6 A_5, alternoiva ryhmä ja muita yksinkertaisia ryhmiä

Tutustukaamme ensin ryhmään S_5. Jos käytämme syklinotaatiota, toteamme, että se sisältää syklejä, jotka ovat muotoa (12), (123), (1234), (12345), (12)(34), (123)(45). Kukin syklityyppi määrittää konjugaattiluokan. Jos rajoitamme vain parillisiin sykleihin, niin saamme alternoivan ryhmän A_5

Kuten totesimme edellisessä kappaleessa, ei syklityyppi määritä enää täysin konjugaatioluokkia ryhmässä A_5. Viitossyklien luokka hajoaa kahteen yhtäsuureen osaan.

Taulukko 8: Ryhmän A_5 alkiot

Konjugaatioluokka	1	2	3	4a	4b
edustaja	1	(12)(34)	(123)	(12345)	(13524)
alkion kertaluku	1	2	3	5	5
konjugaattien määrä	1	15	20	12	12
keskittäjän koko	60	4	3	5	5

Tehtävä 36.

1. Kuinka monta nelossykliä on ryhmässä S_5, entä ryhmässä S_n?
2. Kuinka monta alkiota, jonka syklityyppi on (123)(45) on ryhmässä S_5, entä ryhmässä S_n?
3. Osoita, että jos $H \leq S_n$, joko kaikki H:n alkiot ovat parillisia permutaatioita, tai täsmälleen puolet ovat parillisia ja puolet parittomia.

Määritelmä 6.1. Äärellistä ryhmää G kutsutaan yksinkertaiseksi, jos sen ainoat normaalit aliryhmät ovat ryhmä itse ja ykkösalkio.

Esimerkki 6.2.

1. Jokainen syklinen ryhmä C_p, jonka kertaluku on joku alkuluku p, on yksinkertainen.
2. Ryhmä A_4 ei ole yksinkertainen, sillä $V_4 \lhd A_4$.

Pienin epätriviaali esimerkki yksinkertaisesta ryhmästä on A_5. Tämä on erityisen tärkeä myös todistuksessa, että viidennen asteen polynomille ei ole olemassa ratkaisukaavaa. Todistamme hieman laajemmin.

Propositio 6.3. *Alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$.*

Huomautus 6.4. Todistamme myöhemmin, että jos G on yksinkertainen ryhmä ja sen kertaluku on 60, on $G \cong A_5$.

Todistus. Jaamme todistuksen kolmeen osaan.

1. Jos $H \neq 1$ ja $H \lhd A_n$, silloin H sisältää kolmossyklin.

2. H sisältää kaikki kolmossyklit.

3. kolmossyklit virittävät A_n:n.

Tällöin $H = A_n$, joten A_n on yksinkertainen.

1. Olkoon $H \lhd A_n$ ja olkoon h sellainen alkio, jonka kertaluku on joku alkuluku p. Kirjoitamme h:n nyt alkiovieraina sykleinä, joista luonnollisesti jokaisen pituuden pitää olla p. Vaihtoehdot ovat
(a) $o(h) = p \geq 5$ ja jos $h = (a_1, \ldots, a_p) \ldots (r_1, \ldots, r_p)$ voimme kirjoittaa

$$(a_1a_2a_3)h(a_3a_2a_1)h^{-1} = (a_2a_3a_p),$$

joten H sisältää 3-syklin.
(b) Jos $o(h) = 3$ ja $h = (abc)(def)\ldots$ saamme

$$(abcde)h(edcba)h^{-1} = (bcdef) \in H.$$

Jos nyt käytämme kohtaa (a), saamme todistettua, että h sisältää kolmossyklin.
(c) Jos $o(h) = 2$, silloin $h = (ab)(cd)$ tai $h = (ab)(cd)\cdot(ef)(gh)\ldots$ jälkimmäisessä tietysti parillinen määrä transpositioita. Ensimmäisessä tapauksessa

$$(bde)h(edb)h = (aebdc) \in H$$

ja nyt voimme taas löytää (a)-kohdan perusteella kolmossyklin. Toisessa tapauksessa

$$(bde)(h(edb)h = (afc)(bde)$$

ja voimme käyttää (b)-kohtaa kolmossyklin löytämiseen.

Joten jokaisessa tapauksessa H sisältää kolmossyklin.

2. Haluamme todistaa, että jos H:ssa on yksi kolmossykli, ovat kaikki kolmossyklit H:ssa.

Tiedämme, että kaikki kolmossyklit ovat toistensa konjugaatteja ryhmässä S_n ja niitä on ja yhteensä näitä on $\binom{n}{3} \cdot 2$ kappaletta.

Jos $\alpha = (xyz) \in H$ on kolmossykli ryhmässä S_n, saamme α:n keskittäjän koon laskettua rata-vakauttajalauseella. Sillä $|Orb_{S_n}| = |S_n : C_{S_n}(\alpha)| =$

$\frac{n(n-1)(n-2)}{3}$, mistä seuraa, että $|C_{S_n}(\alpha)| = 3(n-3)!$. Olemme kuitenkin kiinnostuneita konjugoinnista ryhmässä A_n, ja laskemalla $C_{A_n}(\alpha)$:n koon, saamme selville α:n konjugaattien määrän.

Nyt $C_{S_n}(\alpha)$ on symmetrisen ryhmän aliryhmä ja yllä olevan tehtävän perusteella, joko kaikki sen alkiot ovat parillisia, tai täsmälleen puolet ovat parillisia ja puolet parittomia. Olemme selvästikin jälkimmäisessä tapauksessa, sillä $(xyz)(lm)$ on pariton permutaatio, joka keskittää α:n. Muista, että $n \geq 5$. Jos tarkastelemme siis parillisia permutaatioita tässä ryhmässä, on niitä $\frac{1}{2}3(n-3)! = |C_{A_n}(\alpha)|$. Rata-vakauttajalauseen perusteella

$$|A_n : C_{A_n}(\alpha)| = \frac{n(n-1)(n-2)}{3},$$

joten kaikki S_n:n kolmossyklit ovat konjugaatteja keskenään. Koska $H \lhd A_n$, tästä seuraa, että kaikki kolmossyklit kuuluvat H:n.

3. Haluamme osoittaa, että kolmossyklit generoivat A_n:n. Jokainen A_n:n alkio voidaan kirjoittaa parillisena määränä transpositioita. Koska $(ab)(bc) = (abc)$ ja $(ab)(cd) = (ab)(bc)(bc)(ad) = (abc)(bcd)$, jokainen A_n:n alkio voidaan kirjoittaa kolmossyklien tulona.

□

Huomautus 6.5. Yksi esseen aihe on etsiä ja esittää joku toinen todistus sille, että A_n on yksinkertainen, kun $n \geq 5$. Tämä voi liittää myös dodekaedrin ja ikosaedrin symmetriaryhmien käsittelyyn. Minulta saa materiaalia ainakin sellaiseen todistukseen, jossa pyöritellään viitossyklejä. Vielä yksi tuntemani todistus käyttää Sylowin teoriaa.

Yksinkertaiset ryhmät ovat kaikkien äärellisten ryhmien rakennuspalikoita samaan tapaan kuin alkuluvut ovat kaikkien luonnollisten lukujen rakennuspalikoita. Rakennuspalikoiden määritelmä kaipaa tarkempaa tutkimista.

Määritelmä 6.6. Äärellisen ryhmän G hajoamisjono (kompositiojono) on ketju

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G,$$

jossa jokainen $G_{i+1} \lhd G_i$ ja G_i/G_{i+1} on yksinkertainen ryhmä. Kutsumme ryhmiä G_i/G_{i+1} hajoamistekijöiksi.

Esimerkki 6.7.

1. Jos G on yksinkertainen.
2. S_3
3. V_4. Tällä on kolme hajoamisjonoa.

Propositio 6.8. *Jokaisella äärellisellä epätriviaalilla ryhmällä on hajoamisjono.*

Todistus. Olkoon $G \neq 1$ äärellinen ryhmä. Jos G on yksinkertainen, on hajoamisjono $1 \leq G$. Tämä on induktion perustapaus.

Oletetaan, että kaikille ryhmillä H, jotka ovat $1 < |H| < |G|$ on olemassa hajoamisjono. Haluamme tietysti nyt konstruoida hajoamisjonon G:lle. Valitaan kaikista G:n aidoista normaaleista aliryhmistä maksimaalinen, ja kutsutaan tätä N:ksi. Tämä siis tarkoittaa, sitä, että jos $N \leq M \leq G$ ja $M \lhd G$, silloin $M = N$ tai $M = G$. Nyt kolmannen isomorfialauseen perusteella G/N on yksinkertainen.

Induktion perusteella, N:llä on hajoamisjono, ja nyt saamme hajoamisjonon G:lle luonnollisella tavalla. □

Tehtävä 37. Olkoon $H_1 \lhd G$ ja $G_1 \lhd G$. Todista, että $H_1G_1 \lhd G$ sekä $H_1 \cap G_1 \lhd G$.

Lause 6.9 (Jordan-Hölderin lause)**.** *Olkoon G äärellinen epätriviaali ryhmä ja olkoot*

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G \tag{2}$$

ja

$$1 = H_m \lhd H_{m-1} \lhd \ldots \lhd H_1 \lhd H_0 = G \tag{3}$$

kaksi G hajoamissarjaa. Silloin $m = n$ ja kummankin sarjan tekijäryhmät ovat samat (emme vaadi samaa järjestystä). Tässä tapauksessa kompositiojonoja kutsutaan isomorfisiksi.

Todistus. Oletetaan, että meille on annettu kaksi jonoa, kuten yllä. Jos $G_1 = H_1$, silloin saamme kaksi kompositiojonoa G_{n-1}:lle

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1$$

ja

$$1 = H_m \lhd H_{m-1} \lhd \ldots \lhd H_1 = G_1.$$

Nyt induktion perusteella, nämä kaksi kompositiojonoa ovat isomorfiset ja siksi G:n kompositiojonot ovat isomorfiset.

Toinen tapaus on, kun $G_1 \neq H_1$. Kompositiojonon määritelmän perusteella tiedämme, että $H_1 \lhd G$ ja $G_1 \lhd G$. Siispä $H_1G_1 \lhd G$ sekä $H_1 \cap G_1 \lhd G$. Todistamme, että $H_1G_1 = G$. Tämä seuraa siitä, että $G_1 \lneq H_1G_1 \leq G$ ja koska G_1 on G:n maksimaalinen normaali aliryhmä. Nyt voimme käyttää toista isomorfialausetta

$$G/H_1 \cong G_1/H_1 \cap G_1$$

ja

$$G/G_1 \cong H_1/H_1 \cap G_1.$$

Olkoon nyt

$$1 = K_l \lhd K_{l-1} \lhd \ldots \lhd K_1 = H_1 \cap G_1$$

kompositiojono ryhmälle $H_1 \cap G_1$. Tämän perusteella saamme kaksi uutta kompositiojonoa ryhmälle G.

$$1 = K_l \lhd K_{l-1} \lhd \ldots K_1 \lhd H_1 \lhd G \tag{4}$$

$$1 = K_l \lhd K_{l-1} \lhd \ldots K_1 \lhd G_1 \lhd G \tag{5}$$

Nyt ensimmäisen osan perusteella (2) $\cong$ (4) ja (3) $\cong$ (5) ja (4) $\cong$ (5), koska niillä on samat kompositiotekijät, vain ensimmäiset kaksi on vaihdettu keskenään. Siksi (2) $\cong$ (3). □

Tehtävä 38. Laske ryhmän S_4 hajoamissarja. Laske ryhmän D_{24} hajoamissarja. Onko näillä samat hajoamistekijät? Entä ryhmällä C_{24}. Mikä on ryhmän S_n hajoamissarja?

Olemme todistaneet, että ryhmä A_5 on yksinkertainen. Seuraava tavoitteemme on todistaa, että pienin kertaluku, jolloin ryhmä on yksinkertainen, on 60 ja että jos ryhmän kertaluku on 60 ja se on yksinkertainen, on ryhmä isomorfinen ryhmän A_5 kanssa. Tärkeä työkalu tässä todistuksessa ovat Sylowin lauseet.

6.1 Sylowin lauseet

Muistamme, että Lagrangen lause ja Cauchyn lause kertoivat ryhmän rakenteesta jotain pelkästään ryhmän kertaluvun perustella. Vielä hieman Cauchyn lausetta tarkempi tämäntyyppinen lause ovat Sylowin lauseet. Sylowin lauseita voidaan käyttää myös yksinkertaisuuden tutkimiseen.

Sylowin lauseet edustavat myös matemaattisessa ajattelussa yleistä lokaali-globaali-periaatetta. Lukuteoriassa alkuluvut palvelevat samaa tarkoitusta. Mitä voimme sanoa ryhmästä, jos keskitymme kuhunkin alkulukuun kerrallaan. Samaan tapaan kuin lukuteoria ratkaisee yhtälöitä $\pmod p$.

Lause 6.10 (Sylow)**.** *Olkoon G äärellinen ryhmä, kertalukua $p^n r$, jossa p ei jaa r:ää. Tällöin*

(i) G sisältää Sylowin p-aliryhmän P, jonka kertaluku on p^n.

(ii) Mitkä tahansa kaksi Sylowin p-aliryhmää ovat keskenään konjugaatteja.

(iii) Sylowin p-aliryhmien lukumäärä n_p, on $n_p \equiv 1 \pmod{p}$ ja jakaa luvun m.

Todistus. Todistamme lauseen ryhmän toimintojen avulla.
(i) Olkoon $\Omega = \{M \subseteq G : |M| = p^n\}$. Määrittelemme G:n toimimaan tässä joukossa oikeanpuolisella kertolaskulla

$$M * g = \{mg : m \in M\}.$$

Tarkista, että tämä on toiminta. Tarkastelemme G-ratoja. Olkoon Σ tällainen. Silloin $\Sigma = \{M, Mg_2, Mg_3 \ldots, Mg_k\}$. Huomaamme, että Σ:n alkiot kattavat koko G:n. Nimittäin, olkoon $m \in M$, jos g on mikä tahansa G:n alkio, voimme kirjoittaa $g = m * m^{-1}g \in Mm^{-1}g \in \Sigma$. Tästä seuraa, että $k \geq r$. Jaamme tarkastelun kahteen tapaukseen.

Tapaus 1. $k = r$. Tässä tapauksessa G on Σ:n alkioiden pistevieras yhdiste. Alkion M vakauttaja ryhmässä G on kertalukua p^n (rata-vakauttajalauseen nojalla), ja koska vakauttaja on aliryhmä, on se väistämättä kertaluvun perusteella myös Sylowin p-aliryhmä.

Päättelemme, että jokainen vastaava G-rata koostuu yksikäsitteisestä Sylowin p-aliryhmästä ja tämän oikeista sivuluokista.

Tapaus 2. $k \neq r$, siispä $k > r$. Koska rata-vakauttajalauseen nojalla $k \mid |G| = p^n r$, tästä seuraa, että $p \mid k$.

Nyt jokainen rata, jonka koko on r sisältää yksikäsitteisen Sylowin aliryhmän, ja kaikkien muiden ratojen koko on jaollinen p:llä. Tästä seuraa

$$|\Omega| = \binom{p^n r}{p^n} = n_p r + \sum_{p \mid |\Sigma|} |\Sigma| \equiv n_p r \mod p.$$

Toisaalta $\binom{p^n r}{p^n} \equiv r \mod p$ (Yllä oleva tulos on voimassa kaikille ryhmille, joiten kertaluku on $p^n r$, joten se ei voi riippua n_p:stä. Syklisessä ryhmässä $C_{p^n r}$ on vain yksi aliryhmä, jonka koko on p^n ja siksi $n_p = 1$. Tämä todistaa kongruenssin) ja koska $p \nmid r$, tästä seuraa $n_p \equiv 1 \mod p$. Erityisesti huomaamme, että Sylowin aliryhmien lukumäärä ei ole nolla.

(ii) Konjugaatio seuraa seuraavasta aputuloksesta, joka osoittaa, että jokainen G:n p-aliryhmä kuuluu johonkin Sylowin p-aliryhmään.

Lemma 6.11. *Jos Q on G:n p-ryhmä ja P on Sylowin p-aliryhmä. Silloin jollekin $g \in G$ pätee $Q \subseteq g^{-1}Pg$.*

Todistus. Toimikoon Q oikeanpuoleisen kertolaskun avulla P:n sivuluokkien joukossa $(G : P)$. Sivuluokkia on m kappaletta, ja sivuluokat hajoavat radoiksi $O_1, \ldots, O_k$, joitten yhteenlaskettu mahtavuus on $|O_1| + \cdots + |O_k| = r$. Rata-vakauttajalauseen perustella, kunkin radan koko jakaa Q:n koon, eli

on joko 1 tai p. Koska $p \nmid r$, kaikki radat eivät voi olla kokoa p, joten tässä Q-toiminnassa on välttämättä rata, jonka mahtavuus on 1, sanokaamme, että tämä on $\{Pg\}$. Mikä tarkoittaa sitä, etta $Pg * Q \subseteq Pg$, mistä seuraa $gQg^{-1} \subseteq P$ ja näin ollen $Q \subseteq g^{-1}Pg$. □

Jos nyt valitsemme Q:n Sylowin p-aliryhmäksi, tulos seuraa.

(iii) Olemme jo todistaneet, että $n_p \equiv 1 \mod p$. Jäljellä on todistaa, että n_p jakaa r:n. Yllä todistimme, että Sylowin aliryhmien joukko muodostaa yhden radan alkion g konjugaatiotoiminnan kautta. Rata-vakauttajalauseen perusteella $n_p \mid |G|$. Koska p ei jaa n_p:tä, tästä seuraa, että n_p jakaa r:n. □

Tarkastelemme seuraavassa pieniä yksinkertaisia ryhmiä Sylowin lauseen avulla. Ensin kuitenkin todistamme hyödyllisen lemman.

Lemma 6.12 (Poincaré)**.** *Olkoon $H \leq G$, ja $|G : H| = n$. Olkoon $K = \cap_{g \in G} g^{-1}Hg$. Silloin $K \lhd G$, ja $K \leq H$ ja kaiken lisäksi*

$$n \mid |G : K| \mid n!$$

Todistus. Olkoon $\Omega =(G : H)$. Kun G toimii näissä sivuluokissa oikealla kertolaskulla, on toiminnan ydin täsmälleen K, sillä jokaisen sivuluokan Hg vakauttaja on $g^{-1}Hg$. Tämän lisäksi K on normaali aliryhmä (koska se on homomorfismin ydin, tai koska se on sulkettu konjugaatiotoiminnan suhteen). Lisäksi $K \leq H$, sillä voimme valita myös alkion 1 konjugoimaan H:ta ja loppu on leikkausta tämän suhteen. Muista, että toiminta indusoi homomorfismin $G \longrightarrow Sym(\Omega)$, joten ensimmäisen isomorfialauseen perusteella G/K on isomorfinen $Sym(\Omega)$:n (transitiivisen) aliryhmän kanssa. Tästä seuraa, että $|G : K \mid \mid n!$. Koska $K \leq H$, saamme myös $n = |G : H| \mid |G : K|$. □

Tehtävä 39. Osoita, että ryhmä, jonka kertaluku on kahden alkuluvun tulo pq, ei ole yksinkertainen. Voit käyttäää tähän Sylowin lauseita. Edelleen päättele, että jos G on yksinkertainen ryhmä, joka ei ole Abelin ryhmä, niin $|G| \geq 60$.

Lause 6.13. *Jos G on yksinkertainen, ja sen kertaluku on 60, on $G \cong A_5$.*

Todistus. Tarkastellaan ryhmää G Sylowin lauseiden avulla. Ensiksikin $60 = 2^2 \cdot 3 \cdot 5$, joten ryhmässä on Sylowin 5-aliryhmä, jonka on generoinut alkio, jonka kertaluku on 5. Cauchyn lauseen perusteella tällainen alkio on olemassa. Sylowin lauseen kolmannen kohdan perusteella Sylowin 5-aliryhmien lukumäärä on $n_5 \equiv 1 \mod 5$. Koska ryhmä on yksinkertainen, on Sylowin 5-aliryhmiä enemmän kuin yksi (Sylowin lauseen toisen kohdan perusteella kaikki Sylowin 5-aliryhmät ovat toistensa konjugaatteja, joten jos niitä on

vain yksi, on se väistämättä normaali, mikä on ristiriidassa yksinkertaisuuden kanssa). Tämän lisäksi $n_5 \mid 12$, joten ainoastaan $n_5 = 6$ on mahdollinen. Olkoon P siis Sylowin 5-aliryhmä ja $\Omega = \{g^{-1}Pg : g \in G\}$. Ymmärrettävästi $|\Omega| = 6$. Ryhmä G toimii joukossa Ω konjutaatiotoiminnalla, joka indusoi kuvauksen $\rho : G \longrightarrow S_6$. Tämä homomorfismi on injektio, sillä G on yksinkertainen. Olkoon $H \leq S_6$ tämän homomorfismin kuva. $H \cong G$ ja siis yksinkertainen. Nyt $H \cap A_6 \lhd H$ (koska leikkaus on aliryhmä, jonka indeksi on kaksi) ja koska H on yksinkertainen ($H \cong G$) on $H \leq A_6$.

Olkoon $\Gamma := cos(A_6 : H)$. Nyt $|\Gamma| = \frac{1}{2}6!/60 = 6$, joten kun A_6 toimii joukossa Γ, saamme homomorfismin $\sigma : A_6 \longrightarrow S_6$. Itseasiassa σ on ryhmän A_6 automorfismi. Ensinnäkin se on injektio, sillä A_6 on yksinkertainen ja sen kuvan pitää olla A_6:n aliryhmä. Homomorfismi σ kuvaa H:n vakauttajan, vakauttajaksi ryhmässä A_6, joka on A_5, joten olemme osoittaneet, että $G \cong H \cong A_5$. □

Tehtävä 40. Jos pidämme tunnettuna lauseen "Jos G on yksinkertainen ja G:n kertaluku on $2^a \cdot 3 \cdot 5$, on $a = 2$ ja $G \cong A_5$", osoita, että jos ryhmä G on yksinkertainen ja sen kertaluku on korkeintaan 300, on ryhmän kertaluku joko 60 tai 168.

Tehtävä 41. Kirjoita essee yksinkertaisesta ryhmästä, jonka kertaluku on 168. Tämä on ryhmä $\mathrm{PSL}_2(7)$.

6.2 Ratkeavat ryhmät

Tärkeä luokka ryhmiä, jotka eivät varmasti ole yksinkertaisia, ovat ratkeavat ryhmät. Niitä käymme tutkimaan seuraavaksi.

Määritelmä 6.14. Kahden alkion $g, h \in G$ vaihdannaistaja on alkio $[g, h] = g^{-1}h^{-1}gh$. Vaihdannaistajien virittämää aliryhmää $G' = [G, G] = \{g^{-1}h^{-1}gh : g, h \in G\}$ kutsutaan vaihdannaistaja-aliryhmäksi. Jos $G' = G$, kutsumme ryhmää G täydelliseksi.

Huomaa, että Abelin ryhmässä pätee aina $[g, h] = 1$, joten jos A on Abelin ryhmä, on $A' = 1$.

Tehtävä 42. Osoita, että kaikille (äärellisille) ryhmille G, vaihdannaistaja-aliryhmä $[G, G]$ on normaali, ja että $G/[G, G]$ on Abelin ryhmä. Edelleen osoita, että G/H on Abelin ryhmä jos ja vain jos $[G, G] \leq H$.

Määritelmä 6.15. Ryhmää $G/[G, G]$ kutsutaan ryhmän G Abelistukseksi.

Määritelmä 6.16. Ryhmää kutsutaan ratkeavaksi, jos se hajoaa ketjuksi aliryhmiä

$$1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G,$$

jossa kaikki G_i/G_{i+1} ovat syklisiä yksinkertaisia ryhmiä (eli niiden kertaluku on alkuluku). Ketju voi olla joko normaali tai alinormaali.

Esimerkki 6.17.

$$1 \lhd C_2 \lhd C_4 \lhd D_8,$$

joten D_8 on ratkeava ryhmä, sillä kaikki tekijäryhmät ovat isomorfisia C_2:n kanssa.

Määritelmä 6.18. Ryhmä G on ratkeava, jos ketju, jossa $G^{(1)} = [G, G]$ ja $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ päättyy triviaaliin aliryhmään. Kutsumme tätä ketjua vaihdannaistajajonoksi. Pienin n, jolle tämä $G^{(n)} = 1$ on nimeltään ryhmän G vaihdannaistajapituus.

Myöhemmin todistamme, että tämä on yhtäpitävä ensimmäisen määritelmän kanssa.

Lemma 6.19. *Kaikille ryhmille G, on $G^{(k)} \lhd G$ jokaiselle k.*

Todistus. Induktio k:n suhteen. Jos $k = 0$, silloin $G \lhd G$, mikä on selvästi totta. Oletetaan, että $G^{(k)} \lhd G$ ja tarkastellaan $G^{(k+1)}$:n virittäjiä. Virittäjät ovat määritelmän mukaan muotoa $[g, h]$, jossa $g, h \in G^{(k)}$. Nyt jos $x \in G$, silloin $[g, h]^x = [g^x, h^x] \in G^{(k+1)}$, sillä $g^x, h^x \in G^{(k)}$, koska $G^{(k)} \lhd G$. Tästä seuraa, että $G^{(k+1)} \lhd G$ □

Tehtävä 43. Osoita, että seuraavat ryhmät ovat ratkeavia.

1. S_3 laskemalla vaihdannaistajat ja vaihdannaistajajono.

2. S_4 konstruoimalla alinormaali sarja, jonka tekijäryhmät ovat on Abelin ryhmiä tekijäryhmät.

Osoita, että ryhmä S_n ei ole ratkeava, kun $n \geq 5$.

Tehtävä 44. Osoita, että jos G on ratkeava, on jokainen $H \leq G$ ratkeava. Ja edelleen, jos $N \lhd G$, silloin G/N on ratkeava. (Vinkki: tekijäryhmän kohdalla todista, että $(G/N)^{(k)} = G^k N/N$, tarkastelemalla minkä muotoisia alkoita kummallakin puolella on.)

Ratkeavat ryhmät on ensimmäinen ryhmäluokka, joka on suljettu, niin laajennusten kuin aliryhmienkin suhteen.

Lause 6.20. *Olkoon G ryhmä ja $N \lhd G$. Silloin G on ratkeava jos ja vain jos sekä N että G/N ovat ratkeavia.*

Todistus. Jos G on ratkeava, ylläolevasta tehtävästä seuraa, että $N \lhd G$ ja G/N ovat ratkeavia. Olkoon N:n vaihdannaistajapituus k ja G/N:n vaihdannaistajapituus l. Silloin edellisen tehtävän perusteella $(G/N)^{(l)} = G^{(l)}N/N = N/N$, jälkimmäinen yhtäsuuruus ratkeavuuden perusteella, sillä N/N on ryhmän G/N triviaali aliryhmä. Tästä seuraa ensin $G^{(l)}N = N$ ja edelleen, että $G^{(l)} \leq N$. Nyt aliryhmän perusteella $G^{(l+1} \leq N'$ ja induktiivisesti edeten $G^{(l+k)} \leq N^{(k)} = 1$, koska N oli ratkeava ja sen vaihdannaistajapituus oli k. Olemme siis todistaneet, että G on ratkeava ja sen vaihdannaistajapituus on $l + k$. □

Huomaa, että jos sekä N että G/N ovat Abelin ryhmiä, ryhmä G on ratkeava (toisinaan sitä kutsutaan myös meta-abelin ryhmäksi), mutta ei välttämättä Abelinen. Abelin ryhmät eivät siis ole suljettu ryhmäluokka.

Tehtävä 45. Osoita, että $G \times H$ on ratkeava silloin, kun G ja H ovat ratkeavia.

Nimitys ratkeava ryhmä tulee siitä, että alunperin ryhmäteoria syntyi yhtälön ratkaisukaavojen etsinnästä. Viidennen asteen yhtälölle ei ole ratkaisukaavaa, ja se johtuu siitä, että ryhmä A_5 on yksinkertainen, eikä siis ratkeava – kuten ei myöskään tällä perusteella S_5. Nimittäin, polynomiyhtälö ratkeaa radikaalien avulla täsmälleen silloin kun sen yhtälöön liitetty Galois'n ryhmä on ratkeava.

Tehtävä 46. Kirjoita essee ryhmän ratkeavuuden yhteydestä yhtälöitten ratkeavuuteen ratkaisukaavojen avulla. Esseen tarkoituksena on pintapuolisesti käydä läpi Galois'n teorian pääpiirteet. Joitain todistuksia ja teknisyyksiä voi ohittaa. Voit kysyä näistä tarkemmin minulta.

6.3 Äärellisten yksinkertaisten ryhmien luokittelu

Olemme tarkastelleet ryhmiä A_n, ja osoitimme niiden yksinkertaisuuden, kun $n \geq 6$. Alternoivien ryhmien perhe on yksi esimerkki yksinkertaisista äärellisistä ryhmistä. Yksi ryhmäteorian suurimpia saavutuksia 1900-luvulla oli äärellisten yksinkertaisten ryhmien luokittelu. Nämä ovat Jordan-Hölderin lauseen perusteella kaikkien äärellisten ryhmien rakennuspalikoita.

Yksi lopullisen luokitteluhankkeen liikkeellesaattajista oli Feitin ja Thompsonin kuuluisa parittoman kertaluvun lause (the odd order theorem), joka on huima yleistys klassiselle Burnsiden lauseelle.

Lause 6.21 (Burnside)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on $p^a q^b$. Silloin G on ratkeava.*

Lause 6.22 (Feit-Thompson)**.** *Paritonta kertalukua oleva äärellinen ryhmä on ratkeava.*

Tässä tapauksessa siis ryhmän kertaluku jo määrittelee, milloin ryhmä on ratkeava, eikä siis taatusti yksinkertainen. Tästä seuraa helposti.

Korollaari 6.23. *Äärellisen yksinkertaisen ryhmän kertaluku on jaollinen kahdella, lukuunottamatta yksinkertaisia Abelin ryhmiä.*

Olemme jo moneen kertaan itsekin havainneet, että jos ryhmän kertaluku on parillinen, sisältää ryhmä alkion, jonka kertaluku on kaksi, eli involuution. Tämä havainto on tärkeä yksinkertaisten ryhmien luokittelussakin.

Luokittelussa on lisäksi neljä muuta ääretöntä perhettä, jotka kaikki kuuluvat yksinkertaisiin Lien tyypin ryhmiin. Näitä ovat matriisiryhmät projektiivinen spesiaalinen lineaariryhmä, unitaariset, symplektiset ja ortogonaaliset transformaatiot äärellisen kunnan ylitse. Näiden lisäksi on myös poikkeukselliset Lien ryhmät ovat G_2, F_4, E_6, E_7, ja E_8, jotka eivät siis ole äärettömien perheitten jäseniä.

Näiden lisäksi on 26 sporadista yksinkertaista ryhmää. Ensimmäiset niistä olivat viisi Mathieun ryhmää, jotka löysi Emile Mathieu 1860-luvulla. Loput 21 ryhmää löydettiin 1965-1975. Uusien äärellisten yksinkertaisten ryhmien löytämisestä käytiin kovaa kilpailua. Yksi tärkeimmistä matemaatikoista alalla on John Conway. Hänen mukaansa on nimetty Conwayn ryhmät. Suurimman kertaluvun yksinkertainen ryhmä on hirviöryhmä. Se sisältää 20 muuta sporadista ryhmää.

Tehtävä 47. Kirjoita essee joko symplektisistä, ortogonaalisista tai unitaarisista ryhmistä.

Vaikka äärellisistä yksinkertaiset ryhmät luokiteltiinkin jo viimeistään 1980-luvulla, ei yksinkertaisten ryhmien tutkimus tähän loppunut. Ne tuottavat edelleen uutta tutkimusta. Tässä esimerkiksi helposti ymmärrettävä, mutta vaikea lause tältä vuodelta.

Muista, että ryhmän G vaihdannaistaja-aliryhmä on $[G, G]$. Kutsumme ryhmää täydelliseksi, jos pätee $G = [G, G]$. Ennen kaikkea huomaamme, että täydelliset ryhmät eivät ole ratkeavia, koska niiden vaihdannaistajasarja jumiutuu heti ensimmäiseen askeleeseen, eikä siis koskaan saavuta triviaalia ryhmää. Seuraava uusi tulos kertoo jotain äärellisistä yksinkertaisista ryhmistä.

Oren konjektuuri (1960-luvulta).

Lause 6.24 (Liebeck, O'Brien, Shalev, Tiep, 2008)**.** *Jokaisen epäkommutatiivisen äärellisen yksinkertaisen ryhmän jokainen alkio on vaihdannaistaja.*

Yksinkertaisten äärellisten ryhmien luokittelu (Classification of finite simple groups CFSG) on nykyään tärkeä työkalu matemaatikoille. Jos haluaa todistaa jonkun väitteen ryhmäteoriasta, usein jossain vaiheessa todistusta pitää käydä läpi, onko lause totta yksinkertaisille äärellisille ryhmille.