellentétes hatást jelentő α és α^{-1} hat rá. Az előbbi feltétellel ekvivalens módon azt mondhatjuk, hogy pontosan azok a j-k mozognak, melyekre $j = (i_s)\alpha$ valamely $s \in \{1,2,\dots,k\}$. Ezekkel pedig ez történik:

$$j = (i_s)\alpha \mapsto i_s \mapsto i_{s+1} \mapsto (i_{s+1})\alpha.$$

Tehát $\alpha^{-1}(i_1 i_2 \dots i_k)\alpha = \big((i_1)\alpha\,(i_2)\alpha \dots (i_k)\alpha\big)$ (hiszen a ciklust éppen így értelmeztük; az indexelés értelmszerűen modulo k történik).
Eszerint (művelettartóan elvégezve a diszjunkt ciklusokon a konjugálásokat) *egy*

permutáció konjugáltja egy ugyanolyan ciklusszerkezetű permutáció (azaz amelyben ugyanolyan hosszú diszjunkt ciklusok szerepelnek).
„Megfordítva”, ha adottak a $\vartheta_1 = (i_{11}i_{12}\dots i_{1k})(i_{21}i_{22}\dots i_{2\ell})\dots(i_{m1}i_{m2}\dots i_{ms})$ és a $\vartheta_2 = (j_{11}j_{12}\dots j_{1k})(j_{21}j_{22}\dots j_{2\ell})\dots(j_{m1}j_{m2}\dots j_{ms})$ azonos ciklusszerkezetű permutációk, akkor az $\alpha : i_{pq} \mapsto j_{pq}$ permutációval konjugálva előbbi meggondolásunk szerint $\alpha^{-1}\vartheta_1\alpha = \vartheta_2$.
Az előbbiekben a következő tételt bizonyítottuk be:

2.7.3. Tétel: *S_n egy konjugáltosztályát pontosan azok a permutációk alkotják, melyek diszjunkt ciklusok szorzataként való felírásában a ciklushosszak megegyeznek.*
S_n-nek így annyi konjugáltosztálya van, amennyi az n partícióinak száma.

Amint utaltunk rá feljebb, ez a tulajdonság az n-edfokú szimmetrikus csoport centrumának méretét is meghatározza:

2.7.4. Tétel: *Ha $n \geq 3$, akkor $Z(S_n) = e$.*

Bizonyítás: Legyen $\vartheta \in S_n$ $n \geq 3$ tetszőleges $\neq e$ permutáció és α diszjunkt ciklusokra való felbontása „kezdődjön így”: $(i_1 i_2 \dots)\cdots(\dots)$ (legalább 2-ciklusok vannak benne, ha nem az egységelem). Mivel van még legalább egy pont i_1-en és i_2-n kívül, mondjuk j, ezért az $\alpha = (i_1 j)$-vel való konjugálás ϑ-t biztosan nem önmagába viszi a fenti számolás szerint (tehát nem történhet meg az sem, hogy esetleg máshonnan kezdve a ciklus felírását éppen ugyanazt a ciklust kapjuk). Eszerint bármely $\neq e$ permutációhoz létezik olyan permutáció, amely nem önmagába konjugálja, azaz (amint a centrum definíciójánál meggondoltuk) nem cserélhető fel vele; más szóval egyetlen nemtriviális elem sincs a centrumban. ∎

2.7.2. Orbit, stabilizátor

Innentől a pont további részében a permutációcsoportokra vonatkozó általános fogalmakat tárgyalunk.
Először is adósak vagyunk még fő fogalmunk meghatározásával:

2.7.5. Definíció: *Legyen X egy nemüres halmaz.*
*Ekkor az X önmagára menő bijekcióiból álló csoportot (melynek elemei a permutációk) S_X-szel jelöljük; ennek részcsoportjait **permutációcsoportoknak** nevezzük.*
*$|X|$ a permutációcsoport(ok) **foka**.*

Természetesen valójában nem az X maga, hanem $|X|$, azaz a permutációcsoport foka határozza meg a csoportot izomorfia erejéig: ha $|X| = |Y|$, akkor $S_X \cong S_Y$, amint erre már utaltunk is az első pont végén. Véges halmazon ható (azaz véges fokú) permutációcsoport nyilvánvalóan véges, de végtelen fokú permutációcsoport is lehet véges, amint azt pl. $S_{\mathbb{Z}}$-ben $\langle(12)\rangle$ példája mutatja.
Például n-edfokú permutációcsoport az S_n szimmetrikus csoport és az A_n alternáló csoport. Úgyszintén egy n-edfokú permutációcsoport lesz az a részcsoport, amelynek elemei csak (legfeljebb) a $\{2,3,\ldots,n\}$ elemeit mozgatják, az 1-et fixen hagyják.

Ha adott a $G \leq S_X$, akkor az $x \in X$ a csoport valamely $\pi \in G$ eleménél vett képét a szokásos $x\pi$ jelöli. Nem nehéz meggondolni, hogy ha az „y képe x-nek” kapcsolatra „alapozunk” egy $\sim$ relációt X-en, akkor ekvivalenciarelációt kapunk, azaz a $x, y \in X$ $x \sim y : \exists \pi \in G, x\pi = y$ relációra teljesül:
$x \sim x$ $\forall x \in X$, hiszen $x = xe_G$ (reflexív);
$y = x\pi \Leftrightarrow x = y\pi^{-1}$ (szimmetrikus);
$y = x\pi,\ z = y\vartheta \Leftrightarrow z = x(\pi\vartheta)$ (tranzitív).
Eszerint $\sim$ tényleg ekvivalenciareláció X-en, az $x \in X$-et tartalmazó ekvivalen-

ciaosztály pontosan az x képeiből áll (ahová „eljuthatunk” x-ből valamely bijekció révén).

Egyszerű észrevétel, hogy ha $x \in X$ tetszőleges, akkor azok a permutációk részcsoportot alkotnak G-ben, amelyek x-et fixen hagyják, azaz $\{\pi \in G : \ x\pi = x\} \leq$ $\leq G$. Most adjuk meg az előbb leírt két fogalom elnevezését:

2.7.6. Definíció: *Legyen $G \leq S_X$ permutációcsoport.*
$x \in X$ esetén azon $y \in X$ pontokat, melyekre $\exists \pi \in G, \ x\pi = y$, az x ***orbitjának*** *(vagy pályájának) nevezzük és $[x]$-szel jelöljük. Ennek megfelelően X G-orbitjairól beszélünk. Amint láttuk, X előáll a G-orbitok diszjunkt uniójaként. Azok a $\pi \in G$ permutációk, melyekre $x\pi = x$, részcsoportot alkotnak G-ben; ezt $St_G(x)$-szel jelöljük és az x* ***stabilizátorának*** *nevezzük.*

Például az $\{1,2,\ldots,n\}$ halmaznak egyetlen S_n-orbitja van, de az 1-et fixen hagyó permutációkból álló részcsoport (amely előbbi definíciónk szerint éppen $\mathrm{St}_{S_n}(1)$) szerint két orbitja van: az $\{1\}$ és a $\{2,3,\ldots,n\}$.

Ha a $G \leq S_X$ permutációcsoport elemeivel bármely két $x, y \in X$ pont átvihető egymásba, azaz egyetlen G-orbit van X-ben, akkor G-t **tranzitívnak** nevezzük; ez a definíció persze X-től is függ. Ilyen pl. S_n a szokásos halmazon (de nem tranzitív, ha S_{n+1} részcsoportjaként $n+1$ ponton hatónak tekintjük úgy, mint az $n+1$ pont stabilizátorát), nem tranzitív viszont $n \geq 3$ esetén az a kételemű részcsoportja , amely az 1-et és a 2-t felcserélő, a többi elemet fixen hagyó (12) cseréből és az egységelemből áll.

Egy másik fontos speciális tulajdonság az, ha $G \leq S_X$-ben bármely pont stabilizátora egyelemű (azaz csak az egységelemből áll); ekkor G-t *szemireguláris-nak* hívjuk. Ha G egyszerre tranzitív és szemireguláris, akkor **reguláris**. Reguláris permutációcsoportra példa S_4 következő részcsoportja:

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

Feltehetjük azt a kérdést, hogy hány képe van az $x \in X$ elemnek a permutációcsoport elemeivel. A válasz $\mathrm{St}_G(x)$ egy már ismert jellemzőjével kapcsolatos:

2.7.7. Tétel: *Legyen $G \leq S_X$ permutációcsoport, $x \in X$.*
Kölcsönösen egyértelmű megfeleltetés van az $\mathrm{St}_G(x)$ szerinti bal oldali mellékosztályok és x orbitjának elemei, azaz x képei között. Eszerint $|[x]| = |G : \mathrm{St}_G(x)|$.

Bizonyítás: Tegyük fel, hogy $\alpha\mathrm{St}_G(x) = \beta\mathrm{St}_G(x)$. Ekkor

$\alpha^{-1}\beta \in \mathrm{St}_G(x) \Leftrightarrow x(\alpha^{-1}\beta) = x \Leftrightarrow x\alpha = x\beta$, hiszen bijekciókról van szó.

Ez éppen azt jelenti, hogy az $\alpha\mathrm{St}_G(x) \mapsto x\alpha$ hozzárendelés jól definiált, ráadásul bijekció (a szürjektivitás nyilvánvaló). ∎

A tétel közvetlen következménye, hogy ha G tranzitív, akkor tetszőleges $x \in X$-szel $|G| = |X| \cdot |\mathrm{St}_G(x)|$ (mivel G a stabilizátor szerinti bal oldali mellékosztályok diszjunkt uniója), továbbá ha G reguláris, akkor $|G| = |X|$ (amit az ezekre a speciális tulajdonságokra adott példáink is illusztrálnak).

2.7.3. Permutációreprezentáció és csoporthatás

Cayley-től származik az a nevezetes tétel, amely egy csoportnak permutációcsoportként való „megjelenítését” mutatja be: ennek alapján minden csoportra gondolhatunk úgy, mint *reguláris* permutációcsoportra. A tétel bizonyítását követően ezt a gondolatot általánosítjuk majd.

2.7.8. Tétel (Cayley): *Ha G csoport, akkor $G \cong G^*$, ahol $G^* \leq S_G$.*

Bizonyítás: Tekintsük ugyanis azt a $\varphi : G \to S_G$ függvényt, amely

$$x\varphi = x \mapsto xg \quad \forall x \in G$$

Az egyszerűsítési szabály mutatja, hogy ez a függvény injektív, másrészt ha $y \in$ $\in G$ tetszőleges, akkor $y = (yg^{-1})g$, tehát szürjektív is. Emellett az asszociativitási szabály alapján a műveletet is tartja, azaz φ egy izomorfizmus, ezért $S_G \geq$ $\geq \operatorname{Im}\varphi \cong G$, amint állítottuk.
Az előbbi meggondolásokból azt is leolvashatjuk, hogy $\operatorname{Im}\varphi$ reguláris permutációcsoport. ∎

Az imént a csoport elemei természetes módon „hatottak” a csoporton, mégpedig a szorzás révén *permutálták* az elemeket. Most legyen $H \leq G$ olyan részcsoport, amelyre $|G : H| = k$. Az előbbi példából kiindulva definiálhatunk egy homomorfizmust úgy, hogy G elemei a H szerinti jobb oldali *mellékosztályokat permutálják*, így a kép ezúttal S_k egy részcsoportjával lesz izomorf.
Ez a φ homomorfizmus legyen a következő:

$$(g)\varphi = Hx \mapsto Hxg \quad \forall x \in G$$

Most sem nehéz belátni, hogy ez tényleg homomorfizmus, ami az előbb elmondottak szerint a k-adfokú szimmetrikus csoportba képez G-ből.
Vizsgáljuk meg $\operatorname{Ker}\varphi$-t! Ez azon $g \in G$ elemekből áll, amelyekre

$$Hxg = Hx\ \forall x \in G \Leftrightarrow H = Hxgx^{-1}\ \forall x \in G \Leftrightarrow xgx^{-1} \in H\ \forall x \in G \Leftrightarrow$$
$$\Leftrightarrow \forall x \in G\ \exists h \in H, xgx^{-1} = h.$$

Eszerint $\operatorname{Ker}\varphi = \bigcap_{x\in G} x^{-1}Hx = H_G$, vagyis a mag éppen H *normális belseje* (amiről így másodszor is kiderült, hogy normálosztó G-ben).
Láthatjuk, hogy ez a meggondolás $H = e$ esetén éppen a Cayley-tételre vezet, továbbá nemcsak véges, hanem tetszőleges α számosság esetén is érvényes egy α indexű részcsoport szerinti jobb oldali mellékosztályokat tekintve; mi a bemutatott véges indexű esetet fogjuk használni. Vegyük észre azt is, hogy a képként előálló permutációcsoport *tranzitív*, ugyanis $Hy = Hx(x^{-1}y)$, azaz bármely „pontból” bármely pontba eljuthatunk. (Ezenkívül, mint mondtuk, a Cayley-tételben

szereplő permutáció-megjelenítés esetében (ez az ún. *jobb oldali reguláris reprezentáció*, amire Cayley-reprezentációként fogunk hivatkozni) a kapott permutációcsoport nemcsak tranzitív, hanem *szemireguláris* is.)
Az elmondottakat foglaljuk össze a következő tételben:

2.7.9. Tétel: *Legyen G csoport, $H \leq G$ és $|G : H| = k$.*
Ekkor a G-ből a H szerinti mellékosztályok S_k-val izomorf permutációcsoportjába képező $\varphi : g \mapsto (Hx \mapsto Hxg \ \forall x \in G)$ leképezés egy homomorfizmus, melynél G képe az $\mathrm{Im}\,\varphi \leq S_k$ tranzitív permutációcsoport, a mag pedig H normális belseje $\mathrm{Ker}\,\varphi = H_G$.
$H = e$ esetén a G (véges) csoport izomorf S_k egy G^* részcsoportjával, amely egy $|G| = k$-adfokú reguláris permutációcsoport.

Általában ha adott egy G csoport, egy $X(\neq \emptyset)$ halmaz és egy $\varphi : G \to S_X$ homomorfizmus, akkor φ-t G egy **permutációreprezentációjának** hívjuk.

Az előbb tárgyalt permutációreprezentációnál tulajdonképpen a G csoport elemei „hatottak” (amint ezt a szót fentebb már használtuk is) egy bizonyos G-hez „kapcsolódó halmazon” (egy részcsoport szerinti jobb oldali mellékosztályok halmazán) mint permutációk. Hasonló helyzetre más kézenfekvő példákat is nézhetünk: pl. G elemei a konjugálások (mint bijekciók) révén G nemüres részhalmazait is permutálják, úgyszintén permutálják pl. az egymással izomorf részcsoportokat (ilyenek pl. a p-Sylow részcsoportok).
Ezek alapján hasznos definiálni az ún. *csoporthatás* fogalmát:

2.7.10. Definíció: *Legyen G csoport és $T \neq \emptyset$ egy halmaz.*
*Azt mondjuk, hogy G **jobbról hat** a T-en, ha értelmezve van egy $\circ : T \times G \to T$ függvény, amire a következők teljesülnek:*

$$t \circ (g_1 g_2) = (t \circ g_1) g_2 \quad t \circ e_G = t \ \ \forall t \in T, g_1, g_2 \in G$$

Vegyük észre, hogy a definíció alapján a csoport bármely g elemére a $t \mapsto$ $\mapsto t \circ g$ $(\forall t \in T)$ a T elemeinek egy *permutációja*. Ebből kiindulva az is egyszerűen adódik, hogy a $g \mapsto (t \mapsto t \circ g \ \forall t \in T)$ leképezés egy homomorfizmus G-ből S_T-be, azaz G-nek egy *permutációreprezentációja*. Tehát minden jobb hatásnak természetes módon megfelel egy permutációreprezentáció.
Megfordítva: adott $\varphi : G \to S_T$ permutációreprezentációhoz természetes módon hozzárendelhetjük G-nek egy jobb oldali hatását T-n a $(t, g) \mapsto (t)\big(\underbrace{(g)\varphi}_{\in S_T}\big)$ hozzárendeléssel. A fentebb definiált két fogalmunk tehát szoros kapcsolatban van, és egymásnak kölcsönösen egyértelműen megfeleltethetők. Világos továbbá, hogy ha $G \leq S_X$ permutációcsoport, akkor G hat X-en a megfelelő permutációkkal.

Ha a G csoport hat egy T halmazon, akkor a $t \in T$ elem $\mathrm{St}_G(t)$ *stabilizátorának* és $[t]$ *orbitjának* fogalma a korábbi fogalom értelemszerű módosításával most is bevezethető:

$$\mathrm{St}_G(t) \stackrel{\text{def}}{=} \{g \in G \mid t \circ g = t\};$$
$$[t] \stackrel{\text{def}}{=} \{t \circ g \mid g \in G\}.$$

Ez azért célszerű, mert az 2.7.7. tétel szóról szóra igaz marad abban az esetben is, amikor G „csak” hat T-n.

2.7.11. Tétel: *Legyen G csoport, amely a $T \neq \emptyset$ halmazon hat és $t \in T$.*
Ekkor $|[t]| = |G : St_G(t)|$.

Bizonyítás: Egy az egyben úgy érvelhetünk, mint a jelzett 2.7.7. tételnél. ∎

Alkalmazzuk ezt az eredményt arra az esetre, ha a G csoport konjugálással hat saját nemüres részhalmazain! Ekkor ha $\emptyset \neq T \subseteq G$, akkor T stabilizátora éppen az $N_G(T)$ normalizátor, így „fáradság nélkül” megkaptuk a korábbi $|[T]| =$ $= |G : N_G(T)|$ összefüggést. Ugyanennél a példánál maradva minden normálosztó orbitja egyelemű és ugyanez igaz a $Z(G)$ centrum valamennyi nemüres részhalmazára is.

A permutáció-reprezentációk alkalmazásaként most két állítást igazolunk. Először jöjjön az a tétel, amelyet a 2 indexű részcsoportok normálosztóságának általánosításaként ígértünk a $2.2.3.$ pontban.

2.7.12. Tétel: *Legyen G véges csoport, p a legkisebb prímosztója $|G|$-nek és $H \leq G$ olyan részcsoport, amelynek indexe p.*
Ekkor $H \triangleleft G$.

Bizonyítás: Mivel H egy p indexű részcsoport, így tekinthetjük G-nek fent megismert φ permutációreprezentációját az S_p szimmetrikus csoportba. Ennek magja $H_G \leq H$, amint láttuk.
Ha $\operatorname{Ker}\varphi < H$, akkor $|\operatorname{Im}\varphi| = \frac{|G|}{|\operatorname{Ker}\varphi|}$ biztosan összetett szám, hiszen az indexek szorzástétele miatt p-vel osztható és feltevésünk szerint p-nél nagyobb. Így p-n kívül van legalább még egy prímtényezője van, amely esetleg lehet p is (ekkor p legalább a négyzeten szerepel a prímtényezős alakban). Mindkét eset ellentmond a Lagrange-tételnek, hiszen ha egy $q > p$ prímtényezőt találtunk, akkor ez nem osztja $|S_p| = p!$-t, mert p volt a legkisebb prímosztó, így q a faktoriálisban szereplő szorzat egyik tényezőjét sem osztja; az sem lehet, hogy p-nek legalább második hatványa osztja $|\operatorname{Im}\varphi|$-t, mert p^2 nem osztja $p!$-t.
Eszerint $|\operatorname{Ker}\varphi| = p \Rightarrow \operatorname{Ker}\varphi = H \Rightarrow \operatorname{Ker}\varphi \triangleleft G$, amit bizonyítanunk kellett. ∎

A következő, meglepő tétel bizonyításában a Cayley-reprezentáció alkalmazása a fő gondolat, emellett szükségünk lesz majd a permutációk paritásáról és ciklusfelbontásáról elmondottakra is.

2.7.13. Tétel: *Legyen G csoport, $|G| = n = 4k + 2$.*
Ekkor G-ben van 2 indexű, azaz $2k + 1$ elemű normálosztó.
Következmény: ***k*** $\geq$ **1** ***esetén nem létezik 4k+2 elemű egyszerű csoport.***

Bizonyítás: Tekintsük G-nek Cayley-reprezentációját S_n-be, azaz legyen $G \cong$ $\cong G^* \leq S_n$; tudjuk, hogy G^* reguláris permutációcsoport.

Mivel n páros, így a Cauchy-tétel szerint van G-ben 2 rendű elem, amelynek képe G^*-ban is egy 2 rendű elem, mondjuk α. Utóbbit - mint S_n egy elemét - felírhatjuk diszjunkt ciklusok szorzataként; ebben a felírásban (elhagyva az egypontú ciklusokat) csak 2-ciklusok (azaz cserék) szerepelhetnek a permutáció rendjének és ciklusszerkezetének összefüggése miatt. Másrészt mivel G^* reguláris, így az egységelemen kívül minden permutáció fixpontmentes, azaz α-nak mind az n pontot mozgatnia kell, tehát az $2k+1$ db csere szorzata. Ebből következik, hogy α *páratlan permutáció*.
A korábban S_n-nél látott meggondolás általában is érvényes, azaz ha egy permutációcsopotban van páratlan permutáció, akkor ugyanannyi páros és páratlan permutáció van (mert egy rögzített páratlannal, illetve inverzével való balszorzás egy bijekció, mely váltja a paritást). Eszerint G^*-ban $2k+1$ db páros (és ugyanennyi páratlan) permutáció van, amelyek egy 2 indexű részcsoportot, tehát normálosztót alkotnak; ennek képe egy $G^* \to G$ izomorfizmusnál egy 2 indexű normálosztó G-ben. ∎

A feladatok között még számos esetben fogjuk használni a mellékosztályokon történő permutációreprezentációkat a Sylow-tételekkel párosítva, hogy adott elemszámú csoportok „nemegyszerűségét” bizonyítsuk.

2.8. Feloldható és nilpotens csoportok

Ebben a pontban olyan csoportokat vizsgálunk majd, melyek speciális módon „bonthatók le” normálosztók sorozatán keresztül. Először néhány szót szólunk az ilyen lebontásokról általában.

2.8.1. Normállánc, kompozíciólánc

2.8.1. Definíció: *Legyen G csoport.*
*G **normálláncának** nevezünk egy $G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \ldots \triangleright N_k = e$ sorozatot, ahol tehát minden N_i az N_{i-1}-ben normálosztó.*
*Az N_i/N_{i+1} faktorcsoportok a lánc **faktorai**, k a lánc **hossza**.*

Például tetszőleges G-re $G \triangleright e$ egy normállánc; kevésbé triviális példaként $G = A_4 \triangleright \{e, (12)(34), (13)(24), (14)(23)\} \triangleright \{e, (12)(34)\} \triangleright e$; ez a példa is mutatja, hogy a normálosztóság nem „tranzitív”, azaz $N_i \triangleleft G$ nem feltétlenül teljesül (jelen esetben pl. $\big(123\big)^{-1}\big((12)(34)\big)\big(123\big) = \big(14\big)\big(23\big)$, ahogy S_n konjugáltosztályainak tárgyalásánál meggondoltuk; tehát a lánc harmadik tagja nem normálosztó G-ben).

Ha adott normállánc N_i és N_{i+1} tagja közé beillesztünk egy $N_i \triangleright N_{i+\frac{1}{2}} \triangleright \triangleright N_{i+1}$ tagot, akkor a normálláncot **finomítjuk**. Persze ugyanannak a normálosztónak tetszőlegesen sokszori „szerepeltetésével” mindig finomíthatunk (legalábbis definíciónk szerint) egy láncot; ezt *triviális finomításnak* nevezzük. Kitüntetett normállánc az, amely (már) csak triviálisan finomítható. Ekkor már semelyik N_i-ben nincs olyan normálosztó, mely N_{i+1}-et tartalmazza ($i = 0,1,\ldots,k-1$); amint a 2. izomorfizmus tétel után meggondoltuk, ez a pontosan azt jelenti, hogy az N_i/N_{i+1} faktorok egyszerű csoportok minden i-re $(i = 0,1,2,\ldots,k-1)$.

2.8.2. Definíció: *A $G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \ldots \triangleright N_k = e$ normálláncot **kompozíciólláncnak** hívjuk, ha csak triviálisan finomítható.*
*Ez pontosan akkor teljesül, ha az N_i/N_{i+1} $(i = 0,1,\ldots,k-1)$ **kompozíciófaktorok egyszerű csoportok.***

Véges csoportnak mindig van kompozíciólánca, hiszen bármely normálláncából kiindulva (mondjuk a triviális $G \triangleright e$-ből) véges sok lépésben finomítva kompozí-

ciólánchoz jutunk. Emellett van olyan végtelen csoport, amelynek nincs kompozíciólánca; erre egy példa $\mathbb{Z}$, ennek ugyanis tetszőleges $\neq e$ részcsoportja végtelen ciklikus csoport, azaz bármely normállánc utolsó $N_k \triangleright e$ lépése tovább finomítható. Világos, hogy egy kompozíciólánc G-t követő első tagja *maximális normálosztó* G-ben, azaz egy olyan N normálosztó, melyre $N < M \triangleleft G \Rightarrow G = M$ (különben még tudnánk nemtriviálisan finomítani).

$\mathbb{Z}_6$-nak kompozícólánca a $\mathbb{Z}_6 \triangleright \overbrace{\langle(2)\rangle}^{\cong \mathbb{Z}_3} \triangleright e$ és a $\mathbb{Z}_6 \triangleright \overbrace{\langle(3)\rangle}^{\cong \mathbb{Z}_2} \triangleright e$ is, tehát egy csoportnak több kompozíciólánca is lehet. Jegyezzük meg, hogy ha G egyszerű csoport, akkor G-nek egyetlen kompozíciólánca van, a $G \triangleright e$, de látni fogjuk, hogy ilyen tulajdonságú S_n is, ha $n \geq 5$, ennek ugyanis egyetlen kompozíciólánca $S_n \triangleright A_n \triangleright e$ (mivel A_n egyszerű, ha $n \geq 5$, és $S_n/A_n \cong \mathbb{Z}_2$, ez tényleg kompozíciólánc). Az egyik feladatban ugyanakkor kiszámoljuk majd, hogy egy nem is túl bonyolult szerkezetű csoportnak (pontosan) 60 kompozíciólánca van.

$\mathbb{Z}_6$ két kompozícióláncánál láthatjuk, hogy a lánc faktorainak halmaza ugyanaz mindkét esetben ($\{\mathbb{Z}_2, \mathbb{Z}_3\}$). A következő tételben belátjuk, hogy ez minden véges csoport esetében így van; megjegyezzük, hogy az állítás tetszőleges csoportra igaz, melynek van kompozíciólánca. A tétel kimondása előtt gondoljuk meg, hogy általában nem elegendő a faktorok halmazáról beszélni (a halmaz értelme szerint), ugyanis ugyanaz a faktor többször is szerepelhet, mint pl. a fentebb szereplő A_4 esetén, vagy a véges p-csoportok esetén, ahol - mint látni fogjuk - minden faktor $\mathbb{Z}_p$ típusú. A faktorokat tehát „multiplicitással” kell számolni; egy csoport két kompozícióláncát *ekvivalensnek* mondjuk, ha az egyik F_{1i} $(i = = 1,2,\ldots,k)$ és a másik F_{2j} $(j = 1,2,\ldots,k)$ faktorai megfeleltethetők egymásnak úgy, hogy a megfelelő faktorok izomorfak. Világos, hogy a láncok ekvivalenciája „tranzitív”.

2.8.3. Tétel (Jordan, Hölder): *A G véges csoport bármely két kompozíciólánca ekvivalens.*

Bizonyítás: $|G| = n$ szerinti teljes indukciót használunk; $n = 1$-re az állítás persze igaz.

Tegyük fel, hogy minden $k < n$-re már beláttuk az állítást.

Ha G-nek egyetlen M maximális normálosztója van, vagy - mivel minden normállánc kompozíciólánccá finomítható - ami ugyanezt jelenti, minden kompozíciólánca M-mel kezdődik, akkor készen vagyunk az indukciós feltevést használva. Ebben az esetben ui. G bármely kompozícióláncában a faktorok a közös G/M mellett M egy kompozícióláncának faktorai, de az ilyen láncok közül bármely kettő ekvivalens a feltevés szerint.

Legyen tehát K és L két különböző maximális normálosztó G-ben és legyen adott két olyan kompozíciólánc ℓ_1, ℓ_2 is, melyek rendre K-ból és L-ből indulnak/„folytatódnak". Ekkor persze $K \not\leq L$ és $L \not\leq K$ és így $KL \triangleleft G \Rightarrow KL = G$; mindkét állításnál a maximalitásra hivatkozunk (illetve arra a már ismert állításra, hogy két normálosztó részhalmazszorzata is normálosztó).

Az 1. izomorfizmus tétel szerint $K \cap L \triangleleft K, L$ (valójában könnyű belátni, hogy két normálosztó metszete is normálosztó, tehát $K \cap L \triangleleft G$ is igaz) és

$$G/K = KL/K \cong L/K \cap L \qquad G/L = KL/L \cong K/K \cap L$$

Legyen a továbbiakban $K \cap L = N$. Az indukciós feltevés szerint K-nak az a kompozíciólánca, amely ℓ_1-ben szerepel ekvivalens minden olyannal, amelyet N-en keresztül kapnánk; ugyanez elmondható L-lel és ℓ_2-vel is. Rögzítsük tehát N egy ℓ^* kompozícióláncát (amelyek közül bármely kettő ekvivalens, így akármelyiket választhatjuk) és vegyük K-nak a $K \triangleright N \xrightarrow{\ell^*} e$ és L-nek $L \triangleright N \xrightarrow{\ell^*} e$ kompozícióláncát (a nyíl értelemszerűen azt jelenti, hogy az ℓ^* lánc mentén „lépegetünk" e-ig). Ezek valóban kompozícióláncok, ugyanis a láncok első faktorai (csak ezekkel lehetne baj) az előbbi izomorfizmustételek alapján egyszerű csoportok.

Most a $G \triangleright K \triangleright N \xrightarrow{\ell^*} e$ és a $G \triangleright L \triangleright N \xrightarrow{\ell^*} e$ kompozícióláncok ekvivalensek, hiszen

az ℓ^*-ban szereplő faktorokon kívül $G/K \cong L/N$ és $G/L \cong K/N$. Másrészt az első lánc ekvivalens ℓ_1-gyel, a második pedig ℓ_2-vel a korábbiak szerint.
Így ℓ_1 és ℓ_2 is ekvivalensek; éppen ezt kellett igazolnunk. ∎

Egyszerű alkalmazásként gondoljuk meg, hogy (amint feljebb már állítottuk) S_n-nek egyetlen kompozíciólánca van $n \geq 5$ esetén. Mivel $S_n \triangleright A_n \triangleright e$ kompozíciólánc, így a Jordan-Hölder tétel szerint bármely kompozícióláncban egy A_5 és egy $\mathbb{Z}_2$ típusú faktornak kell szerepelni. S_n-ben azonban nincsen kételemű normálosztó, ugyanis ha $\{a, a^2 = e\}$ ilyen lenne, akkor a-nak minden konjugáltja önmaga (e nem lehet a konjugálás injektivitása miatt) és így $e \neq a \in Z(S_n) = e$, ami ellentmondás. Eszerint olyan kompozíciólánc nincs, ahol az A_n típusú faktor megelőzi a $\mathbb{Z}_2$ típusút; csak annyit kell meggondolnunk, hogy 2 indexű normálosztó csak A_n lehet. Valóban, ha N egy másik 2 indexű (így maximális) normálosztó, akkor $A_n N = S_n$ a maximalitás miatt, ezért

$$A_n/A_n \cap N \cong \underbrace{A_n N}_{=S_n}/N = S_n/N \cong \mathbb{Z}_2$$

Ezzel A_n-ben egy (2 indexű) nemtriviális normálosztót kapnánk, de A_n $(n \geq 5)$ egyszerű, így ilyen nem létezik.

2.8.2. Feloldható csoportok

Most, hogy a pont elején jelzett lebontásról már szóltunk, jöjjön a „speciálisan lebontható” csoportok definíciója:

2.8.4. Definíció: *A G csoportot **feloldhatónak** nevezzük, ha van olyan normállánca (ezt **kommutatív láncnak** hívjuk majd), amelynek faktorai Abel-csoportok. A G feloldható csoport legrövidebb kommutatív láncának hossza G **derivált hossza**.*

A definícióból világos, hogy minden K Abel-csoport feloldható (mert $K \triangleright e$ egy kommutatív lánc). Emellett feloldható pl. D_n is $(n \geq 3)$, (bár nem kommutatív, mert $tf \neq ft$), amint a $D_n \triangleright \langle f \rangle \triangleright e$ lánc mutatja, melynek faktorai rendre $\mathbb{Z}_2$ és $\mathbb{Z}_n$ típusúak. Azt is látjuk, hogy egy csoport pontosan akkor kommutatív, ha derivált hossza legfeljebb 1 és 0 derivált hossza kizárólag az egyelemű csoportnak van. Nem feloldható csoportot is ismerünk már, ilyen ugyanis az A_n $5 \leq n$ esetén, mert ennek az egyszerűség miatt triviális finomításoktól eltekintve egyetlen normállánca van. Könnyű meggondolni, hogy az előbbi általánosan is igaz: egy nemkommutatív egyszerű csoport biztosan nem feloldható.

A következő tételben a feloldhatóság néhány fontos tulajdonságát foglaljuk össze.

2.8.5. Tétel: *Legyen G csoport.*
i) Ha G feloldható és $H \leq G$, akkor H is feloldható.
ii) $N \triangleleft G$ esetén G feloldható $\Leftrightarrow$ N és G/N feloldható.
iii) Véges sok feloldható csoport direkt szorzata is feloldható.

Bizonyítás: i) Legyen $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_k = e$ egy normállánca G-nek és tekintsük ennek tagjainak H-val vett metszetét, azaz $M_i := N_i \cap H$. Azt állítjuk, hogy ezek (a természetes sorrendben) éppen egy kommutatív láncát alkotják H-nak.
Egyrészt $M_i \triangleright M_{i+1}$, ugyanis az első izomorfizmustétel szerint az $N_i \to N_{i+1}$ természetes homomorfizmus M_i-re való megszorításának magja $N_{i+1} \cap M_i = = N_{i+1} \cap (N_i \cap H) = N_{i+1} \cap H = M_{i+1}$ (azt használtuk ki, hogy $N_i \geq N_{i+1}$). De a jelzett tétel alapján M_i/M_{i+1} az N_i/N_{i+1} egy részcsoportjával izomorf, tehát (maga is) Abel-csoport.

ii) A $\Rightarrow$ irányból annyit már tudunk i) alapján, hogy N feloldható. A faktorcsoport feloldhatóságához az előbbi jelöléssel legyen $F_i := N_i N/N$, azaz vegyük

G normálláncában a tagok képét a $G \to G/N$ természetes homomorfizmusnál (megszorítva azt az N_i-kre). Homomorfizmusnál normálosztó képe normálosztó, így $N_i \triangleright N_{i+1}$ miatt $F_i \triangleright F_{i+1}$ és a faktorok is homomorf módon képződnek le, a fejezet 3. pontjának végén tett észrevétel szerint; mivel kommutatívak voltak, így képeik is Abel-csoportok. Eszerint az imént G/N egy kommutatív láncát kaptuk, a faktorcsoport tehát feloldható.

A $\Leftarrow$ irány természetesen úgy értendő, hogy adottak az N^* és az M^* feloldható csoportok és a G-ben van olyan $N \cong N^*$ normálosztó, melyre $G/N \cong M^*$ (ezt úgy mondjuk, hogy G *bővítése* M^*-nak N^*-gal).

Vegyük G/N egy $G/N = G_0/N \triangleright G_1/N \triangleright \ldots \triangleright G_k/N = N/N = e_{G/N}$ kommutatív láncában a tagok teljes inverz képét a $G \to G/N$ természetes homomorfizmusnál (az a tény, hogy G/N láncának tagjai ilyen alakban írhatóak, a 2.3.7. tétel következménye). Ebben $G_0 \triangleright G_1 \triangleright \ldots \triangleright G_k = N$ és $G_i/G_j \cong {}^{G_i/N}\!/_{G_j/N}$ a második izomorfizmus tétel szerint, tehát ennek a láncnak kommutatívak a faktorai. A lánc „végéhez illesztve” N egy kommutatív láncát, G-nek egy kommutatív láncát kapjuk.

iii) Legyen $D = G_1 \times G_2 \times \ldots \times G_k$, ahol G_i feloldható csoportok és tegyük fel, hogy $G_1 = G_{10} \triangleright G_{11} \triangleright G_{12} \triangleright \ldots \triangleright G_{1\ell} = e$ egy kommutatív lánca G_1-nek. Tekintsük a $D^* = G_{11} \times G_2 \times \ldots \times G_k \leq D$ csoportot. Ez a direkt szorzat tulajdonságai miatt normálosztó D-ben, és a (direkt szorzat tulajdonságai mellett) a 2. izomorfizmustételt is felhasználva:

$$D/D^* \cong {}^{D/(G_2\times\ldots\times G_k)}\!/_{D^*/(G_2\times\ldots\times G_k)} \cong G_1/G_{10}$$

Eszerint D/D^* kommutatív. A megkezdett eljárást folytatva előbb G_1 fenti kommutatív láncának mentén, majd a többi G_i (valamely) kommutatív láncainak mentén haladva D egy kommutatív láncához jutunk, tehát D feloldható, amint állítottuk. ∎

Megjegyzendő, hogy $i)$-ben nem feltétlenül egyezik meg H és G ottani láncának hossza (mert $H \cap N_i = e$ a „triviálisnál korábban” is teljesülhet), de a bizonyítás mutatja, hogy $H \leq G$ *derivált hossza legfeljebb annyi, mint G-é.* $G = D_n$ és $H = \langle f \rangle$ esetén az utóbbi hossz 1 a kommutativitás miatt, míg az előbbi 2 (ui. 1 nem lehet, mert D_n nem kommutatív, viszont fent szerepelt olyan normállánca, amelynek hossza 2).
Előbbi tételünk szerint pl. S_n nem feloldható $n \geq 5$ esetén, mert van olyan részcsoportja (nevezetesen A_n ilyen), amely nem feloldható. Még egy egyszerű alkalmazást mutatunk be:

2.8.6. Tétel: *Minden véges p-csoport feloldható.*

Bizonyítás: Teljes indukciót használunk. Legyen $|G| = p^k$ $k \geq 2$; $k = 1$-re persze az állítás igaz. Tegyük fel, hogy a k-nál kisebb kitevőkre már beláttuk az állítást. Amint a 2.4.4. tételből tudjuk, G centruma nem állhat csak az egységelemből, így $Z(G)$ p^ℓ elemű (p-)csoport valamely $1 \leq \ell \leq k$-ra; $k = \ell$ esetén persze készen vagyunk, mert ekkor G Abel-csoport (tehát feloldható).
Egyébként $\ell < k$, így $G/Z(G)$ és $Z(G) \triangleleft G$ az indukciós feltevés szerint feloldhatóak, tehát 2.8.5. $ii)$ alapján G is az. ∎

„Ezzel szemben” megmutatható, hogy van olyan végtelen feloldható p-csoport, melynek centruma triviális.

A G véges csoportnak, mint már említettük, mindig van kompozíciólánca, sőt bármely normálláncot finomítva kompozíciólánchoz jutunk. Ha G *feloldható* véges csoport, akkor tetszőleges kommutatív láncát finomítva egy olyan kompozíciólánchoz jutunk, melynek faktorai kommutatív egyszerű csoportok, azaz $\mathbb{Z}_p$ típusúak valamilyen prímekre (viszont végtelen feloldható csoport kommutatív lánca nem feltétlenül finomítható kompozícióláncca). Az iménti állításhoz még meg

kell gondolnunk, hogy kommutatív lánc finomítása is kommutatív láncot eredményez. Elég persze olyan finomításra belátnunk, amelynél egyetlen tagot illesztünk be. Valóban, ha $G = N_0 \triangleright N_1 \triangleright \ldots N_i \triangleright N_{i+1} \triangleright \ldots \triangleright N_k = e$ egy kommutatív lánc volt és az $N_i \triangleright N_{i+\frac{1}{2}} \triangleright N_{i+1}$ finomítást végezzük, akkor az $N_{i+\frac{1}{2}}/N_{i+1}$ faktor kommutatív, mivel az N_i/N_{i+1} Abel-csoport egy részcsoportjával egyezik meg, másrészt a második izomorfizmus tétel szerint $N_i/N_{i+\frac{1}{2}} \cong^{N_i/N_{i+1}} \big/_{N_{i+\frac{1}{2}}/N_{i+1}}$, azaz $N_i/N_{i+\frac{1}{2}}$ egy Abel-csoport homomorf képe, tehát ez is kommutatív.
Eszerint egy véges csoport tetszőleges kommutatív láncát finomítva a jelzett faktorokkal bíró kompozíciólánchoz jutunk; a Jordan-Hölder tétel alapján ezek a faktorok egyértelműen meghatározottak a G csoport esetén, tehát nem függenek a kiindulási lánctól.
Az előbbiekben beláttuk a következő tételt:

2.8.7. Tétel: *A G véges csoport akkor és csak akkor feloldható, ha kompozíciólláncának faktorai $\mathbb{Z}_p$ típusú ciklikus csoportok.*

2.8.3. Kommutátorok

A következőkben a feloldhatóságnak egy másfajta, általános (tehát végtelen csoportokra is érvényes) jellemzését adjuk meg, amely egy speciális részcsoporttal kapcsolatos.
Legyen G csoport, $N \triangleleft G$ és vizsgáljuk meg, mikor lesz a G/N faktorcsoport kommutatív:

$$aNbN = bNaN \ \forall a, b \in G \Leftrightarrow a^{-1}b^{-1}abN = N \ \forall a, b \in G \Leftrightarrow$$

$$\Leftrightarrow a^{-1}b^{-1}ab \in N \ \forall a, b \in G$$

Azt látjuk, hogy a faktorcsoport kommutativitásának szükséges és elégséges feltétele, hogy az N normálosztó tartalmazza az összes $[a, b] = a^{-1}b^{-1}ab$ ún. *kom-*

mutátort. Ez pontosan akkor teljesül, ha N tartalmazza az ezek által generált részcsoportot is, amelyet G *kommutátorrészcsoportjának* nevezünk.

2.8.8. Definíció: *Legyen G csoport.*
Az $[a,b] = a^{-1}b^{-1}ab$ $(a,b \in G)$ elemeket ***kommutátoroknak****, a kommutátorok által generált részcsoportot G* ***kommutátorrészcsoportjának*** *nevezzük. Utóbbit G' jelöli.*
Ha $N \triangleleft G$, akkor G/N kommutatív $\Leftrightarrow G' \leq N$.

Vegyük észre, hogy $G' \triangleleft G$, ui. a kommutátorok halmaza zárt a konjugálásra: $g^{-1}\,[a,b]\,g = [g^{-1}ag, g^{-1}bg]$ a konjugálás művelettartása miatt; utóbbiból pedig egyszerűen belátható, hogy ha $\emptyset \neq X \subseteq G$ zárt a konjugálásra, akkor $\langle X \rangle \triangleleft G$. Ebből rögtön adódik, hogy ha $N \leq G$ tartalmazza G'-t, akkor N a G/G' Abel-csoport egy részcsoportjának teljes inverz képe a $G \to G/G'$ természetes homomorfizmusnál; mivel Abel-csoportban minden részcsoport normális, így $N \triangleleft G$ (normálosztó teljes inverz képe).
G/G'-at szokás G_{ab}-vel jelölni; a fentiek és a második izomorfizmus tétel szerint G_{ab} a *homomorf értelemben legnagyobb kommutatív képe G-nek.*
Világos, hogy $[a,b] = e$ pontosan akkor teljesül az $a, b \in G$ elemekre, ha egymással felcserélhetők, azaz $ab = ba$ és így $G' = e \Leftrightarrow G$ kommutatív. Jegyezzük meg, hogy ha pl. G nemkommutatív egyszerű csoport (mint pl. A_5), akkor $G' = G$ az előbbiek szerint, így G minden deriváltja önmaga. A kommutátorrészcsoportjukkal megegyező csoportokat *perfektnek* hívjuk.
Mielőtt továbbmennénk, egy érdekesség. Látható, hogy egy csoport kommutátorainak halmaza tartalmazza az egységelemet (pl. $[e,e] = e$ miatt) és zárt az inverzképzésre is, hiszen $[a,b]^{-1} = [b,a]$. Ebből még nem következik, hogy részcsoport, mert ezekkel a tulajdonságokkal rendelkezik pl. $\mathbb{Z}_9$-ben a $\{(0),(2),(-2)\}$ (rész)halmaz is, amely persze nem részcsoport. Általában nem is igaz, hogy rész-

csoport, tehát a generálás nem hagyható el, azonban *a legfeljebb 95 elemű (!) csoportok körében a kommutátorrészcsoport megegyezik a kommutátorok halmazával*. [7]

Természetes módon értelmezhetjük egy G csoport $G^{(m)}$ $m \geq 1$ „magasabb rendű deriváltjait" is a deriválás szokásos rekurzív képletével: $G^{(m)} \stackrel{\text{def}}{=} (G^{(m-1)})'$; persze $G^{(0)} \stackrel{\text{def}}{=} G$. Például $G'' = G^{(2)}$ G kommutátorrészcsoportjának kommutátorrészcsoportja. Fontos észrevétel, hogy a konjugálás művelettartása miatt minden $m \geq 0$-ra $G^{(m)} \triangleleft G$ teljesül.

Most már meg tudjuk fogalmazni a feloldhatóság fentebb ígért általános kritériumát. Ha $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_k = e$ egy kommutatív lánca a G (feloldható) csoportnak, akkor itt a kommutátorrészcsoport alapvető tulajdonsága miatt $N_k \geq$ $\geq G^{(k)}$ teljesül (mert a faktorok kommutatívak). Ebből adódik, hogy $G^{(k)} = e$. Megfordítva, ha a $G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \ldots \triangleright G^{(k)} = e$, azaz az ún. **kommutátorlánc** „leér" az egységelemig, akkor ez egy kommutatív lánca G-nek, így az feloldható. Ezzel beláttuk a következőt:

2.8.9. Tétel: *A G csoport pontosan akkor feloldható, ha $G = G^{(0)} \triangleright G^{(1)} \triangleright \ldots \triangleright$ $\triangleright G^{(k)} = e$ teljesül valamely $k \geq 0$-ra.*
A G feloldható csoport minden kommutatív lánca „tartalmazza a kommutátorláncot", így G derivált hossza éppen a kommutátorláncának hossza.

Érdemes megemlíteni, hogy ezzel a tétellel a feloldható csoport részcsoportjának és a feloldható csoportok direkt szorzatának (2.8.5. $i)$ és $iii)$) feloldhatóságára a fentinél egyszerűbb és elegánsabb bizonyítást adhatunk. Ugyanis nyilvánvalóan $H \leq G$ esetén $H^{(n)} \leq G^{(n)}$, így ha utóbbi megegyezik e-vel valamely n-re, akkor $H^{(n)} = e$ is teljesül; ebből a bizonyításból is kiderült, hogy H derivált hossza legfeljebb akkora, mint G-é. A másik állításhoz csak arra van szükség, hogy ha $G_1, \ldots, G_k$ feloldható csoportok, akkor $(G_1 \times \ldots \times G_k)^{(m)} = G_1^{(m)} \times \ldots \times G_k^{(m)}$

a direkt szorzatból adódóan. Ez mutatja, hogy a direkt szorzat kommutátorlánca max $\{\ell_i : i = 1,2,\ldots,k\}$ lépésben leér az egységelemig, ahol ℓ_i a G_i derivált hossza. Az is világos, hogy ennél kevesebb lépés viszont nem elég (mert akkor valamelyik G_i kommutátorláncának még nincs vége), így a direkt szorzat derivált hossza megegyezik a direkt faktorok derivált hosszainak maximumával.

A „kommutátorok nyelvén” egyszerűen leírható néhány fontos eddigi fogalmunk.
Először is kézenfekvő rekurzív módon általánosítjuk a (kettős) kommutátor definícióját. Legyen G csoport, $x_i \in G$ $(i = 1,2,\ldots,k)$. Ha $k-1$ elem kommutátorát már értelmeztük, akkor az $[x_1, x_2, \ldots, x_k]$ kommutátort így definiáljuk:

$$[x_1, x_2, \ldots, x_k] \stackrel{\text{def}}{=} [[x_1, x_2, \ldots, x_{k-1}], x_k]$$

Egyetlen x elem $[x]$ kommutátora legyen saját maga. Egyszerűen „kiszámolható” a következő azonosság: $[ab, c] = [a, c]^b [b, c]$, ahol a b-edik hatványra emelés a b-vel való konjugálást jelenti. Ebből természetesen $[a, bc]$ is könnyen származtatható, hiszen mint láttuk $[a, bc] = [bc, a]^{-1}$.

A kommutátorképzés részhalmazokra is definiálható. Legyenek tehát $X, Y \subseteq$ $\subseteq G$ nemüres részhalmazok. Értelmezzük e két részhalmaz ún. *ferde kommutátorát* a következőképpen:

$$[X, Y] \stackrel{\text{def}}{=} \langle [x, y] \mid x \in X, y \in Y \rangle$$

Világos, hogy ezzel a definícióval $G' = [G, G]$, $G'' = [G', G']$, $G^{(k)} = \left[G^{(k-1)}, G^{(k-1)}\right]$. Továbbmenve értelmezhetjük (tetszőleges) $X_1, X_2, \ldots, X_m$ véges sok nemüres részhalmaz ferde kommutátorát is a következő rekurzióval:

$$[X_1, X_2, \ldots, X_m] \stackrel{\text{def}}{=} [[X_1, X_2, \ldots, X_{m-1}], X_m]$$

Néhány, a ferde kommutátorokkal felírt egyszerű állítást foglalunk össze a következő tételben:

2.8.10. Tétel: *Legyen G csoport.*

i) Legyen $N \leq G$. Ekkor $N \triangleleft G \Leftrightarrow [N, G] \leq N$.

ii) Az $X, Y \leq G$ nemüres részhalmazok bármely két eleme felcserélhető egymással $\Leftrightarrow [X, Y] = e$.

Speciálisan $X = H \leq G$, $Y = G$ esetén ez a következőt jelenti:

$H \leq Z(G) \Leftrightarrow [H, G] = e$.

iii) A $G = N_0 \triangleright N_1 \triangleright N_2 \ldots \triangleright N_k = e$ normállánc pontosan akkor kommutatív lánc, ha $[N_i, N_i] \leq N_{i+1}$ $\forall i = 0,1, \ldots, k-1$-re.

iv) Ha $N, M \triangleleft G$, akkor $N \cap M \geq [N, M] \triangleleft G$.

v) Ha $K, L, M \triangleleft G$, akkor $[KL, M] = [K, M]\,[L, M]$.

Bizonyítás: $i)$ $N \leq G$ pontosan akkor normálosztó, ha a konjugálásra zárt, azaz $g^{-1}ng \in N$ $\forall g \in G$. A részcsoportság miatt ez ekvivalens azzal, ha n^{-1}-zel „balról szorozzuk a feltételt”, azaz $N \triangleleft G \Leftrightarrow n^{-1}g^{-1}ng = [n, g] \in N$ $\forall g \in \in G \Leftrightarrow [N, G] \leq N$ (a generált részcsoport legszűkebbségi tulajdonsága miatt).

$ii)$ $xy = yx$ $\forall x \in X, y \in Y \Leftrightarrow x^{-1}y^{-1}xy\,[x, y] = e$ $\forall x \in X, x \in Y \Leftrightarrow \langle [x, y] \rangle = [X, Y] = e$.

$iii)$ Mint láttuk, $(N_i)' \leq N_{i+1}$ $(i = 0,1, \ldots, k-1)$ az N_i/N_{i+1} faktor kommutativitásának szükséges és elégséges feltétele; de $(N_i)' = [N_i, N_i]$ a ferde kommutátor definíciója szerint.

$iv)$ A direkt szorzatnál már láttuk, hogy egy kommutátorban tulajdonképpen két konjugált van „összefűzve”; ezt most $n \in N$ és $m \in M$-re alkalmazva $[n, m] = = \underbrace{n^{-1}m^{-1}n}_{\in M} m = n^{-1}\,\underbrace{m^{-1}nm}_{\in N}$, tehát $[N, M]$ generátorelemei benne vannak $N \cap \cap M$-ben, így a generált ferde kommutátor is. A normálosztóság ismét a konjugálás művelettartásából adódik: $g^{-1}\,[n, m]\,g = \left[\underbrace{g^{-1}ng}_{\in N}, \underbrace{g^{-1}mg}_{\in M}\right]$, azaz a generátorelemek halmaza zárt a konjugálásra, ezért a generált $[N, M]$ is.

$v)$ Definíció szerint $[KL, M] = \langle [k\ell, m] \mid k \in K, \ell \in L, m \in M \rangle$ és a fenti kom-

mutátorazonosságot használva $[k\ell, m] = [k, m]^{\ell}\,[\ell, m]$. Itt $[k, m]^{\ell} = [k^*, m^*]$ valamely $k^* \in K, m^* \in M$ elemekkel a kommutátor konjugáltjára vonatkozó összefüggés és K, M normalitása miatt. Az előbbi eredményt is figyelembe véve írhatjuk, hogy

$$\langle [k\ell, m] \rangle = [k, m]^{\ell}\,[\ell, m] \leq \underbrace{\langle [k, m] \mid k \in K, m \in M \rangle}_{=[K,M]} \underbrace{\langle [\ell, m] \mid \ell \in L, m \in M \rangle}_{=[L,M]}.$$

A másik irányú tartalmazáshoz csak azt a nyilvánvaló tényt kell észrevennünk, hogy $[K, M] \leq [KL, M]$ és $[L, M] \leq [KL, M]$; ekkor persze $[K, M]\,[L, M] \leq$ $\leq [KL, M]$. ∎

2.8.4. Nilpotens csoportok

Most elérkeztünk oda, hogy definiálni tudjuk a nilpotens csoportokat.

Az imént láttuk, hogy a feloldhatóság a kommutátorok nyelvén egy olyan láncot jelent, amelynél a „megelőző” N_i tag saját magával vett $[N_i, N_i]$ (ferde) kommutátora benne van az N_{i+1}-ben. A tetszőleges részcsoportokra kiterjesztett kommutátordefinícióval az előbbinél erősebb feltételt is megfogalmazhatunk:

2.8.11. Definíció: *A G csoportot **nilpotensnek** mondjuk, ha van olyan $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_k = e$ lánca, ahol $[N_i, G] \leq N_{i+1}$ $\forall i = 1,2,\ldots,k-1$ esetén.*

*Az ilyen láncot **centrális láncnak** hívjuk, k a lánc **hossza**.*

*A G nilpotens csoport legrövidebb centrális láncának hossza G **nilpotenciaosztálya**.*

Valójában a definícióban a „$\triangleright$” jelek helyett elég lett volna „$\geq$” jeleket írnunk, ugyanis az $[N_i, G] \leq N_{i+1} \leq N_i$-ből 2.8.10. $i)$ szerint következik, hogy *egy centrális lánc minden tagja normálosztó G-ben is.*

Világos, hogy *minden nilpotens csoport feloldható,* de fordítva nem igaz, mint

hamarosan kiderül. Látjuk, hogy *minden Abel-csoport nilpotens*, mert ezekben bármely két elem kommutátora e-vel egyezik meg; sőt a legfeljebb 1 nilpotenciaosztályú csoportok pontosan az Abel-csoportok (és 0 nilpotenciaosztálya csak az egyelemű csoportnak van). Emellett a véges p-csoportokról bebizonyítjuk majd, hogy nilpotensek is (nemcsak feloldhatóak).

Most fogalmazzuk át a nilpotencia definíciójában szereplő feltételt egy másik szemléletes módon.
$[N_i, G] \leq N_{i+1} \Leftrightarrow [N_i, G]\, N_{i+1}/N_{i+1} = e_{G/N_{i+1}}$, a természetes homomorfizmus tulajdonsága miatt.
Vegyük észre, hogy az előbbi $[N_i, G]\, N_{i+1}/N_{i+1}$ megegyezik $[N_i/N_{i+1}, G/N_{i+1}]$-vel, ugyanis a kommutátor definíciója (és ismét a természetes homomorfizmus tulajdonsága) szerint

$$[N_i/N_{i+1}, G/N_{i+1}] = \left\langle n_i^{-1} g^{-1} n_i g N_{i+1} \mid n_i \in N_i, g \in G \right\rangle =$$

$$= \left\langle n_i^{-1} g^{-1} n_i g \mid n_i \in N_i, g \in G \right\rangle N_{i+1}/N_{i+1} = [N_i, G]\, N_{i+1}/N_{i+1}$$

Mint azt 2.8.10. $ii)$-ben meggondoltuk, az utóbbi pontosan azt jelenti, hogy $N_i/N_{i+1} \leq$ $\leq Z(G/N_{i+1})$, vagyis *egy centrális lánc pontosan egy olyan speciális kommutatív láncot jelent, amelyben (korábbi jelöléseinkkel) minden N_i tag normálosztó G-ben is és az N_i/N_{i+1} faktorcsoport benne van G/N_{i+1} centrumában* $(i = 0,1 \ldots,$ $\ldots, k-1)$*, vagyis N_i része az előbbi centrum teljes inverz képének a $G \to G/N_{i+1}$ természetes homomorfizmusnál.*

Az előbbi átfogalmazás nyomán most két olyan láncot „rendelünk” egy G csoporthoz, melyek hasonló szerepet játszanak a nilpotenciánál, mint a kommutátorlánc a feloldhatóságnál.
Ha G egy tetszőleges csoport, akkor képezhetjük az önmagával való ferde kommutátorait egymás után, azaz legyen $\gamma_1 G = G \geq \gamma_2 G = [G, G] \geq \gamma_3 G =$ $= [\gamma_2(G), G] \geq \ldots \geq \gamma_k G = [\gamma_{k-1} G, G] = \underbrace{[G, G, \ldots, G]}_{k \text{ db}}$. Az így kapott lánc-

ra persze teljesülnek a nilpotencia definíciójában szereplő követelmények, azaz hogy a „megelőző” tag és G kommutátora benne van a következő tagban (mert azt éppen így definálták); emellett semmi nem garantálja, hogy a lánc „leér” az egységelemig, azaz teljesül-e $\gamma_k G = e$ valamely k-ra. Ez nem is feltétlenül van így, hiszen pl. $(A_5)' = A_5$, amint meggondoltuk, tehát ennél a csoportnál a lánc minden tagja A_5. Az előbb definiált láncot G **alsó centrális láncának** nevezzük.

G **felső centrális láncát** így értelmezzük: legyen $\zeta_0 G = e \leq \zeta_1 G = Z(G)$ és általában legyen $\zeta_k G$ a $G/\zeta_{k-1}G$ centrumának teljes inverz képe a $G \to G/\zeta_{k-1}G$ természetes homomorfizmusnál. Látjuk, hogy ez a lánc definíciója alapján ezúttal a fenti átfogalmazásban szereplő centrális lánc-feltételt teljesíti, de most azt nem tudjuk, hogy „felér-e” a G-ig, azaz van-e olyan k, hogy $\zeta_k G = G$. Ez sincs mindig így, ugyanis ha mondjuk G centruma triviális (ilyen pl. S_5), akkor a felső centrális lánc csak az egységelemből áll.

Ahogy a kommutátorlánc, melyet „minden kommutatív lánc tartalmaz”, jelenti a feloldható csoportoknál a legrövidebb kommutatív láncot, úgy az alsó és felső centrális láncok jelentik az „optimális” centrális láncot nilpotens csoportoknál a következő tétel szerint, mely ugyanúgy bizonyítható, ahogy feloldható csoportokra vonatkozó párja:

2.8.12. Tétel: *Legyen G nilpotens csoport és $G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \ldots \triangleright N_k = e$ egy centrális lánca G-nek. Ekkor fennállnak a következők:*
$\gamma_i G \leq N_{i-1}\ \forall i = 1,2,\ldots,k+1$*;*
$\zeta_j G \geq N_{k-j}\ \forall j = 0,1,\ldots k$.
Speciálisan tehát $\gamma_{k+1} G = e$ és $\zeta_k G = G$ és ***G nilpotenciaosztálya megegyezik az alsó és a felső centrális lánc hosszával*** *(ami itt k).*

Előbbi tételünk mutatja, hogy ha egy $e \neq G$ csoport centruma triviális, akkor nem lehet nilpotens; így pl. S_3 nem nilpotens, habár feloldható ($S_3 \triangleright \langle(123)\rangle \triangleright e$ egy

kommutatív lánc).

Most igazoljuk a nilpotencia néhány „öröklődési” tulajdonságát:

2.8.13. Tétel:

i) Ha G nilpotens és $H \leq G$, akkor H is nilpotens.

ii) Ha G nilpotens és $N \triangleleft G$, akkor G/N is nilpotens.

iii) Ha $G_1, G_2, \ldots, G_n$ nilpotens csoportok, akkor $G_1 \times G_2 \times \ldots \times G_k$ is nilpotens.

Bizonyítás: $i)$ Világos, hogy $\gamma_n G \geq \gamma_n H \ \forall n = 1,2,\ldots$; ebből következik az állítás és persze az is, hogy H nilpotenciaosztálya legfeljebb annyi, mint G-é.

$ii)$ Megvizsgáljuk G és G/N alsó centrális láncának kapcsolatát. Nézzük először $[G/N, G/N] = \gamma_2(G/N)$-et!

Ez definíció szerint $\gamma_2(G/N) = \langle [g,h]\, N \mid g,h \in G \rangle = (\gamma_2 G)N/N$ a természetes homomorfizmus tulajdonsága alapján.

Ugyanilyen meggondolással: $\gamma_3(G/N) = [\gamma_2(G/N), G/N] = [(\gamma_2 G)N/N, G/N] =$

$= [(\gamma_2 G)N, G]\, N/N = \big(\underbrace{[\gamma_2 G, G]}_{=\gamma_3 G} \underbrace{[G, N]}_{\leq N} \big) N/N = (\gamma_3 G)N/N.$

Folytatva azt kapjuk, hogy $\gamma_m G/N = (\gamma_m G)N/N$, azaz a *homomorf kép alsó centrális lánca az eredeti lánc (tagonként vett) homomorf képe*; mivel $\gamma_k G = e$ valamely k-ra, így legkésőbb a k-adik lépésben $\gamma_k G/N = e_{G/N}$.

G/N tehát nilpotens és nilpotenciaosztálya legfeljebb annyi, mint G nilpotenciaosztálya.

$iii)$ Ennek igazolása a feloldhatóság véges direkt szorzatra való öröklődésének igazolására látott kommutátorláncos érvelés párja:

$\gamma_k(G_1 \times G_2 \times \ldots \times G_n) = \gamma_k G_1 \times \gamma_k G_2 \times \ldots \times \gamma_k G_n$; eszerint max $\{c_i : i = 1,2,\ldots,n\}$ lépésben, ahol c_i a G_i nilpotenciaosztálya, a direkt szorzat alsó centrális lánca eléri az egységelemet (kevesebb lépésben pedig nem, azaz a nilpotenciaosztálya az előbbi maximum). ∎

Amint ígértük, most bebizonyítjuk, hogy a véges p-csoportok nilpotensek; az érvelés hasonló lesz, mint amit a feloldhatóságnál láttunk.

2.8.14. Tétel: *Minden* $|G| = p^k$ $(k \geq 1)$ *p-csoport nilpotens.*

Bizonyítás: Teljes indukció k-ra; $k = 1$ esetén az állítás igaz (hiszen $\mathbb{Z}_p$ kommutatív is), így legyen most $k \geq 2$.
Mint tudjuk $Z(G) > e$ és $Z(G) = G$ esetén G kommutatív, ebben az esetben tehát készen vagyunk; feltehető emiatt, hogy $Z(G) < G$. Ekkor $G/Z(G)$ az indukciós feltevés szerint nilpotens; legyen egy centrális lánca $G/Z(G) = G_0/Z(G) \triangleright$ $\triangleright G_1/Z(G) \triangleright \ldots \triangleright G_k/Z(G) = e_{G/Z(G)}$ (ld. a 2.8.5. tétel bizonyításában tett megjegyzésünket arra vonatkozólag, hogy a lánc tagjait ilyen alakban írhatjuk).
Írjuk fel, mit jelent, hogy a lánc centrális:
$[G_i/Z(G), G/Z(G)] \leq G_{i+1}/Z(G) \Leftrightarrow \forall g_i \in G_i, g \in G\, \exists\, g_{i+1} \in G_{i+1}$, $z \in$ $\in Z(G)$ $[g_i, g] = \underbrace{zg_{i+1}}_{\in G_{i+1}} \Rightarrow [G_i, G] \leq G_{i+1} (i = 0,1,\ldots,k-1)$

Itt egyszerűen a centrum szerinti bal oldali mellékosztályok egyezésének feltételét írtuk fel és kihasználtuk, hogy elég a $[g_i, g]$ alakú kommutátorelemekre (mint generátorokra) vizsgálni az állítást. Azt kaptuk, hogy $G/Z(G)$ láncában a tagok G_i teljes inverz képét képezve egy $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_k = Z(G)$ centrális lánchoz jutunk G és $Z(G)$ között; ez továbbra is centrális lánc marad, ha a végére írjuk e-t (ami tulajdonképpen $Z(G)$ centrális lánca), ugyanis $[G, Z(G)] = e \leq e$. Az imént tehát G-nek egy centrális láncát állítottuk elő. ∎

Jegyezzük meg, hogy a bizonyításból az derült ki, hogy tetszőleges $N \triangleleft G$ esetén G/N egy centrális láncának megfelel G-nek egy N-ig terjedő centrális lánca. Az előbbi érvelést azért fejezhettük be, mert $Z(G) = N$ mellett a láncot $N \triangleright e$-vel „lezárhattuk”. A bizonyítás tehát tetszőleges csoportra működik, amelyben a centrumnak van olyan részcsoportja, mely szerinti faktor nilpotens.

A nilpotencia azonban (szemben a feloldhatósággal) általában *nem öröklődik a bővítésnél*, pl. S_3 nem nilpotens, mert triviális a centruma, viszont $\mathbb{Z}_3 \cong N = \langle (123) \rangle \triangleleft S_3 = G$ és $G/N \cong \mathbb{Z}_2$ is nilpotens. Tehát *G/N és N nilpotenciájából nem következik G nilpotenciája* (szemben a feloldhatósággal).

A véges csoportok esetében a nilpotencia több „szép” tulajdonsággal ekvivalens.

2.8.15. Tétel: *Legyen G véges csoport. A következő tulajdonságok ekvivalensek:*
$i)$ G nilpotens.
$ii)$ Minden $H \leq G$ részcsoporthoz van G és H között normállánc (az ilyen részcsoportokat szubnormálosztóknak hívják).
$iii)$ G minden maximális részcsoportja normálosztó G-ben.
(Maximális részcsoport alatt értelemszerűen olyan $H < G$ részcsoportot értünk, melyre $H < M \leq G \Rightarrow M = G$.)
$iv)$ G a p-Sylow részcsoportjainak direkt szorzata.

Bizonyítás: $i) \Rightarrow ii)$: Tekintsük $K_i = H\gamma_i G$-t! Ekkor $K_i \triangleright K_{i+1}$, mivel utóbbi a $G \to G/\gamma_{i+1}G$ természetes homomorfizmus K_i-re való megszorításánál a $\gamma_{i+1}G \triangleleft K_i$ normálosztó képének teljes inverz képe. G nilpotens, így $\gamma_c G = e$ valamely $0 \leq c$ egészre, ezért legfeljebb $j \leq c$ lépésben $K_j = H$, vagyis létezik legfeljebb c hossszúságú G és H közötti normállánc.

$ii) \Rightarrow iii)$: Legyen $H < G$ maximális részcsoport. Ekkor H szubnormálosztó G-ben, de ha legalább „két lépésben” lenne az, akkor tartalmazná egy valódi részcsoportja G-nek, ami ellentmond a maximalitásnak. Így $H \triangleleft G$.

$iii) \Rightarrow iv)$: Először belátjuk, hogy minden p-Sylow normálosztó, azaz (ami a III. Sylow alapján, mint láttuk, ugyanezt jelenti) pontosan egy db p-Sylow részcsoport van minden szóba jövő p prímre. Tegyük fel indirekt, hogy valamely q prímre $\left|\mathrm{Syl}_q(G)\right| = |G : N_G(Q)| > 1$, ahol Q egy q-Sylowot jelöl. Ekkor tehát

Q normalizátora egy valódi részcsoport G-ben és benne van egy R maximális részcsoportban (véges sok $N_G(Q)$-t tartalmazó részcsoportot kell végignézni). De itt $R \triangleleft G$, azaz $N_G(R) = G$, ami ellentmond annak a tételnek, hogy egy olyan részcsoport, mely tartalmazza egy p-Sylow részcsoport normalizátorát, saját magát kell hogy normalizálja (2.6.6. tétel).
Mivel különböző prímekhez tartozó Sylow-részcsoportok csak az egységelemben metszhetik egymást (amint a rend tulajdonságából látszik), így a 2.2.14. tételt valamint a részcsoportok normalitását felhasználva $G = P_1P_2 \cdots P_k$ és
$P_i \bigcap \langle P_j \mid j \neq i \rangle = e$. Ehhez még azt kell meggondolnunk, hogy egy kiválasztott P_i nem lehet benne *néhány* P_{j_s} $(j_s \neq i)$ *által generált* $\langle P_{j_s} \rangle$ *részcsoportban sem*. Valóban, mint láttuk, egymást triviálisan metsző normálosztók elemenként felcserélhetők; ebből adódik, hogy az utóbbi generált részcsoport egy elemének rendje az egyes részcsoportokba eső „komponensek” rendjeinek legkisebb többszöröse, amely relatív pím lesz a P_i-hez tartozó p_i prímhez. Eszerint valóban $G \cong \prod_{i=1}^{k} P_i$.

$iv) \Rightarrow i)$: Mint láttuk, minden véges p-csoport nilpotens és véges sok nilpotens csoport direkt szorzata is az. ∎

A tétel szerint az összes véges nilpotens csoport szerkezetének leírása az összes véges p-csoport szerkezetének leírásával egyenértékű; utóbbi azonban (szintén) nagyon nehéz problémát jelent, mert a véges p-csoportok minden speciális tulajdonságuk ellenére elég bonyolultak lehetnek.

2.8.5. A Frattini-részcsoport

Végül ismerkedjünk meg a nilpotens csoportokkal kapcsolatban még egy fogalommal, melynek segítségével egy másik, szemléletes leírás adható a véges nilpotens csoportokra.

2.8.16. Definíció: *A G csoport maximális részcsoportjainak metszetét* Frat G*-vel jelöljük és G* ***Frattini-részcsoportjának*** *nevezzük.*
Ha G-nek nincsen maximális részcsoportja, akkor Frat $G \stackrel{def}{=} G$.

Például Frat $\mathbb{Z}_6 = e$, ugyanis mindkét prím elemszámú részcsoportja (melyekből egy-egy van) maximális és metszetük csak az egységelemből áll. Jegyezzük meg, hogy *véges csoportnak mindig van maximális részcsoportja* (e-ből elindulva véges sok tartalmazáson keresztül G-hez érünk). Ezzel szemben meggondolható, hogy pl. a kváziciklikus p-csoportoknak nincsen maximális részcsoportjuk.
Világos, hogy Frat $G \triangleleft G$, sőt a Frattini-részcsoport ún. **karakterisztikus részcsoportja** G-nek, azaz G minden automorfizmusánál (amely persze maximális részcsoportot maximális részcsoportba kell hogy vigyen) fixen marad (így a konjugálásoknál is).
A Frattini-részcsoport a következő meglepő módon is karakterizálható:

2.8.17. Tétel: *Legyen G csoport.*
Frat G megegyezik G ún. nemgenerátorainak halmazával, azaz pontosan az olyan $g \in G$ elemekből áll, melyekre $\langle g, X\rangle = G \Rightarrow \langle X\rangle = G$ tetszőleges $\emptyset \neq X \subseteq G$ részhalmazra.

Bizonyítás: Legyen először $g \in$ Frat G és tegyük fel, hogy $\langle g, X\rangle = G$, de $\langle X\rangle \neq G$ valamely $X \subseteq G$-re.
Ekkor $g \notin \langle X\rangle$ és itt nem részletezendő halmazelméleti megfontolásokkal belátható (a *Zorn-lemmát* használva), hogy létezik egy *legnagyobb* olyan $\langle X\rangle$-et tartalmazó M részcsoport G-ben, melyre $g \notin M$; tehát ha $M < N \leq G$, akkor $g \in N$. Nyilván $M \neq G$ (mert g nincs benne). Azt állítjuk, hogy ebben az esetben M maximális részcsoport G-ben: ha ugyanis az előbbi $M < N < G$ teljesülne, akkor $\langle g, N\rangle = N$, ami nem lehet, hiszen $\langle g, N\rangle \geq \langle g, X\rangle = G$. De így is ellentmondást kaptunk, mert eredményünk szerint g nincs benne az M ma-

ximális részcsoportban, de benne van a Frattini-részcsoportban (persze ha G-nek nincsenek is maximális részcsoportjai, akkor egy ilyen megtalálása jelenti az ellentmondást).

Megfordítva tegyük fel, hogy a $g \in G$ elemre $\langle g, X\rangle = G \Rightarrow \langle X\rangle = G$ minden nemüres X részhalmazra, de valamely $M < G$ maximális részcsoportban nincs benne g (persze ha $G = Frat\, G$, akkor ez eleve nem lehet). De ezzel az M-mel a maximalitás miatt $\langle g, M\rangle = G$ és $\langle M\rangle = M \neq G$, ami ellentmondás. ∎

Most megadjuk az ígért jellemzését a véges nilpotens csoportoknak.
Először is a 2.8.15. tétel szerint egy ilyen csoportban minden maximális részcsoport indexe prím kell hogy legyen. Ugyanis a feladatok között belátjuk majd, a korábbi jelöléssel $G = P_1 \times P_2 \times \ldots \times P_k$ minden részcsoportja $P_1^* \times P_2^* \times \times \ldots \times P_k^*$ alakú, ahol $P_j^* \leq P_j$. Mivel minden részcsoport szubnormálosztó, és minden normállánc kompozícólánccá finomítható, így egy ilyen részcsoport pontosan akkor lesz maximális, ha pontosan az egyik p-Sylow-ból választunk egy p indexű részcsoportot (ui. a p-csoportokban a feloldhatóság miatt csak a prím indexű részcsoportok maximálisak).
Mivel a maximális részcsoportok normálosztók is, így előbbi állításunkat is használva ha $M \leq G$ maximális, akkor $G/M \cong \mathbb{Z}_p$ valamely p-re, így $G' \leq M$ a kommutátorrészcsoport tulajdonsága szerint. Vagyis G' minden maximális részcsoportban benne van, így $G' \leq Frat\, G$.
Megfordítva, $G' \leq$ Frat G esetén minden M maximális részcsoport tartalmazza G'-t, ezért (mint láttuk) $M \triangleleft G$, és a 2.8.15. tételre hivatkozva G nilpotens.
A következő tételt láttuk be:

2.8.18. Tétel: *A G véges csoport pontosan akkor nilpotens, ha $G' \leq Frat\, G$.*

2.9. Szabad csoportok és prezentációk

Ebben a részben először természetes módon definiálunk „teljesen absztrakt” csoportokat, melyekről kiderül, hogy ilyenek homomorf képeként minden csoport előáll. Ezután az ilyen előállításokról esik majd pár szó.

2.9.1. Szabad csoportok

Legyen $X \neq \emptyset$ egy halmaz és vegyünk egy ezzel azonos számosságú, de tőle diszjunkt másik halmazt, melyet (szuggesztív módon) X^{-1}-zel jelölünk, az elemekre is alkalmazva a jelölést; tehát ha α egy $X \to X^{-1}$ tetszőleges bijekció és $x \in X$, akkor $X^{-1} \ni x^{-1} := (x)\alpha$.
Készítsünk **szavakat** a $x_\tau^{\beta_\tau} : x_\tau \in X,\ \beta_\tau = \pm 1$ **betűk** véges sokszori egymás mellé írásával, azzal a megállapodással, hogy nem írunk egymás mellé x_τ-t és x_τ^{-1}-t; az ilyet **tiltott szónak** mondjuk. (A τ indexelés arra utal, hogy X tetszőleges számosságú halmaz lehet.) Természetesen egyetlen betűt is szónak tekintünk és *két szó akkor és csak akkor egyezik meg, ha megfelelő komponenseik (betűik) megegyeznek*. Két példa szavakra az $x_1x_1x_1$ és az $x_2^{-1}x_5x_3x_6^{-1}$ $\big($itt mondhatjuk, hogy $X = \{x_1, x_2, \ldots, x_5\}\big)$. Jelöljük az **üres szót** (amelyben 0 db betű szerepel) 1-gyel. A szó **hosszának** nevezzük a benne szereplő $x_i^{\beta_i}$-k számát $(\beta_i = \pm 1)$, tehát az előbbi példánkban a szavak hossza rendre 3 és 4 és az egyetlen 0 hosszúságú szó az üres szó.

Most a szavak halmazán értelmezünk egy szorzást, amely „vizuálisan” teljesen egyezik az eddigi szorzással. Legyen ugyanis a $w_1 = x_1^{\beta_1}x_2^{\beta_2}\ldots x_k^{\beta_k}$ és a $w_2 = y_1^{\gamma_1}y_2^{\gamma_2}\ldots y_\ell^{\gamma_\ell}$ $(x_i, y_j \in X,\ \beta_i, \gamma_j = \pm 1)$ *szavak szorzata* az ezek egymás mellé írásával kapott szó:

$$w_1w_2 \stackrel{\text{def}}{=} x_1^{\beta_1}x_2^{\beta_2}\ldots x_k^{\beta_k}y_1^{\gamma_1}y_2^{\gamma_2}\ldots y_\ell^{\gamma_\ell}.$$

Az üres szóval akármelyik irányból való szorzás persze bármely szót fixen hagy. Megtörténhet, hogy $x_k = y_1$ és $\beta_k = -\gamma_1$, tehát egy tiltott szó keletkezik a szorzásnál: ekkor úgy járunk el, hogy ezt töröljük. Ha most újra tiltott szó keletkezik, akkor azt is töröljük és így tovább, egészen addig folytatjuk az eljárást, míg nincs több tiltott szó. Amint látható, előfordulhat, hogy egészen az üres szóig kell „egyszerűsítenünk", ha ugyanis w_1-ben és w_2-ben éppen fordított sorrendben szerepeltek ugyanazok a betűk és ellenkező előjelű „kitevőn" (amely kitevő egyelőre csak egy jelölés), akkor $w_1 w_2 = 1$ (látjuk: itt éppen a szorzat inverzének már megszokott alakja bukkan fel).

Az előbbi módon értelmezett szorzásról pl. a középső szó hossza szerinti teljes indukcióval könnyű meggondolni, hogy *asszociatív*; ez a tiltott szavak „felbukkanása" miatt nem egészen nyilvánvaló. Az eddigiek alapján tehát definiálhatunk egy csoportot:

2.9.1. Tétel: *Legyen $X \neq \emptyset$ egy halmaz, X^{-1} pedig jelöljön egy ugyanakkora számosságú, X-től diszjunkt halmazt.*
Az $x_1^{\beta_1} x_2^{\beta_2} \dots x_k^{\beta_k} : \ x_j \in X, \beta_j = \pm 1$ alakú szavak az üres szóval együtt csoportot alkotnak az „egymás mellé írás" műveletére nézve.
Egységelem az üres szó és a $w = x_1^{\beta_1} x_2^{\beta_2} \dots x_k^{\beta_k}$ szó inverze a $w^* = x_k^{-\beta_k} x_{k-1}^{-\beta_{k-1}} \dots x_1^{-\beta_1}$.
*Ezt a csoportot az **X által generált szabad csoportnak** nevezzük és F_X-szel jelöljük.*
*X elemei F_X **szabad generátorai** és azt is mondjuk, hogy F szabad X-en.*
Azt mondjuk, hogy F szabad csoport, ha létezik $\emptyset \neq X$ halmaz, melyre $F_X = F$.

Például ha $X = \{a\}$ egyelemű halmaz, akkor az előbbi szabad csoport a jól ismert végtelen ciklikus csoport:

$$F_X = \{\dots, a^{-1}a^{-1}, a^{-1}, 1, a, aa, aaa, \dots\} \cong \mathbb{Z}$$

Emellett a szavak egyezéséről mondottak szerint egy legalább kételemű X hal-

maz által generált szabad csoport *nemkommutatív*, hiszen az $x_1, x_2 \in X$ elemekre $x_1x_2 \neq x_2x_1$. Ugyancsak egyszerűen végiggondolható észrevétel, hogy minden szabad csoport *torziómentes*. Definíciónkból az is látszik, hogy $\emptyset \neq Y \subseteq X$ esetén $F_Y \leq F_X$.
Amint már most is sejthető, a szabad csoport szerkezete igazából csak $|X|$-től függ, tehát azonos számosságú halmazok által generált szabad csoportok izomorfak; ezt hamarosan be is bizonyítjuk.

Ha adott F_X-ben egy szó, akkor benne ugyanazon betű egymás melletti példányait az egyszerűbb jelölés miatt „összevonhatjuk", pl. $w = x_1x_2x_2x_2x_2x_3^{-1}x_3^{-1}x_4$-ben az x_2-kből és x_3^{-1}-ekből álló részeket összevonva ezt kapjuk: $w = x_1x_2^4x_3^{-2}x_4$. Ezt az egyértelmű felírást, amely a szorzási definícióval összhangban van és amelyből a szó eredeti alakja persze leolvasható, a szó **normálalakjának** hívjuk és a továbbiakban általában ekként gondolunk majd a szabad csoport elemeire.

Most belátjuk azt az egyszerű tételt, majd annak közvetlen következményét, mely a szabad csoportoknak a pont elején jelzett jelentőségére mutat rá. A bizonyítás (és a tétel állítása) némileg arra hasonlít, ahogyan vektorterek közötti lineáris leképezéseket egyértelműen meghatároznak a báziselemek képei.

2.9.2. Tétel: *Legyen $\emptyset \neq X$ egy halmaz, G egy csoport.*
Ekkor minden $f : X \to G$ függvényhez létezik pontosan egy $\varphi : F_X \to G$ homomorfizmus, amelynél $(x)\varphi = (x)f \ \forall x \in X$.

Bizonyítás: Világos, hogy ha a keresett homomorfizmus létezik, akkor egyértelmű, ugyanis minden szó képe ismert a művelettartás miatt, ha az összes betű (azaz az üres betűn/szón kívül X összes elemének) képét ismerjük; ezeket pedig az $x \mapsto (x)f$ függvénnyel megadtuk:

$$\left(x_1^{\beta_1}x_2^{\beta_2}\dots x_k^{\beta_k}\right)\varphi = \left((x_1)\varphi\right)^{\beta_1}\cdots\left((x_k)\varphi\right)^{\beta_k} = \left((x_1)f\right)^{\beta_1}\cdots\left((x_k)f\right)^{\beta_k}$$

Itt a β_i-k már tetszőleges egész kitevőket jelölnek. Fontos észrevétel, hogy az

előbbi megadás azért értelmes, mert minden szó egyértelműen írható betűk szorzataként: ha valamelyiket többféleképpen írhatnánk fel, akkor a különböző felírásokhoz tartozó függvényértékeket „össze kéne hangolni”, amiről egyáltalán nem tudjuk, hogy mindig megvalósítható.
Persze $(1)\varphi \stackrel{\text{def}}{=} e_G$ és nem nehéz látni, hogy az így definiált $X \to G$ függvény valóban homomorfizmus, ezért a bizonyítással készen is vagyunk. ∎

Az előbbi, függvények közötti kapcsolatot így jelöljük majd: $X \overset{\sigma}{\underset{f}{\rightrightarrows}} F_X \xrightarrow{\beta} G$, ahol σ az X beágyazását jelöli F_X-be. Megjegyezzük, hogy a bizonyításban kiemelt egyértelmű felírás tulajdonság jellemzi is a szabad csoportokat, ugyanis igaz a következő: ha a G csoportot generálja az $X \subseteq G$ részhalmaza és G minden $\neq e$ eleme egyértelműen írható $\prod x_i^{\alpha_i} : x_i \in X, \alpha_i \neq 0$ alakban, akkor $G \cong F_X$.

A 2.9.2. tételt alkalmazhatjuk pl. úgy, hogy tetszőleges G csoport mellett $G = X$-et választjuk a szabad csoport szabad generátorrendszerének, és az f függvény egyszerűen legyen a $G \to G$ identikus függvény. Ekkor a fent leírt egyértelműen létező $F_X \to G$ homomorfizmus egy epimorfizmus, azaz $G \cong F/N$ valamely $N \lhd F_X$ mellett: G az F_X homomorf képe. Persze a fenti X helyett választhatjuk G tetszőleges olyan X részhalmazát, melyre $\langle X \rangle = G$ és f függvénynek az $x \mapsto x \in G$ „injektálást”; ekkor ugyanis a φ homomorfizmusnál $\operatorname{Im}\varphi = \langle (x)f \mid x \in X \rangle = \langle X \rangle = G$.
Az imént a következő tételt láttuk be:

2.9.3. Tétel: *Minden G csoport előáll egy szabad csoport faktorcsoportjaként, azaz $G \cong F/N$ valamely F szabad csoporttal és annak $N \lhd F$ normálosztójával.*

Egy G csoport előállítását F/N alakban G (egy) **prezentációjának** hívjuk. A fenti meggondolások mutatják, hogy ez az előállítás nem egyértelmű, hiszen pl. $\mathbb{Z}_n$ esetén $F_n = F_{\{1,2,\ldots,n\}}$-nel és $F_1 \cong \mathbb{Z}$-gyel is történhet a fent bemutatott kétféle megvalósítás ($\mathbb{Z}_n$ egyetlen elemmel is generálható). Még akkor sem egyértelmű,

ha adott F, ui. többféleképpen választhatjuk pl. az f függvényt. Hamarosan lesz még szó prezentációkról.

A 2.9.2. tételnek most egy elvi fontosságú alkalmazását mutatjuk be:

2.9.4. Tétel: *Legyen $\neq X, Y$ két halmaz, $|X| = |Y|$.*
Ekkor $F_X \cong F_Y$: azonos számosságú halmazok által generált szabad csoportok izomorfak.

Bizonyítás: Jelölje rendre σ_1 és σ_2 az X-et F_X-be és Y-t F_Y-ba injektáló függvényt (minden betűhöz önmagát rendeljük) és rögzítsünk egy $f : X \to Y$ bijekciót (ami az egyező számosság miatt létezik).
Ekkor fenti tételünk szerint egyértelműen léteznek olyan β_1 és β_2 $F_X \to F_Y$ és $F_Y \to F_X$ homomorfizmusok, melyekről a következőket tudjuk:

$$X \xrightarrow[f\sigma_2]{\sigma_1} F_X \xrightarrow{\beta_1} F_Y \quad \text{és} \quad Y \xrightarrow[f^{-1}\sigma_1]{\sigma_2} F_Y \xrightarrow{\beta_2} F_X$$

Vizsgáljuk meg a $\sigma_1\beta_1\beta_2$ függvényt; ez a kompozíció értelmes és X-ből F_X-be képez:

$$\overbrace{\sigma_1\beta_1}^{f}\beta_2 = f\overbrace{\sigma_2\beta_2}^{f^{-1}\sigma_1} = ff^{-1}\sigma_1 = \sigma_1.$$

Eszerint a $\beta_1\beta_2$ egy olyan $F_X \to F_X$ homomorfizmus, melyre fennáll, hogy $X \xrightarrow[\sigma_1]{\sigma_1} F_X \xrightarrow{\beta_1\beta_2} F_X$; de tudjuk, hogy az id_{F_X} függvény is ilyen, ezért az egyértelműség miatt $\beta_1\beta_2 = id_{F_X}$. Ugyanilyen érveléssel kapjuk ($\sigma_2\beta_2\beta_1$-t átalakítva), hogy $\beta_2\beta_1 = id_{F_Y}$. Ezek szerint β_1 egy $F_X \to F_Y$ bijekció, így a művelettartás miatt izomorfizmus: $F_X \cong F_Y$, amint állítottuk. ∎

Bizonyítás nélkül közöljük, hogy előbbi állításunk megfordítása is igaz:
Ha $F_1 \cong F_2$ szabad csoportok az X_1 és X_2 halmazokon, akkor $|X_1| = |X_2|$.
Az előbbiek alapján kölcsönösen egyértelmű megfeleltetés van a nemnulla számosságok és a szabad csoportok (izomorfiatípusai) között: adott α számossághoz létezik egy ilyen számosságú halmazon szabad csoport (ahogy fent megadtuk),

amely imént bizonyított tételünk szerint (izomorfia erejéig) csak α-tól függ; két különböző számossághoz pedig egymással nem izomorf szabad csoportok tartoznak a nem bizonyított állítás értelmében. Az F szabad csoport szabad generátorrendszerének számosságát F **rangjának** nevezzük. Amint láttuk, pl. $\mathbb{Z} \cong F_1$ rangja 1.

Rövid halmazelméleti kitérőt téve emeljük ki az előbbi tétel két közvetlen (egymással is összefüggő) és önmagukban is érdekes következményét:

2.9.5. Tétel: *Tetszőleges $\alpha \neq 0$ számosságra létezik α számosságú csoport.*
Következmény: Az összes csoport(izomorfiatípus)ok nem alkotnak halmazt.

Bizonyítás: Ha $\alpha = n$ véges számosság, akkor persze $\mathbb{Z}_n$ egy ilyen számosságú (elemszámú) csoport (és mint jeleztük, van olyan n, amikor nincs is más).
Ha α végtelen számosság, akkor F_α-val jelölve egy α számosságú halmaz által generált szabad csoportot, $|F_\alpha| = \alpha$, hiszen világos, hogy $\alpha \leq |F_\alpha|$ (mert „α"-nyi betű van), másrészt $|F_\alpha| = (1+)\alpha + \alpha^2 + \alpha^3 + \ldots = \alpha + \alpha + \ldots = \alpha\aleph_0 \leq \alpha^2 = \alpha$.
Itt a szavak uniójaként írtuk fel F_α-t azok hossza szerint csoportosítva, ahol az $(1+)$ az egyetlen 0 hosszúságú szó „járuléka" ($1 + \alpha = \alpha$ miatt van zárójelben) és a számosságaritmetika (összeomlásának) szabályait használtuk (a felsorolásban semmi nem szerepel kétszer, mert a szavak egyértelműen írhatók betűk szorzataként).
Kaptuk: $\alpha \leq |F_\alpha| \leq \alpha \Rightarrow |F_\alpha| = \alpha$ a Schröder-Bernstein tétel alapján.

A következmény igazoláshoz tegyük fel indirekt, hogy mégis egy Γ halmazt alkot az összes csoport. Ekkor ennek egy Ω részhalmaza az összes szabad csoport(izomorfiatípus)ból álló osztály. Az előbbi részhalmaz képe a $H \mapsto |H|$ „számosságoperációnál" a pótlás axiómája miatt halmaz, ami az összes végtelen számosságot tartalmazza (hiszen minden ilyen fellép mint egy szabad csoport számossága az előbbi meggondolásunk szerint). A végtelen számosságok azonban

nem alkotnak halmazt, hiszen ellenkező esetben az összes számosságok is azt alkotnának (mert a véges számosságok azt alkotnak), ami nem igaz; ezzel kész az ellentmondás. ∎

2.9.2. Prezentációk

Mint az előző részben kiderült, minden G csoport előáll egy F szabad csoport homomorf képeként, azaz F/N alakban, valamely $N \triangleleft F$-vel. Amint mondtuk, ez előállítás „nagyon nem” egyértelmű, tehát a prezentációhoz meg kell adni F-et és N-et is. Most egy olyan jelölést ismertetünk, amellyel csoportokat prezentációikkal adhatunk meg.

Egy tetszőleges $G = \langle X \rangle$ csoport abban különbözik F_X-től, hogy előbbinél a generátorelemek között lehetnek bizonyos összefüggések. Nevezetesen a generátorelemekből készített „szavak” közül egyesek „nemtriviálisan egybeesnek”, mint pl. $D_n = \langle t, f \rangle$ esetén $tft = f^{-1}$; ilyen összefüggések persze nincsenek az F_X szabad csoportban, annak definíciója szerint. Ezeket az összefüggéseket, melyeket **relációknak** hívunk, mindig megadhatjuk úgy, hogy $g_1^{n_1} \cdot g_2^{n_2} \cdot \ldots \cdot g_k^{n_k} = e$ a megfelelő egyenlőséget egy oldalra rendezve; itt g_i a G néhány (X-ben lévő) generátorelemét jelöli. Egyszerű észrevétel, hogy két relációt összeszorozva, relációt invertálva és konjugálva ismét relációhoz jutunk; ezt persze úgy értjük, hogy a bal oldalon lévő kifejezésekkel és a jobb oldalon lévő e-vel külön-külön végezzük a műveletet. Az előbbi eljárásokkal kapott relációkat az eredeti relációk **következményeinek** mondjuk. Pl. az $x^2y^3 = e$ reláció következménye az $y^{-3}x^{-2} = e$ (invertálás) és az $y^{-1}x^2y^3y = y^{-1}x^2y^4 = e$ (konjugálás).
Az eddig elmondottak alapján definiáljuk a csoportok ún. **definiáló relációkkal** történő megadását:

2.9.6. Definíció: *Legyen $\emptyset \neq X$ egy halmaz és $s_\lambda = e$ $(\lambda \in \Lambda)$ tetszőleges relációk, azaz formális egyenlőségek, amelyeket X elemeivel írunk fel.*
A $G = \langle X \mid s_\lambda = e : \lambda \in \Lambda \rangle$ csoporton a következő csoportot értjük:
$G = F/N$, ahol
$F = \langle X^* \rangle$, α egy $X \to X^*$ bijekció és
N azon szavak által generált normálosztó F-ben, melyeket az s_λ relációkból úgy nyerünk, hogy minden x betűt $(x)\alpha$-ra cserélünk.
*Az X elemeit G **generátorainak** hívjuk, az $s_\lambda = e$ egyenlőségek pedig a **definiáló relációk**.*

Például a $C_n = \langle x \mid x^n = e \rangle$ csoport definíciónk szerint az egyetlen elem (jelölje mondjuk x^*) által generált F_1 szabad csoport azon N normálosztó szerinti faktorcsoportjával izomorf, melyet x^{*n} generál; mivel, mint láttuk, $F_1 \cong \mathbb{Z}$, így látjuk, hogy C_n éppen a már jól ismert $\mathbb{Z}_n$ n elemű ciklikus csoport.
Meggondolható, hogy a definiált faktorcsoportban *pontosan* a definícióban szereplő relációk és azok következményei teljesülnek majd, ui. egy tetszőleges $G = F/N$-beli elemekkel felírt reláció bal oldalának megfelel az $F \to F/N$ természetes homomorfizmus N magjának egy eleme, amely előáll X^* elemeiből szorzásokkal, invertálásokkal és konjugálásokkal.

Amint az érezhető is, az előbbi megadásunk nem feltétlenül működik „fordítva". Ezt úgy értjük, hogy ha adott egy G csoport, akkor nem feltétlenül tudjuk annak összes „független" (azaz nem következmény-kapcsolatban álló) relációját feltárni, így a néhány reláció megadásával fenti értelemben definált csoport nem feltétlenül lesz izomorf G-vel. Például ha $G = e$ az egyelemű csoport, akkor persze G-ben is fennáll a fenti $x^n = e$ reláció, és $x = e$ generálja G-t, de $\mathbb{Z}_n$-et adja a definíció.
A következő tétel éppen azt mondja, hogy a definíció a *homomorf értelemben leg-*

nagyobb olyan G csoportot adja meg, mely teljesíti a megadott relációkat. Ez segít majd abban, hogy bizonyos ismert csoportoknak megadjuk egy-egy prezentációját.

2.9.7. Tétel (Dyck tétele): *Legyen G és H két csoport, amelyeket ugyanazon generátorokkal értelmeztünk és G minden definiáló relációja szerepel H definiáló relációi között.*
Ekkor H a G egy homomorf képével izomorf.

Bizonyítás: A definíciónk szerint $G \cong F/N_1$ és $H \cong F/N_2$, ahol a feltevés miatt $N_1 \leq N_2$.
Ebben az esetben a második izomorfizmustételt felírva:

$$H \cong F/N_2 \cong \underbrace{F/N_1}_{\cong G}\Big/_{N_2/N_1}$$

Éppen ezt kellett belátnunk. ∎

Illusztrációként megadjuk D_n egy prezentációját. Mint már tudjuk, $D_n = \langle t, f \rangle$-ben fennállnak a következő relációk: $t^2 = f^n = tftf = e$; a diédercsoport tehát definiálható ezekből a relációkból (és generátorokból) kiindulva, melyekhez esetleg további relációkat kell hozzávennünk:

$$D_n = \langle t, f \mid t^2 = f^n = tftf = \ldots = e \rangle$$

Dyck tétele szerint ekkor D_n az $G = \langle t, f \mid t^2 = f^n = tftf = e \rangle$ csoport egy faktorcsoportjával izomorf. De a megadott relációk szerint $G = F \rtimes T$, ahol $F \cong \mathbb{Z}_n$, $F \cong \mathbb{Z}_2$ és $t_*^{-1} f_*^k t_* = f_*^{-k}$ $t_* \in T, f_* \in F$; itt a x_* jelöli az xN mellékosztályt a szóban forgó $F \to F/N$ természetes homomorfizmusnál.
Eszerint éppen D_n-et adja a prezentáció: $D_n \cong \langle t, f \mid t^2 = f^n = tftf = e \rangle$.
Másik példánk legyen S_3, amelyről azt állítjuk, hogy

$$S_3 = \langle a, b \mid a^3 = b^2 = (ab)^2 = e \rangle := G.$$

Először is az $a = (123)$ és $b = (12)$ választással láthatjuk, hogy ezek teljesítik a relációkat és $\langle a, b \rangle = S_3$, mivel $6 = |S_3| \geq |\langle a, b \rangle| \geq \frac{|\langle a \rangle||\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|} = |\langle a \rangle|\,|\langle b \rangle| = 6$. S_3 tehát G egy homomorf képével izomorf. De a relációk alapján $abab = e \Rightarrow ba = = a^{-1}b^{-1} (= a^2 b)$, ezért G minden eleme $a^k b^m N$ alakban írható (N a definícióban szereplő generált normálosztó), ahol ráadásul elég a $k = 0{,}1{,}2\ ;\ m = 0{,}1$ eseteket néznünk. Emiatt G legfeljebb hat elemű, így $S_3 \cong G$, amit igazolnunk kellett.
A következő fejezet feladatai között további csoportokhoz keresünk majd prezentációkat.

Érdemes megemlíteni, hogy általában egy adott prezentáció alapján nem feltétlenül könnyű információt nyerni egy csoportról. Számos megválaszolatlan kérdést szolgáltatnak például a viszonylag természetesen adódó $B(k, n)$ *(szabad) Burnside-csoportok*: $B(k, n)$ az a csoport, melynek k generátora van és a relációk azt fejezik ki, hogy minden elem n-edik hatványa az egységelem; a korábbiak szerint $B(k, n) \cong F_k/(F_k)^n$, ahol $(F_k)^n$ persze az n-edik hatványok által generált normálosztót jelenti az F_k szabad csoportban (igazából elég csak generált *részcsoportot* mondani, ui. nem nehéz belátni, hogy tetszőleges G csoportban az előbbi értelmezéssel G^k normálosztó minden $k \in \mathbb{Z}$-re). Amellett, hogy mint látjuk $B(1, n) \cong \mathbb{Z}_n$ a fenti meggondolásunk szerint, a Burnside-csoportok jó részénél (több jelentős részeredmény mellett) az sem ismert, hogy egyáltalán *véges-e a csoport*.

Végül bizonyítás nélkül közöljük azt a fontos tételt, mely szerint a szabad csoportok részcsoportjai elég speciálisak (ellentétben homomorf képekben való gazdagságukkal):

2.9.8. Tétel (Nielsen, Schreier): *Ha F szabad csoport és $e < H \leq F$, akkor H is szabad csoport.*

3. fejezet

Feladatok

3.1 Feladat: *Adjuk meg azokat a G csoportokat, amelyeknek pontosan három részcsoportjuk van!*

Megoldás: A feltevés szerint G nem állhat csak az egységelemből; jelölje az egyetlen valódi részcsoportját H. Legyen $x \in G \setminus H$. Ekkor $\langle x \rangle = G$, ugyanis x nyilván nem generálhatja H-t, másrészt $x \neq e$. Eszerint G *ciklikus csoport*.

Amint a 2.2.12. tételből rögtön adódik, G-nek pontosan annyi részcsoportja van, ahány osztója $|G|$-nek, a kanonikus alakból pedig látjuk, hogy három osztója pontosan az $n = p^2$ számoknak van. Tehát $|G| = p^2$; 2.5.3. szerint ekkor $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ vagy $G \cong \mathbb{Z}_{p^2}$.

Könnyen látható, hogy az előbbinek háromnál több részcsoportja van, ugyanis két valódi részcsoportja pl. $\langle (1,0) \rangle$ és $\langle (0,1) \rangle$, így ilyen nem lehet a keresett csoport, csak $\mathbb{Z}_{p^2}$ típusú. Ezek pedig eleget tesznek a feltételnek a már hivatkozott 2.2.12. tételnek megfelelően.

A válasz tehát a következő:

Azok a csoportok, melyeknek pontosan három részcsoportja van, éppen a p^2 rendű ciklikusak.

3.2 Feladat: *Mutassuk meg, hogy Cauchy tételének (2.6.2. tétel) megfordítása semmilyen összetett számra nem igaz!*

Megoldás: Adott m tetszőleges összetett számra mutatunk olyan G (véges) csoportot, melyre $m \mid |G|$, de G-ben nincs m rendű elem.

Először foglalkozzunk azzal az esettel, ha m *nem négyzetmentes*; legyen $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, ahol mondjuk $\alpha_1 \geq 2$. Tekintsük a következő, m elemű Abel-csoportot: $G = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1^{\alpha_1 - 1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$. Egyszerű meggondolás mutatja, hogy (tetszőleges véges direkt szorzat esetén) a direkt szorzat egy elemének rendje megegyezik a komponensei rendjeinek legkisebb közös többszörösével (ha valamelyik végtelen, akkor az elem rendje is végtelen); ebből következik, hogy G-ben nincs m rendű elem (azaz G nem ciklikus), mert a legnagyobb előforduló rend $p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} < |G| = m$. Ezzel az esettel tehát készen vagyunk.

Legyen most m négyzetmentes összetett szám és jelölje p az m legnagyobb prímosztóját. Tekintsük a p-edfokú szimmetrikus csoportot, azaz S_p-t. Látható, hogy $m \mid |S_p| = p!$, ugyanis a faktoriálisban minden p-nél kisebb (természetes) szám szerepel, így m prímtényezői is (a szükséges ≥ 1 kitevővel). Meggondoljuk, hogy S_p-ben nincs m rendű elem. Ha $\vartheta \in S_p$ ilyen lenne, akkor ennek diszjunkt ciklusokra való felbontásában a ciklushosszak legkisebb közös többszöröse éppen m (a rend és a ciklusszerkezet kapcsolatáról az 2.7.1 részben mondottak értelmében). Ez azonban lehetetlen, hiszen ha a ciklushosszak $c_1, c_2, \ldots, c_\ell$, akkor $p \mid m = c_1 c_2 \cdot \ldots \cdot c_\ell \Rightarrow p \mid c_i$ valamely i-re, azaz van egy legalább p hosszúságú ciklus; ez csak akkor lehet, ha ϑ egy p-ciklus, így viszont $o(\vartheta) = p \neq m$, ami ellentmondás. (Az is látható, hogy a Cauchy-tételnek megfelelő $m = p$ esetén nem jutunk ellentmondásra.) Az állítást ezzel igazoltuk. ∎

3.3 Feladat: *Jelölje a G véges csoport részcsoportjainak számát $s(G)$.*
Mutassuk meg, hogy $s(A \times B) \geq s(A) \cdot s(B)$ és pontosan akkor áll egyenlőség, ha $(|A|, |B|) = 1$.

Megoldás: Az állítás első fele azonnal adódik abból, hogy ha $A_1 \leq A$ és $B_1 \leq$ $\leq B$, akkor $A_1 \times B_1 \leq A \times B$ (ez gyorsan ellenőrizhető); $A \times B$-nek tehát legalább annyi részcsoportja van, amennyit a direkt faktorok részcsoportjainak „összeszorzásából" nyerhetünk, azaz legalább $s(A)s(B)$.

Vizsgáljuk meg, mikor áll egyenlőség. Először tegyük fel, hogy $\big(|A|, |B|\big) > 1$ és legyen p egy közös prímosztója a két elemszámnak. Cauchy tétele szerint létezik mindkét csoportban p rendű elem, mondjuk $a \in A$ és $b \in B$ ilyenek. Ekkor $\langle (a, b) \rangle$ egy p elemű részcsoportja $A \times B$-nek, amely azonban nem írható $A_1 \times B_1$ alakban (pl. azért nem, mert az elemszám miatt csak egy egyelemű és egy p elemű részcsoport direkt szorzata lehetne, azaz az egyik direkt faktor valamelyik egységelem lenne, ami nem áll fenn). Ezt a részcsoportot tehát nem számoltuk meg az $A_1 \times B_1$ alakúakkal együtt, így $s(A \times B) > s(A)s(B)$.

Legyen most $\big(|A|, |B|\big) = 1$; a direkt szorzat tetszőleges részcsoportjáról meg kell mutatnunk, hogy az tulajdonképpen $A_1 \times B_1$ alakú (az is lehet, hogy valamelyik direkt faktor az egyelemű csoport). Legyen egy ilyen részcsoport $H =$ $= \{(a_i, b_i) \mid i = 1,2, \ldots, k\}$. Világos, hogy $A_1 := \{a_i\} \leq A$ és $B_1 := \{b_i\} \leq B$. A relatív prímségi feltevés miatt $\big(o(a_i), o(b_i)\big) = 1$ $(i = 1,2, \ldots, k)$; ekkor minden i-re van olyan $\gamma_i \in \mathbb{N}$ szám, hogy $a_i^{\gamma_i} = a_i$ és $b_i^{\gamma_i} = e_B$, azaz $(a_i, b_i)^{\gamma_i} =$ $= (a_i, e_B)$, ugyanis a $\begin{cases} \gamma_i \equiv 1 & \big(o(a_i)\big) \\ \gamma_i \equiv 0 & \big(o(b_i)\big) \end{cases}$ szimultán kongruenciarendszer a modulusok relatív prímsége miatt biztosan megoldható (kínai maradéktétel). Ugyanezzel a gondolatmenettel adódik, hogy alkalmasan megválasztott γ_j^* pozitív egészekre $(a_j, b_j)^{\gamma_j^*} = (e_A, b_j)$. Mivel H részcsoport, ezért (a_i, e_B) és (e_A, b_j) is H-ban vannak (lévén H-beli elemek hatványai), tehát a szorzatuk is, ami (a_i, b_j).

Ez éppen azt jelenti, hogy az összes $A_1 \times B_1$-beli elem benne van H-ban (nemcsak a megadott (a_i, b_i) párok), azaz $H = A_1 \times B_1$; ezt kellett igazolnunk. ∎

Megjegyzés: Illusztrációként és önmagában is érdekes volta miatt számoljuk ki a legegyszerűbben adódó esetet: hány részcsoportja van $G = \mathbb{Z}_p \times \mathbb{Z}_p$-nek? A két triviális részcsoporton kívüli (valódi) részcsoportok mind $\mathbb{Z}_p$ típusúak, így ezek az egységelemtől eltekintve diszjunktak és G összes egységelemtől különböző eleme pontosan egy ilyen részcsoportban van benne. Ha tehát k db van belőlük, akkor fennáll a következő:

$$1 + (p-1)k = p^2 \to k = p + 1 \to \mathbf{s(\mathbb{Z}_p \times \mathbb{Z}_p) = p + 3}$$

Tehát $p + 3$ db részcsoportja van a direkt szorzatnak, míg $\left(s(\mathbb{Z}_p)\right)^2 = 4$: az első érték p növekedtével a végtelenhez tart, a második p-től függetlenül 4.

3.4 Feladat: *Írjuk le a P^∞ kváziciklikus p-csoport (amelyet a 2.6.1. definíció után ismertettünk) részcsoportjait!*

Megoldás: A kváziciklikus csoportot most a kényelmesebb/egységesebb jelölés miatt így „építjük fel": $P^\infty = \mathbb{Z}_p < \mathbb{Z}_{p^2} < \mathbb{Z}_{p^3} < \ldots$[1] Azt fogjuk megmutatni, hogy a „vizuálisan sejthető" válasz a helyes: P^∞ nemtriviális részcsoportjai $\mathbb{Z}_{p^k}$ alakúak $(k = 1,2,\ldots)$ és minden ilyen részcsoportból pontosan egy van. A megoldás két kisebb lépésből áll.

i) Legyen $H \leq P^\infty$ egy véges részcsoport, $H = \{a_1, a_2, \ldots, a_\ell\}$. Ekkor H benne van valamely $\mathbb{Z}_{p^k}$-ban, ugyanis minden a_i eleme benne van valamelyik $\mathbb{Z}_{p^{k_i}}$ ciklikus csoportban és ezek közül a legnagyobb k_i „indexű" az összeset tartalmazza. H tehát ennek a ciklikus csoportnak egy részcsoportja, azaz $\ell = p^s$ valamilyen s-re és $H \cong \mathbb{Z}_{p^s}$, valamint H *egyértelmű* (adott ciklikus csoport adott elemszámú

[1] Ez az eljárás precíze(bbe)n is kivitelezhető az ún. *direkt limesz* segítségével, amelyet a szakdolgozatban terjedelmi okokból nem ismertettünk.

részcsoportja). Véges részcsoportok eszerint pontosan a P^∞-t „felépítő” prímhatványrendű ciklikusak.

$ii)$ Legyen most H egy végtelen részcsoportja P^∞-nek. Tegyük fel, hogy H-ban van legnagyobb rendű elem; legyen ez az elem a és a rendje $o(a) = p^k$. Eszerint (i)-t is használva) a az *egyetlen* p^k elemű ciklikus részcsoportot generálja P^∞-ben míg H többi elemei p^ℓ elemű $(\ell \leq k)$ ciklikus részcsoportokat generálnak; az ilyenek azonban mind benne vannak $\mathbb{Z}_{p^k} \cong \langle a \rangle$-ban. Arra jutottunk, hogy $H \leq \mathbb{Z}_{p^k}$, ami ellentmondás. H-ban tehát nem lehet legnagyobb rendű elem, azaz tetszőlegesen nagy rendű elem létezik. Ha $g \in P^\infty$, akkor van olyan $h \in H$ elem, melyre $o(h) > o(g)$, ekkor $g \in H$ a korábbi érvelés szerint. Tehát $P^\infty \leq H$, így $H = P^\infty$ és a leírás teljes. ∎

3.5 Feladat: *Írjuk le azoknak a véges kommutatív p-csoportoknak a szerkezetét, melyekben az egységelemen kívül minden elem rendje p (a véges Abel-csoportok alaptételének felhasználása nélkül)!*

Megoldás: A feladatot kétféleképpen is megoldjuk.

I. megoldás: A csoportot szokás szerint jelölje G és legyen $|G| > 1$. Válasszunk egy tetszőleges $g_1 \neq e$ elemet; ez egy p rendű G_1 ciklikus részcsoportot generál. Ha $G_1 = G$, akkor megállunk, ellenkező esetben létezik $g_2 \in G \setminus G_1$, amely (szintén) egy G_2 p-cikl(ik)ust generál; ez természetesen G_1-et triviálisan metszi. Az eddigiek szerint $\langle G_1, G_2 \rangle = G_1 G_2 = G_1 \times G_2$, hiszen egymást csak az egységelemben metsző normálosztókról van szó. Ha most $G_1 \times G_2 = G$, akkor készen vagyunk, egyébként létezik $g_3 \in G \setminus G_1 \times G_2$ és az előbbi érvelést elismételhetjük. Az eljárást folytatjuk: ha $G_1 \times \ldots G_k < G$, akkor választunk egy g_{k+1} elemet, amely G_{k+1}-et generálja és $\langle G_1, G_2, \ldots, G_{k+1} \rangle = G_1 \times G_2 \times \ldots G_{k+1}$. G végessége miatt a algoritmus biztosan véget ér, tehát a következőt láttuk be: ha G olyan véges kommutatív p-csoport, melyben az egységelemen kívül csak p rendű elemek vannak, akkor G a $\mathbb{Z}_p$ direkt hatványa, azaz $G \cong (\mathbb{Z}_p)^k$. Ezeket a

csoportokat *elemi kommutatív p-csoportoknak* hívják.

II. megoldás: Megmutatjuk, hogy értelmezhető egy skalárral való szorzás $\mathbb{Z}_p$ (amely ezúttal mint test szerepel természetesen) elemeivel - melyekre a $(0), (1), (2),$ $\ldots, (p-1)$ jelölést használjuk - G-n úgy, hogy vektorteret kapjunk ($\mathbb{Z}_p$ felett); ebből adódik, hogy G mint vektortér (speciálisan mint Abel-csoport az összadásra nézve) $(\mathbb{Z}_p)^k$-nal izomorf, ahol k a tér dimenziója.
Jelöljük kivételesen a G-beli műveletet $+$-szal és a $(k) \in \mathbb{Z}_p$ elemmel való $\odot$ szorzást értelmezzük a következőképpen:

$$(k) \odot g \stackrel{\text{def}}{=} \overbrace{g + g + \ldots + g}^{k \text{ db}}$$

A összeadásra vonatkozó vektortéraxiómák automatikusan teljesülnek (mivel Abel-csoportról van szó), tehát a szorzásra vonatkozóakat kell ellenőrizni hogy megmutassuk, valóban vektorteret kaptunk.

$i)$ $(k) \odot (g_1 + g_2) = \overbrace{(g_1 + g_2) + (g_1 + g_2) + \ldots + (g_1 + g_2)}^{k \text{ db}}$
$= \underbrace{(g_1 + g_1 + \ldots + g_1)}_{k \text{ db}} + \underbrace{(g_2 + g_2 + \ldots + g_2)}_{k \text{ db}} = (k) \odot g_1 + (k) \odot g_2$

$ii)$ $\big((k) + (\ell)\big) \odot g = \underbrace{g + g + \ldots + g}_{k+\ell \text{ db}} = \underbrace{g + g + \ldots + g}_{k \text{ db}} + \underbrace{g + g + \ldots + g}_{\ell \text{ db}} =$
$= (k) \odot g + (\ell) \odot g.$

Itt kihasználjuk az elemek rendjére vonatkozó feltevést, azaz hogy bármely elemet önmagával p-szer összeadva („p-edik hatványra emelve") az eredmény 0, ugyanis a bal oldalon lévő $(k) + (\ell)$ összeg csak ekkor felel meg a jobb oldalon lévőnek, ahol *a tagok száma az előbbiek szerint szintén csak mod p számít*. Ezen alapul a következő axióma teljesülése is:

$iii)$ $\big((k)(\ell)\big) \odot g = \underbrace{g + g + \ldots + g}_{k\ell \text{ db}} = \underbrace{g + \ldots + g}_{\ell \text{ db}} + \underbrace{g + \ldots + g}_{\ell \text{ db}} + \ldots + \underbrace{g + \ldots + g}_{\ell \text{ db}} =$
$= (k) \odot \big((\ell) \odot g\big).$

$iv)$ Végül $(1) \odot g = g$ definíció szerint. G tehát tényleg „vektortérré tehető" $\mathbb{Z}_p$ felett és az állítást beláttuk. ∎

Megjegyzés: Érdemes észrevenni, hogy az első bizonyításból a következő tulajdonság is kiderül: az ilyen szerkezetű csoportokban minden p elemű részcsoport direkt faktor, hiszen bárhonnan elkezdhettük az eljárást. Ez nem minden Abel-csoportra igaz, amelynek „faktorizációja” tartalmaz $\mathbb{Z}_p$ típusú csoportot. Vegyük pl. $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$-et és annak $H = \langle (0,p) \rangle$ p elemű részcsoportját. Nem nehéz meggondolni, hogy ennek nem létezik „direkt komplementuma”, azaz olyan $K \leq \leq G$, amelyre $H \times K = G$. Ha lenne ilyen K, akkor annak egyrészt $\mathbb{Z}_{p^2}$ típusúnak kéne lennie G szerkezete miatt[2], másrészt triviálisan kéne metszenie H-t. Hogy néznek ki a p^2 elemű ciklikus részcsoportjai G-nek? A direkt szorzat egy elemének rendjéről 3.3 feladatban mondottak értelmében a generátorelem (a,b) alakú, ahol $o(b) = p^2$ és a tetszőleges. Eszerint $H \cap \langle a,b \rangle = H$, hiszen a generátort p,$2p$, $\ldots$, p^2-edik hatványra emelve az összes $(0,kp)$: $k = 0,1,\ldots,p-1$ elemet megkapjuk; ezzel ellentmondásra jutottunk.

3.6 Feladat: *Határozzuk meg a G véges (multiplikatívan írt) Abel-csoport elemeinek szorzatát!*

Megoldás: Először jegyezzük meg, hogy a feladat (a fenti formában) csak Abel-csoportra értelmes, hiszen egyébként meg kellene adni a szorzat tényezőinek sorrendjét.

Rátérve a megoldásra a szorzat tényezőit csoportosítsuk úgy, hogy egy elem és az inverze egymás után kerüljön: $g_1 g_1^{-1} g_2 g_2^{-1} \ldots$. Ez persze nem minden elemnél megy, méghozzá pontosan akkor nem működik, ha $g = g^{-1} \Leftrightarrow g^2 = e \Leftrightarrow g = e$ vagy $o(g) = 2$ (amint ezt a 2.6.2. Cauchy-tétel $p = 2$-re vonatkozó eseténél már meggondoltuk). Eszerint a kérdéses szorzat megegyezik a másodrendű elemek (ha vannak ilyenek) és az egységelem szorzatával (utóbbi persze nincs érdemi hatás-

[2] Általában is igaz a dolgozatban nem szereplő *Krull-Remak-Schmidt tétel* értelmében, hogy egy csoport tovább nem bontható csoportokra való direkt faktorizációjában a faktorok izomorfia erejéig egyértelműek; itt azonban ez elemi úton is meggondolható.

sal a szorzatra).

Vegyük észre, hogy ezek valójában részcsoportot alkotnak (Abel-csoport esetén): ha $x^2 = e$ és $y^2 = e$, akkor $(xy^{-1})^2 = xy^{-1}xy^{-1} = x^2y^{-2} = e$, így a 2.2.4. tételre hivatkozhatunk. Jelölje ezt a részcsoportot K. Ha $K > e$, azaz ha G-ben ténylegesen van másodrendű elem, akkor az előbbi feladat alapján $K \cong (\mathbb{Z}_2)^\ell$ valamely $\ell \geq 1$-re; elegendő tehát elemi kommutatív 2-csoportokra megválaszolni a kérdést.

Ha $\ell = 1$, akkor a szorzat az egyetlen másodrendű (G-beli) elemmel egyezik meg. Ha $\ell > 1$, akkor a valamelyik $\mathbb{Z}_2$ típusú direkt faktorban lévő másodrendű elem pontosan $2^{\ell-1}$ tényezőben szerepel (ennyi olyan elem van $(\mathbb{Z}_2)^\ell$-ben, melynek egyik direkt komponensét rögzítettük), ezért az összes elemet összeszorozva az egységelemet kapjuk.

Kérdésünkre a választ tehát röviden így foglalhatjuk össze:

A G véges Abel-csoport összes elemének szorzata az e egységelemmel egyezik meg, ha G-ben a másodrendű elemek száma 0 vagy ≥ 2, illetve ha egyetlen másodrendű a eleme van a csoportnak, akkor ezzel. ∎

Megjegyzés: Az előbbi összegzést megfogalmazhatjuk másként is.

Tudjuk (2.6.2.-ből), hogy (tetszőleges) G pontosan akkor *nem* tartalmaz másodrendű elemet, ha $|G|$ *páratlan*. Másrészt 2.5.4. szerint G 2-Sylowja néhány 2-hatványrendű ciklikus csoport direkt szorzata; eszerint és 2.2.12. alapján pontosan akkor van egyetlen másodrendű elem G-ben, ha egyetlen ciklikus csoport szerepel az előbbi felírásban, ami éppen azt jelenti, hogy G 2-Sylowja ciklikus.

Összefoglalva: a G véges Abel-csoport elemeinek szorzata az e egységelemmel egyezik meg, ha $|G|$ páratlan, vagy G (nemtriviális) 2-Sylowja nem ciklikus, és az egyetlen másodrendű elemmel, ha a (nemtriviális) 2-Sylow ciklikus.

3.7 Feladat: *Jelölje $d(G)$ azt, hogy G véges csoport minimálisan hány elemmel generálható.*
Mutassuk meg, hogy $|G| \geq 2^{d(G)}$!

Megoldás: A $d(G) = k$ jelölés mellett legyen $\{g_1, g_2, \ldots, g_k\}$ egy minimális elemszámú generátorrendszer, amelynek rögzítsük ezt a számozását. Tekintsük a $g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k}$ (esetleg egytényezős) szorzatokat, ahol $\alpha_i = 0{,}1$; ezekből 2^k db van. Most megmutatjuk, hogy a szorzatok mind különbözőek, ebből adódik a bizonyítandó állítás.

Tegyük fel ugyanis, hogy $g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k} = g_1^{\beta_1} g_2^{\beta_2} \ldots g_k^{\beta_k}$ és van olyan i index, hogy $\alpha_i \neq \beta_i$. Nyilván feltehetjük, hogy pl. $\alpha_1 \neq \beta_1$, különben egyszerűsítünk vele; mondjuk $\alpha_1 = 1$ és $\beta_1 = 0$ (azaz utóbbi helyen e áll a szorzatban). Ekkor átrendezve az egyenlőséget $g_1 = g_2^{\beta_2} \ldots g_k^{\beta_k} g_k^{-\alpha_k} g_{k-1}^{-\alpha_{k-1}} \cdot \ldots \cdot g_2^{-\alpha_2}$, ami mutatja, hogy $g_1 \in \langle g_2, g_3, \ldots, g_k \rangle$, ellentmondva annak, hogy k elemű a minimális generátorrendszer. ∎

Megjegyzések: A bizonyított állítás úgy is megfogalmazható, hogy minden n elemű véges csoport generálható legfeljebb $\lfloor \log_2 n \rfloor$ elemmel. Ez - amint a 3.5 feladatból kiderül - $(\mathbb{Z}_2)^k$ esetén éppen a pontos érték és persze egy (kellően sok elemű) ciklikus csoport esetén (amelyre $d(G) = 1$) elég nagyvonalú becslés.
Érdemes megjegyeznünk azt az érdekes (és messze nem triviális) tényt is, hogy *minden véges egyszerű csoport generálható legfeljebb két elemmel* (egyetlen elemmel persze csak a $\mathbb{Z}_p$ típusúak). Utóbbi állításnak egyelőre csak olyan bizonyítása ismeretes, amely az összes véges egyszerű csoport áttekintését adó ún. *Klasszifikációra* hivatkozik, amelynek (számos cikkből álló) teljes dokumentációja 10000 oldalnál is több (!).
Könnyen megállapíthatjuk, hogy a (feladatban szereplő) becslés nem javítható $|G| \geq 3^{d(G)}$-re, amint $\mathbb{Z}_2$ vagy $\mathbb{Z}_2 \times \mathbb{Z}_2$ példája mutatja.

3.8 Feladat: *Legyen G véges csoport, $|G| = n > 1$.*
Igazoljuk, hogy $|Aut\, G| \leq \prod_{i=0}^{k-1}(n - 2^i)$, ahol $\lfloor k = \log_2 n \rfloor$.

Megoldás: G végesen generált (mivel véges) és a 3.7 feladat szerint (annak jelölését használva) $d(G) \leq \lfloor \log_2 n \rfloor := k$. Vegyük G-nek egy legfeljebb k elemű minimális generátorrendszerét, ami álljon a $g_1, g_2, \ldots, g_k$ elemekből (amelyek közül esetleg néhány „nincs is"), továbbá legyen $\alpha \in \operatorname{Aut} G$. Az automorfizmusok elemi tulajdonságaiból azonnal adódik, hogy $(g_1)\alpha, \ldots, (g_k)\alpha$ is minimális generátorrendszer G-ben (különben az α^{-1}-nél vett képük egy kisebb elemszámú generátorrendszert adna). Szintén egyszerű észrevétel, hogy az $(g_i)\alpha$ értékek megadásával α is egyértelműen meg van határozva (mint a vektorterek homomorfizmusainál); nem feltétlenül adhatunk meg azonban bármilyen k elemű minimális generátorrendszert képként (szemben a vektortérizomorfizmusokkal).
Az előbbiek alapján $(g_1)\alpha$-t legfeljebb $n - 1 = n - 2^0$-féleképpen választhatjuk, mert e nem lehet. $(g_2)\alpha$ nem eshet $\langle (g_1)\alpha \rangle$-ba, ami legalább $2 = 2^1$ elemű; tehát $(g_2)\alpha$ legfeljebb $n - 2^1$ értéket vehet fel. Hasonlóképpen $(g_3)\alpha \notin \langle (g_1\alpha, (g_2)\alpha \rangle$, ami legalább 2^2 elemű a 3.7 feladatra hivatkozva, mert ha $\{(g_1)\alpha, (g_2)\alpha\}$ nem lenne minimális generátorrendszer az általuk generált részcsoportban, akkor ezeket minimális generátorrendszerre cserélve és a többi $(g_i)\alpha$-t megtartva G-nek egy k-nál kevesebb elemű generátorrendszeréhez jutnánk. $(g_3)\alpha$-t tehát legfeljebb $n - 2^2$ érték közül választhatjuk, és az imént elmondottak alapján $(g_i)\alpha$-t legfeljebb $n - 2^{i-1}$ érték közül $(i = 1,2, \ldots, k)$.
A „legkedvezőbb esetben" a képekről függetlenül dönthetünk; ebből éppen a kívánt becslést nyerjük:

$$|\operatorname{Aut} G| \leq (n - 2^0)(n - 2^1)(n - 2^2) \cdot \ldots \cdot (n - 2^{k-1}) = \prod_{i=0}^{k-1}(n - 2^i).$$

■

3.9 Feladat: *Bizonyítsuk be, hogy Aut $D_4 \cong D_4$!*

Megoldás: Először is ha $\alpha \in \mathrm{Aut}\, D_4$, akkor α az f negyedrendű forgatást f-be vagy f^3-be kell hogy vigye (mert ez az összes negyedrendű elem) és a t tükrözést valamely olyan másodrendű elembe, amely *nem négyzete egy negyedrendűnek*; ezek pontosan a tf^i $(i = 0{,}1{,}2{,}3)$ *tükrözések*. Mivel $\langle t, f\rangle = D_4$, így az előbbiek mutatják, hogy $\mathrm{Aut}\, D_4$ legfeljebb nyolcelemű. Most megmutatjuk, hogy a jelzett alakú automorfizmusok közül *valamennyi meg is valósul*.

Vegyük ugyanis azt az $\alpha_{k,\ell} :\ D_4 \to D_4$ függvényt, amelyet így definiálunk:

$$t^m f^i \mapsto t^m f^k \cdot f^{i\ell} = t^m f^{k+i\ell} \quad (m = 0{,}1\ ;\ i = 0{,}1{,}2{,}3\ ;\ \ell = 1{,}3)$$

Könnyű meggondolni, hogy ez bijekció, ami a t, f generátorelemeken éppen a fent leírt módon hat: $t \mapsto tf^k$ és $f \mapsto f^\ell$ (valójában ezekből a képekből „sejthető meg" $\alpha_{k,\ell}$ alakja). Lássuk be, hogy $\alpha_{k,\ell}$ műveletartó is; ehhez vegyük a $t^{m_1} f^{i_1}$ és $t^{m_2} f^{i_2}$ elemeket, melyek rendre a $t^{m_1} f^{k+i_1\ell}$ és $t^{m_2} f^{k+i_2\ell}$ elemekbe képződnek. A szemidirekt szorzat tulajdonságai szerint (kihasználva a konjugálás műveletartását):

$$(t^{m_1} f^{i_1}) \cdot (t^{m_2} f^{i_2}) = t^{m_1+m_2} \left(f^{i_1}\right)^{t^{m_2}} f^{i_2} = t^{m_1+m_2} \underbrace{\left(f^{t^{m_2}}\right)^{i_1}}_{f\ v.\ f^{-1}} f^{i_2} =$$

$$= t^{m_1+m_2} f^{(i_2 \pm i_1)} \mapsto t^{m_1+m_2} f^{k+(i_2\pm i_1)\ell}$$

Másrészt

$$(t^{m_1} f^{k+i_1\ell}) \cdot (t^{m_2} f^{k+i_2\ell}) = t^{m_1+m_2} \underbrace{\left(f^{k+i_1\ell}\right)^{t^{m_2}}}_{f^{\pm(k+i_1\ell)}} f^{k+i_2\ell} =$$

$$= t^{m_1+m_2} f^{k+(i_2\pm i_1)\ell}$$

$\alpha_{k,\ell}$ tehát műveletartó, így tényleg automorfizmus. Mivel (amint megállapítottuk) $\mathrm{Aut}\, D_4$ legfeljebb nyolcelemű és pontosan ennyi db $\alpha_{k,\ell}$ van, így azt látjuk, hogy $|\mathrm{Aut}\, D_4| = 8$ és minden automorfizmus $\alpha_{k,\ell}$ alakú.

Az egyszerűbb jelölés kedvéért jelölje innentől kezdve $\alpha_{k,\ell}$-et (k, ℓ). Amellett az

észrevétel mellett, hogy a k, ℓ (egész) kitevők nyilván csak mod 4 számítanak, számítsuk ki a $(k_1, \ell_1)(k_2, \ell_2)$ szorzatot. Definíció szerint az első tényező $t^m f^i$-t $t^m f^{k_1+i\ell_1}$-be viszi, erre alkalmazva a második tényezőt (függvényt) $t^m f^{k_2+k_1\ell_2+i\ell_1\ell_2}$-t kapunk, azaz $(k_1, \ell_1)(k_2, \ell_2) = (k_1\ell_2 + k_2, \ell_1\ell_2)$. Eszerint az automorfizmuscsoport $\mathbb{Z}_4$ és $\mathbb{Z}_4{}^* \cong \mathbb{Z}_2$ szemidirekt szorzata, ugyanis $\{(k,1)\}$ egy negyedrendű normálosztó és $\{(0, \ell) \mid \ell \equiv \pm 1 (\mathrm{mod}\, 4)\}$ egy kételemű részcsoport Aut D_4-ben. A fenti szorzási szabály miatt Aut D_4 nem kommutatív, tehát a $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ szemidirekt szorzatban $\mathbb{Z}_2$ egy másodrendű automorfizmus(rész)csoportjába kell hogy képződjön $\mathbb{Z}_4$-nek:
Aut $D_4 \cong \langle a, b \mid a^4 = b^2 = baba = e \rangle \cong D_4$; ezzel az állítást beláttuk. ∎

3.10 Feladat:

i) Mutassuk meg, hogy a G csoport azonos konjugáltosztályaiban lévő elemek centralizátorai konjugáltak (tehát izomorfak)!

ii) Legyen G véges csoport és az i-edik konjugáltosztályban lévő elemek centralizátorainak elemszáma legyen c_i $(i = 1,2, \ldots, h)$.
Bizonyítsuk be, hogy $\sum_{i=1}^{h} \frac{1}{c_i} = 1$!

iii) **Következmény**: Csak véges sok véges csoport létezik adott osztályszámmal.

Megoldás: $i)$ Az elméleti részben használt jelöléssel legyen $y \in [x]$, azaz $y = x^g$ valamely $g \in G$-vel, továbbá legyen $c \in C_G(x)$, azaz $x^c = x$. Ekkor fennáll a következő:

$$y^{g^{-1}cg} = (y^{g^{-1}})^{cg} = x^{cg} = (x^c)^g = x^g = y$$

tehát $g^{-1}cg = c^g \in C_G(y)$ és a φ_g konjugálás x centralizátorát y centralizátorának egy részcsoportjába viszi. Fordítva: ha $y^d = y$, akkor $x^{gdg^{-1}} = x$ és $d^{g^{-1}} \in C_G(x)$. Ezzel megmutattuk, hogy a (rögzített) g-vel való konjugálás egy $C_G(x) \to C_G(y)$

izomorfizmus.

$ii)$ Amint azt meggondoltuk a 2.4.3. tételben, $|[x_i]| = |G : C_G(x_i)|$, ahol x_i az i-edik konjugáltosztály tetszőleges eleme. Innen $\frac{1}{|C_G(x_i)|} = \frac{1}{c_i} = \frac{|G:C_G(x_i)|}{|G|}$.
A bizonyítandó állítás eszerint ez:

$$\sum_{i=1}^{h} \frac{|G : C_G(x_i)|}{|G|} = 1$$

azaz

$$\sum_{i=1}^{h} |G : C_G(x_i)| = |G| .$$

Utóbbi egyenlőség viszont pontosan azt mondja, hogy G elemszáma a (diszjunkt) konjugáltosztályok elemszámainak összege, ami igaz, lévén a „konjugáltnak lenni" ekvivalenciareláció (amint azt beláttuk a konjugálás tulajdonságainak vizsgálatánál). A kívánt állítást ezzel igazoltuk.

$iii)$ A(z egyébként egyáltalán nem nyilvánvaló) következmény igazolásához azt mutatjuk meg, hogy a $\sum_{i=1}^{h} \frac{1}{x_i} = 1 \ ; \ 0 < x_i \in \mathbb{N}$ egyenletnek rögzített h mellett csak véges sok megoldása van. Mivel adott G véges csoportra $|G| = = \max\{c_i : i = 1,2,\ldots,h\}$ (hiszen pl. $G = C_G(e)$), így az előbbi (még bizonyításra váró) eredményt használva adott h osztályszámú csoportnak legfeljebb annyi eleme lehet, amennyi a fenti egyenlet legnagyobb x_i megoldása; tehát csak véges sok véges csoport jöhet szóba.
Rátérve a jelzett bizonyításra legyen $x_1 \leq x_2 \leq \ldots \leq x_h$.
Ekkor $1 = \sum_{i=1}^{h} \frac{1}{x_i} \leq \frac{h}{x_1}$, amiből $h \geq x_1$; x_1 tehát legfeljebb az $1,2,\ldots,h$ értékeket veheti fel. Most levonva $\frac{1}{x_1}$-et ugyanez a gondolatmenet mutatja, hogy x_2-re is csak véges sok érték jön szóba és így tovább: minden x_i-re véges sok lehetőségünk van. Ezzel a bizonyítás teljes. ∎

Megjegyzés: Végtelen csoportok nagyon „vad" módon viselkedhetnek konjugáltosztályok szempontjából, amint azt a nevezetes *Higman, Neumann és Neumann*

beágyazási tétel mutatja: minden torziómentes csoport beágyazható egy olyan G végtelen csoportba, amelynek két konjugáltosztálya van, azaz az egységelemen kívül bármely két elem konjugált G-ben(!!). Távolról sem nyilvánvaló már az sem, hogy ilyen csoport egyáltalán létezik. Ennek nagyon egyszerű és enyhe érzékeltetésére megemlítjük, hogy (amint az egyébként könnyen meggondolható) véges csoportok közül kizárólag $\mathbb{Z}_2$-nek van két konjugáltosztálya.

3.11 Feladat:

i) **(Burnside-lemma)** Legyen $X \neq \emptyset$ egy véges halmaz és $G \leq S_X$ permutációcsoport. A $\mathrm{Fix}(\pi)$ jelölje a π permutáció fixpontjainak halmazát.
Mutassuk meg, hogy X G-orbitjainak száma megegyezik az „átlagos fixpontszámmal”, azaz az alábbi kifejezéssel:

$$\frac{1}{|G|}\sum_{\pi\in G}|\mathrm{Fix}(\pi)|$$

ii) Igazoljuk, hogy ha G legalább kételemű, véges, tranzitív permutációcsoport, akkor G tartalmaz fixpontmentes elemet.

Megoldás: $i)$ A megoldás kulcslépése az, hogy a bizonyítandó képletben szereplő összeget másként írjuk fel a „kettős leszámlálás” módszerét alkalmazva.
Készítsünk (gondolatban) egy $|G|$ sorból és $|X|$ oszlopból álló táblázatot, amelyben az ij pozícióba tegyünk egy piros pontot, ha a j-edik oszlopban lévő $x_j \in X$ elem fixpontja az i-edik sorban lévő π_i permutációnak. Tehát pl. az egységelem sorában minden pozícióban van egy pont és egy $x \in X$ elem oszlopában pontosan az $\mathrm{St}_G(x)$ stabilizátor elemeinek megfelelő helyeken vannak pontok.
Hány piros pontot írtunk összesen a táblázatba? Soronként összeszámolva az állításban szereplő $\sum_{\pi\in G}|\mathrm{Fix}(\pi)|$-t kapjuk, ami persze megegyezik azzal, ha oszloponként számoljuk össze: $\sum_{x\in X}|\mathrm{St}_G(x)|$. Tudjuk, hogy $|[x]| = |G : \mathrm{St}_G(x)|$,

azaz a bizonyítandó állítás $|G|$-vel való egyszerűsítés után a következő alakot ölti:

$$X\ G\text{-orbitjainak száma} = \sum_{x \in X} \frac{1}{|[x]|}$$

Ez pedig teljesül, hiszen egy-egy orbit elemeire összegezve az adott orbit elemszámának reciprokát 1-et kapunk, tehát az összes orbit összes elemére (azaz X minden elemére) összegezve éppen az orbitok száma adódik. A bizonyítás ezzel teljes.

Megjegyzés: Láthatjuk, hogy az érvelés működik valamivel általánosabban is, nevezetesen akkor, ha a G véges csoport *hat* az X véges halmazon (G végességét most fel kell tennünk, különben esetleg végtelen táblázatot kellene készíteni).

$ii)$ Mivel G tranzitív, így X szükségképpen véges és egyetlen G-orbit van. Az imént bizonyított lemmát alkalmazva $1 = \frac{1}{|G|} \sum_{\pi \in G} |\mathrm{Fix}(\pi)|$, amiből $|G| = = \sum_{\pi \in G} |\mathrm{Fix}(\pi)|$. Az egységelemnek legalább két fixpontja van, hiszen a feltevés szerint $|X| \geq 2$.

Tegyük fel indirekt, hogy minden $\pi \in G$ esetén $|\mathrm{Fix}(\pi)| \geq 1$, ekkor az előbbiek alapján $|G| = \sum_{\pi \in G} |\mathrm{Fix}(\pi)| \geq 2 + |G| - 1 = |G| + 1$, ami ellentmondás, tehát valóban létezik olyan permutáció, melynek nincs fixpontja. ∎

3.12 Feladat: *Írjuk le a $|G| = pq$ rendű csoportok szerkezetét, ahol $p > q$ prímek!*

Megoldás: Sylow 1. tétele (vagy Cauchy tétele) alapján G-nek léteznek prímrendű ciklikus p- és q-Sylow részcsoportjai. A két különböző prímhez tartozó (valamely) P és Q Sylow-részcsoport természetesen csak az egységelemben metszi egymást és $PQ = G$, ugyanis $|PQ| = |P|\,|Q| = |G|$, $P \cap Q = e$ miatt. A Sylow tételekből tudjuk még, hogy $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$, valamint $\left|\mathrm{Syl}_p(G)\right| \mid q$; $p > q$ miatt ez a két feltétel egyszerre csak úgy teljesülhet, ha egyetlen p-Sylow van, ami így normálosztó (G tehát biztosan nem egyszerű).

Eszerint G mindenképpen $P \rtimes Q$ alakú, tehát az a kérdés, hogy a (kiválasztott) q-Sylow hogyan hat a konjugálással P-n, azaz milyen részcsoportjába képződik $\operatorname{Aut} P$-nek; ez - lévén Q egyszerű csoport - vagy a triviális, vagy egy $\mathbb{Z}_q \cong Q$ típusú automorfizmus(rész)csoport lehet.
A q-Sylowok számára is az előző két feltétel teljesül a megfelelő módosításokkal, ami rögtön mutatja, hogy $q \nmid p-1$ esetben q-Sylowokból is csak egy van és így az is normálosztó. Ebben az esetben G a két, egymást csak az egységelemben metsző, így elemenként felcserélhető normálosztó szemidirekt szorzata, amelyből - mint láttuk - $G \cong P \times Q$ adódik. G tehát $\mathbb{Z}_{pq}$ típusú ciklikus csoport. Ez pontosan annak felel meg, amikor a q-Sylow a triviális automorfizmusába képződik P-nek. Érdemes megemlíteni, hogy az iménti eredmény szerint pl. $15 = 5 \cdot 3$ és $35 = $ $= 5 \cdot 7$ elemű csoportból csak egyféle van, sőt végtelen sok olyan *összetett* számot adhatunk meg, amelyekre (mint elemszámokra) csak egyféle csoport létezik (ami persze az adott rendű ciklikus csoport).

Rátérve a $p \equiv 1 \pmod q$ esetre az egyik lehetőség persze most is a $G \cong P \times Q$, azaz amikor mindkét típusú Sylow-részcsoportból egy van; ekkor Q triviálisan hat a konjugálással P-n.
A másik esetben Q egy $\mathbb{Z}_q$ típusú automorfizmus-részcsoportjába képződik $\operatorname{Aut} P$-nek. Ezen a ponton felhasználjuk azt a(z egyébként nem túl bonyolult) tételt, mely szerint $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$, azaz az n-edrendű ciklikus csoport automorfizmuscsoportja a modulo n redukált maradékosztályok multiplikatív csoportjával izomorf és minden $(1) \mapsto (\ell)$ $(\ell, n) = 1$ hozzárendelés alapján az egész csoportra kiterjesztett leképezés valóban automorfizmus. Speciálisan, ha $n = p$ prím (vagy más olyan modulus, amelyre nézve létezik *primitív gyök*), akkor ez a csoport ciklikus, amint azt számelméletből tudjuk. Jelen esetben tehát a $p-1$ elemű $\operatorname{Aut} P$ ciklikus csoport egy q elemű részcsoportjáról van szó, amelyből pontosan egy van, és az is ciklikus, ahogyan azt 2.2.12.-ban beláttuk.

Rögzítsük most P és Q egy-egy generátorelemét, azaz legyen pl. $P = \langle x \rangle$ és $Q = \langle y \rangle$, továbbá legyen $k \in \mathbb{N}$ egy rögzített primitív gyök mod p. Ekkor a szemidirekt szorzatban szereplő $Q \to \mathrm{Aut}\, P$ automorfizmust egyértelműen meghatározza, ha (korábban már használt jelöléssel) $x^y := x^m \quad (1 \leq m \leq p-1)$-et megadjuk. Itt m-nek olyannak kell lennie, hogy a k primitív gyök által generált $\mathbb{Z}_{p-1}$ elemű ciklikus csoport egyetlen q elemű ciklikus részcsoportját generálja; ilyen m-ből a hatvány rendjére vonatkozó összefüggés alapján éppen $\varphi(q)$ van (φ az Euler-féle függvényt jelöli). Részletesebben m lehet $k\frac{p-1}{q}$, ahol $k = 1,2,\ldots,q$ és $(k,q) = 1$.

Ezen a ponton felmerül a kérdés, hogy ha m_1 és m_2 két lehetséges (m-)
érték, akkor az ezeknek megfelelő G_1 és G_2 csoportok vajon tényleg különbözőek-e? Megmutatjuk, hogy ez valójában *nem így van*.

Ugyanis tekintsük valamelyik fenti (módon definiált) $Q \ltimes P$ szemidirekt szorzat alábbi leképezését önmagára: $y^c x^d \mapsto y^c x^{d\alpha}$, ahol $c, d, \alpha \in \mathbb{N}$ és $(\alpha, p) = 1$ (α rögzített). Világos, hogy ez bijekció, sőt *művelettartó* is, ami rövid számolással ellenőrizhető (kihasználva a konjugálás művelettartását). Tehát ez a leképezés automorfizmusa a szemidirekt szorzatnak, amelynél $(x^{m_1})^y = x^{m_1\alpha}$. Ha adott m_1 és m_2, akkor (mivel m_1 és m_2 relatív prím p-hez) létezik olyan α^*, hogy $m_1\alpha^* \equiv$ $\equiv m_2 \pmod p$ és $(\alpha^*, p) = 1$; az ehhez tartozó $x \mapsto x^{\alpha^*}$ $y \mapsto y$ automorfizmus mutatja, hogy ugyanazt a csoportot definiáltuk mindkét esetben, azaz $G_1 \cong G_2$.

Most már teljes a pq elemű csoportok leírása:

Ha $|G| = pq$, ahol $p > q$ prímek, akkor $q \nmid p-1$ esetén $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$, $q \mid p-1$ esetén pedig vagy $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$, vagy $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$, ahol $\mathbb{Z}_q$ az egyetlen q elemű részcsoportjába képződik $\mathrm{Aut}\, P$-nek. ∎

Megjegyzés: Korábbi ismereteinkkel együtt most már *teljes leírást* ismerünk azokról a csoportokról, melyek elemszáma *két* (nem feltétlenül különböző) *prím szorzata*.

3.13 Feladat:

i) Mutassuk meg, hogy $A_4 = \langle x, y \mid x^2 = y^3 = (xy)^3 = e \rangle$!

ii) Igazoljuk, hogy $S_4 = \langle x, y \mid x^4 = y^2 = (xy)^3 = e \rangle$!

Megoldás: $i)$ Először vegyük az $x^* = (12)(34)$ és $y^* = (123)$ elemeket (melyek páros permutációk); látható, hogy ezek teljesítik a relációkat. Be akarjuk látni, hogy $A_4 = \langle x^*, y^* \rangle$. Tudjuk, hogy $\langle x^*, y^* \rangle \leq A_4$ és a generált részcsoport legalább hatelemű a 2.2.14. tétel alapján. Ha tehát meggondoljuk, hogy A_4-ben nincs hat elemű részcsoport, akkor a generátumnak egybe kell esnie a teljes alternáló csoporttal.

Tegyük fel indirekt, hogy $M \leq A_4$ egy hatelemű részcsoport; ekkor $M \triangleleft A_4$, mivel a részcsoport indexe 2. Tekintsük az $N = \{e, (12)(34), (13)(24), (14)(23)\} \leq$ $\leq A_4$ részcsoportot (a 2.7.2. tétel előtti megjegyzésünkben megállapítottuk, hogy ez valóban részcsoport, amely A_4 2-Sylowja). Mivel (a permutációk rendjéről és A_4-ről elmondottak alapján) ez a részcsoport *az összes másodrendű elemet* tartalmazza, így $N \triangleleft A_4$, ugyanis egy konjugálás ezeket egymás között permutálja. Ekkor $MN \leq A_4$ és így $MN = A_4$, hiszen $MN > M$, mert $N \not\leq M$ Lagrange tétele miatt.

Az 1. izomorfizmustétel szerint $N/N \cap M \cong NM/M = A_4/M \cong \mathbb{Z}_2$, amiből $|N \cap M| = 2$. Mivel normálosztók metszete is normálosztó, így egy kételemű normálosztót kaptunk. Általában is igaz azonban a 2.8.3. miatt, hogy egy *kételemű normálosztó a centrumban van*. Ezzel ellentmondásra jutottunk, mert $Z(A_4) = e$; emellett hasonlóan érvelhetünk, mint a 2.7.4. tételben.

Kiderült tehát, hogy $A_4 = \langle x^*, y^* \rangle$ és a megadott elemek teljesítik a relációkat; Dyck tétele szerint tehát A_4 a definiáló relációkal megadott csoport egy faktorcsoportjával izomorf. K-val jelölve az utóbbit tekintsük K szorzással való jobb hatását a következő, mellékosztályokból álló halmazon:

$$\left\{ \langle y \rangle, \langle y \rangle x, \langle y \rangle xy, \langle y \rangle xy^2 \right\}$$

Persze ellenőriznünk kell (a definiáló relációk alapján), hogy ez tényleg jobb hatás; ehhez elég, hogy mind az x, mind az y generátorokkal való jobb szorzás valóban egymás között permutálja a megadott mellékosztályokat. Csak két eset nem olvasható le közvetlenül; amikor az $\langle y\rangle\, xy$ és az $\langle y\rangle\, xy^2$ mellékosztályokat szorozzuk jobbról x-szel. Azt sejtjük, hogy $\langle y\rangle\, xyx = \langle y\rangle\, xy^2$ és vegyük észre, hogy amennyiben ez igaz, úgy jobbról szorozva éppen a másik bizonyítandó egyenlőséget kapjuk. Az előbbi pedig valóban teljesül:

$$\langle y\rangle\, xyx = \langle y\rangle\, xy^2 \Leftrightarrow xyx(xy^2)^{-1} = xyxyx \in \langle y\rangle$$

ami igaz, hiszen az $(xy)^3 = xyxyxy = e$ relációból $xyxyx = y^{-1} \in \langle y\rangle$. Ezen a ponton meg kell jegyeznünk, hogy a fentiekből derül ki az is, hogy *valóban négy különböző mellékosztályról beszélünk*; ezt a fontos tényt eddig nem gondoltuk meg. Ugyanis $\langle y\rangle$ nyilván nem eshet egybe semelyik továbbival (mert ekkor x is y-hatvány és így K háromelemű ciklikus lenne, amelynek nem lehet A_4 homomorf képe), másrészt ha a többi háromból *bármely kettő* egybeesne, akkor könnyen adódóan *mind a három* egybeesne, ez pedig ellentmond annak, amit az x-szel való jobb szorzásnál meggondoltunk.

Adott tehát K-nak egy permutációreprezentációja S_4-be, aminek magját azok az elemek alkotják, amelyek mind a négy mellékosztályt fixen hagyják. Tudjuk, hogy az $\langle y\rangle$ mellékosztályt pontosan y hatványai hagyják fixen, amelyek közül azonban csak a triviális $y^3 = e$ hagyja fixen (mondjuk) $\langle y\rangle\, x$-et; eszerint a permutációreprezentáció magja e és így K az S_4 egy részcsoportjával izomorf. Már csak azt kell meggondolnunk, hogy $K \ncong S_4$. Ez viszont kiderül az előbbiekből, hiszen mint láttuk nincs olyan $\neq e$ permutáció K-ban (illetve izomorf képében), amely $\langle y\rangle$-t és $\langle y\rangle\, x$-et is fixen hagyná (míg S_4-ben van ilyen), ezért $|K| \leq 12$ és van A_4-gyel izomorf homomorf képe $\Rightarrow K \cong A_4$, amit igazolnunk kellett.

$ii)$ Most is azt gondoljuk meg először, hogy S_4 teljesíti a relációkat. Valóban, tekintsük az $x^* = (1234)$ és $y^* = (12)$ permutációkat; ekkor $x^*y^* = (234)$, így

az összes reláció teljesül. Mivel a 2.2.14. miatt a két elem által generált részcsoport legalább nyolcelemű és az előbbiek alapján tartalmaz harmadrendű elemet, így vagy tizenkét, vagy huszonnégy elemű kell hogy legyen. Ha az előbbi állna fenn, akkor a 2.8.3.-t követő meggondolás szerint S_4 centruma nem csak az egységelemből állna (ami nem igaz); tehát $\langle x^*, y^* \rangle = S_4$ és S_4 a fenti prezentációval definált csoport homomorf képe. Utóbbit jelölje K.

Tekintsük K-ban az $\langle x \rangle = H$ szerinti következő mellékosztályokat:

$$\{H, Hy, Hyx, Hyx^2, Hyx^3, Hyx^2y\}$$

Meg fogjuk mutatni, hogy legfeljebb ennyi jobb oldali mellékosztály van H szerint, ebből adódóan K legfeljebb $4 \cdot 6 = 24$ elemű, tehát $K \cong S_4$.

A definiáló relációkból közvetlenül látszik, hogy az y-nal jobbról való szorzás a következő mellékosztály-cseréket hajtja végre: $H \leftrightarrow Hy$ és $Hyx^2 \leftrightarrow Hyx^2y$; gondoljuk meg, hogy a fennmaradó két mellékosztályt is cseréli. Mivel $(xy)^3 = = xyxyxy = e$, így $yxy = x^{-1}y^{-1}x^{-1} = x^3yx^3$, tehát $Hyxy = Hx^3yx^3 = = Hyx^3$, ezzel az egyik irány meg is van. A $Hyx^3y = Hyx$ másik irányhoz az kell, hogy $yx^3yx^{-1}y^{-1} = yx^3yx^3y$ H-ba essen, ami igaz, hiszen

$$yx^3yx^3y = y\underbrace{(yxyxy)}_{x^3}y(yxyxy)y = \underbrace{(yy)}_{e}xyxy(yy)xyx(yy) = (xyxyxy) = x \in H.$$

Most az x generátorelemel szorozzuk meg jobbról az összes mellékosztályt; ekkor H fixen marad és világos, hogy a következő 4-ciklus szerint permutálódik a benne szereplő 4 mellékosztály: $(Hy\ Hyx\ Hyx^2\ Hyx^3)$. Azt kell tehát meggondolnunk, hogy a Hyx^2y mellékosztály (is) fixen marad, azaz $z := yx^2yxy^{-1}(x^2)^{-1}y^{-1} = = yx^2yxyx^2y \in H$.

Ez is teljesül, hiszen $z = \underbrace{(yxyyxy)}_{yx^2y}x\underbrace{yxyyxy}_{yx^2y} = yxyy\underbrace{(xyxyxy)}_{e}yxy = yx\underbrace{yy}_{e}yxy = = yxyxy = x^{-1}$. Mivel minden H szerinti (jobb oldali) mellékosztály valamely, a generátorelemekkel felírt szóval való szorzással kapható meg, így az előbbi meggondolások azt mutatják, hogy az *összes mellékosztályt* felsoroltuk.

A bizonyítás ezzel teljes. ∎

Megjegyzés: Látható, hogy a feladat $i)$ részére is igaz az állítás (és érv), hogy ott valójában az összes, az adott részcsoport szerinti mellékosztályt előállítottuk; az $i)$-beli gondolatmenet tehát úgy is befejezhető, ahogy az $ii)$-beli.

3.14 Feladat: *Legyen F szabad csoport az $X \neq \emptyset$ halmazon.*
Bizonyítsuk be, hogy F' azon szavakból áll, amelyekben minden x_α betű kitevőinek összege$= 0$!

Megoldás: Nevezzük a fenti szavakat *nullösszegűnek* és jelölje a nullösszegű szavak halmazát K. Az állítás egyik fele könnyen adódik a kommutátor definíciójából. Ha w_1 és w_2 két szó, akkor a $[w_1, w_2] = w_1^{-1}w_2^{-1}w_1w_2$ „kommutálásnál" minden betű kitevőinek összege 0 lesz (az esetleges $x_\alpha x_\alpha^{-1}$ tiltott szavak megjelenése miatti egyszerűsítések természetesen nem változtatnak az összegen). Eszerint minden kommutátorra igaz az állítás és világos, hogy kommutátorok szorzataira is igaz; ezzel be is láttuk, hogy $F' \subseteq K$.

A másik irányhoz használt „trükköt" az egyszerűbb jelölés- és fogalmazásmód miatt egy konkrét példán mutatjuk be, de látható lesz, hogy a módszer általánosan is működik.
Tekintsük például F_3-ban a következő (normálformában felírt) nullösszegű szót:

$$w_1 = x_1^2x_2x_3^2x_2^2x_3x_1^{-1}x_2^{-1}x_3\overbrace{x_2^{-2}x_1^{-1}x_3^{-4}}^{\oslash_1}$$

Szorozzuk meg w-t jobbról $\oslash_1^{-1}x_3^{-4} \oslash {}_1x_3^4 = [\oslash_1, x_3^4] = k_1$-vel; gyors számolás mutatja, hogy ekkor a következőt kapjuk:

$$w_2 = x_1^2x_2x_3^2x_2^2x_3x_1^{-1}\overbrace{x_2^{-1}x_3^{-3}x_2^{-2}x_1^{-1}}^{\oslash_2}$$

„Eltűnt" tehát a szó végéről az x_3^{-4} és az x_3 kitevő hozzáadódott egy, a szóban őt megelőző x_3 hatvány kitevőjéhez; eközben persze semelyik betű kitevőinek

összege nem változott meg. A w_2-ben megjelölt $\oslash_2$-t használva, azaz $[\oslash_2, x_1] =$ $= k_2$-ral jobbról szorozva w_2-t most „eltüntetjük” a szó végén szereplő x_1-hatványt, amelynek kitevője hozzáadódik egy korábbi x_1-hatványéhoz. Az eljárást folytatjuk az eddigiek szerint: az ℓ-edik w_ℓ szó végén lévő betűből (pl. x_1) keresünk egy továbbit a szóban (ha a betű kitevője nemnulla, akkor a változatlan nullösszeg miatt ilyennek lennie kell) és a fent leírtak értelmében készített k_ℓ kommutátorral jobbról szorozva az előző betűt „eltüntetjük”, a kitevőt hozzáadva a (tetszés szerint választott korábbi, azonos betű) hatványához. Látjuk, hogy ez az eljárás véget ér tetszőleges F_3-beli szóból kiindulva, és pontosan akkor, amikor az eredeti szó minden betűjéből már csak egy szerepel. Ennek az egyetlen betűnek a kitevője meg fog egyezni a kiindulási szó adott betűje kitevőinek összegével. Speciálisan ha nullösszegű szóból indulunk ki, akkor az eljárás végén (mondjuk az ℓ-edik lépésben) az üres szót kapjuk, azaz $w \cdot k_1 k_2 k_3 \cdot \ldots \cdot k_\ell = 1$ és így $w =$ $= k_\ell^{-1} k_{\ell-1}^{-1} \cdot \ldots \cdot k_1^{-1}$, azaz (lévén kommutátor inverze is kommutátor) w kommutátorok szorzata: $K \subseteq F'$, így $K = F'$, amint állítottuk. ∎

3.15 Feladat: *Hány kompozíciólánca van $G = Q \times \mathbb{Z}_{15}$-nek, ahol Q a(z alább definiált) kvaterniócsoport?*

Megoldás: A Q *kvaterniócsoport* a következő (ismertként kezelt) kvaterniók halmaza:

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

A művelet a kvaterniószorzás, azaz a „nemtriviális” szorzások a következők:

$$ij = -ji = k,\ ki = -ik = j,\ jk = -kj = i,\ i^2 = j^2 = k^2 = 1$$

Q nilpotens, hiszen 2-csoport, de nem kommutatív. A(z elemeket végignézve) -1 az egyetlen másodrendű elem és könnyű kiszámolni, hogy $Z(Q) = Q' = \langle -1 \rangle =$ $= \{-1,1\}$; mivel ezt minden $\neq e$ részcsoport tartalmazza, így Q-ban *minden*

részcsoport normálosztó.[3]

Rátérve a feladatra tudjuk, hogy G feloldható, hiszen feloldható csoportok direkt szorzata. Eszerint G kompozícióláncaiban (amelyek a végesség miatt biztosan léteznek) a faktorok prímrendűek, és $|G| = 120 = 2^3 \cdot 3 \cdot 5$ miatt minden kompozícióláncban három db $\mathbb{Z}_2$ és egy-egy db $\mathbb{Z}_3$ ill. $\mathbb{Z}_5$ típusú faktornak kell szerepelnie (a Jordan-Hölder tételt is felhasználva).

A 3.3 feladat alapján G-nek csak olyan részcsoportjai vannak, amelyek $A \times B$ alakúak, ahol $A \leq Q$ és $B \leq \mathbb{Z}_{15}$.

Az eddigiek szerint egy kompozíciólánc ilyen alakú:

$$G = A_0 \times B_0 \triangleright A_1 \times B_1 \triangleright A_2 \times B_2 \triangleright \ldots \triangleright A_5 \times B_5 \cong e$$

ahol az öt db faktor a fentiek valamilyen „ismétléses permutációja” és $A_{i+1} \triangleleft A_i$, $B_{i+1} \triangleleft B_i$ $(i = 0, \ldots, 4)$ (sőt, igazából $A_i \triangleleft Q$ és $B_i \triangleleft B_0$ is teljesül).

Vegyük észre továbbá, hogy *bármilyen permutációhoz* tartozik legalább egy kompozíciólánc, ugyanis egy még szóbajövő p prím indexszel mindig találunk részcsoportot $A_i \times B_i$-ben, továbbá ez $p = 3,5$ esetén csak úgy történhet, hogy az A_i „kvaterniókomponenst” megtartva $\mathbb{Z}_{15} \cong \mathbb{Z}_5 \times \mathbb{Z}_3$ valamely p-Sylowját választjuk B_{i+1}-nek, $p = 2$ esetén pedig a $\mathbb{Z}_{15}$-beli komponenst megőrizve A_i-ben keresünk egy 2 indexű részcsoportot. Nevezzük az előbbi ismétléses permutációt a kompozíciólánc permutációjának. Például a $(3,2,2,5,2)$-höz tartozó egyik kompozíciólánc ($\mathbb{Z}_{15}$ előbbi direkt felbontásával):

$$G \triangleright Q \times \mathbb{Z}_5 \times e \triangleright \langle i \rangle \times \mathbb{Z}_5 \times e \triangleright \langle -1 \rangle \times \mathbb{Z}_5 \times e \triangleright \langle -1 \rangle \times e \times e \triangleright e \times e \times e$$

Az előző láncban $\langle i \rangle$ helyett választhattuk volna $\langle j \rangle$-t vagy $\langle k \rangle$-t is, ez indokol-

[3] *Dedekind és Baer* alábbi tétele mutatja, hogy egy pontosan meghatározott értelemben nemkommutatív csoportoknál mindig a kvaterniócsoport „felbukkanása” okozza azt, hogy minden részcsoport normálosztó: Ha G nemkommutatív csoport, amelyben minden részcsoport normálosztó, akkor $G \cong Q \times E \times O$, ahol Q a kvaterniócsoport, E egy elemi kommutatív 2-csoport és O egy Abel-csoport, amelyben minden elem rendje páratlan.

ja az „egyik” szó használatát és mutatja, hogy meg kell még gondolnunk, egy adott permutációjú kompozícióláncból hány van, azaz adott elemszámú részcsoport választásánál hány lehetőségből választhatunk. Mivel $\mathbb{Z}_{15}$-nek (mint ciklikus csoportnak) egyetlen 3 és 5 rendű részcsoportja van, ezért a „multiplicitást” kizárólag a kvaterniócsoport okozza. Ennek egyetlen másodrendű eleme van, a -1; ez egyrészt mutatja, hogy a második $\mathbb{Z}_2$ típusú faktornál a „kvaterniókomponens” egyértelműen meghatározott, másrészt az adódik, hogy nincsen $\mathbb{Z}_2 \times \mathbb{Z}_2$ típusú részcsoportja Q-nak (ui. ebben három db másodrendű elem is lenne). Így az első $\mathbb{Z}_2$ típusú faktornál egy négyelemű ciklikus részcsoportot kapunk a kvaterniócsoportban (mivel $4 = 2^2$ elemű csoportra ez az egyetlen további lehetőség), amelyből három db van: $\langle i \rangle, \langle j \rangle, \langle k \rangle$. A kompozíciólánc permutációjának megadása mellett ezek közül választhatunk tetszőlegesen, amikor az első $\mathbb{Z}_2$ faktor fellép, így G összes kompozícióláncainak száma:

$$\frac{5!}{3!} \cdot 3 = 60$$

■

3.16 Feladat:

a) Bizonyítsuk be, hogy ha a G véges csoport elemszáma három (nem feltétlenül különböző) prím szorzata, akkor G feloldható.

b) Igazoljuk, hogy a legkisebb n, amelyre létezik n elemű nemkommutatív egyszerű csoport, az $n = 60$.

Megoldás: $a)$ Először is vegyük észre, hogy a 3.12. feladat (beleértve a végén lévő megjegyzést is) alapján elég *egyetlen* nemtriviális normálosztót találnunk G-ben, ez ui. szükségképpen feloldható lesz a faktorcsoporttal együtt.
Legyen $|G| = pqr$, ahol $p \geq q \geq r$ prímek. Négy eset lehetséges aszerint, milyen a három prím egymáshoz való viszonya:

$i)\ p = q = r$

Ekkor $|G| = p^3$ és így G feloldható (sőt, nilpotens).

$ii)\ p = q > r$

A Sylow-tételek alapján $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$ és r-nek osztója, ami jelen esetben csak úgy teljesülhet, ha egyetlen p-Sylow van, ami így normálosztó és készen vagyunk.

$iii)\ p > q = r$

Tudjuk, hogy 1, q vagy q^2 db p-Sylow lehet; nyilván feltehetjük, hogy 1-nél több van.

Ha q darab van, akkor a Sylow-tételek alapján $|G : N_G(P)| = q$ (P valamelyik p-Sylow), de mivel q a G elemszámának legkisebb prímosztója, ezért $N_G(P) \triangleleft G$ a 2.7.12. tétel szerint; ezzel találtunk egy nemtriviális normálosztót.[4]

Végül tegyük fel, hogy q^2 db p-Sylow van. Mivel ezek prímrendű ciklikusak, ezért összesen $q^2 \cdot (p-1) + 1 = pq^2 - q^2 + 1 = |G| - (q^2 - 1)$ elemet tartalmaznak. A fennmaradó $q^2 - 1$ elem közül kell hogy kikerüljenek a q-Sylow(ok) $\neq e$ elemei, de ezek szerint csak egyetlen q-Sylow „fér el”, azaz $\left|\mathrm{Syl}_q(G)\right| = 1$: a q-Sylow normálosztó.

$iv)\ p > q > r$

Szokás szerint a p-Sylowok számát kezdjük el vizsgálni, ami lehet $1, r, q, qr$; feltehető, hogy nem 1 és a $\bmod p$ „maradékos feltételt” is figyelembe véve az r és a q is kizárható. Tehát $\left|\mathrm{Syl}_p(G)\right| = qr$. Ezek a prímrendű ciklikusok összesen $(p-1)\cdot qr + 1 = rqp - rq + 1$ elemet tartalmaznak. Feltéve most, hogy nem egyetlen q-Sylow van (egyébként az normálosztó lenne) legalább $q + 1$ db-nak kell lennie

[4] Valójában $N_G(P) \triangleleft G$-ből az is következik, hogy $P \triangleleft G$. Ez közvetlenül adódik 2.6.6.-ból, de megindokolhatjuk enélkül is. Ugyanis $N_G(P)$-ben egyetlen p-Sylow van, ami így $N_G(P)$ minden automorfizmusánál fixen kell hogy maradjon, tehát tetszőleges G-beli elemmel való konjugálásnál is. A fenti feltevés így tulajdonképpen ellentmondásra vezet, hiszen G-ben is csak egyetlen p-Sylow lehetne.

a „maradékos feltétel” miatt, amelyek összesen legalább $(q+1)(q-1) = q^2 - 1$ db nemtriviális (q-adrendű) elemet jelentenek az eddigiek mellett. Ez ellentmondás, hiszen $q^2 > rq$ miatt már most is $rqp - rq + 1 + q^2 - 1 = rqp - rq + + q^2 > rqp = |G|$ elemünk van (és még nem is számoltunk az r-Sylowokkal). A bizonyítás ezzel teljes.

b) Előbbi eredményünk szerint egy véges, nemkommutatív egyszerű csoport elemszáma legalább négy db (nem feltétlenül különböző) prím szorzata. Mivel $n = 60$-ig az elemszám legfeljebb öt (nem feltétlenül különböző) prím szorzata, így a 2 legnagyobb hatványa szerint szétválasztva az eseteket a következő értékek jöhetnek szóba:
$n = 2^5 = 32$; $2^4 = 16$ $2^4 \cdot 3 = 48$; $2^3 \cdot 3 = 24$ $2^3 \cdot 5 = 40$ $2^3 \cdot 7 = 56$; $2^2 \cdot 3^2 = 36$ $2^2 \cdot 3 \cdot 5 = 60$ és $2 \cdot 3^3 = 54$.

A véges 2-csoportok feloldhatóak, így $n = 16{,}32$ nem lehet. Kizárhatjuk továbbá az $n = 54$-et is, hiszen a 2.7.12. miatt ebben van 2 indexű normálosztó. 60 elemű egyszerű csoportok már ismerünk, ilyen pl. A_5; vizsgáljuk a többi esetet.

Ha létezne huszonnégy elemű egyszerű csoport, akkor abban három db 2-Sylow lenne, amelyek magukat normalizálják; ekkor azonban a szokásos permutációreprezentációval $G \cong H \leq S_3$, ami az elemszám miatt ellentmondás. Ugyanez az érvelés kizárja az $n = 48$-at is.

A $|G| = 40$ esetben öt db 2-Sylownak kéne lennie, így $G \cong H \leq S_5$, ahol H egy negyven elemű részcsoportja S_5-nek. Ilyen azonban nem létezik, hiszen most S_5-nek a feltételezett H szerinti mellékosztályokon vett $S_5 \to S_3$ permutációreprezentációjának magja e kell hogy legyen, ugyanis S_5-nek csak A_5 a nemtriviális normálosztója, de utóbbi persze nem lehet benne H-ban. Ebből az $S_5 \cong S_3$ képtelenség adódik, tehát egyetlen 2-Sylow van G-ben.

Maradt az $n = 36$ és $n = 56$. Utóbbi esetén (az egyszerűség miatt) nyolc db 7-Sylow van, amelyek az ismert számolás szerint együtt $8 \cdot 6 + 1 = 49$ elemet

jelentenek. Ezek mellett csak egyetlen 2-Sylow fér el, ami így normálosztó. Ez ellentmondás, tehát G nem egyszerű.
Végül legyen $n = 36$ és tegyük fel, hogy G egyszerű. Ekkor négy db 3-Sylow van, tehát $G \cong H \leq S_4$, ellentmondás.
Az állítást igazoltuk. ∎

Megjegyzés: További meggondolásokkal viszonylag röviden megmutatható, hogy valójában *egyetlen* hatvan elemű nemkommutatív egyszerű csoport létezik, a már ismert A_5. Ilyen rend még pl. az $n = 168$ is; ennek igazolása már jóval nehezebb.[5]
A már említett *Klasszifikációból* kiderül, hogy minden n-re legfeljebb két, egymással nem izomorf n elemű egyszerű csoport létezik. Erre az állításra nem ismert elemi bizonyítás.

Végül említést érdemel a (XX. századi) csoportelmélet egyik legnevezetesebb és legjelentősebb eredménye; a néhány szóban megfogalmazható állítást egy 250 oldalas (!!) cikkben bizonyította a két szerző:

Tétel (Feit, Thompson): Minden páratlan rendű csoport feloldható.

3.17 Feladat: *Nevezzük a G véges csoportot p-láncszerűnek, ha $Syl_p(G) = \{P_1, P_2, \ldots, P_\ell\}$ $\ell \geq 3$ és a p-Sylowokra teljesül a következő két feltétel:*

$$\bigcap_{P \in Syl_p(G)} P = e \quad \text{és}$$

$$|P_i \cap P_j| > 1 \Leftrightarrow i \equiv j \pm 1 \,(mod\, \ell)$$

(megfelelően indexelve a részcsoportokat).
(Ez szemléletesen éppen azt jelenti, hogy a Sylow-részcsoportok „láncszerűen" metszik egymást.)
Bizonyítsuk be, hogy nem létezik p-láncszerű csoport semmilyen p prímre.

[5] Lásd (pl.) Michio Suzuki: Group Theory, Springer-Verlag 1977. 107-110.o.

Megoldás: Tegyük fel, hogy a fenti jelölés mellett G p-láncszerű.
Hasson G a szokásos módon konjugálással $\mathrm{Syl}_p(G)$-n, azaz tekintsük azt a $\vartheta: G \to S_\ell$ homomorfizmust, amelynél

$$g \mapsto (P_i \mapsto g^{-1}P_i g)\ \forall g \in G,\ P_i \in \mathrm{Syl}_p(G)$$

Ekkor $\mathrm{Im}\,\vartheta$ a II. Sylow-tétel miatt tranzitív permutációcsoport ℓ ponton, így $\ell \mid |\mathrm{Im}\,\vartheta|$.

A továbbiakban legyen $\mathrm{Im}\,\vartheta = H$. Mivel minden φ_g konjugálás bijekció, így $\varphi_g(P_i \cap P_j) = \varphi_g(P_i) \cap \varphi_g(P_j)\ \forall g \in G, 1 \le i,j \le \ell$. Ez mutatja, hogy tetszőlegesen megadva mondjuk P_1 képét egy konjugálásnál, P_2 képe csak P_1 képével „szomszédos” p-Sylow lehet és ezt a kettőt megadva az összes többi p-Sylow képe már egyértelműen adódik (ugyanúgy, mint D_n-nél).
Kaptuk: $|H| \le 2\ell$, amiből a korábbi észrevétel szerint $|H| = \ell$, vagy 2ℓ.

Most meggondoljuk, hogy ℓ nem lehet. Indirekt legyen a kép ℓ elemű, ekkor a fenti ϑ homomorfizmus $\mathrm{Ker}\,\vartheta := N$ magjának indexe $|G:N| = |H| = \ell$. Másrészt ϑ definíciója miatt $N = \bigcap_{i=1}^{\ell} N_G(P_i)$. Mivel $|G : N_G(P_i)| = \left|\mathrm{Syl}_p(G)\right| = \ell$ minden i-re, így az adódik, hogy valamennyi normalizátor egybeesik:

$$N = \bigcap_{i=1}^{\ell} N_G(P_i) = N_G(P_j)\ \forall j$$

Ekkor azonban pl. $P_1 \le N_G(P_1) = N_G(P_2)$ és így $\langle P_1, P_2\rangle \triangleright P_2$, azaz $\langle P_1, P_2\rangle = P_1P_2$, ami ellentmondás, hiszen ekkor $|P_1P_2| = \frac{|P_1||P_2|}{|P_1\cap P_2|} \ge \frac{p^{2k}}{p^{k-1}} = p^{k+1}$, tehát a generált részcsoport egy legalább p^{k+1} elemű p-részcsoport, ami persze nem létezik.[6] Eszerint $|H| = 2\ell$.

Tegyük fel, hogy $p \nmid 2\ell$, azaz $p \ne 2$ (ui. $p \mid 2\ell \Rightarrow p \mid \ell$, mert $\ell \equiv 1 \pmod p$ miatt $(p,\ell) = 1$). Ekkor, mivel homomorfizmusnál p-Sylow részcsoport képe a kép p-Sylowja, minden P_i e_H-ba képződik, azaz $\forall i\ P_i \le N \Rightarrow P_1 \le N_G(P_2)$

[6] Látható, hogy ez a gondolat voltaképpen a II. és III. Sylow-tétel bizonyításának egy részlete.

(mondjuk); ez ugyanúgy ellentmondás, mint az imént. Eszerint $p \mid 2\ell$ és így $p = 2$; legyen $2^k \mid\mid |G|$.

Az első izomorfizmustétel miatt $P_i \cap N$ p-Sylowjai N-nek, és $2 = \frac{|P_i|}{|P_i \cap N|}$, ami mutatja, hogy $|P_i \cap N| = 2^{k-1}$. Ekkor a $P_i \cap N = Q_i$ jelölést bevezetve $Q_1 \leq N$, ezért $Q_1 \leq N_G(P_3) \Rightarrow |\langle Q_1, P_3 \rangle| = 2^{2k-1} > 2^k$ $(k \geq 2)$ abban az esetben, ha $\ell > 3$ (mert $|Q_1 \cap P_3| = 1$ ilyenkor); így a fentihez hasonló ellentmondást kaptunk. Legyen tehát $\ell = 3$.

Az iménti érvelés mutatja, hogy ebben az esetben $|Q_1 \cap P_3| = 2^{k-1}$ kell hogy legyen és mivel csak három db 2-Sylow van, így $Q_2 \cap P_3$ elemszáma is ugyanennyi. Mivel $P_i \cap P_3 \geq Q_i \cap P_3$ $(i = 1,2)$, ezért a 2-Sylowok metszetei is a lehető legnagyobbak. Jelölje R_i a $P_i \cap P_3$ metszetet. $R_1, R_2 \leq P_3$ miatt az előbbiekből adódik, hogy $\langle R_1, R_2 \rangle = R_1 R_2 = P_3$ a szokásos érvelést követve.$(*)$ De mindkét részcsoport 2^{k-1} elemű, így az uniójuk elemszáma is majdnem ennyi:

$$|R_1 \cup R_2| = |R_1| + |R_2| - |R_1 \cap R_2| = 2^k - 1$$

Ez azt jelenti, hogy P_3-nak egyetlen olyan x eleme van, amely nincs benne sem R_1-ben, sem R_2-ben. Ennek az elemnek $x = r_1 r_2$ alakúnak kell lennie, ahol $r_i \in R_i$ és egyik sem e, sőt, bármely két „nemegység” elemet választva a két részcsoportból, szorzatuk x-et kell hogy adja. Csakhogy $k \geq 3$ esetén egy rögzített r_1-et véve választhatunk két $r_2 \neq r_2^*$ elemet, melyekre $x = r_1 r_2 = r_1 r_2^* \Rightarrow r_2 = r_2^*$, ami ellentmondás.[7]

Eszerint $k = 2$ és a 2-Sylowok $\mathbb{Z}_2 \times \mathbb{Z}_2$ típusú kommutatív csoportok (ciklikusak nem lehetnek, mivel ezeknek egyetlen kételemű részcsoportjuk van, tehát a három Sylow ugyanabban a részcsoportban metszené egymást).

Ismert, hogy ha a p-Sylowok kommutatívak, akkor az összes metszete előáll mint (alkalmasan választott) kettőnek a metszete [4]; ez jelen esetben a feltevésünk

[7] Lényegesen rövidebben eljuthatunk idáig $(*)$-tól a következő „érveléssel”:

$$\underline{2^{2k-2}} = 2^{k-1} \cdot 2^{k-1} = |R_1|\,|R_2| = |R_1 R_2| = |\langle R_1, R_2 \rangle| = |P_3| = \underline{2^k} \Rightarrow k = 2$$

miatt nem igaz, tehát a $(p,k,\ell) = (2,2,3)$ eset is kizárt és a bizonyítás teljes. ∎

Megjegyzés: Az iménti probléma eredetileg abból származik, hogy ha valamely p-re a p-Sylowok legalább p^2 eleműek, akkor pusztán a csoport elemszámát ismerve nem tudunk becslést adni ezen Sylowok uniójának elemszámára (és így az eddig a 3.16 feladatban bemutatott bizonyítási módszerek elakadnak), hiszen a metszetek (esetleg) nagyon bonyolultak lehetnek.

Általában vizsgálhatjuk azt a gráfot, melynek csúcsai a p-Sylowok és két csúcsot pontosan akkor kötünk össze, ha a megfelelő részcsoportok nemtriviálisan metszik egymást. Itt természetesen ésszerű kiróni azt a feltételt, hogy az összes (és egynél több) p-Sylow metszete triviális legyen (ez tetszőleges G esetén $G/O_p(G)$-re mindig igaz). Erről a gráfról, amely a Sylow-tételek miatt reguláris, több dolgot kérdezhetünk, pl.: hány komponense van? mennyi az egyes csúcsok (egymáséval megegyező) foka? adott komponens (amely összefüggő) hogyan nézhet ki?

A fenti eredmény arra válaszol (illetve annak a lehetetlenségét állítja), amikor 1 komponensű a gráf és 2-reguláris (egy ilyen ui. biztosan kör). Egy cikkből, mely alapvetően nem ezzel a kérdéssel foglalkozik, kiderül például, hogy S_8 2-Sylowjainál teljes gráfot kapunk. [5]
A szakirodalomban (a `MathScineten` [8] hozzáférhető részében legalábbis) nem találtam olyan cikket, amely „explicite” ezekkel a kérdésekkel foglalkozna.

3.18 Feladat: *Mutassuk meg, hogy minden G csoportnak egyértelműen létezik maximális perfekt részcsoportja, továbbá ha G véges, akkor ez a kommutátorlánc legkisebb (elemszámú) tagja.*

Megoldás: A bizonyításhoz szükségünk lesz a halmazelméletből ismert *Zorn-lemmára*:
Ha egy Λ részben rendezett halmazban minden lánc felülről korlátos, akkor van Λ-ban (legalább egy) maximális elem.

A perfekt részcsoportok között (és általánosan, G összes részcsoportját tekintve) a halmazelméleti tartalmazás egy részben rendezést jelent. Megmutatjuk, hogy G-nek egy perfekt részcsoportokból álló láncában a tagok uniója szintén perfekt részcsoport, ami persze felső korlátja az összesnek. Eszerint létezik legalább egy maximális perfekt részcsoport a Zorn-lemma szerint; az egyértelműséget külön meg kell gondolnunk.

Legyen $\{G_\lambda : \lambda \in \Lambda\}$ perfekt részcsoportok egy lánca, azaz $G'_\lambda = G_\lambda \ \forall \lambda \in \Lambda$ és $H = \bigcup_{\lambda\in\Lambda} G_\lambda$. Ekkor $H' \leq H$ teljesül (mint mindig), vegyük $h \in H$-t. H definíciója miatt $h \in G_\lambda$ valamely λ-ra, ezért $h \in G'_\lambda = G_\lambda$. Az előbbiek szerint $\forall h \in H\, \exists \lambda \in \Lambda \ h \in G'_\lambda \leq H'$, azaz $H \leq H'$ és így $H = H'$ perfekt, amint állítottuk.

Most rátérhetünk az *egyértelműség* bizonyítására. Legyenek $R_1 \neq R_2$ a G maximális perfekt részcsoportjai; ekkor nyilván egyik sem tartalmazza a másikat. Mivel mindkettő perfekt, ezért $\langle R_1, R_2\rangle' \leq \langle R_1, R_2\rangle = \langle R'_1, R'_2\rangle$ (az egyenlőséghez használtuk a perfektséget), másrészt $\langle R'_1, R'_2\rangle \leq \langle R_1, R_2\rangle$ mindig igaz. Eszerint $\langle R_1, R_2\rangle$ olyan perfekt részcsoport, amely R_1-et és R_2-t is valódian tartalmazza; ez ellentmond ezek maximalitásának. Következésképpen $R_1 = R_2$, az egyértelműséget is beláttuk.

Megjegyzés: Ha G véges, akkor nincs szükség a Zorn-lemmára ahhoz, hogy maximális perfet részcsoportot találjunk, hiszen $e \leq G$ perfekt és csak véges sok részcsoportot kell végignézni.

Legyen most G véges és $G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \ldots \triangleright G^{(n)} = G^{(n+1)} = \ldots$ a kommutátorlánc, amely tehát az n-edik lépésben „akad el” (esetleg, pontosan az n derivált hosszú feloldható csoportoknál, az egységelemhez érkezve); ekkor $G^{(n)} = R$ perfekt. Ha $H \leq G$ perfekt, akkor $H = H^{(1)} = H^{(2)} = \ldots = H^{(n)} \leq G^{(n)} = R$, tehát $H \leq R$ és így R valóban maximális.

A bizonyítás teljes. ∎

3.19 Feladat:

i) Igazoljuk, hogy tetszőleges csoport bármely u, v elemeire fennáll:

$$[u^m, v] = [u, v]^{u^{m-1}+u^{m-2}+\ldots+u+1}$$

(az összeg alakú kitevőt a szokásos módon értelmezzük).

ii) Mutassuk meg, hogy ha egy G nilpotens csoport tartalmaz p-edrendű elemet, akkor a centruma is.

Megoldás: *i)* A 2.8.10. tétel előtt szereplő $[ab, c] = [a, c]^b [b, c]$ azonosság szerint a bizonyítandó formula átírható így: $[u^m, v] = [u, v]^{u^{m-1}} [u^{m-1}, v]$. A második tényezőt ugyanúgy tovább bonthatjuk, végül m lépésben éppen a bizonyítandó állítást nyerjük.
Emeljük ki azt a (folytatás szempontjából is) fontos esetet, amikor $[u, v] \in Z(G)$ $\big($illetve elég annyi, hogy $[u, v] \in Z(\langle u, v\rangle)\big)$; ekkor $[u, v]$ minden konjugáltja önmaga, és ezt kapjuk: $[u^m, v] = [u, v]^m$.

ii) A bizonyításhoz szükségünk lesz a következő észrevételre: ha a G nilpotens csoportnak $e = \zeta_0(G) \leq \zeta_1(G) = Z(G) \leq \zeta_2(G) \leq \ldots \leq \zeta_n(G) = G$ felső centrális lánca, akkor $G/\zeta_1(G)$ felső centrális lánca „tagonként" származtatható ebből a láncból:

$$e_{G/\zeta_1(G)} = \zeta_1(G)/\zeta_1(G) \leq \zeta_2(G)/\zeta_1(G) \leq \ldots \leq \zeta_n(G)/\zeta_1(G) = G/\zeta_1(G)$$

Az egyszerűség kedvéért legyen $Z_k = \zeta_k(G)$. Az előbbi állítás igazolásához vizsgáljuk meg, hogy a $gZ_1 \cdot Z_c/Z_1$ $(c = 1, \ldots, n-1)$ mellékosztály mikor van benne $G/Z_1\big/_{Z_c/Z_1}$ centrumában:

$$gZ_1 \cdot Z_c/Z_1 \in Z\big({}^{G/Z_1}\big/_{Z_c/Z_1}\big) \Leftrightarrow \big[gZ_1 \cdot Z_c/Z_1\,,\ {}^{G/Z_1}\big/_{Z_c/Z_1}\big] = e_{G/Z_1\big/_{Z_c/Z_1}}$$

$$\Leftrightarrow \forall h \in G\,[gZ_1, hZ_1] = [g, h]\,Z_1 \in Z_c/Z_1 \Leftrightarrow \forall h \in G\,[g, h] \in Z_c \Leftrightarrow g \in Z_{c+1}$$

Tehát ${}^{G/Z_1}\!/_{Z_c/Z_1}$ centrumának teljes inverz képe pontosan Z_{c+1}/Z_1 a megfelelő természetes homomorfizmusnál; pontosan ezt kellett belátnunk.

Rátérve a bizonyítandó állításra tudjuk, hogy G felső centrális lánca „felér" G-ig:

$$e = Z_0(G) \leq Z_1(G) = Z(G) \leq Z_2(G) \leq \ldots \leq Z_n(G) = G.$$

Legyen $x \in G$ egy p-edrendű elem.

Ha $x \in Z(G)$, akkor nincs mit bizonyítani. Tegyük fel, hogy $x \in Z_2(G) \backslash Z_1(G)$. A nilpotencia definíciója miatt ekkor $\forall g \in G \ \ [x, g] \in Z_1(G)$ és az $i)$ végén tett megállapítás szerint fennáll: $[x, g]^p = [x^p, g] = [e, g] = e \ \forall g \in G$. Tehát minden x-szel képzett kommutátor a centrumban van és rendje p-nek osztója; mivel nem lehet mindegyik$= e$ (ui. $x \notin Z(G)$), ezért valamelyik egy p-edrendű elem lesz $Z(G)$-ben.

Tegyük fel most, hogy az $x \in Z_i(G) \backslash Z_{i-1}(G)$, $i = 0{,}1, \ldots, k-1$ esetekre már beláttuk az állítást (minden G nilpotens csoportra) és legyen $x \in Z_k(G) \backslash Z_{k-1}(G)$. Tekintsük G felső centrális láncának (tagonkénti) képét a $G \to G/Z_1(G) := G_1$ természetes homomorfizmusnál. Ekkor a fenti észrevétel alapján $xZ_1(G) \in$

$\in Z_{k-1}(G_1) \backslash Z_{k-2}(G_1)$ egy p-edrendű elem G_1 -ben, így a feltevés szerint $Z(G_1) =$

$= Z_2(G)/\zeta_1(G)$ tartalmaz p-edrendű elemet, mondjuk $yZ_1(G)$ ilyen. Ez pontosan azt jelenti, hogy $Z_2(G) \ni y \notin Z_1(G)$, de $y^p \in Z_1(G)$. Ekkor azonban tetszőleges $h \notin C_G(y)$ elemre fennáll:

$$[y, h]^p = [y^p, h] = e$$

Ez azért van így, mert az $[y, h]$ komutátor $y \in Z_2(G)$ miatt biztosan a centrumba esik, így az $i)$ végén szereplő azonosság alkalmazható, másrészt $y^p \in Z(G)$, tehát a jobb oldali kommutátor e-vel egyezik meg; mivel y és h nem felcserélhetők (h megválasztható így, hiszen y nincs a centrumban), ezért $[y, h] \neq e$ egy p-edrendű elem $Z(G)$-ben. A bizonyítás teljes. ∎

3.20 Feladat: *Számítsuk ki S_n Frattini-részcsoportját!*

Megoldás: Bizonyos részcsoportokról, melyek metszete nyilvánvalóan triviális, megmutatjuk, hogy maximálisak S_n-ben; ebből azonnal adódik, hogy Frat $(S_n) = e$.

Jelölje St(i) az i pont (S_{n-1}-gyel izomorf) stabilizátorát S_n-ben. Ekkor világos, hogy $\bigcap_{i=1,2,\ldots,n}$ St$(i) = e$. Legyen most i rögzített és $\sigma \in S_n \backslash$St$(i)$ tetszőleges permutáció, amelyre $(i)\sigma = \ell$, valamint legyen $\rho \in S_n \backslash$St(i) is rögzített és $(k)\rho = i$ (ekkor persze $k, \ell \neq i$). Fennáll, hogy $(k\ell) \in$ St(i) továbbá látható, hogy a következő, α permutáció i-t fixen hagyja:

$$\alpha = \sigma(kl)\rho$$

Eszerint $\alpha \in$ St(i) és $\sigma = \alpha\rho^{-1}(k\ell) \in \langle$St$(i), \rho\rangle$ (az eddig nem részletezett $k = \ell$ esetén is igaz az iménti állítás, csak a (kk) „cserét” egyszerűen figyelmen kívül lehet hagyni). Ezzel beláttuk, hogy tetszőleges $\rho \in S_n \backslash$St(i) elemre $\langle$St$(i), \rho\rangle = S_n$, más szóval egy St(i)-nél bővebb részcsoport már minden elemet tartalmazni fog: a stabilizátor maximális részcsoport. A bizonyítás teljes. ∎

Megjegyzés: Azokat a tranzitív permutációcsoportokat, melyekben minden pont stabilizátora maximális, *primitívnek* hívják. Belátható, hogy ez a tulajdonság azzal ekvivalens, hogy az alaphalmaznak (melyen a permutációcsoport hat) nem létezik olyan nemtriviális partíciója, amelynek elemeit a csoport egymás között permutálná. Könnyen adódik, hogy S_n ilyen, hiszen itt bármely két rendezett n-es átvihető egymásba (ún. n-szeres tranzitivitás). A bizonyítás nem erre épült, de ezt felhasználva az előbbi eredményünk általánosítható:

Ha G primitív permutációcsoport, akkor Frat$(G) = e$.

4. fejezet

Egy középiskolás szakkör

Ebben a fejezetben azzal a szakköri foglalkozással/előadással kapcsolatos tervekről és tapasztalatokról lesz szó, amelyet az *ELTE Apáczai Csere János Gyakorlógimnáziumban* tartottam 2008. november 12-én a *12.A* osztály tanulói számára. Az osztály, ezen belül a foglalkozáson részt vevők egyik felével matematika gyakorlótanítás során volt alkalmam megismerkedni és talán nyugodtan mondhatom: jó kapcsolatot kialakítani. A foglalkozáson 11 tanuló mellett részt vett *Dr. Kiss Géza* (matematika) vezetőtanár (az osztály matematikatanára), továbbá *Vitéz Ildikó* matematikus és *Vidor Sára* ötödéves matematikus hallgató is. Valamennyiüket megkérdeztem a szakkörrel kapcsolatos (utólagos) észrevételeikkel, véleményükkel kapcsolatban, amelyekre ki is fogok térni.

4.1. Tervezés

4.1.1. Általános észrevételek

Egy „egyetemi anyagról” szóló és - részben külső okok miatt - egyetlen alkalomból álló szakkör célkitűzései szükségszerűen szerények kell hogy legyenek. Ennek megfelelően nem lehetett és nem is volt célom, hogy a csoportelmélet - akár legenyhébb értelemben vett - mélyeibe bevezessem a tanulókat, és az sem, hogy számos szellemes, középiskolához kapcsolódó alkalmazást tárgyaljak; utóbbival persze vállalva a kockázatot, hogy az egész újdonság kissé „lóg majd a levegőben”. Amit szerettem volna elérni ezzel szemben az az, hogy valamiféle, középiskolai ismereteken alapuló ízelítőt adjak arról, a felsőbb matematika ezen része nagyjából miről szól. Talán pontosabb, ha kissé misztikusnak is hat, ha úgy fogalmazok: egyfajta „érzetet”/ráérzést szerettem volna kiváltani a tanulókból, ahhoz hasonló érzetet, amely talán magának a csoportelméletnek a kialakulásához is vezetett, mindenesetre alapvető szerepet játszik az egyetemi tananyag elsajátításában: a (közös) műveleti tulajdonságok megjelenése és (közös) következményei különböző (alap)halmazok esetében, ebből kiindulva magának a csoportaxiómákban megfogalmazott tulajdonságokkal rendelkező műveletnek az absztrakciója.

A már említett időtényezőt is figyelembe véve a megvalósítás módjára az „interaktív kiselőadás” látszott legalkalmasabbnak. Ez azt jelenti, hogy bár én „diktáltam” az elég feszes tempót a táblára írva és magyarázva, de ahol csak lehetett, kérdésekkel igyekeztem kisebb-nagyobb „részmunkálatokba” bevonni a tanulókat is, illetve folyamatosan arra ösztönözni őket, hogy kérdezzenek. Ugyanakkor éppen a „ráéreztető” jelleg és az eleve sok utánagondolást igénylő absztrakció miatt nehéz megítélni, hogy adott pillanatban melyik tanuló éppen hol tart ebben a folyamatban, illetve vajon eléggé tudta-e követni a már elhangzottakat ahhoz, hogy

esetleg csak intuitív módon, de követni tudja a hátralévőket. Ennek megfelelően felkészültem arra, hogy (némi kockázattal) ne essem kétségbe, ha éppen kétkedő/értetlen arcokat látok (bár általában ezekre is rákérdeztem), viszont a hozzájuk intézett kérdéseimet úgy válasszam meg, ill. annyira alapozzam meg (esetleg már „túlságosan” is), hogy a halványabb ráérzés is célba találjon és segítsék a remélt (otthoni) továbbgondolást.

Úgy gondolom, a fentiek megvalósításának egyik feltétele mindenképpen az optimális tanulói létszám, hiszen túl sok tanuló esetén elvész esetleg (érthető módon) az interaktivitás és mindenféle egyéni különbség, míg túl kevés tanuló esetén esetleg az „egyénre szabás” felfokozott lehetősége jelentősen eltérítheti az előadót (rám legalábbis ez biztosan igaz) eredeti céljától. Érzésem szerint a 11 fős létszám kiegyensúlyozottnak bizonyult az említett szempontokból.

Annak is van azonban jelentősége, hogy a diákok egy részét ismertem; ugyanis ennek a (kölcsönösen pozitív) ismeretségnek fontos szerepe volt abban, hogy egy ilyen interaktivitás egyáltalán létrejöhetett. „Idegennel” szemben, legyen az bármennyire közvetlen/hiteles, valószínűleg nehezebben hozható működésbe (ilyen rövid időn belül) a kétirányú kommunikáció.

Végül az egyik legfontosabb aspektus, amelyet nem lehet eléggé hangsúlyozni: a szakkörön részt vevők valamennyien kiváló képességű (és magaviseletű), a matematika felé (is) őszinte érdeklődéssel forduló tanulók voltak (amint ezt előre tudtam), akiknek együttműködő, inspiráló és előremutató, a megértést célzó hozzáállására nyugodtan számíthattam.

4.1.2. A téma vázlata

Ahhoz, hogy a csoport fogalmának (a szakkör vége felé) történő bevezetése a hosszú „előkészítés” végére indokoltnak tűnjön, mindenekelőtt szükség van arra,

hogy valamilyen „nemtriviális” csoporttal (persze még nem ezen a néven) megismerkedjünk, hiszen (amint ezt utólag *Kiss Géza* is megjegyezte) pusztán a mod n maradék(osztály)ok és a $\frac{k\cdot 2\pi}{n}$ szögű forgatások által „képviselt” ciklikus csoportok még nem jelentenek akkora újdonságot, nem elég bonyolultak ahhoz, hogy ezek motiválják az absztrakt csoportok vizsgálatát.

Emellett arra a középiskolás szemmel valószínűleg szokatlan tényre is rá kell mutatni, hogy a (sok évnyi matematikatanuláson alapuló) „megszokással” és intucióval ellentétben nem annyira a művelet *kommutativitása*, mint az *asszociativitása* „nélkülözhetetlen” (erre alább részletesebben visszatérek). Itt talán érdemes megjegyezni, hogy bár egy középiskolás tanuló számára a „szokásos” összeadás és szorzás furcsa nevű műveleti azonosságai (elvileg) ismertek (én egy kilencedikeseknek szóló dolgozatban is találkoztam azzal a kérdéssel, amely ezek felsorolását kérte), mindamellett ezeknek a tulajdonságoknak a tényleges jelentősége nem világosodik meg, amíg nem találkoznak nem asszociatív/nem kommutatív művelettel. A középiskolás anyagban nemigen találni „explicit példát” arra, hogy milyen egy nemkommutatív „szorzás/összeadás”.
Amint a fentiekből látszik, maga a csoport mint absztrakt fogalom csak a foglalkozás vége felé, az ismert és kevésbé ismert elemekből, gondolatokból álló előkészítés után kerül majd megfogalmazásra.

Viszonylag könnyen adódó, de már „nemtriviális” csoport a D_n diédercsoport és az S_n szimmetrikus csoport; úgy döntöttem, hogy az előbbivel való ismerkedéssel kezdem a tárgyalást. D_n a szabályos n-szöghöz kapcsolódik, mégpedig ennek szimmetriái alkotják; az eddig csupán vizuálisan „megcsodált” szimmetriákat most önmagukban kezdjük el vizsgálni. D_n (mint egybevágóságok halmaza) után megismerkedünk a K-val jelölt, négyelemű halmazzal, amelyet a téglalap szimmetriái alkotnak (tehát K a Klein-csoport). Az előbbiekben a sokszögek csúcsait megszámozzuk, és némi meggondolást követően a csúcsok (bizonyos) sor-

rendjeivel azonosítjuk az egybevágóságokat. Ezért választottam D_n-et a fenti S_n helyett, ugyanis míg a szimmetrikus csoport esetén a sorbarendezések mint függvények eleve kissé absztrakt fogalmával dolgoztunk volna, addig itt szellemes áttekintést adunk a szemléletes transzformációkról (mert az is kiderül, hány ilyen van), amelyekkel közben megtanulunk „ügyesen” számolni.

A D_n-beli művelet, azaz a kompozíció megismerése után az a cél, hogy több lépésben eljussunk oda: ez a művelet, melyet hamarosan egyébként szorzásként is fogunk jelölni, több szempontból teljesen úgy viselkedik, mint a jól ismert nemnulla racionális, valós(, komplex) számok szorzása, egyetlen lényeges különbséggel: a D_n-beli „szorzás” *nem kommutatív*, amint ez hangsúlyosan többször is előkerül (ki is számoljuk). Ha ettől a kellemetlen jelenségtől eltekintünk, akkor viszont a szorzással jelölt művelettel végül $t^k f^\ell$ $(k = 0,1\ ;\ \ell = 0,\ldots,n-1)$ alakban felírt D_n halmazzal tulajdonképpen úgy lehet dolgozni, hogy a geometriai háttérről meg is feledkezhetünk és csak a „betűk világában” dolgozunk a megismert számolási szabályokkal.

Az előbbi tematikus egység végén kiderül, hogy a szokásos $ax = ay \Rightarrow x = y$ „a-val való egyszerűsítésnél” titkon az asszociativitást használjuk ki. Hogy illusztráljam az asszociativitás jelentőségét, ezután egy kissé talán mesterkélt, de elemi példát mutatok nem asszociatív műveletre (ld. később). Ezt vizsgálva azonnal kiderül, hogy a(z adott művelet szerinti) hatványozás értelmezése (is) nehézségekbe ütközik akkor, ha a művelet nem asszociatív, de ha értelmezzük is egy természetesen adódó zárójelezéssel, akkor sem marad igaz pl. a megszokott $a^{m+n} = a^m \cdot a^n$ azonosság.

A következőkben felidézzük a $\mathbb{Z}_4 = \{0,1,2,3\}$ mod 4 maradékok összeadását, és ennek tulajdonságait, majd az alábbi felírás sugallata hatására felismerjük, hogy itt nagyon hasonló dolog történik, mint korábban D_4 forgatásainál (a négyzet szimmetriacsoportjával a korábbi részben kiemelten foglalkoztunk - ld. alább):

$$\mathbb{Z}_4 = \{1{,}1+1{,}1+1+1{,}1+1+1+1=0\} \quad .$$

Ezután a $\mathbb{Z}_n = \{0{,}1,\ldots,n\} \mod n$ maradékokra való általánosítást követően megfogalmazunk két fontos észrevételt: egyrészt ha D_n-ben megfeledkezünk a tükrözésekről és csak az $F_n = \{f, f^2, \ldots, f^n = id\}$ forgatásokat tekintjük, akkor ezek közül a D_n-beli szorzás nem vezet ki, sőt még kommutatív is, másrészt ha az F_n és $\mathbb{Z}_n$ halmazok között f-nek az 1-et, id-nek (ez D_n egységeleme) a 0-t és az előbbin értelmezett $\cdot$ szorzásnak az utóbbi $+$ összeadását feleltetjük meg, akkor ezekkel a megfeleltetésekkel mondhatjuk, hogy a két halmazban „tulajdonképpen ugyanaz" történik a műveletek során, bár azok konkrét jelentése egészen más; a műveletek speciális tulajdonságai alakilag teljesen megegyeznek.
Az előbbiek, mint kiderült, kettős célt szolgálnak: természetes példát akarok mutatni részcsoportra, emellett „mélyebb" célként a „tkp. ugyanaz" jelenségével az izomorfia fogalmát akarom érzékeltetni.

A következő lépésben a már megismert f, t és id szimbólumokkal (értelemszerűen módosítva azok jelentését) leírjuk a korábban szerepelt K halmazt is, amelyről megállapítjuk, hogy $ft = tf$, tehát K-n a szorzás kommutatív és minden elem négyzete id. Ekkor felmerül a kérdés: vajon K „tulajdonképpen ugyanaz"-e, mint a szintén négyelemű, kommutatív F_4?
A nemleges választ (az izomorfizmus fogalmának és tulajdonságainak ismertetése nélkül) az mutatja, hogy ha létezne „jó megfeleltetés", akkor K-t is megkaphatnánk mint valamely elemének hatványait; ez azonban nem teljesül, hiszen - mint kiderült - minden elemének négyzete az id elemmel egyezik meg, eszerint minden elemnek legfeljebb két különböző hatványa van (és id-en kívül mindegyik elemnek pontosan ennyi). Tehát a három megismert négyelemű művelettel ellátott halmaz, azaz K, F_4 és $\mathbb{Z}_4$ közül az utóbbi kettő „tkp. ugyanaz", az első pedig „lényegesen különbözik" tőlük.

Ennyi előkészület után jött el az idő, hogy a csoport fogalmát definiáljuk a csoportaxiómákkal. Számos „összeadásos” és „szorzásos” példát felsorolunk a már említettek és esetleg újonnan javasoltak közül, továbbá az alaposan megtárgyalt D_n kapcsán még egyszer kiemeljük azt is, hogy a kommutativitást (miért) nem követeljük meg az axiómákban (de ha az is teljesül, akkor *Abel-csoport*okról beszélünk).

Miután megismertük a csoportokat, a csoportelmélet tárgyát, kérdezzünk csoportokkal kapcsolatban: pl. minden n-re van n elemű csoport?; hány n elemű csoport van? - megállapítjuk, hogy ebben a formában erre a kérdésre *végtelen* a válasz, de nem pontosan erre gondoltunk, így módosítunk a kérdésfeltevésen: hány n elemű csoport van, ha nem tekintjük különbözőknek azokat, amelyek „tulajdonképpen ugyanazok”?
Erre a nehéz kérdésre „mese” a válasz, azaz néhány n-re megtudjuk, hány n elemű csoport van, ezek között pl. az $n = p$ esetet és azt is, hogy $n = 4$-re csak a megismert K és $\mathbb{Z}_4$ vannak. A „mesének” több eleme van: a „felvillantott” műveleti tábla kizárólag kombinatorikusan számolt „kitöltési számának” és az n elemű csoportok számának kontrasztja; az a tény, hogy az összes adott elemszámú csoport megkonstruálása és két megadott, megegyező elemszámú csoport „tulajdonképpen ugyanaz”-ságának eldöntése is nehéz feladat általában; a *Klasszifikáció* (persze nem ezen a néven) mint a csoportelmélet egyik nevezetes programjának időbeli és terjedelmi dimenziói.

A szakkör végén megemlítek pár tudományterületet, ahol a csoportelmélet szerepet játszik.

4.1.3. A foglalkozás tervezett anyaga

1. **Keressük meg az összes olyan egybevágósági transzformációt a síkon, amelyek egy szabályos**

   a) **háromszöget**

   b) **négyszöget**

   c) **n-szöget önmagába visznek!**

1. lépés: Előbb keresünk „gyorsan” minél több egybevágóságot mindhárom részében a feladatnak; világos hogy az $a)$-ban és a $b)$-ben adódó forgatások, beleértve a legnyilvánvalóbb/legkevésbé nyilvánvaló identitást is (melyet id-del fogunk jelölni) és tükrözések általában is jók lesznek (a megfelelő, értelemszerű változtatásokkal). Ezzel a konstrukcióval tehát az $a)$-ban a középpont körüli három db forgatást és három db tengelyes tükrözést, a $b)$-ben ezekből négy-négy darabot, míg általában a $c)$-ben n-n forgatást és tükrözést, összesen $2n$ db egybevágóságot állítottunk elő. Utóbbiak páros n esetén a szemköztes csúcsokat összekötő, páratlan n-nél pedig a csúcsokat a szemköztes oldal felezőpontjával összekötő egyenesekre történnek.

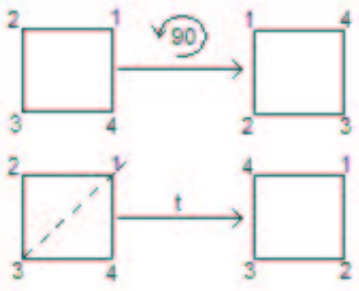
Kérdés: Van-e ennél több?

2. lépés: Bebizonyítjuk, hogy az összeset megtaláltuk. Ehhez előbb észrevesszük, hogy egy egybevágóság csúcsot csúcsba visz (részletes véggiggondolás HF), és az észrevétel alapján számozzuk meg a csúcsokat 1-től n-ig. Minden egybevágósághoz hozzárendelhetjük a csúcsoknak egy sorrendjét, amint az 4.1. ábra példái illusztrálják. Ennek a hozzárendelésnek fontos tulajdonsága, hogy *injektív*, azaz különböző egybevágóságokhoz nem tartozhat ugyanaz a sorrend, másképpen: adott sorrend egyértelműen meghatározza az egybevágóságot. Ugyanis ha a csúcsok egy sorrendjét már megadtuk, akkor a sokszög tetszőlegesen választott

pontjának képét a megadott csúcsoktól való távolságok (melyek, egybevágóságról lévén szó, nem változnak) meghatározzák (részletes végiggondolás itt is HF). Az előbbi meggondolások következménye, hogy legfeljebb annyi egybevágóság van, mint ahány sorrendje az n csúcsnak (azaz legfeljebb $n!$) és pontosan annyi, ahány lehetséges sorrend van: könnyű észrevenni ugyanis, hogy nem minden sorrendhez tartozik egybevágóság. A lehetséges sorrendeket pedig nem nehéz megszámolni: az 1 csúcsnak ugyanis n képe lehet (mondjuk forgatásokkal bármely csúcsba „el tudjuk vinni"), és ha ezt már megadtuk, akkor a 2 képére csak az 1 képével szomszédos két csúcs valamelyike jöhet szóba. Ez tehát összesen legfeljebb $n \cdot 2 = 2n$ lehetőség és ennyit meg is tudtunk adni, tehát az összeset megtaláltuk.
Az előbbi egybevágóságok, azaz az n csúcsú szabályos sokszöget fixen hagyó egybevágóságok halmazát D_n-nel fogjuk jelölni.

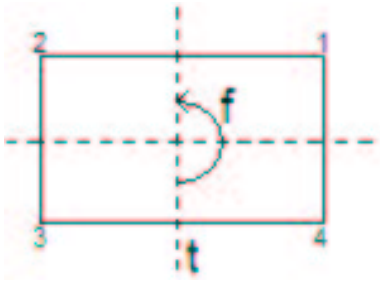
2. Oldjuk meg az előző feladatot általános téglalapra is!

Az előbbi receptet követve előbb megadunk annyit, amennyit ránézésre tudunk: két db tengelyes tükrözés (a szemköztes oldalak felezőpontjain átmenő egyenesekre) és két db forgatás: a középpont körüli $180°$-os forgatás (azaz középpontos tükrözés), illetve itt is az id-del jelölt, minden pontot fixen hagyó identitás. A már hasznosnak bizonyult csúcsszámozással kiderül, hogy legfeljebb négy egybevágó-



4.1. ábra. Egybevágóságok számozása

ság lehet (ui. az 1 csúcs négy helyre mehet, de ezután a különböző oldalak miatt a 2 már csak egyetlen helyre), tehát készen vagyunk (ezt szemlélteti a 4.2. ábra, melyre később is fogunk hivatkozni).



4.2. ábra. A téglalap egybevágóságaihoz

Az általános téglalapot önmagába vivő egybevágóságok halmazát K jelöli majd.
„Szorgalmi házifeladat": Oldjuk meg az előbbi feladatokat

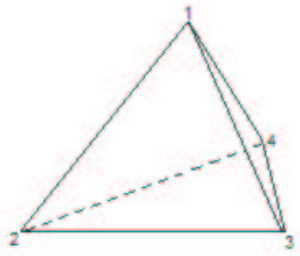
$i)$ *általános rombuszra,* $ii^*)$ *(szabályos) tetraéderre!*

Utóbbi elemszám(á)ra milyen felső becslést adhatunk az eddigiek alapján? Egy kiválasztott csúcs négy helyre mehet, ezután valamelyik további még három helyre, a harmadikra még két lehetőség van, végül a negyedik helye már egyértelmű; tehát legfeljebb $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ egybevágóságról lehet szó (4.3.ábra). $\longrightarrow$ *Állítás*: Ezek mind megvalósulnak (tehát a nehézség most abban rejlik, hogy geometriailag megadjuk az összeset).

25′

3. „Hogyan lehet számolni $\mathrm{D_n}$-ben?"

„Mit tudunk csinálni két egybevágósággal?" $\longrightarrow$ Alkalmazzuk őket egymás után! Ekkor persze ismét valamelyik (D_n-beli) egyvevágóságot kapjuk.



4.3. ábra. A szabályos tetraéder

Tekintsük pl. D_4-et. A 4.4.ábra szerint (162. oldal) vizsgáljuk meg, hogy az óramutató járásával ellentétes irányban történő $90°$-os forgatás egyszeri, kétszeri, háromszori alkalmazása után egy (a síkon) rögzített tengelyre vonatkozó tükrözést alkalmazva melyik egybevágóság adódik, végül pedig azt is, hogy *előbb* a tükrözést majd a forgatást alkalmazva mit kapunk. Az egyszerűség kedvéért jelölje rendre f és t a fenti $90°$-os forgatást és (rögzített) tükrözést, továbbá tf jelentse azt, hogy előbb az f-et, majd a t-t alkalmaztuk $\Big($éppúgy, ahogy a függvények kompozícióját általában is kiolvassuk: $gh(x) = g\big(h(x)\big)\Big)$; ugyanez a jelölés persze több egybevágóság egymásutánjára is működik.

Az ábrán látható számolás mutatja, hogy az összes tükrözés megadható így:

$$t, tf, tff, tfff$$

Azt persze tudjuk, hogy az összes forgatás megkapható az f egymás utáni alkalmazásával: $f, ff, fff, ffff = id$. Fontos „eredmény”, hogy $ft = tfff \neq tf$, azaz nem mindegy az egybevágóságok sorrendje!

Állítás (ezt nem bizonyítjuk, bár a későbbiek alapján be lehet): általában is igaz, hogy a t rögzített tükrözéssel és a középpont körüli $\frac{360°}{n}$ szögű forgatással D_n megadható így:

$$D_n = \left\{ f, ff, \ldots, \underbrace{ff\ldots f}_{n \text{ db „tényező”}} = id, t, tf, \ldots, t\underbrace{ff\ldots f}_{n-1 \text{ db „tényező”}} \right\}$$

Az első n db elem a forgatásokat, a további n pedig a tükrözéseket írja le.

Természetesen pl. D_{2008}-ban könnyű megmondani azt is, mennyi lesz $\underbrace{ff\dots f}_{\text{2010 db „tényező”}}$, hiszen ez azt jelenti, hogy a fenti forgatást 2010-szer hajtottuk végre egymás után, ami ugyanaz, mintha csak kétszer hajtottuk volna végre, mert a 2008-szor való forgatás az identitás lesz.

Hasonlóan $\underbrace{t\dots t}_{\text{„sok”}} = \begin{cases} t & \text{ha „sok” páratlan} \\ id & \text{ha „sok” páros} \end{cases}$.

A fenti, D_4-beli vizsgálódás mintájára felmerül a kérdés: melyik eleme lesz D_n-nek ft? $\longrightarrow$ Tudjuk: ft vagy tükrözés, vagy forgatás.

$i)$ ft forgatás? Ezt kétféleképpen is megcáfoljuk; egyrészt azzal a „frappáns” észrevétellel, hogy ft váltja a körüljárást, ezért biztosan nem forgatás (ez lesz a második megoldás). Másrészt íme egy rövid „számolás” mint „indirekt bizonyítás arra”, hogy ft nem forgatás (ez tehát az első, fő megoldás, amely továbbvisz majd minket):

Tegyük fel, hogy $ft = \underbrace{f\dots f}_{k\text{ db}}$; ebből az egyenlőségből „ki akarjuk fejezni” t-t. Ehhez *írjunk balról mindkét oldal elé* $\underbrace{f\dots f}_{n-1\text{ db}}$-et (azaz geometriailag: alkalmazzuk mindkét egybevágóság után az $(n-1)\frac{360^\circ}{n}$ szögű elforgatást), ekkor ezt kapjuk:

$$\underbrace{f\dots f}_{n\text{ db}}t = id\,t = \underbrace{f\dots f}_{n-1\text{ db}}\underbrace{f\dots f}_{k\text{ db}} = \underbrace{f\dots f}_{n-1+k\text{ db}}$$

Itt a bal oldalon megjelent $id\,t = t$, a jobb oldalon pedig egy forgatás; eszerint t is egy forgatás lenne, ami ellentmondás.

$ii)$ ft tehát egy tükrözés, az a kérdés, hogy D_n fenti megadásába vajon melyik. Most egy, az előbbihez hasonló „bűvészkedés” következik abból kiindulva, hogy a tükrözések tulajdonságai miatt $ftft = id$:

$$ftft = id \quad /\text{„}\cdot t\text{"}$$
$$ftf\underbrace{tt}_{id} = ftf = id\,t = t \quad /\text{„}\cdot \underbrace{f\dots f}_{n-1\text{ db}}\text{”}$$

$$ft = t\underbrace{f \dots f}_{n-1 \text{ db}}$$

Tehát azt kaptuk, hogy az ft ismeretlen tükrözés a $t\overbrace{f \dots f}^{n-1 \text{ db}}$-nel egyezik meg; ez egybevág a D_4-re kapott $ft = tfff$ eredménnyel.

Emeljük ki (még egyszer), hogy eszerint $ft \neq tf$!

Alkalmazzuk az előbbieket pl. annak megválaszolására, hogy melyik eleme lesz D_4-nek az $ftfffttfffttt$? Először is $tt = id$ miatt ez $ftfffffft$ alakban írható, amelyben a korábbiak szerint $ft = tfff$, tehát további alakítással $t\underbrace{fffff}_{id}\underbrace{fffff}_{id}t =$ $= tt = id$.

Láthatjuk, hogy most már hosszadalmas „rajzolás” nélkül meg tudjuk mondani tetszőleges „kifejezésről”, hogy az melyik elemmel egyezik meg.

Az eddig elmondottak is sugallják, hogy talán egyszerűbb módon is lehetne jelölni D_n elemeit.

Hívjuk ezentúl az egybevágóságok egymás utáni végrehajtását *szorzásnak* (amelyet $\cdot$ jelét a „hagyományos” szorzásnál megszokott módon általában el is hagyjuk majd), ennek szellemében jelölje $\underbrace{f \dots f}_{k \text{ db}}$-et f^k, ugyanígy $\underbrace{t \dots t}_{\ell \text{ db}}$-t t^ℓ és ezek legyenek a megfelelő elemek k-adik és ℓ-edik *hatványai*. Ezzel az új jelöléssel a korábbi számolási szabályaink D_n-ben ezt az alakot öltik: $f^n = id$, $t^2 = id$ és $ft = tf^{n-1}$. Emellett pl. $f^{2n+3} = f^3 \cdot f^{2n} = f^3$ és $t^{2009} = t$.

A hatványok nyelvén tehát kényelmesen megfogalmazhatóak a már megismert tulajdonságok és ugyanúgy megadhatjuk D_n elemeit, ahogy azt már feljebb (hosszas f, t-sorozatokkal) megtettük.

Figyeljük meg, hogy időközben tulajdonképpen „feleslegessé”/*nélkülözhetővé vált az f és a t betűk konkrét, geometriai jelentése*. Minden további nélkül megtehetjük ugyanis, hogy pusztán a rendelkezésre álló számolási szabályokkal alakítgatunk f-ekből és t-kből álló kifejezést, ahogyan azt a fenti példában is tettük.

Ezek után (már az „új” jelöléssel felírt) az $f^n = f \cdot f^{n-1} = f^{n-1} \cdot f = id$ egyenlőségekre hivatkozva az f^{n-1}-t nevezzük el f^{-1}-nek (f „reciproka”), azaz f *inverzének*, ehhez hasonlóan $t^2 = id$ miatt $t^{-1} := t$.
D_n minden elemének van inverze, mégpedig a tükrözéseknek a korábbiak szerint saját maguk: $tf^k tf^k = id$, az f^k forgatásnak pedig $(f^{-1})^k$ („a másik irányban csináljuk az elforgatást”). Fennáll a következő: $ft = tf^{-1}$.

Nézzük meg, mi következik abból, hogy az elemeknek van inverze. Tegyük fel pl., hogy valamely $x, y \in D_{2008}$ elemekre $f \cdot x = f \cdot y$ (f a szokásos forgatás). Ezt az egyenlőséget a már látott bűvészkedés mintájára átalakítjuk úgy, hogy balról szorozzuk (most már jogos ez a megfogalmazás) f^{-1}-zel:

$$fx = fy \Rightarrow (f^{-1}f)x = (f^{-1}f)y \Rightarrow id \cdot x = id \cdot y \Rightarrow x = y$$

Azt kaptuk tehát, hogy $x = y$: a „szokásos” egyenletrendezés következtetése itt is működik. Persze ugyanígy járhattunk volna el, ha f helyett tetszőleges másik elemet veszünk, hiszen annak is van inverze. (A *balról* szorzás viszont fontos, mert tudjuk, hogy pl. $ft \neq tf$!)

Vizsgáljuk meg azonban az előbbi átalakítást részletesebben! Amikor a kiindulási sort megszorozzuk (balról) f^{-1}-zel, akkor először csak ennyit mondhatunk:

$$f^{-1}(fx) = f^{-1}(fy)$$

Ezt a lépést az előbb átugrottuk, méghozzá a szorzatokat *átzárójeleztük* a következő módon:

$$f^{-1}(fx) = (f^{-1}f)x$$

(Ugyanígy a másik oldalt.) Itt tehát tulajdonképpen kihasználtunk egy, a szokásos szorzásnál megszokott műveleti tulajdonságot, amely azt garantálja, hogy egy szorzatot bárhogyan lehet zárójelezni, mindig ugyanazt az értéket kapjuk; ezt *asszociativitásnak* hívjuk. Felmerül most a kérdés, hogy a szóban forgó geometriai transzformációk szorzása, azaz egymás után végrehajtása, asszociatív-e?

Állítás (végiggondolása HF): a szokásos függvénykompozíció (amiről itt is szó van) asszociatív.
Figyeljük meg, hogy ezt a tulajdonságot a korábbi példáinkban is használtuk, ahol pl. id-eket „különítettünk el” egy sokténye zős szorzaton belül! Szerencsére, mint az állítás mutatja, nem csaltunk ezzel.

Foglaljuk össze az eddig elmondottakat. D_n-ben van egy szorzásnak (el)nevezett művelet (ennek semmi köze a szokásos szorzáshoz), amely a következő tulajdonságokkal rendelkezik:

i) asszociatív,

ii) létezik az id nevű elem, amellyel bármelyik elemet akármelyik irányból szorozva önmagát kapjuk,

iii) minden elemnek van inverze („reciproka”), amellyel akármelyik irányból megszorozva id-et kapjuk.

Ehhez hasonló jelenséggel találkoztunk már korábban? Igen: ilyen a „szokásos” szorzás, azaz a racionális, vagy bővebben valós számok szorzása.(?→ `Szándékos pontatlanság!`) Ez ugyanis asszociatív, az 1-gyel bárkit bármelyik irányból szorozva önmagát kapjuk, és minden *nemnulla* elemnek van inverze, azaz reciproka⟶ a „nemnullaságot” tehát ki kell kötnünk (erre utalt az előbbi kérdőjel).
Van azonban egy lényeges különbség: a valós számok szorzása *kommutatív*, azaz $\forall a, b \in \mathbb{R}\ a \cdot b = b \cdot a$, míg pl. D_n-ben $ft \neq tf$. Eszerint mégsem egészen olyan az újonnan megismert művelet, mint a „régi”, de több közös tulajdonsága is van.

`60'`

4. Írjuk le a(z általános) téglalappal kapcsolatos K halmazt a D_n-nél bemutatott módon!

A 4.2. ábra (150. oldal) szerint rögzítsünk most is egy t tengelyes tükrözést és legyen f a téglalap középpontja körüli $180°$-os forgatás. A műveletet rutinosan jelöljük szorzásként (melynek jelét esetleg ki sem írjuk).
Ekkor „betűzve" K a következőképpen adható meg: $K = \{id, t, f, tf\}$; ezt ellenőrizhetjük újra a számozásos nyomonkövetéssel, de elég annyi, hogy itt négy különböző elem áll, azaz K minden eleme szerepel. Utóbbihoz csak annyi kell, hogy tf a három további elem közül semelyikkel nem egyezik meg; ez gyorsan igazolható a (már) szokásos(nak mondható) „bűvészkedéssel": pl. $tf = t \Rightarrow f = id$, ellentmondás ($tf \neq f$ most is közvetlenül látszik a körüljárás vizsgálatával). Látjuk tehát, hogy tf a másik tükrözés; fennáll, hogy $t^2 = f^2 = (tf)^2 = id$. Kérdés persze „most is", hogy mi lesz ft? Az ismert (előbbi) módon id, t és f azonnal kizárható, így $ft = tf$ adódik (amelyet a rajzon ellenőrizhetünk is).

A K-beli szorzásra minden tulajdonság teljesül, amelyet D_n-nél felsoroltunk: a művelet (mint kompozíció) asszociatív, létezik a minden elemet szorzásnál fixen hagyó id is és persze minden elemnek van inverze, mellyel bármely irányból szorozva id adódik, nevezetesen *minden elem saját maga inverze*. Ráadásul a K-beli szorzás *kommutatív* is, amint ezt a fenti $tf = ft$ mutatja.

5. „Asszociativitás nélkül nincs élet..."

Az asszociativitás „elsődlegességét" illusztrálandó, most vizsgáljunk meg egy példát. Értelmezzünk a pozitív egész számokon egy $\circ$-rel jelölt műveletet a következőképpen:

$$a \circ b \stackrel{\text{def}}{=} a^b \quad \text{(utóbbi a szokásos hatványozás)} \quad .$$

Például $2 \circ 5 = 2^5 = 32$ és $5 \circ 2 = 5^2 = 25$; világos, hogy $\circ$ nem kommutatív.

Azt az egyszerű kérdést tesszük most fel, hogy mennyi lesz „3^3”, azaz a $\circ$ művelet szerinti harmadik hatványa a 3-nak: „3^3” $= 3 \circ 3 \circ 3$?
(A továbbiakban is, a félreértések elkerülése végett, idézőjelben lesz majd az új fajta hatvány.)
Ezt könnyen kiszámolhatjuk: az értéke éppen $3 \circ (3 \circ 3) = 3 \circ 27 = 3^{27}$. De máshogy is „kiértékelhettük” volna a szorzatot, nevezetesen $(3 \circ 3) \circ 3 = (3^3) \circ$ $\circ\, 3 = (3^3)^3 = 3^9$, ez más eredményt ad!! *Az előbbi kérdés (ebben a formában) értelmetlen!*

A $\circ$ szorzás tehát nem asszociatív és látjuk, hogy már a hatványozás értelmezésénél is problémák vannak. Pontosabban a hatványozást még értelmezhetjük egy megadott zárójelezéssel, mondjuk mindig jobbról balra haladva: „a^k” $=$ $= \underbrace{a \circ a \circ \ldots \circ a \circ a}_{\text{k db tényező}} = a \circ \Big(a \circ \ldots \Big(a \circ \big(a \circ (a \circ a)\big)\Big) \ldots \Big)$; ekkor nem lehet értelmezésbeli „vita” egy hatvánnyal kapcsolatban, de nem marad érvényben a megszokott „$a^{k+\ell}$” $=$ „a^k” $\circ$ „a^ℓ” azonosság (amelyet egyébként számtalanszor kihasználunk), hiszen az előbbinek (iménti) értelmezése alapján egyáltalán nincs feltétlenül köze az utóbbi kettő szorzatához.

A fenti észrevételek, összevetve D_n példájával, arra utalnak, hogy az asszociativitás bizonyos értelemben lényegesebb tulajdonsága a műveletnek, mint a kommutativitás, ellentétben azzal, amit talán első látásra gondolnánk. Az utóbbi nélkül még egészen jól lehet boldogulni (ld. D_n), az előbbi híján azonban alapvető műveleti azonosságokról kell lemondanunk. Mint már említettük, a D_n vizsgálata során látott „bűvészkedések” alapja is minden esetben az volt, hogy egy soktényezős szorzatot bárhogy lehetett zárójelezni, mindig ugyanaz maradt az értéke.

80′

6. $\mathbb{Z}_n$ vizsgálata

Jelöljük $\mathbb{Z}_4$-gyel a $\{0,1,2,3\}$ halmazt, amelyen legyen az *összeadás* a 4-es maradékok szokásos összeadása (azaz a modulo4 összeadás): pl. $2+2=1+3=$ $=0$, $3+3=2$ stb.
Vizsgáljuk most ezt az összadást a korábbi „szempontjaink" alapján. Világos, hogy asszociatív. Van egy olyan kitüntetett elem, amelyet bárkihez hozzáadva (bármelyik irányból) önmagát kapjuk: ez a 0. Emellett minden x elemnek van egy párja, amelyiket hozzáadva (bármelyik irányból) a 0-t kapjuk; ezt $-x$-szel jelöljük és az x *ellentett*jének nevezzük. Mindezeken felül a $\mathbb{Z}_4$-beli összeadás *kommutatív* is.
Azt láthatjuk, hogy az itteni összadásra (összeadásnak nevezett műveletre) jellemző műveleti tulajdonságok alakilag teljesen egyeznek a korábban vizsgált szorzásokra (szorzásoknak nevezett műveletekre) jellemzőekkel.
Egyszerű észrevételként $\mathbb{Z}_4$-et írjuk fel így:

$$\mathbb{Z}_4 = \{1, 1+1, 1+1+1, 1+1+1+1=0\}$$

Hasonlóval már találkoztunk, nevezetesen D_4-ben az $\{f, ff, fff, ffff = id\}$ forgatások éppen így viselkedtek!

Ezen a ponton jegyezzük is meg, hogy ha D_4-ben, általában D_n-ben csak a forgatásokat tekintjük, akkor ezek a forgatások a D_n-beli szorzással önmagukban is eleget tesznek a fentebb vizsgált műveleti tulajdonságoknak sőt, itt a művelet még kommutatív is.

Visszatérve a már megkezdett gondolatra, ha az F_4-gyel jelölt D_4-beli forgatások és $\mathbb{Z}_4$ között az 4.1 táblázat szerinti megfeleltetéseket hajtjuk végre, akkor az egyikben végrehajtott művelet „átmásolódik" a másikra; a két halmaz (a műveletek szemszögéből) csak a jelölés tekintetében különbözik.

A fenti állítást általánosan is megfogalmazhatjuk az „n-nel való osztási ma-

$\mathbb{Z}_4$	F_4
$+$	$\cdot$
1	f
$\underbrace{1+\ldots+1}_{k\text{ db}}$	$\underbrace{f\cdot\ldots\cdot f}_{k\text{ db}}$

4.1. táblázat. Megfeleltetések $\mathbb{Z}_4$ és F_4 között

radékok, összeadás" $\mathbb{Z}_n$ halmaza és a D_n-beli forgatások F_n halmaza között. Azt mondhatjuk tehát, hogy ezek „tulajdonképpen ugyanazok", mert (pl.) a fenti kölcsönösen egyértelmű megfeleltetést végrehajtva bármelyik halmazban dolgozhatunk az ottani művelettel, a végén egyszerűen kicserélve a műveleti jeleket és a megfeleltetett elemeket megkapjuk az eredményt a másik halmazban.

Eddig megismertünk három db négyelemű, kommutatív művelettel ellátott halmazt: F_4-et, $\mathbb{Z}_4$-et és K-t; ezek közül az első kettőről kiderült, hogy „tulajdoképpen ugyanazok". Természetesen vetődik fel a kérdés, hogy vajon a téglalap egybevágóságainak halmaza is tkp. ugyanaz-e, mint két társa? Tegyük fel, hogy találunk egy „jó megfeleltetést" pl. $\mathbb{Z}_4$ és K között. Ekkor - lévén a művelet átmásolódik - az 1 képének hatványai előállítják K-t, hiszen az 1 „hatványai" (azaz az $1, 1+1, \ldots$ elemek) előállítják $\mathbb{Z}_4$-et. Korábban már észrevettük azonban, hogy K-ban minden elem négyzete id, eszerint nincsen olyan eleme, melynek négy különböző hatványa lenne és így ezek a hatványok K minden elemét előállítanák (hiszen, ugyanúgy mint $D_n \ni t$-nél, a kitevő paritása szerint az x elem hatványai x-szel vagy id-del egyeznek meg). Ez a meggondolás mutatja, hogy K és a másik két halmaz „*lényegesen különböznek*", bár mindnyájan négyeleműek.

100'

7. A csoport fogalma

Elérkeztünk oda, hogy definálju k a foglalkozás fő fogalmát:

Definíció: A $G \neq \emptyset$ halmazt *csoport*nak nevezzük, ha értelmezve van rajta egy (pl.) $\cdot$-tal jelölt(kétváltozós) művelet, amely eleget tesz a következő tulajdonságoknak:

- *asszociatív*: egy sokténye zős szorzat bárhogyan zárójelezhető

- *létezik* egy 1-gyel jelölt kitüntetett elem, mellyel való bármelyik irányú szorzás minden elemet fixen hagy,

- *minden $g \in G$ elemnek* létezik egy párja, melyet a *g inverzének* hívunk és g^{-1}-zel jelölünk: ezzel teljesül, hogy $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Az előbbi tulajdonságokat *csoportaxiómák*nak hívják. Sok példát láttunk eddig csoportra, ilyen volt D_n (melynek neve: n-edfokú diédercsoport) és benne F_n a (szorzásnak hívott) kompozíció műveletével, $\mathbb{Z}_n$ a mod n összeadás műveletével, a nemnulla valós számok a (szokásos) szorzásra. Ezenkívül csoportot alkot pl. az összes valós szám a (szokásos) összeadásra nézve; ennek a csoportnak az „1” egységeleme a 0 lesz és egy elem inverze egyszerűen az ellentettje. Ugyanilyen jó példa a racionális számok és az egész számok az összadásra. A nemnulla racionális számok a szorzásra is jók (a valósakhoz hasonlóan), de például a nemnulla egészek már nem, hiszen csak a ± 1-nek van inverze (azaz reciproka).
Látjuk: vannak véges (elemszámú) és végtelen csoportok és D_n példáját is figyelembe véve kommutatív és nemkommutatív csoportok.

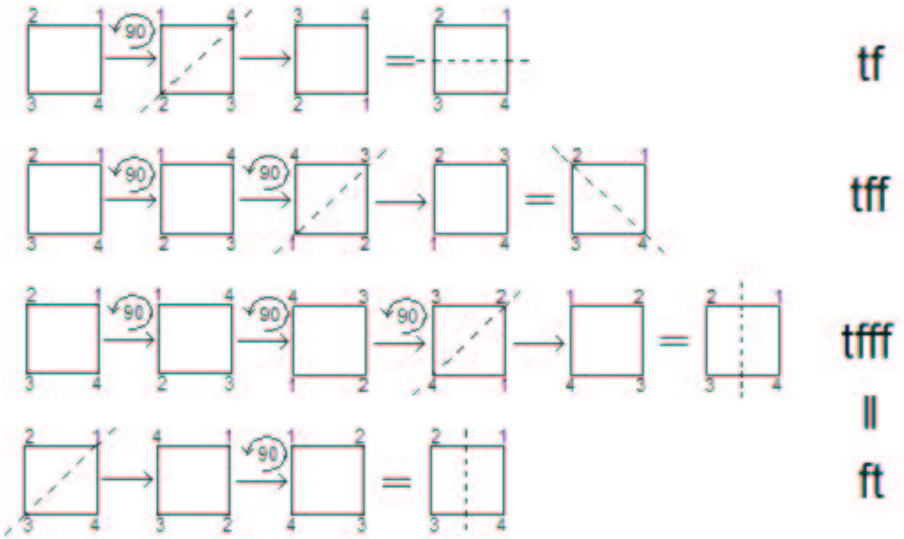
Tegyünk fel kérdéseket (véges) csoportokkal kapcsolatban!
Kérdezhetjük például hogy, hogy tetszőleges elemszámú véges csoport létezik-e. Erre tulajdonképpen már megadtuk a választ: $\mathbb{Z}_n$ tetszőleges n-re egy n elemű csoport, azaz a válasz igenlő.

Ezután természetesen adódik a következő kérdés: hány n elemű csoport van

adott n-re? Ebben a formában erre is könnyű válaszolni: minden n-re végtelen sok csoport van. Ugyanis a síkon felvehetünk úgy végtelen sok szabályos n-szöget, hogy mindnek a középpontja más-más pontban legyen; ekkor nyilván végtelen sok „D_n-szerű” csoportot kapunk, a forgatások ui., lévén különböznek a középpontok, biztosan különbözni fognak. Csak a forgatásokat tekintve tehát végtelen sok n elemű csoportot nyerünk (a „teljes csoportokból” pedig végtelen sok $2n$ eleműt). Persze érezzük, hogy ez az ellenpélda kissé „ügyetlen”, hiszen látjuk, hogy ez a végtelen sok csoport valójában mind „tulajdonképpen egyforma” (a fenti „tulajdonképpen ugyanaz” fogalmának megfelelően), és így csak egyféle n elemű csoportot állítottunk elő. Világos, hogy a kérdést kéne ügyesebben megfogalmazni, az előbbiek sugallatára valahogy így:

Hány n elemű csoport van, ha nem tekintjük azokat különbözőknek, amelyek „tulajdonképpen ugyanazok”?

Ezzel a módosított kérdéssel már egy valódi, nehéz csoportelméleti feladványhoz érkeztünk. Például belátható, hogy négyelemű csoport csak kétféle van, amelyeket megismertünk: a K ún. Klein-csoport és $\mathbb{Z}_4$; emeljük ki újra, hogy ezekről meggondoltuk, hogy tényleg lényegesen különböznek.
A 4.2. táblázat (162. oldal) néhány n-re ismerteti a választ. A táblázat alapján prím elemszámú csoportból csak egyféle van (ez persze a $\mathbb{Z}_p$ típusú kell hogy legyen) és nemcsak $n = 4 = 2^2$-re, hanem minden $n = p^2$-re igaz, hogy kétféle n elemű csoport van. Az is kiderül viszont, hogy pl. $n = 35$ elemű csoportból is egyféle van ($\mathbb{Z}_{35}$). Ez azt jelenti, hogy egy 35 elemű halmazon lényegében csak *egyféleképpen* lehet úgy műveletet értelmezni, hogy a szokásos műveleti azonosságok teljesüljenek, ugyanez minden prím elemszámú halmazra is igaz.
Korántsem ismerjük azonban minden n-re a választ; pl. $n = p^9$-ra általánosan nem tudjuk megmondani az n elemű („lényegesen különböző”) csoportok szá-



4.4. ábra. Számolás D_n-ben

n	Hányféle n elemű csoport van?
p (prím)	1
p^2	4
p^3	5
$2p$ $(p > 2)$	2
pq ($p < q$ prím)	1 v. 2 (pontosan ismert, hogy melyik áll fenn)
35	1
60	13

4.2. táblázat. Az n elemű csoportok száma

mát. Jegyezzük meg, hogy az a célkitűzés, hogy valamilyen n-re megtaláljuk az összes n elemű csoportot, két dolgot foglal magában: találnunk kell „minél többet”, végül megmutatni, hogy bármely ilyen csoport valójában „tkp. ugyanaz”, mint a már megtaláltak valamelyike.

A csoportelmélet azonban nem csak ezzel a kérdéssel foglalkozik. Például egy több mint 100 éven át húzódó „projektben” meg akarták adni az összes, bizonyos jól meghatározott tulajdonsággal (melyet most itt nem tudunk részletezni) rendelkező véges csoportot (melyek általában nem azonos elemszámúak). A sok-sok matematikus munkája révén végül eredményesen végződő vállalkozás dokumentációja - mely alatt számos cikket, közöttük esetleg több száz oldalasakat is, kell érteni - 10000 oldalnál is hosszabb (!).

A csoportelmélet önmagában rejlő érdekessége mellett más tudományágakban is szerephez jut; itt említhetjük a geometriát, az elméleti fizikát, ezen belül pl. a magfizikát (mondjuk a *kvarkok* csoportelméleti megfontolások alapján történő felfedezését).

120′

4.2. Kivitelezés - reflexió

A szakköri foglalkozás a fenti napon 15:15-tól 17:30-ig tartott. A 15 perces „hosszabbítás” mellett megjegyzendő még két „terhelő” körülmény: a tanulóknak aznap eleve hét „reguláris” órájuk volt, ráadásul a szakkört szünet nélkül tartottuk (külső okokból). Utólag persze világossá vált, hogy ez a rendkívül hosszú időtartam előadónak, befogadónak egyaránt megterhelő, különösen ebben a kései órában. Eredetileg még több anyagot terveztem, ugyanis még be akartam bizonyítani a *rend* fogalmának bevezetése után azt, hogy prím elemszámú csoportból csak egyféle van. Azonban - amint ez be is igazolódott - a szakkör tervének végső

letisztázása során az időbeosztást is vázolva nyilvánvalóvá vált, hogy ez hiú ábránd.

Mindamellett a foglalkozás - nyugodtan mondhatom - a tervezett, „irányítottan interaktív", felszabadult légkörben telt. A tanulók aktívan követték a táblára is nagyrészt felkerülő eseményeket és jegyzeteltek is; mint utólag egyikük megjegyezte, 11 oldalt írt (magához képest példátlan módon) - az én kézzel írott vázlatom 8 oldalas volt. Igyekeztem megtalálni az egyensúlyt abban, hogy a nagyon beszédesen kérdő tekintetekre reagáljak, egyébként azonban hagyjam működni, illetve hozzam működésbe az intuíciót.

Érdemes kiemelni néhány konkrét mozzanatot. A „mi lesz D_n-ben ft?" kérdésnél az egyik diák rögtön jelezte, hogy biztosan nem forgatás, hiszen váltja a körüljárást, így - használva a szép észrevételt - célszerű rövidítésként a „számolós" bizonyítást kihagytam, miután néhány másodpercig morfondíroztam, vajon nem kéne-e mégis elmondani az érvelést, az „inverzzel való szorzást" illusztrálandó. Végül úgy döntöttem, ennyi lendületre szükség van, különösen a még hátralévő anyag mennyiségének figyelembevétele mellett. Az inverzzel szorzás úgyis előkerült a következő lépésben, ahol megtudtuk, melyik tükrözés ft. Itt érdekes módon arra nem kérdeztek rá, hogy miért szabad a „betűsorozatból" néhányat elkülöníteni, és az asszociativitás (szándékosan későbbre csúsztatott) problémája egészen a tervezett pillanatig nem merült fel. Persze meglepő jelenség volt a jobbról és balról való szorzás „irányfüggése", fel is merült ezzel kapcsolatos kérdés az „egyenletrendezés" első lépésében. Utólag (már a szakkör után) rájöttem, hogy érdemes lett volna a (megfelelő elemmel) balról való szorzással kezdődő átalakítást is megnézni.

A szemfüles tanulóknak köszönhetően az is kiderült, hogy a D_4-beli tetszőleges szorzat kiszámítását illusztráló kifejezésem ($ftfffttfffttt$) nem a legügyesebbre sikerült, ugyanis ezt a fentiekben leírtaktól (amelyre ki akartam hegyezni

a dolgot) eltérő módon is ki lehet számítani, nevezetesen meg lehet „spórolni” az $ft = t\underbrace{f\dots f}_{n\,\text{db}}$ felhasználását: $ftff(tt)ffftttt = ftf(ffff)t = ftft = id$, ehhez csak annyi kell, hogy ft egy tükrözés, amelyet kétszer alkalmazva az identitást kapjuk.

Később, az $fx = fy \Rightarrow x = y$ átalakításnál, amikor már felvetettem, hogy itt tulajdonképpen azt használjuk, hogy egy szorzatot át lehet zárójelezni, és ennek a nevét is megmondták, felvetette az egyik fiú, hogy „miért lenne a D_n-beli szorzás asszociatív, amikor nem is kommutatív?”.

A racionális/valós számok „nemnullaságával” való csalás is gyorsan lelepleződött; ebben a kontextusban ez most nem annyira nyilvánvaló észrevétel, mint pl. esetleg egy egyenletmegoldás kapcsán. Talán itt érdemes megjegyezni azt is, hogy amikor már a csoport fogalmának definíciója után felidéztük az említett példákat, egy tanuló felvetette a komplex számokat is (amelyeket fakultáción tanultak), az összeadásra nézve.

A nem asszociatív szorzás példája egy-két nem várt problémát okozott, ennek megfelelően több időt is vett igénybe a tervezettnél. Egyrészt, mint a példa végére kiderült, kezdetben azt gondolták, hogy a már megkezdett utat követjük majd, nem volt tehát egészen világos, hogy D_n és a műveleti azonosságok után hirtelen miért nézzük ezt a mesterkélt műveletet. Megjegyzendő, hogy az eredeti tervemben a fenti 4. és 5. rész megcserélve szerepelt, csak a szakkörön alakult így a sorrend, mivel ott azt éreztem, hasznosabb, ha előbb illusztrálom, mennyire fontos az asszociativitás és ezután, viszonylag gyorsan „túlesünk” a Klein-csoport leírásán. Nem biztos, hogy ez a csere okozta a nehézséget; valamennyire mindenképpen az előzményektől eltérő „mélyvíznek” szántam ezt a részt, amely az említett szemponton kívül tényleg csak beékelődött az anyagba, de kézzelfoghatóan akartam érzékeltetni a műveleti azonosság szerepét, nem csak egy félmondatban megjegyezni. Problémák voltak még a jelöléssel is, ui. a táblán első lejegyzés al-

kalmával nem szerepeltek a (fentebb is látható) leírást megkönnyítő idézőjelek, és először a régi és új művelet összekavarodása többeket megzavart. Ezt a tervezés hiányosságának tekintem; különösen egy ilyen eléggé elvont jelenség esetén, amikor egy ismert műveletből kiindulva értelmezek egy újat, amely „szerint vett hatványozásról" beszélek, gondosabban kitalálhattam volna a jelölést.
Szerencsére a tartalmi egység végére úgy tűnt, hogy megértették a példa célját; ebben - minden idétlensége ellenére - a fenti tervezetben címként szereplő, táblára is felkerülő mondatnak is lehetett szerepe.

Sikeresnek bizonyult az $1{,}1+1,\ldots$ felíráson alapuló (fenti jelöléssel) F_n és $\mathbb{Z}_n$ közötti hasonlóság felfedeztetése, ugyanis az egyik tanuló rögtön leleplezte, hogy a forgatásoknál láttunk már ilyet. Meggyőzőnek tűnt az is, ahogyan a máshogyan jelölt műveletek azonos logikájú műveleti tulajdonságaiban megfeleltették egymásnak az egyes elemeket (id-nek a 0-t, inverznek az ellentettet). Persze az izomorfizmus/izomorfia fogalmának (csoport definíciója utáni) pontos értelmezése nagyon messzire vezetett volna, így meg kellett elégednem azzal a kétes sikerrel, amelyet a K és $\mathbb{Z}_4$ különbözőségéről szóló heurisztikus érvelés okozott. Talán ez volt a foglalkozás legnehezebb része.

A csoport fogalmának definiálása, melyet egyébként is csak kb. a 100-adik percre terveztem, végül az időközben felhalmozódott (időbeli) csúszásokkal együtt tényleg szinte a finálé lett a hosszú foglalkozásnak. Több tanuló mondta utólag, hogy bár sokáig nem teljesen volt világos, merre haladunk, a végén megértették.
Sajnos, amint nagyjából előre is lehetett sejteni, érzésem kissé „távolinak" tűntek a csoportokról feltett kérdéseim („minden n-re van-e n elemű csoport?", stb.); ennek persze egyrészt bizonyára a tanulók fáradása volt az oka, másrészt talán a feldolgozás módja csak részben előlegezte ezt meg. Emiatt is került bele a Klein-csoport az anyagba, hiszen így legalább egy példán érzékeltetni lehetett azt, hogy adott elemszámú csoportból több „lényegesen különböző" is lehet. Az adott elem-

számú csoportok számáról szóló táblázat kapcsán megjegyeztem, hogy eredetileg az $n = p$ esetet szerettem volna igazolni, a szakkör (hivatalos) végeztével az egyik fiú erre érdeklődően megkérdezte, hogy ahhoz még mennyi idő kellett volna. Eredetileg terveztem itt egyfajta kombinatorikus meggondoláson alapuló érzékeltetést is, nevezetesen azt számoltuk volna ki, hányféleképpen lehet egy $n \times n$-es „műveleti táblát" kitölteni, ha először semmit nem szabunk meg, majd a „kommutativitást" kikötjük; ezeket az eredményeket persze azzal vetettük volna össze, hogy - tudván, hogy ténylegesen hány csoport van adott n-re - hány kitöltés lehetséges a csoportaxiómák figyelmbevételével. Erre végül is az idő szorítása miatt nem került sor, de utólag így jobbnak is látom, hiszen a számolás (csoportaxiómás része) valójában túl bonyolult lett volna.
Felmerült azonban a kérdés, hogy milyen „ismert csoportok" vannak még, amire a permutációkat mint függvényeket említettem anélkül, hogy a részletekbe mentem volna; ez így a jelek szerint elsőre nem volt teljesen érthető (ami bizonyos értelemben megerősíti azt a korábbi észrevételemet, amely miatt a permutációk helyett inkább a diédercsoportra alapoztam a feldolgozást).

Említést érdemel még, hogy a szakkör végeztével négy tanuló még mintegy fél órán át „faggatott" matematikával és nagyrészt csoportokkal kapcsolatos kérdésekről; ez némileg megnyugtat afelől, hogy az estébe hajló, fárasztó algebrázás talán érdekes volt pár ember számára.

♠

Pár szóban összefoglalom még a szakkörön jelenlévő, fent nevezett felnőttek véleményét is, az egyszerűség kedvéért a monogramjukkal jelölve őket.

KG a szakkört (a tanulókat is figyelve) érdekesnek, a téma felépítését jónak találta, kiemelve azt, hogy jó ötlet volt nem az absztrakt definícióval kezdeni, hanem „kézzelfogható" példákon és meggondolásokon keresztül eljutni a csoport fogalmához.

Ezt hangsúlyozta *VS* is, aki (hozzám hasonlóan) úgy gondolja, hogy valamiféle „érzet”/kép nagyon fontos a csoporthoz hasonló absztrakt fogalmakkal kapcsolatban. Szerinte a szakkör hozzásegítette a tanulókat ennek kialakulásához.

VI (aki egyébként több foglalkozást is tartott ebben az osztályban) szintén elismerően nyilatkozott a szakkörről, hozzátéve, hogy talán a „nem asszociatív művelet”-es rész nem jött a legjobbkor - ezzel teljesen egyetértek (amint ezt fentebb részletesebben kifejtettem).

KG a foglalkozás távlataival kapcsolatban is érdeklődött, illetve javaslatokat tett. Elmondta pl. azt, amelyet az általános észrevételek között én is említettem, hogy a „mire lehet ezt használni?” kérdésre nem derült ki igazából a válasz a foglalkozáson (ezt az egyik jelenlévő tanulóval folytatott utólagos beszélgetésem is megerősítette), érdeklődött arról, hogy milyen alkalmazásokat gondolok „elmondhatónak” és megjegyezte, hogy az időtartammal kapcsolatos tapasztalatokat figyelembe véve alapján egy ilyen kibővített anyag akár 2-3 szakkörre is elegendő lehet. Ő a diédercsoport megismerése után a permutációk tárgyalásával folytatná, ezután esetleg a részcsoportok és az izomorfia fogalmának tisztázásával. Ezzel én is egyetértek (főleg a permutációkra vonatkozó ötlettel).

Az alkalmazásokról: figyelembe véve a tanulók kiemelkedő érdeklődését és tudását, elképzelhetőnek tartom pl. azt, hogy az (önmagában is szép és érdekes) *Euler-Fermat tétel* megismertetése után meg lehetne mutatni ennek csoportelméleti általánosításaként a *Lagrange-tételt*, amelyet aztán esetleg alkalmazni lehetne valamilyen játékkal (pl. a *Rubik-kocka*) kapcsolatos kérdés megválaszolására. Kellő előkészítéssel talán a Cauchy-tétel McKay-féle bizonyítása (2.6.2.) is elmondható, amely egyszerűségében nagyon mutatós, a „felsőbb matematikán” belül egy elemi(bb) trükk alkalmazásának szellemes példája. Tudomásom van az előbbiek mellett olyan *kártyatrükkről* is, amelynek működésének van csoportelméleti aspektusa.

Végül még egyszer szeretném megköszönni a 12.A osztály jelenlévő tanulóinak és az említett látogatóknak az aktív részvételt és az építő észrevételeket.

Irodalomjegyzék

[1] Derek J.S. Robinson: A course in the theory of groups, *Springer-Verlag, Graduate Texts in Mathematics* **80**

[2] Fuchs László: Algebra, *egyetemi jegyzet*

[3] Kiss Emil: Bevezetés az algebrába, *TypoTeX 2007*

[4] J. Brodkey: A note on finite groups with an abelian Sylow group, *Proc. Amer. Math. Soc.* **14** (1963), 132-133.

[5] V.D. Mazurov, V.I. Zenkov: Intersections of Sylow subgroups in finite groups, *London Mat. Soc. Lecture Note Series **249**: The Atlas of finite simple groups - Ten years on, 194-195.o.*

[6] James H. McKay: Another proof of Cauchy's group theorem. *American Mathematical Monthly* **66** (1959), p.119

[7] http://en.wikipedia.org/wiki/Commutator_subgroup

[8] http://www.ams.org/mathscinet