1. Feloldható csoportok

Csoportok bővítése.

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: *bővítés*. N és G/N már kisebb csoport, így egyszerűbb szerkezetű. Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk. Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Nem egyértelmű!

Példa
$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
Tehát ugyanazokat az egyszerűeket kapjuk ($\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$), mégis $\mathbb{Z}_6^+$ és S_3 nem izomorfak.

Ennek ellenére a „G-be bezárt egyszerű csoportok” listája fontos információ minden csoportról.

Feloldható csoportok.

Meseszerű definíció (precízen lásd 4.13.5. Definíció)
Feloldható: bővítéssel összerakható prímrendű ciklikusakból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$, és itt A_5 egyszerű, de nem prímrendű.

A G-be „bezárt” egyszerű csoportok listája egyértelmű (mindegy, hogyan bontjuk le): Jordan–Hölder-tétel (4.13.3).

Feloldhatóság és gyökképlet.

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta a szimmetriacsoportját. Belátta, hogy ez a csoport pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni a négy alapművelet és gyökvonás segítségével.

Lásd Kiss-jegyzet, 6.9. szakasz. Részletek: következő félév.

6.6.15. Feladat (NB)
$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5. Ezért ennek a polinomnak a gyökei nem gyökkifejezések.

$x^5 + 3x^4 - 4x^3 - 5x^2 + x + 1$ Galois-csoportja D_5, feloldható. Ezért ennek a polinomnak a gyökei gyökkifejezések.

2. A véges egyszerű csoportok osztályozása

Prímhatványrendű csoportok.

Cauchy, *Sylow*, 1840–80: prímhatványrendű csoportok.

Lásd Kiss-jegyzet, 4.11 szakasz.

4.11.5. Következmény (NB)
Ha egy prímhatványrendű csoport egyszerű, akkor az prímrendű ciklikus csoport.

4.13.10. Következmény
Minden prímhatványrendű csoport feloldható.

Mert a lebontáskor keletkező egyszerűek prímhatványrendűek.
Jelentősége a *geometriai szerkeszthetőség* elméletében (következő félév).

A Mathieu-csoportok.

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek
Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: *Steiner-rendszer*. Lényegében csak egyféleképpen lehet megcsinálni.

M_{24} ennek a szimmetriacsoportja. M_{23} ebben egy pont stabilizátora, M_{22} az M_{23}-ban stabilizátor.

Burnside kétprímes tétele.

Burnside, *Frobenius*: áttörés a századfordulón.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: *reprezentációelmélet*.

4.13.11. Burnside „kétprímes" tétele
Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Szellemes bizonyítás, az elmélet felépítésével együtt 30 oldal.

Következmény
Ha $|G| = p^a q^b$ (p, q prímek), akkor G feloldható.

Páratlan rendű csoportok.

Suzuki, *Feit*, *Thompson*: 1963. Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel
Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Számos elméletet kellett kidolgozni hozzá. Nagyon nehéz bizonyítás, körülbelül 250 oldal. Használja a reprezentációelméletet is.

Következmény
Minden páratlan rendű véges csoport feloldható.

A klasszifikáció.

Sok matematikus összefogásával, 1982-re sikerült megtalálni az összes *véges egyszerű csoportot*.

Az emberiség egyik csúcsteljesítménye, a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja
18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó, mátrixokkal leírható csoportokból áll.
26 *sporadikus* egyszerű csoport: amik nem illenek bele a sorozatokba. Például az öt Mathieu-csoport sporadikus.

Számos alkalmazás az algebrán kívül is.

A Szörnyeteg.

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5. A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a *Szörnyeteg* (Monster).
Felfeldezője *Fisher* és *Griess* (1982). Elemszáma:

$$808\,017\,424\,794\,512\;\;875\,886\,459\,904\,961\,710\,757\,005\,754\;\;368\,000\,000\,000$$

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak, vagy az ősrobbanástól mostanáig eltelt nanoszekundumoknak a száma. Vagyis számítógépben nem fér el például a szorzástáblája.

A véges egyszerű csoportokról további táblázatok találhatók a Kiss-jegyzet T. Függelékében.
Csoportelméleti fogalmak összefoglaló ábrája: *543. oldal*