Eötvös Loránd Tudományegyetem
Természettudományi Kar

Csoportkonstrukciók és kis elemszámú csoportok

Szakdolgozat

Czira Eszter
Matematika BSc
Matematikai elemző szakirány

Témavezető:
Ágoston István
Egyetemi docens
Algebra és Számelmélet Tanszék

Budapest
2017

Köszönetnyilvánítás

Ez úton szeretném megköszönni témavezetőmnek, Ágoston Istvánnak a sok-sok segítséget, támogatást és türelmet, melyekkel hozzájárult a szakdolgozatom elkészítéséhez.

Tartalomjegyzék

1. fejezet

Bevezetés

Szakdolgozatom címe, a "Csoportkonstrukciók és kis elemszámú csoportok" elég árulkodó. Nem másról szól, mint hogy a különböző elemszámú csoportokból hány darab van izomorfia erejéig, melyek ezek, hogyan épülnek fel és hogy milyen elemeik vannak. A dolgozat legnehezebb része abban áll, hogy hogyan látjuk be azt, hogy azokon a csoportokon kívül, amiket megmutattunk nincsen másik.

A következőkben sorra vesszük a csoportokat, hol egyszerűbb, hol bonyolultabb módon bizonyítva az állításunkat. A kapott csoportokat táblázatban is szemléltetjük a könnyebb átláthatóság végett.

A dolgozat felépítésére az egyik legkézenfekvőbb módszer talán az lenne, ha növekvő sorrendben végigmennénk a különböző elemrendű csoportokon, szépen egyről a kettőre belátva őket.

Én azonban mégsem ezt az utat választom.

Mégpedig azért nem, mert ahogy dolgoztam észrevettem, hogy sok hasonlóság bújik meg a hasonló elemszámú csoportok között. Igyekeztem tehát inkább felépítés alapján a hasonló csoportokat egy kalap alá venni és egymás után bemutatni őket. Látni fogjuk majd, hogy vannak egyszerűbb részek, mint például a prím rendű csoportok, melyeken hamar túllendülünk. Ugyanakkor a különböző prímek szorzatai, illetve a prímhatványok már nagyobb falat lesznek. A dolgozat menete a könnyebbektől halad majd a nehezebbek felé. Eljutunk majd az egyelemű csoporttól egészen a tizenhat elemű csoportig, mely mint kettő hatvány sokkal bonyolultabb lesz és külön kategóriaként kezelendő. (Itt megemlíteném például az 1024 elemű csoportokat, melyek a 2000-nél kisebb elemszámú csoportok izomorfia típusainak 99%-át teszik ki.)

Sor kerül majd néhány tétel és definíció bevezetésére is, melyek a későbbiekben elengedhetetlenek lesznek a kidolgozás során.

Ahogy említettem, 16-ig mutatom be a csoportok izomorfiaosztályait, de természetesen sokkal nagyobb elemszámra is ismert az adott elemszámú csoportok osztályozása. Ezek a csoportok - mátrix- vagy permutáció reprezentációikkal, esetleg generátorokkal és definiáló relációkkal való leírásukkal - számos, a szimbolikus számolásra alkalmas algebrai programcsomag könyvtárának is részét képezik. Azonban ahogy azt a tizenhat elemű csoportok fejezeteben látni fogjuk, az izomorfiaosztályok száma nagyon gyorsan nő (különösen a kettőhatványoknál), így hamar lehetetlenné válik a "kézi" leírásuk. A csoportelméletben gyakran nincs is szükség a teljes osztályozásra, hiszen számos tulajdonság már a csoportok kisebb részein (úgynevezett "szeletein") is ellenőrizhető.

Kezdjük is el!

2. fejezet

Szükséges előismeretek

Mindenek előtt szükséges előismeretek címszó alatt bevezetjük azokat a hasznos tételeket és definíciókat, melyekre támaszkodni fogunk a csoportok osztályozása során. Jöjjön először a ciklikus és a kommutatív csoportok pár hasznos tulajdonsága!

2.1. Tétel. Lagrange-tétel: *Ha G véges csoport és H részcsoportja G-nek, akkor a H rendje osztja a G rendjét.*

2.2. Állítás. *Ha G csoport elemszáma prím, akkor a G ciklikus és C_p-vel izomorf. Ha G ciklikus és $H \leq G$, H is ciklikus.*

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja, ha G prímrendű. Ilyenkor G ciklikus csoport.

Tehát minden prímrendű csoport ciklikus, és mivel azonos rendű ciklikus csoportok izomorfak, így izomorfia erejéig egyetlen prímrendű csoport létezik minden p prímszámra.

2.3. Definíció. *A G csoport kommutatív (Abel csoport), ha : $\forall a, b \in G$, $ab = ba$.*

Tudjuk még, hogy véges csoport minden elemének a rendje osztója a csoport rendjének. Tetszőleges csoportelemet a csoport rendjére, mint kitevőre emelve az egységelemet kapjuk.

2.1. Direkt szorzat és szemidirekt szorzat

Amikor csoportot szeretnénk készíteni elég sok lehetőség közül választhatunk, mégis az egyik legjobb és legtisztább módja ennek a direkt szorzat konstrukció. Ekkor az adott csoportok Descartes-szorzatán értelmezzük a csoportstruktúrát.

2.4. Definíció. *Legyenek G_1 és G_2 csoportok, és jelölje $G_1 \times G_2$ a két csoport Descartes-szorzatát, ahol $G_1 \times G_2 = \{(g_1, g_2) \mid g_i \in G_i\}$. Értelmezzük $G_1 \times G_2$-n az alábbi műveletet: legyen $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$, azaz szorozzuk a rendezett párokat tagonként. Ekkor könnyen látható, hogy így egy asszociatív műveletet kapunk, melynél az $(1_{G_1}, 1_{G_2})$ pár egységelemként hat, és $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. Ez azt jelenti, hogy $G_1 \times G_2$ csoport a most megadott műveletekre nézve: ezt nevezzük a G_1 és a G_2 csoportok direkt szorzatának. Hasonlóképpen értelmezhetjük $G_1 \times G_2 \times \cdots \times G_n$ többtényezős direkt szorzatot.*

Mivel a direkt szorzatban olyan könnyű számolni, mint annak komponenseiben, így gyakran jól járunk azzal, ha felismerjük, hogy épp egy direkt szorzattal van dolgunk. Különösen hasznos, ha nagy elemszámokkal dolgozunk, s ezáltal visszavezethetjük őket kisebb elemszámú, akár már ismert szerkezetű csoportokra.

A direkt szorzat felismerésére szolgál a következő tétel, mely azok "belső jellemzését" mutatja meg.

2.5. Tétel. *Legyenek G, G_1 és G_2 csoportok. Ekkor ekvivalensek az alábbi állítások:*

1. *$G \cong G_1 \times G_2$.*
2. *Megadhatók G-ben olyan N_1 és N_2 normálosztó, melyekre :*
   - *i. $N_1 \cong G_1$ és $N_2 \cong G_2$;*
   - *ii. $N_1 \cap N_2 = \{1\}$ és $N_1N_2 = G$.*
3. *Megadhatók G-ben olyan N_1 és N_2 normálosztók, melyekre:*
   - *i. $N_1 \cong G_1$ és $N_2 \cong G_2$;*
   - *ii. minden $g \in G$ elemhez van egyetlen olyan $n_1 \in N_1$ és $n_2 \in N_2$, hogy $g = n_1n_2$.*

Ennek a tételnek is megadható a többtényezős változata.

Érdemes megjegyeznünk, hogy az (1) $\Rightarrow$ (2) következtetésnél az N_1 és N_2 normálosztókat a $G_1 \times \{1_{G_2}\}$ és $\{1_{G_1}\} \times G_2$ részhalmazok adják.

A fönti jellemzésből megkapjuk például, hogy ha a tétel 2.ii. feltételének eleget tevő nem triviális normálosztókat találunk egy csoportban, akkor a csoport kisebb csoportok direkt szorzatával izomorf. Szoktuk még a G csoportot az N_1 és N_2 normálosztók (ún. belső) direkt szorzatának is nevezni.

Direkt szorzatokat használunk a véges Abel-csoportok alaptételében is, mely az egyik legalapvetőbb tétel, ha csoportkonstrukciókról van szó.

2.6. Tétel. Véges Abel csoportok alaptétele: *Ha G véges Abel csoport, akkor $\exists q_1, ..., q_k$ prímhatványok, hogy $G \cong C_{q_1} \times ... \times C_{q_k}$, és a q_i-k a sorrendtől eltekintve egyértelműek.*

Vegyük észre, hogy diszjunkt normálosztók esetén minden $n \in N$ és $m \in M$ elemekre $nm = mn$ teljesül még a nem kommutatív csoportok esetén is.

A direkt szorzat egy speciális eset volt, ahol két diszjunkt normálosztónk volt, de mi történik akkor, ha csak egy normálosztót és egy tőle diszjunkt részcsoportot találunk?

Szerencsénkre, a konstrukció számos előnye megmarad ebben az esetben is.

2.7. Tétel. *Legyen G csoport. Ekkor ekvivalensek az alábbi állítások:*

1. *Megadható G-ben egy olyan N normálosztó és H részcsoport, melyekre $N \cap H = \{1\}$ és $NH = G$.*
2. *Megadható G-ben egy olyan N normálosztó és H részcsoport, melyekre minden $g \in G$ elemhez létezik egyetlen olyan $n \in N$ és $h \in H$, hogy $g = nh$.*

A 2. feltétel alapján láthattuk, hogy ekkor G elemei kölcsönösen egyértelműen megfeleltethetők az N és a H elemeiből alkotott rendezett pároknak, vagyis az $N \times H$ elemeinek. A szorzási művelet azonban eltér a direkt szorzatban használt komponensenkénti művelettel.

2.8. Definíció. *Ha egy G csoportban megadható olyan $N \lhd G$ normálosztó és $H \leq G$ részcsoport, amelyek kielégítik az előbbi tétel feltételeit, akkor azt mondjuk, hogy a G csoport az N normálosztó és a H részcsoport szemidirekt szorzata. Jele: $G = N \rtimes H$.*

De hogyan is jönnek létre ilyen csoportok, vagyis hogyan tudjuk megkonstruálni G-t két absztrakt csoportból, N-ből és H-ból? Ehhez megnézzük, hogy ilyen esetben hogyan szorzódnak G elemei. Reprezentáljuk őket rendezett párokkal, hiszen minden elem felírható egy N-beli és egy H-beli elem szorzataként.

Legyen $g_1 = n_1h_1$ és $g_2 = n_2h_2$. Ekkor a két elem szorzata a következőképpen néz ki:

$$g_1g_2 = (n_1h_1)(n_2h_2) = (n_1(h_1n_2h_1^{-1}))(h_1h_2) = (n_1n_2')(h_1h_2),$$

ahol a $h_1n_2h_1^{-1}$ elem az n_2-nek a h_1-gyel vett konjugáltja, vagyis N-beli. A fenti felírás utolsó része azt mutatja meg, hogy g_1g_2 szorzat rendezett párként való fölírását $(n_1\varphi_{h_1}(n_2))(h_1h_2)$ alakban kapjuk meg, ahol $\varphi_{h_1} \in \operatorname{Aut} N$ a h_1 elemmel való konjugálás.

2.9. Tétel. *Legyenek adva N és H csoportok és egy $\varphi : H \to \operatorname{Aut} N$ csoporthomomorfizmus, melynél $h \in H$ képe φ_h. Ekkor az $N \times H$ Descartes-szorzaton értelmezhetünk egy szorzást a következő módon:*

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1, h_2)$$

Így egy csoportot kapunk, melyet az N és H szemidirekt szorzatának nevezünk, és $G \cong N \rtimes_\varphi H$-val jelöljük. Itt $\tilde{N} \cong N \times \{1_H\} \lhd G$ részhalmaz normálosztó, mely izomorf N-nel, $\tilde{H} \cong \{1_N\} \times H \lhd G$ részhalmaz pedig részcsoport, mely izomorf H-val, ahol $\tilde{N} \cap \tilde{H} = 1$ és $\tilde{N}\tilde{H}$ kiadja az egész Descartes-szorzatot. Az is igaz, hogy az $\tilde{N}$-beli elemek $\tilde{H}$-beliekkel való konjugálását épp a φ homomorfizmus írja le: $(1, h)(n, 1)(1, h^{-1}) = (\varphi_h(n), 1)$.

Láthattuk tehát, hogy a szemidirekt szorzat megkonstruálásához szükségünk van az N és H részcsoportokra, valamint a $\varphi : N \longrightarrow \operatorname{Aut} H$ homomorfizmusra. Ha φ triviális, akkor a direkt szorzatot konstrukciót kapjuk.

Még itt a szemidirekt szorzatoknál érdemes megjegyezni egy egyszerű észrevételt:

2.10. Állítás. *Ha $\varphi, \psi : H \to \operatorname{Aut} N$ olyan homomorfizmusok, melyekre vannak olyan $\sigma \in \operatorname{Aut} H$ és $\tau \in \operatorname{Aut} N$ automorfizmusok, hogy $\psi = \tau\varphi\sigma$, akkor $N \rtimes_\varphi H \cong N \rtimes_\psi H$, azaz φ és ψ izomorf szemidirekt struktúrát definiálnak a Descartes-szorzaton.*

2.2. p csoportok

A csoportok körében speciális szerepet játszanak azok a csoportok, melyek rendje prímhatvány. Ezeknek sokkal szebb a szerkezetük, s ezek révén a speciális tulajdonságaik révén speciális figyelmet is érdemelnek. Most róluk mutatunk be néhány tételt és definíciót.

2.11. Definíció. *Legyen p prímszám. Azt mondjuk, hogy a G véges csoport $p -$ csoport, ha G rendje p hatványa.*

2.12. Definíció. *G csoport centrumán azon $x \in G$ elemek halmazát értjük, melyek G minden elemével felcserélhetőek. Jele: $Z(G)$.*

A következő tételek egyszerűnek tűnhetnek, mégis nagyon hasznosak lesznek számunkra az osztályozások során, különös tekintettel arra, amikor a tizenhat elemű csoportokkal foglalkozunk.

2.13. Tétel. *Legyen p prímszám. Ha P (véges) p-csoport, akkor $Z(P)$ sem egyelemű.*

2.14. Tétel. *Ha $G/Z(G)$ ciklikus akkor a centrum megegyezik magával a csoporttal, azaz G kommutatív.*

Itt még érdemes megjegyezni egy állítást:

2.15. Állítás. *Ha G csoportban minden elem másodrendű, akkor G kommutatív.*

A 2.13. és 2.14.-es tételből könnyedén beláthatjuk a következő állítást, mely az első konkrét osztályozással foglalkozó levezetésünk lesz.

2.16. Következmény. *Minden prímnégyzet rendű csoport kommutatív és izomorf vagy C_{p^2}-tel vagy $C_p \times C_p$-vel.*

Bizonyítás. Legyen G egy p^2 rendű csoport, ahol p prím. $Z(G)$ elemszáma ekkor az eddigiek alapján csak 1, p vagy p^2 lehet. Ha $|Z(G)| = p^2$, akkor kész is vagyunk, mert a csoport kommutatív. A $|Z(G)| = 1$ eset nem teljesülhet a 2.13. Tétel miatt. Végül $|Z(G)| = p$ sem teljesülhet, mert akkor $|G/Z(G)| = p$ lenne, amikor is $G/Z(G)$ ciklikus, mely ellentmondana a 2.14. Tételnek.

Az, hogy ekkor a csoport izomorf vagy C_{p^2}-tel vagy $C_p \times C_p$-vel következik a véges Abel-csoportok alaptételéből.

A csoportok osztályozása során hatalmas segítséget jelent, ha ismerjük a p hatvány rendű csoportoknak ezen tulajdonságait. Sylow tételei szerint a prímhatvány rendű csoportoknak alapvető szerepük van minden csoport felépítésében. Bemutatjuk ezeket a tételeket és láthatjuk, hogy valóban mindenhol előfordulnak, és ha nem is adnak konkrét választ arra, hogy hogyan épül fel egy csoport, lényegesen közelebb visznek hozzá.

A következő tételek a Sylow részcsoportok létezéséről fognak szólni.

2.17. Definíció. *Legyen G véges csoport, és a rendjének prímtényezős felbontása $|G| = p_1^{\alpha_1} ... p_i^{\alpha_i}$. A $p_i^{\alpha_i}$ rendű részcsoportokat a G csoportnak a p_i-Sylow részcsoportjainak nevezzük. Egy részcsoport tehát akkor p-Sylow részcsoport, ha rendje p-hatvány, indexe pedig p-vel nem osztható.*

2.18. Tétel. *Legyen G véges csoport, és p a G rendjének tetszőleges prímosztója. Ekkor igazak a következő állítások:*

1. *Van G-ben p-Sylow részcsoport.*
2. *G minden p-hatványrendű részcsoportja része G egy p-Sylow részcsoportjának.*
3. *Bármely két p-Sylow részcsoport konjugált G-ben.*

4. *Ha q egy G rendjét osztó p-hatvány, akkor a q-rendű G-beli részcsoportok száma kongruens 1-gyel modulo p.*

5. *A p-Sylow részcsoportok száma osztója $|G:P|$-nek.*

A Sylow tételek következménye lesz a Cauchy tétel:

2.19. Tétel. Cauchy tétel: *Ha $|G| = n < \infty$, p prím és $p|n$, akkor G-ben van p-rendű elem.*

2.20. Következmény. *Legyenek $p > q$ prímek, és $|G| = pq$. Ekkor a G-ben a p-Sylow részcsoport normálosztó. Ha $p-1$ nem osztható q-val, akkor a q-Sylow is normálosztó, és így G ciklikus.*

Ezen a pár bemutatott példán láthattuk, hogy a prímhatvány rendű csoportok valóban speciálisak, és érdemes velük komolyabban is foglalkozni. Még érdekesebb lesz, amikor majd konkrét esetekben használjuk a felsorolt tételeket és definíciókat, és a "való életben" láthatjuk, hogyan is működnek.

A későbbiekben még szükségünk lesznek a faktorcsoportokra, melyeket most tömören be is vezetünk.

2.21. Állítás. *Legyen G csoport és N normálosztó a G-ben, azaz olyan részcsoportja G-nek, melyre $gN = Ng$ minden $g \in G$-re. Álljon a K halmaz az N szerinti mellékosztályokból, és vezessünk be rajta szorzást a*

$$(g_1N) * (g_2N) = g_1g_2N$$

képlettel. Ekkor K csoport lesz, melynek egységeleme az $N = 1 \cdot N$ mellékosztály, a gN inverze pedig a $g^{-1}N$. Az a $\psi : G \longrightarrow K$ leképezés, ami g-hez gN-et rendeli, homomorfizmus lesz, melynek a képe K, a magja N.

2.22. Definíció. *Legyen N normálosztó a G csoportban. Az előző* 2.19. Állításban *definiált K csoportot a G csoport N szerinti fatorcsoportjának nevezzük és G/N-nel jelöljük.*

3. fejezet

p és $2p$ rendű csoportok

A szükséges tételek és definíciók bemutatása után el is kezdhetjük a csoportok osztályozását. Ebben a fejezetben, ahogy a cím is mutatja, a p és a $2p$ rendű csoportokkal fogunk foglalkozni. Szépen fokozatosan felépítjük a csoportokat, melyekre a későbbiekben is támaszkodhatunk. Először ejtünk pár szót az egy elemű csoportról, a prímrendű csoportokról, majd rátérünk a $2p$ rendűekre is, melyek között a hat, a tíz és a tizennégy fog sorra kerülni.

Elsőként lássuk az egyelemű csoportot! Nem lesz vele sok gondunk, az egyelemű csoport ugyanis csupán az egységelemből áll, és csak egy létezik belőle. Így néz ki:

C_1	$\{1\}$

Az egyelemű csoport

3.1. Prím rendű csoportok

Rá is térünk a következő pontunkra, a prím rendű csoportokra.

Tudjuk, hogy egy prímrendű csoport mindig ciklikus és C_p-vel izomorf (vagyis $\mathbb{Z}_p^+$-szal, azaz ők lesznek az egészek mod p az összeadásra nézve). Ők lesznek a legegyszerűbb csoportok. Már Lagrange tételéből is láthatjuk, hogy a bennük előforduló elemrendek nem túl változatosak, csupán maga a p és az egy. Most tekintsük az egy és húsz közé eső prímszámokat, vagyis az ilyen elemrendű csoportokat! Ezek lesznek a 2, 3, 5, 7, 11 és 13. Ezeket is megmutatjuk táblázatban. Mind ciklikus, azaz csak egyetlen egy elem generálja őket, a felépítésük hasonló lesz.

C_2	$\{1, a\}$
C_3	$\{1, a, a^2\}$
C_5	$\{1, a, a^2, a^3, a^4\}$
C_7	$\{1, a, a^2, a^3, a^4, a^5, a^6\}$
C_{11}	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, \}$
C_{13}	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, \}$

A prím rendű csoportok

3.2. Hatelemű csoportok

A $2p$ elemű csoportokból elsőként vizsgáljuk meg a hateleműeket, melyekből izomorfia erejéig két darab létezik, ezek lehetnek:

- $C_6 \cong C_3 \times C_2$
- $D_3 \cong S_3$

Ennek belátásához ismét az elemrendeket hívjuk segítségül, és azok vizsgálásával kezdjük a csoportok meghatározását.

Ha van hatodrendű elemünk, ami kigenerálja az egész csoportot, akkor az csak a hatelemű ciklikus csoport lehet, vagyis a C_6. (Később látni fogjuk, hogy ez izomorf a két és a háromelemű ciklikus csoportok direkt szorzatával.)

Most nézzük azt az esetet, amikor nincs hatodrendű elem. Ekkor a Cauchy tétel miatt lesz másodrendű és harmadrendű elem is a csoportban. Legyenek ezek f és t. A harmadrendű elem által generált részcsoport indexe a G-ben 2, így tétel szerint ez normálosztó lesz G-ben. Vegyük észre, hogy t és f együtt kigenerálja az egész G-t.

Legyen a csoportunk $G = \{1, f, f^2, t, tf, tf^2\}$, és vizsgáljuk meg benne a konjugálást! Mivel t másodrendű tudjuk róla, hogy $t^{-1} = t$. Vajon mit kapunk, ha f-et konjugáljuk t-vel? A konjugálás nem változtatja meg az elem rendjét, így $o(tft) = o(f) = 3$, vagyis a tft egyenlő lesz vagy f-fel, vagy f^2-tel.

Első lehetőségünk, hogy $tft = f$. Ha ezt beszorozzuk t-vel balról, azt kapjuk, hogy $ft = tf$. Ekkor a csoportunk kommutatív lenne és hatodrendű elem is lenne benne, mivel ez esetben $o(ft) = [o(f), o(t)] = 6$. Ismét megtaláltuk az elsőnek vizsgált csoportot. Azt is láthatjuk, hogy $C_6 \cong C_2 \times C_3$. Viszont ne felejtsük el, hogy feltettük, hogy a csoportban nincsen hatodrendű elem! Így itt most ellentmondásra jutottunk. Nézzük a második esetet!

Legyen most $tft = f^2$, és megint szorozzunk t-vel balról! Ekkor azt kapjuk, hogy $ft = tf^2$, amit ha kicsit másképp írunk fel rögtön láthatjuk, hogy ez a diéder csoportok szorzási szabálya. Ugyanis tudjuk, hogy f harmadrendű, így $ft = tf^{-1}$.

Megkaptuk tehát, hogy ekkor $G \cong D_3$, mivel ez már teljesen meghatározza a G-beli szorzást. Azt is láthatjuk még, hogy a $D_3 \cong S_3$, hiszen ezek a háromszög szimmetriái, a csúcsok permutációi.

És ezzel a hatelemű csoportok végére értünk.

C_6	$\{1, a, a^2, a^3, a^4, a^5\}$
D_3	$\{1, f, f^2, t, tf, tf^2\}$

A hatelemű csoportok

3.3. Tízelemű csoportok

Most pedig következzenek a tízelemű csoportok! Izomorfia erejéig két darab létezik belőle:

- $C_{10} \cong C_2 \times C_5$
- D_5

Ha van tizedrendű elem, akkor az a tízelemű ciklikus csoport lesz, azaz C_{10}.

Ha nincs tizedrendű elem a csoportban, akkor pedig D_5-öt kapjuk, hasonlóan a hatelemű csoportokhoz. Nézzük meg bővebben miért!

Az alap feltevésünk az, hogy nincs tizedrendű elem. Legyen $g \in G$ egy ötödrendű elem, ekkor az általa generált részcsoport normálosztó G-ben, hiszen az indexe kettő. Vegyünk ekkor egy másodrendű $h \in G$ elemet! Ha konjugáljuk g-t h-val, ahol $h = h^{-1}$, nem lépünk ki az általa generált csoportból. Mivel a g által generált részcsoport elemei, $< g >= \{1, g, g^2, g^3, g^4\}$, a g konjugáltja is ezek valamelyikével kell hogy egyenlő legyen.

Az egységelemet rögtön ki is zárhatjuk.

Ha $hgh = g$, az egyenletet átrendezve azt kapjuk, hogy $gh = hg$, vagyis hogy G kommutatív, s így visszajutottunk C_{10}-hez.

Nézzük mit kapunk, ha a konjugált g^2-tel egyenlő! Azt a cselt alkalmazzuk, hogy g-t kétszer konjugálunk h-val, vagyis felhasználva hogy $hgh = g^2$, ezt átrendezve megkapjuk, hogy $g = hhghh = hg^2h = hghhgh = g^2g^2 = g^4$. De $g = g^4$ nyilván nem igaz, tovább keresgélünk.

(Itt zárójelben megjegyeznénk, hogy a h-val való kétszer konjugálás gyakorlatilag a helybenhagyás lesz, $|h| = 2$ miatt, viszont a levezetés szempontjából sokat segít nekünk)

Ha $hgh = g^3$ hasonlóképpen járunk el, mint az előbb. Ugyanazt a módszert alkalmazva megkapjuk, hogy $g = hhghh = hg^3h = hghhghhgh = g^3g^3g^3 = g^9 = g^4$, ahol megint ellentmondásra jutottunk.

Az utolsó lehetőségünk, ha $hgh = g^4$. Ha ezt inkább úgy írjuk fel, hogy $hgh = g^{-1}$, és átrendezzük, azt kapjuk, hogy $gh = hg^{-1}$, ami pedig a diéder csoport szorzási szabálya. (g helyett használhatnánk f-et, mint forgatás és h helyett t-t, mint tükrözés, akárcsak a hatelemű csoportoknál.)

Láthatjuk, hogy így csak C_{10} vagy D_5 lehetséges.

C_{10}	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$
D_5	$\{1, f, f^2, f^3, f^4, t, tf, tf^2, tf^3, tf^4\}$

A tízelemű csoportok

3.4. Tizennégy elemű csoportok

A hat és a tízelemű csoportok után rá is térhetünk a tizennégy elemű csoportokra, melyekből izomorfia erejéig csak kettő létezik. Ezek lesznek:

- $C_{14} \cong C_2 \times C_7$
- D_7

Ha létezik tizennegyed rendű elem, akkor a tizennégy elemű ciklikus csoportot kapjuk, azaz a C_{14}-et.

Ha nincs tizennegyed rendű elemünk, akkor az egységelemen kívül előforduló elemek rendjei lehetnek a 2 és a 7.

Nézzük ekkor hogy nézhet ki a csoport! Legyen $f \in G$ egy hetedrendű elem. Az f által generált részcsoport $< f >= \{1, f, f^2, f^3, f^4, f^5, f^6\}$ normálosztó lesz G-ben, hiszen az indexe kettő. Vegyünk egy másodrendű $t \in G$ elemet, és konjugáljuk meg vele f-et! A konjugálással nem lépünk ki az f által generált csoportból, így $tft \in \{1, f, f^2, f^3, f^4, f^5, f^6\}$. Vizsgáljuk meg a lehetséges kimeneteleket!

Az egységelem nyilván nem lehet.

Abban az esetben, ha $tft = f$, egy egyszerű szorzással után megkapjuk, hogy $ft = ft$, vagyis megtaláltuk a kommutatív csoportot, a C_{14}-et.

Ha $tft = f^2$, a tízelemű csoportokban vizsgáltakhoz hasonlóan kétszer konjugálva t-vel $f = ttftt = tf^2t = tfttft = f^2f^2 = f^4$-t kapunk, vagyis $f = f^4$, ami nyilvánvalóan nem igaz.

Nézzük mit kapunk, ha a konjugált f^3-nal egyenlő! Az előző módszert alkalmazva ismét ellentmondásra jutunk, ugyanis $f = ttftt = tf^3t = tfttfttft = f^3f^3f^3 = f^9$.

A maradék három esetből kettőben hasonló ellentmondást kapunk. Ha az f konjugáltja f^4, akkor $f = f^2$-et kapunk, ha a konjugált f^5, akkor pedig $f = f^4$-t. Ezek közül nyilván egyik sem jó megoldás. Az utolsó esetben $tft = f^6$, vagyis a $tft = f^{-1}$ már használható eredményt ad, hiszen ebből megkaphatjuk a $ft = tf^{-1}$-et, ami a diéder csoport szorzási szabálya. Így mivel ennek a tulajdonságai illenek a D_7 diéder csoportra, megtaláltuk a második és egyben utolsó tizennégy elemű csoportot.

C_{14}	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}\}$
D_7	$\{1, f, f^2, f^3, f^4, f^5, f^6, t, tf, tf^2, tf^3, tf^4, tf^5, tf^6\}$

A tizennégy elemű csoportok

3.5. $2p$ rendű csoportok általában

Egymás után megvizsgálva ezeket az esetek észrevehetjük, hogy gyakorlatilag feleslegesen dolgoztunk ilyen sokat. Láthatjuk, hogy ugyanazon a gondolatmeneten haladva ugyanazokat az eredményeket kaptuk, csupán ahogy egyre nőnek az elemrendek, egyre nehezebben és lassabban. Milyen szerencsénk van, hogy a $2p$ rendű csoportok osztályozására tétel is létezik!

Most lássuk be általánosan is a szabályt, amit az előbbiekben megtapasztaltunk!

3.1. Állítás. *Ha G egy $2p$-rendű csoport, ahol $p > 2$ prím, akkor G izomorf C_{2p} és D_p közül az egyikkel.*

Bizonyítás. A Cauchy-tétel alapján tudjuk, hogy G-nek van olyan f és t eleme, melyre $o(f) = p$, és $o(t) = 2$. Továbbá a 2.20. Következményből az is adódik, hogy az $F =< f >$ részcsoport normálosztó, mely diszjunkt a $H =< t >$ részcsoporttól. Így tehát G az F és H részcsoportok szemidirekt szorzata. De H-ból csak kétféle homomorfizmus megy $\mathrm{Aut}\, F = \mathrm{Aut}\, C_p = C_{p-1}$-be, hiszen C_{p-1}-ben összesen egy másodrendű és egy elsőrendű elem van, ezért összesen két szemidirekt struktúrát kaphatunk. Ha $\varphi : H \longrightarrow \mathrm{Aut}\, F$ a triviális homomorfizmus, akkor a $G = F \rtimes_\varphi H$ csoport kommutatív, és izomorf C_{2p}-vel. Ha viszont $\psi : H \longrightarrow \mathrm{Aut}\, F$ nem triviális, akkor a kapott $G = F \rtimes_\psi H$ csoport nem kommutatív, és így csak a D_p-vel lehet izomorf.

4. fejezet

Néhány további egyszerű eset

Most, hogy befejeztük a $2p$ rendű csoportok osztályozását, mind a konkrét, mind az általános esetekben, továbblépünk a következő nagyobb fejezetre. Mivel a szakdolgozatomban csak a tizenhat eleműig vizsgálom a csoportokat, most három eltérő csoportkonstrukció fog következni. Ha a nagyobb elemrendekkel is foglalkoznánk, az itt tárgyalt 9, 12 és a 15 elemű csoportok már nem lennének ilyen magányosak, de az sajnos meghaladja a dolgozatom kereteit.

Lássuk akkor a kilencelemű csoportokat!

4.1. Kilencelemű csoportok

A kilencelemű csoportokból kétféle létezik:

- C_9
- $C_3 \times C_3$

Tudjuk, hogy prímnégyzet rendű csoport mindig kommutatív, valamint izomorf vagy C_{p^2}-tel $C_p \times C_p$-vel.

Először is nézzük meg az elemrendeket! Mivel az elem rendje mindig osztja a csoport rendjét, a 9 osztóiban kell gondolkodnunk. A csoport elemeinek rendjei lehetnek tehát: 1, 3 vagy 9.

Ha van kilencedrendű elem a csoportban, akkor a kilencelemű ciklikus csoporttal van dolgunk, a C_9-cel.

Ha nincs kilencedrendű elem, akkor az egységelemen kívül minden elem rendjének háromnak kell lennie, és így nem kaphatunk mást, mint a $C_3 \times C_3$-at.

C_9	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$
$C_3 \times C_3$	$\{1, a, a^2\} \times \{1, b, b^2\}$

A kilencelemű csoportok

Mivel a dolgozatom csupán a tizenhat elemű csoportokig terjed, így nem találkozunk több p^2 rendű csoporttal. Azonban a $2p$ rendűekhez hasonlóan itt is van általános tétel, melyet már beláttunk a bevezető részben.

4.2. Tizenkét elemű csoportok

Lépjünk tovább a következő részre, ahol a tizenkét elemű csoportokat fogjuk osztályozni. Ezekből izomorfia erejéig öt darab létezik, melyek az alábbiak lehetnek:

- $C_4 \times C_3$
- $C_2^2 \times C_3$
- $C_2^2 \rtimes C_3 \cong A_4$
- $C_3 \rtimes C_4$
- D_6

Hogy megtaláljuk mindet, először bevezetünk néhány jelölést.

Legyen G a tizenkét elemű csoport, P egy 2-Sylow részcsoport és Q egy 3-Sylow részcsoport G-ben. Ekkor n_2 a 2-Sylowok száma, míg n_3 a 3-Sylowok száma.

Kiindulásként megmutatjuk, hogy valamelyik Sylow normálosztó lesz.

A Sylow-tételek miatt, valamint amiatt, hogy a Sylow részcsoportok számának osztaniuk kell a csoport rendjének és a prímhatványnak a hányadosát láthatjuk, hogy a 2-Sylowok száma csak 1 vagy 3 lehet, míg a 3-Sylowoké 1 vagy 4. Nézzük át részletesen a lehetséges eseteket!

Tegyük fel, hogy $n_3 = 1$, ekkor Q normálosztó lesz G-ben. Ha viszont $n_3 = 4$, akkor négy darab háromelemű csoportunk van. Ezek egymástól diszjunktak, így az uniójuk kilencelemű, hiszen minden háromelemű csoportban két darab harmadrendű elem található, valamint az egységelem. Mivel $|G| = 12$, így a 2-Sylowok nem egységelemei ezen a $12 - 9 = 3$ helyen találhatóak. Ebből viszont már következik, hogy csak egy darab 2-Sylow van, vagyis hogy $n_2 = 1$ és így $P \triangleleft G$. Így tehát beláttuk, hogy valamelyik Sylownak normálosztónak kell lennie.

Mivel $G = PQ$, G-re mindenképp szemidirekt szorzatot kapunk, valamint mivel a három és négyelemű csoportokat már ismerjük, tudjuk, hogy P és Q alakjai következőek lehetnek:

- $P = C_4$ vagy $C_2 \times C_2 (= C_2^2)$
- $Q = C_3$

Tehát G az alábbi típusok valamelyike lehet:

- $C_4 \rtimes C_3$ vagy $C_2^2 \rtimes C_3$, ha $P \triangleleft G$
- $C_3 \rtimes C_4$ vagy $C_3 \rtimes C_2^2$, ha $Q \triangleleft G$

Most elkezdjük megvizsgálni az egyes eseteket.

Ha P normálosztó G-ben, akkor két alesetet kapunk: P izomorf C_4-gyel vagy $C_2 \times C_2$-vel.

A $C_4 \rtimes C_3$ szemidirekt szorzat csak triviális lehet, mivel $\varphi : C_3 \longrightarrow \mathrm{Aut}\, C_4$ triviális. Ez azért van így, mert a C_4 automorfizmus-csoportja kételemű, így $\mathrm{Aut}\, C_4$-nek nincs harmadrendű eleme, ezért a hozzárendelés csak triviális lehet. Így ez valójában egy direkt szorzat lesz, azaz $G = C_4 \rtimes C_3 = C_4 \times C_3$.

Nézzük a $C_2^2 \rtimes C_3$ esetet! Ekkor két esetet kapunk aszerint, hogy $\varphi : C_3 \longrightarrow \mathrm{Aut}\, C_2^2 = GL(2,2)$ triviális-e. Itt a kételemű testek feletti kétszer kettes invertálható mátrixok csoportjába képzünk. Ha a hozzárendelés triviális, akkor G direkt szorzat, vagyis $G = C_2^2 \rtimes C_3 = C_2^2 \times C_3$.

Abban az esetben, ha $C_2^2 \rtimes C_3$ nem triviális kicsit nehezebb dolgunk van. Mivel $|GL(2,2)| = 6$, $\mathrm{Aut}\, C_2^2$-ben ($\cong C_3$) egy harmadrendű részcsoport van. Nem triviális $\varphi : C_3 \longrightarrow \mathrm{Aut}\, C_2^2$ csak kétféle van, (C_3 generátoreleme az S_3 valamely 3-ciklusába képződik), de ez a kétféle φ tulajdonképpen izomorf csoportokat ad, hiszen $\varphi_1 = \varphi_2 \circ \phi$, ahol $\phi \in \mathrm{Aut}\, C_3$, vagyis C_3 egy automorfizmusával egymásba átvihetőek (gyakorlatilag csak átszámozzuk a C_3 elemeit a szemidirekt szorzatban).

Mivel most megmutattuk, hogy a tizenkét elemű csoportok között csak egy olyan nem kommutatív szemidirekt szorzat van, ahol a 2-Sylow normálosztó, és mivel az A_4 ilyen csoport, ezért $C_2^2 \rtimes C_3 \cong A_4$-gyel.

(Itt a 2-Sylow részcsoport tulajdonképpen $\{(1), (12)(23), (13)(24), (14)(23)\}$, C_3 pedig például $\{(1), (123), (132)\}$.)

Ha P nem normálosztó G-ben, akkor, ahogy azt a bizonyítás elején beláttuk, Q lesz az. Ekkor ismét két esetet kapunk aszerint, hogy P izomorf C_4-gyel vagy $C_2 \times C_2$-vel. Így a lehetséges esetek $G = C_3 \rtimes C_4$ és $G = C_3 \rtimes C_2^2$.

Tekintsük először a $C_3 \rtimes C_4$ esetet! Ha $\varphi : C_4 \longrightarrow \operatorname{Aut} C_3$ triviális, akkor $G \cong C_3 \times C_4$, vagyis eljutottunk egy olyan esethez, amit már láttunk. Ha viszont $\varphi : C_4 \longrightarrow \operatorname{Aut} C_3 \cong C_2$ nem triviális, akkor csak egyféle lehet, vagyis C_4 generátoreleme az invertálással hat C_3-on.

Ha $C_3 =< a >, C_4 =< b >$, akkor:

$$G = C_3 \rtimes C_4 = \{(a^i, b^j)|0 \le i \le 2, 0 \le j \le 3\}$$

$$(a^i, b^j)(a^k, b^l) = (a^i(a^k)^{-j}, b^j b^l) = (a^{i-kj}, b^{jl})$$

Ezt szokás diciklikus csoportnak is nevezni.

Lássuk most a második esetet, vagyis ha a 2-Sylow C_2^2 alakú! Itt három nem triviális φ létezik, ahol $\varphi : C_2^2 \longrightarrow C_2 (\cong \operatorname{Aut} C_3)$. C_2^2 -ből az egyik másodrendű elem megy 1-be, a másik kettő a C_2 generátorelemébe. Így tulajdonképpen három hozzárendelést kapunk, de ezek C_2^2 egy automorfizmusával egymásba átvihetőek, vagyis izomorfia erejéig csak egy ilyen nem triviális leképezés van. Mivel a D_6 diéder csoport teljesíti ezeket, így $G = C_3 \rtimes C_2^2$.

Beláttuk, hogy a tizenkét elemű csoportokból öt különböző létezik, melyek nem izomorfak egymással. Van két kommutatív és három nem kommutatív csoportunk. Ebből a két kommutatív nyilván nem izomorf egymással, sem a nem kommutatívokkal. A nem kommutatívak különbözőségét pedig többek között úgy láthatjuk be a, hogy megszámoljuk a másodrendű elemeik számát.

- D_6-nak 7 db van: a hat tükrözés és f^3
- A_4-nek 3 darab van: $(12)(34), (13)(24), (14)(23)$
- $C_3 \rtimes C_4$-nek 1 darab van: $(0, 2)$

Az első két nem kommutatív csoportnál nem kellett sokat gondolkodnunk a másodrendű elemeken, a harmadiknál viszont kicsit nehezebb dolgunk van.

Vegyük alaposabban szemügyre a csoport felépítését! A harmadrendű részcsoport miatt van két harmadrendű elemünk, valamint az egységelem. A négy negyedrendű részcsoportban van $4 \cdot 2 = 8$ negyedrendű elem, és a számolásban máris $3 + 8 = 11$-nél tartunk. Így nem is marad más, minthogy a negyedrendű részcsoportok metszetében az egységelem mellett egy darab másodrendű elem bújjon meg.

Ezzel be is fejeztük a tizenkét elemű csoportok osztályozását.

$C_4 \times C_3$	$\{1, a, a^2, a^3\} \times \{1, b, b^2\}$
$C_2^2 \times C_3$	$\{1, a, b, c\} \times \{1, d, d^2\}$
$C_2^2 \rtimes C_3$	$\{1, a, b, c\} \rtimes \{1, d, d^2\}$
$C_3 \rtimes C_4$	$\{1, a, a^2\} \rtimes \{1, b, b^2, b^3\}$
D_6	$\{1, f, f^2, f^3, f^4, f^5, t, tf, tf^2, tf^3, tf^4, tf^5\}$

A tizenkét elemű csoportok

4.3. Tizenöt elemű csoportok

A tizenöt elemű csoportokkal nem lesz nehéz dolgunk, ugyanis csak egy van belőle. Ez nem más, mint a:

- $C_3 \times C_5 = G$

A tizenöt elemű csoportok esetén ismét Sylow tételeit hívjuk segítségül. Használjuk a megszokott jelöléseinket! Legyen a 3-Sylowok száma n_3, az 5-Sylowoké pedig n_5.

Ekkor a tételek miatt, valamint mert a Sylow részcsoportok számának osztaniuk kell a csoport rendjének és a prímhatványnak a hányadosát (vagyis: $n_3 \equiv 1(3)$, és $n_3|5$). Ezekből következik, hogy $n_3 = 1$, vagyis hogy a 3-Sylow részcsoport normálosztó G-ben.

Ugyanígy láthatjuk, hogy az n_5 is csak az egy lehet, így az 5-Sylow részcsoport is normálosztó G-ben.

Mivel mind a három, mind az ötelemű részcsoport rendje prímszám, így csak egyféleképpen nézhetnek ki, ezt az előzőekben már megmutattuk. A 3-Sylow a C_3 lesz, míg az 5-Sylow a C_5, és mivel mindkettő normális részcsoport, és $C_3 \cap C_5 = 1$, így a direktszorzatuk kiadja az egész csoportot. Vagyis $C_3 \times C_5 = G$, és csakis ez az egy megoldás létezik.

$C_3 \times C_5$	$\{1, a, a^2\} \times \{1, b, b^2, b^3, b^4\}$

A tizenöt elemű csoport

5. fejezet

2^n rendű csoportok

Ismét elérkeztünk egy újabb fejezethez, mely önmagában is ki tudna tölteni egy egész szakdolgozatot. Már a bevezetésben említettük, hogy a kettőhatvány rendű csoportok máshogy viselkednek. Általánosságban is észrevehettük, hogy ha a kettőről van szó, akkor kivételek és érdekességek következnek. Lévén a kettő prímszám, de mégis csak páros, speciális tulajdonságokkal rendelkezik. Ezek gyakran jól megbonyolítják mind a matematikus, mind bárki más életét, aki találkozik vele.

Ugyan itt csak a 4, 8 és 16 elemű csoportokkal foglalkozunk, de már itt is szemmel láthatóan egyre bonyolultabb és hosszadalmasabb lesz a vizsgálódás elemrendről elemrendre.

Kezdjük is el az osztályozásukat!

5.1. Négyelemű csoportok

Négyelemű csoportból kettő létezik:

- C_4
- $C_2 \times C_2 \cong V$

Hogy épp melyikről van szó azt úgy dönthetjük el, hogy megnézzük a csoportok elemeinek rendjét. Tudjuk, hogy az elem rendje mindig osztja a csoport rendjét, így a csoportban előfordulható elemrendek a következők lehetnek: 1, 2 és 4.

Ha van negyedrendű elem, akkor az kigenerálja az egész csoportot és így a négyelemű ciklikus csoportot kapjuk, azaz a C_4-et.

Ha viszont nincs negyedrendű elemünk, akkor az egységelemen kívül az összes elemnek másodrendűnek kell lennie. Ez pedig nem lesz más, mint a Klein csoport. Meg is mutatom, hogy miért.

Legyen a csoportunk $G = \{1, a, b, c\}$. Nézzük meg G szorzástábláját! Az első oszlopban és sorban eggyel szorzunk, így azok ugyanúgy 1, a, b és c lesznek. Mivel az elemek másodrendűek, ezért az átlóban, ahol az elemeknek az önmagukkal vett szorzata szerepel, végig egyesek lesznek.

Nézzük azt az esetet, amikor két különböző, nem egységelemet kell összeszoroznunk egymással. Az $a * b$ nem lehet egyenlő az eggyel, hisz akkor $b = 1 * b = a * b * b = a$, ami nem igaz. Az $a * b$ nem lehet a sem, mivel $a * b = a$-ból $b = 1$ következne. A két elem szorzata ugyanebből az okból kifolyólag b sem lehet, vagyis, hogy $a \neq 1$. Nincs más lehetőségünk, minthogy $a * b = c$ legyen. Ugyanígy megkapjuk, hogy $a * c = b$, és hogy $b * c = a$. A táblázatot így már teljesen ki tudjuk tölteni.

Egyértelmű, hogy ez a két csoport nem izomorf egymással.

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

A Klein csoport művelettáblája

C_4	$\{1, a, a^2, a^3\}$
V	$\{1, a, b, c\}$

A négyelemű csoportok

5.2. Nyolcelemű csoportok

Tovább lépünk a nyolcelemű csoportokra, ahol ugyan csak eggyel növeltük a kettő hatványkitevőjét, mégis a lehetőségek száma több, mint a kétszeresére nőtt. A nyolcelemű csoportokból már öt különböző van:

- C_8
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$
- D_4
- Q

Ezek közül az első három kommutatív, a maradék kettő viszont nem az.

Az elemrendek csak 1, 2, 4 vagy 8 lehetnek. Ha van nyolcadrendű elemünk, akkor az kigenerálja az egész csoportot, és így megkapjuk C_8-at.

Ha az egységelemen kívül minden elem rendje kettő, akkor a csoport kommutatív és a $G \cong C_2 \times C_2 \times C_2$-t kapjuk.

Nézzük azt az esetet, ha nyolcadrendű elem nincs, de negyedrendű elem található a csoportban. Egy negyedrendű $a \in G$ által generált részcsoport izomorf lesz a C_4-gyel, ami pedig normálosztó G-ben (az indexe miatt). Itt két esetre bontjuk a vizsgálatot.

Az első esetben legyen olyan másodrendű $b \in G$ elemünk, mely nincs benne az a által generált részcsoportban. Ekkor az egész csoportot megkapjuk az a és b által generálva, vagyis $G =< a, b >= \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$ alakban áll elő.

Nézzük meg hogyan szorzunk a csoportban! Vegyük az a b-vel való konjugáltját. Tudjuk, hogy konjugáláskor a rend nem változik és a konjugált is eleme lesz az a által generált részcsoportnak. Az a konjugáltja nem lehet az egységelem, sem pedig a^2. Tehát bab vagy az a vagy az a^3 lehet csak.

Ha $bab = a$, akkor $ab = ba$-t kapunk, és a csoportunk kommutatív lesz és izomorf $C_4 \times C_2$-vel.

Ha a másik lehetőséget nézzük, vagyis hogy $bab = a^3$, akkor megkapjuk hogy $ab = ba^3$ ($ab = ba^{-1}$), ami a diédercsoport szorzási szabálya. Így kapjuk D_4-et.

A második esetben azt tesszük fel, hogy az a által generált részcsoporton kívül nincsen másodrendű b elem. A lehetséges elemrendeket figyelembe véve, így csak negyedrendű lehet b. Ekkor a b által generált részcsoport hasonló lesz az a által generáltéhoz, vagyis $< b >= \{1, b, b^2, b^3\}$. Mivel b^2 rendje kettő, így annak benne kell lennie $< a >$-ban, hisz ezt feltettük. Ebből viszont az következik, hogy $a^2 = b^2$.

Akkor mit kapunk viszont, ha a-t és b-t szorozzuk össze? Az ab nem lehet eleme $< a >$-nak, mert akkor b is eleme lenne ami nem igaz. Ugyanígy nem lehet eleme $< b >$-nek sem, hisz akkor a lenne rossz helyen. Nincs más lehetőségünk, minthogy egy új elemmel tesszük egyenlővé. Nevezzük ezt az elemet c-nek. Ekkor a negyedrendű elemeink: a, a^3, b, b^3, c, c^3. Látjuk azt is, hogy $a^2 = (a^3)^2 = b^2 = (b^3)^2 = c^2 = (c^3)^2$. Ugyanakkor, ha $ab = c$, ba mivel egyenlő? Ha $ba = c$ lenne, a csoportunk megint kommutatív, ami nekünk jelen esetben nem jó. Meg is mutatom miért. Ha $ab = ba$, akkor $c^2 = (ab)^2 = a^2b^2 = a^2a^2 = 1$, vagyis c másodrendű lenne, holott feltettük, hogy negyedrendű. Marad az a lehetőség, hogy $ba = c^3 = c^{-1}$. Itt már gyanakodhatunk, hiszen ez igencsak hasonlít a kvaterniócsoportra. Ha a-t, b-t és c-t i, j, k-nak nevezzük és $a^2 = b^2 = c^2 = -1$, meg is kaptuk: $Q = \{1, -1, i, -i, j, -j, k, -k\}$.

Megtaláltuk hát az összes lehetséges nyolcelemű csoportot, de vajon ezek tényleg különbözőek?

Legjobban a másodrendű elemek számával tudjuk belátni, hogy ezek a csoportok nem izomorfak. A kommutatív csoportok között C_8-ban egy másodrendű elem van, $C_4 \times C_2$-ben három, míg a $C_2 \times C_2 \times C_2$-ben az egységelemet leszámítva mind az, vagyis hét darabot találunk benne.

A nemkommutatív esetekben is nagy segítséget nyújtanak az elemrendek, mivel D_4-ben öt darab, Q-ban pedig egy darab másodrendű elem van.

C_8	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$
$C_4 \times C_2$	$\{1, a, a^2, a^3\} \times \{1, b, \}$
$C_2 \times C_2 \times C_2$	$\{1, a\} \times \{1, b\} \times \{1, c\}$
D_4	$\{1, f, f^2, f^3, t, tf, tf^2, tf^3\}$
Q	$\{1, -1, i, -i, j, -j, k, -k\}$

A nyolcelemű csoportok

Habár logikailag itt kéne következniük a tizenhat elemű csoportoknak, bonyolultsága miatt jobbnak láttuk egy külön fejezetben vizsgálni. Rögtön neki is látunk!

6. fejezet

Tizenhat elemű csoportok

Ahogy azt már korábban is említettük, a kettő hatványaival úgymond egy új területre tévedtünk. A négyelemű csoportokból kettő darab volt, a nyolceleműből öt, de a tizenhat eleműből már tizennégy darab lesz. Ez az eddigiekhez képest nagy ugrásnak, számít és a teljeskörű vizsgálata is sokkal hosszabb és bonyolultabb lenne, mint amit mi most megmutatunk. A hirtelen növekedés oka, hogy a kettő hatványoknál lényegesen több lehetséges csoportot kapunk. Vegyük például a 32 elemű csoportot, melyekből 51 darab van izomorfia erejéig, ami több, mint a 100 alatti rendű csoportok közül bármelyiknek, ami nem kettő hatvány.

Az érdekesség kedvéért egy kis táblázatban szemléltetjük a növekedést.

Elemszám	Izomorfia típus
64	267
128	2328
256	56092
512	10494213
1024	49487365422

2^n *elemszámú csoportok izomorfiaosztályainak száma*

Az eddigiektől eltérően nem vezetünk le mindent, csupán konstrukció szinten mutatjuk be a tizenhat elemű csoportokat. A "csupán" szó használata ne vezesse félre, így is sok munkát fog igényelni az osztályozás és részletesen bemutatjuk a lehetséges csoportokat. Ha valaki esetleg mélyebben is szeretné beleásni magát a témába, ajánlom figyelmébe az Irodalomjegyzékben említett forrásokat.

Neki is állunk a kidolgozásnak. Kezdetben szokásunkhoz híven felsoroljuk a lehetséges csoportokat, mely már önmagában előrevetíti a feladatunk nagyságát:

- C_{16}
- $C_8 \times C_2$
- $C_4 \times C_4$
- $C_4 \times C_2^2$
- C_2^4
- $D_4 \times C_2$
- $C_2^2 \rtimes C_4$
- $Q \times C_2$
- $C_4 \rtimes C_4$
- $SU(2)$
- M_{16}
- Dic_4
- SD_2
- D_8

A felsorolásban a sok ismerős csoport mellett már vannak számunkra eddig ismeretlenek is, melyeket a szakirodalomban is fellelhető generátorokkal és definiáló relációkkal a fejezet végén, egy táblázatban fogunk bemutatni.

Az eddigiekhez képest annyi lesz a változás, hogy nem megyünk bele a bizonyítások teljes mélységeibe, és nem térünk ki minden részletre. Arra, hogy ezek a csoportok miért nem izomorfak egymással, már gyakorlatilag az osztályozás közben sor kerül.

Ez azonban még odébb van, kezdjük az osztályozással, aminek az alapja nem lesz más, mint a csoport centrumának elemszáma. Vágjunk is bele!

Lagrange tétele alapján nem nehéz végiggondolni, hogy hány elemű lehet a centrum. Mivel a 16 osztóit kell sorra vennünk, így az 1, 2, 4, 8 és 16 jöhetnek szóba.

1. $|Z(G)| = 16$

Az egyszerűség kedvéért tekintsük az eseteket fordított sorrendben, vagyis kezdjük a $|Z(G)| = 16$ esettel! Itt nincs sok teendőnk, ekkor ugyanis a csoportunk mindig kommutatív lesz. Ebből az esetből kapjuk meg a C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2^2$ és C_2^4 csoportokat, melyek felbontása a véges Abel-csoportok alaptétele miatt egyértelmű.

2. $|Z(G)| = 8$

A következő esetet is hamar magunk mögött fogjuk tudni, de az már egy picit trükkösebb lesz. Ha G centruma nyolcelemű lenne, vagyis $|Z(G)| = 8$, akkor a $Z(G)$ szerinti faktorcsoport rendje $|G/Z(G)| = |G|/|Z(G)| = 16/8 = 2$ lenne. Azt már tudjuk a , hogyha a faktorcsoport rendje kettő, akkor az ciklikus. Mivel egy csoport akkor és csak akkor ciklikus, ha a centruma megegyezik magával a csoporttal, így a centrum rendje tizenhat kéne hogy legyen, nem pedig nyolc. Itt ellentmondásra jutottunk, így tehát nincs olyan tizenhat elemű csoport, ahol a centrum nyolcelemű. Jegyezzük meg ezt az ellentmondást, mert a későbbiekben is még többször elő fog kerülni.

Mondhatni elértünk a "könnyű rész" végére, most evezzünk át bonyolultabb vizekre!

Jelöljük a továbbiakban $G_1, G_2, \ldots G_i$-vel a G csoport azon nyolcelemű részcsoportjait, melyre $Z(G) \subseteq G_i$. Most nézzük a következő esetet!

3. $|Z(G)| = 4$

Továbbra is haladjunk visszafelé a $Z(G)$ lehetséges elemszámai alapján, vagyis következőnek tekintsük azt, ahol a centrum négyelemű!

Ha a centrumunk négyelemű, akkor $|G/Z(G)| = |G|/|Z(G)| = 16/4 = 4$. Ekkor két különböző alesetet kapunk aszerint, hogy milyen alakú a faktorcsoport. Már megmutattuk, hogyha egy csoport rendje négy, akkor izomorfnak kell lennie vagy C_4-gyel vagy V-vel, vagyis a Klein csoporttal.

Ha $G/Z(G) \cong C_4$, akkor a faktorcsoport ciklikus, ami ahogy már láthattuk azt eredményezi, hogy a centrum rendje tizenhat és nem négy (2.14.).

Megkaptuk tehát, hogy a faktorcsoportnak muszáj izomorfnak lennie $C_2 \times C_2$-vel.

Vegyük észre, hogy G_i csoportok jelen esetben kommutatívak, hiszen

$Z(G) \subseteq G_i$ miatt $Z(G) \subseteq Z(G_i)$, és így $|G_i/Z(G_i)| \leq 2$, tehát a faktorcsoportja ciklikus és így egyelemű.

Mivel a négyelemű centrumunk kétféleképpen nézhet ki, megbontjuk ezt a pontot.

3.1. $Z(G) \cong C_2 \times C_2$

Ha a centrum $C_2 \times C_2$-vel izomorf, a fent említett G_i részcsoportból pontosan három darab van, hiszen a $C_2 \times C_2$-nek három darab másodrendű részcsoportja van, melyek meghatároznak egy-egy ilyen nyolcelemű részcsoportot. Ezen G_i-k lehetséges típusai közül csak $C_4 \times C_2$ és $C_2 \times C_2 \times C_2$ jöhetnek szóba (mivel C_8-nak nincsen $C_2 \times C_2$-vel izomorf részcsoportja).

Itt több lehetséges kombinációt is kapunk a G_i-k felépítésére, melyekből nem fog mind eredményre vezetni. Például az az eset, ahol mindhárom G_i $C_2 \times C_2 \times C_2$ alakú biztosan rossz lesz, hiszen akkor minden nem egységelem másodrendű lenne, ekkor pedig a csoport kommutatív lenne. Máris találkoztunk az előző problémánkkal, hogy ebben az esetben a centrumnak tizenhat eleműnek kéne lennie.

Más felosztásokból születnek meg a jó csoportok, melyeket most fel is sorolunk:

- $D_4 \times C_2$, amit akkor kapunk meg, ha a G_i-k közül kettő izomorf $C_2 \times C_2 \times C_2$-vel, egy pedig $C_4 \times C_2$-vel
- $C_2^2 \rtimes C_4$, amit úgy kapunk, ha a G_i-k közül egy izomorf $C_2 \times C_2 \times C_2$-vel, kettő pedig $C_4 \times C_2$-vel
- $Q \times C_2$ és $C_4 \rtimes C_4$, ha mind a három G_i izomorf $C_4 \times C_2$-vel

Így tehát megkaptunk még négy csoportot a tizennégyből. Mehetünk is tovább a következő pontra, még mindig a négyelemű centrumoknál, de ezúttal $Z(G) \cong C_4$.

3.2. $Z(G) \cong C_4$

Hasonlóan indulunk neki ennek az esetnek is, mint az előzőnek. Tudjuk, hogy minden G_i részcsoportnak van C_4-gyel izomorf részcsoportja, így most a $C_2 \times C_2 \times C_2$ marad ki a sorból, mint lehetséges G_i, mivel neki nincsen C_4-gyel izomorf részcsoportja.

Itt sem kapunk minden lehetséges esetből tizenhat elemű csoportot:

- SU_2, amennyiben mindhárom G_i részcsoport $C_4 \times C_2$-vel izomorf

- M_{16}, amennyiben a G_i-k közül kettő izomorf C_8-cal, egy pedig $C_4 \times C_2$-vel

Ezt a két csoportoknak is a fejezet végén lévő táblázatban mutatjuk be generátorok és definiáló relációk segítségével. Ezzel a két csoporttal együtt már tizenegy csoportnál tartunk a tizennégyből. Lássuk tovább!

4. $|Z(G)| = 2$

Amikor a centrum rendje kettő, akkor a centrum szerinti faktorcsoport rendje $|G/Z(G)| = |G|/|Z(G)| = 16/2 = 8$ lesz, és izomorf a korábban már bemutatott nyolcelemű csoportok egyikével. Tudjuk azt is, hogy a centrum csakis a C_2 lehet.

Végigmenve mind az öt lehetséges nyolcelemű csoporton meg lehet mutatni, hogy csak akkor kapunk jó konstrukciót tizenhat elemű csoportra, ha $G/Z(G) \cong D_4$.

Vagyis a $G/Z(G) \cong C_8$, $G/Z(G) \cong C_4 \times C_2$, $G/Z(G) \cong C_2 \times C_2 \times C_2$ és a $G/Z(G) \cong Q$ esetek egyike sem lesz megfelelő.

Azt például már láttuk, hogy a centrum szerinti faktorcsoport nem lehet ciklikus, így például a $G/Z(G) \ncong C_8$ (2.14.).

4.1. $G/Z(G) \cong D_4$

Tekintsük a már az előbb említett esetet, melyben D_4 a faktorcsoport. Itt is különböző eseteket figyelhetünk meg aszerint, hogy milyen alakúak a G_i részcsoportok.

Jelen esetben az egyik $G_i \cong C_8$ a maradék két G_i izomorf vagy Q-val vagy D_4-gyel.

Lássuk azokat az eseteket, melyek tizenhat elemű csoportot adnak!

- Dic_4, abban az esetben, amikor mindkét nem kommutatív G_i izomorf Q-val
- SD_2, amikor az egyik G_i izomorf Q-val a másik pedig D_4-gyel
- D_8 pedig amikor mindkét nem kommutatív G_i izomorf D_4-gyel

Ugyan a struktúránkat követve még hátra lenne az az eset, ahol $|Z(G)| = 1$, de a 2.14. Tétel miatt tudjuk, hogy ez nem lehetséges.

Ezzel a tizenhat elemű csoportok végére is értünk, mikor is meg szeretnénk mutatni, hogy a kapott csoportok miért nem izomorfak. Szerencsére az osztályozást úgy végeztük el, hogy erre szinte nincs is szükség, hiszen invariánsok alapján végeztük a vizsgálatot. Így szinte minden esetben már a fentiekben láthattuk, hogy nem izomorfak egymással. A maradék pár esetben, ahol nem egyértelmű a "nem izomorfia", finomabb analízisre lenne szükség ennek belátására. Jó módszerek lehetnek például a bizonyos rendű elemek száma vagy a kommutátor részcsoport alaposabb megvizsgálása.

Az osztályozás arra is alkalmas lehet, hogy belássuk más izomorfia típus nem létezik ezen a tizennégyen kívül, de mi erre most nem térünk ki.

Most szokásunkhoz híven egy táblázatban összefoglaljuk az eredményt. Annyiban változtatjuk meg ennek a felépítését, hogy a korábban említett módon definiáló relációkkal mutatjuk meg a csoportok szerkezetét, nem pedig az elemek felsorolásával. Szintén egy újdonság lesz, hogy mivel az osztályozást a centrum elemszáma alapján végeztük, azt is feltüntetjük a táblázat utolsó oszlopában.

Csupán a táblázat tanulmányozásával is sokat megtudhatunk a csoportokról. Lássuk!

A G csoport	Definiáló reláció	Centrum
C_{16}	$\{a^\alpha : a^{16} = e\}$	G
$C_8 \times C_2$	$\{a^\alpha b^\beta : a^8 = b^2 = e, ab = ba\}$	G
$C_4 \times C_4$	$\{a^\alpha b^\beta : a^4 = b^4 = e, ab = ba\}$	G
$C_4 \times C_2 \times C_2$	$\{a^\alpha b^\beta c^\gamma : a^4 = b^2 = c^2 = e, ab = ba,$ $ac = ca, bc = cb\}$	G
$C_2 \times C_2 \times C_2 \times C_2$	$\{a^\alpha b^\beta c^\gamma d^\delta : a^4 = b^2 = c^2 = d^2 = e, ab = ba,$ $ac = ca, bc = cb, ad = da, bd = db, cd = dc\}$	G
$D_4 \times C_2$	$\{a^\alpha b^\beta c^\gamma : a^4 = b^2 = c^2 = e, ba = a^{-1}b,$ $ac = ca, bc = cb\}$	$C_2 \times C_2$
$C_2^2 \rtimes C_4$	$\{a^\alpha b^\beta : a^4 = b^4 = e, ab = b^{-1}\}$	$C_2 \times C_2$
$Q \times C_2$	$\{a^\alpha b^\beta c^\gamma : a^2 = b^2, a^4 = b^4 = c^2 = e,$ $ab = b^{-1}, ac = ca, bc = cb\}$	$C_2 \times C_2$
$C_4 \rtimes C_4$	$\{a^\alpha b^\beta : a^4 = b^4 = e, ab = b^{-1}a\}$	$C_2 \times C_2$
$SU(2)$	$\{a^\alpha b^\beta c^\gamma : a^4 = b^2 = c^2 = e, ab = ba,$ $ac = ca, cb = a^2bc\}$	C_4
Dic_4	$\{a^\alpha b^\beta : a^4 = b^2 a^8 = b^4 = e, ba = a^{-1}b\}$	C_2
SD_2	$\{a^\alpha b^\beta : a^8 = b^2 = e, ba = a^3b\}$	C_2
D_8	$\{a^\alpha b^\beta : a^8 = b^2 = e, ba = a^{-1}b\}$	C_2

A tizenhat elemű csoportok

Irodalomjegyzék

(1) Kiss Emil: Bevezetés az absztrakt algebrába

(2) David Clausen: Classifying All Groups of Order 16
http://buzzard.ups.edu/courses/2012spring/projects/clausen-groups-16-ups-434-2012.pdf

(3) Marcel Wild: The Groups of Order Sixteen Made Easy
The American Mathematical Monthly, 112.1:20?31, 2005.
https : //www.researchgate.net/publication/259147732_The_Groups_of_Order_Sixteen_Made_Easy

(4) http : //www.icm.tu−bs.de/ag_algebra/software/small/number.html