Symmetristen ja alternoivien ryhmien yksinkertaisuus ja ratkeavuus

Pro gradu
Tuomo Holma
2379771
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2018

Sisältö

Johdanto

Tutkielman pääaiheena on symmetristen ja alternoivien ryhmien yksinkertaisuuden ja ratkeavuuden tarkastelu.

Ensimmäinen luku käsittelee permutaatioita. Permutaatiot ovat sellaisia bijektiivisiä kuvauksia, joiden lähtö- ja maalijoukot ovat samat. Heti työn alussa määritellään myös permutaatioista koostuva symmetrinen ryhmä, joka on tässä työssä erittäin keskeisessä roolissa. Luvussa esitellään melko laajasti permutaatioiden eri ominaisuuksia, joita tarvitaan myöhemmin käsiteltäessä symmetristen- ja alternoivien ryhmien yksinkertaisuutta ja ratkeavuutta. Ensimmäisen ja toisen luvun lähteinä on käytetty luentomonistetta [1] ja kirjaa [2].

Toisessa luvussa palautellaan mieliin ryhmiin liittyviä käsitteitä. Lisäksi siinä otetaan esiin ryhmiin liittyviä tuloksia niiltä osin, kuin on tarpeen ryhmien yksinkertaisuuden ja ratkeavuuden tarkastelussa. Luvun 2 lopussa määritellään yksinkertainen ryhmä ja tutkitaan symmetristen ryhmien yksinkertaisuutta. Yksinkertaiset ryhmät ovat sellaisia, joilla on vain triviaalit normaalit aliryhmät.

Kolmannessa luvussa päästään alternoiviin ryhmiin. Luvun alussa määritellään tämä ryhmä, joka siis koostuu kaikista parillisista permutaatioista. Lisäksi tutkitaan alternoivien ryhmien yksinkertaisuutta. Ennen yksinkertaisuuden tarkastelua on kuitenkin todistettava muutamia alternoiviin ryhmiin liittyviä tuloksia. Kolmannessa luvussa on käytetty pääasiallisena lähteenä kirjaa [2]. Lemman 3.7 todistukseen on kuitenkin otettu vinkkejä myös kirjasta [3].

Neljännessä luvussa määritellään ratkeava ryhmä. Ratkeava ryhmä on sellainen ryhmä, jolla on olemassa kaksi ehtoa täyttävä aliryhmien ketju. Ensinnäkin jokaisen aliryhmän on oltava aliryhmien ketjussa edellisenä esiintyvän ryhmän normaali aliryhmä. Lisäksi tässä ketjussa peräkkäisistä ryhmistä muodostettujen tekijäryhmien kertalukujen tulee olla alkulukuja. Ratkeavuuden määrittelyn jälkeen tutkitaan alternoivien- ja symmetristen ryhmien ratkeavuutta. Neljännen luvun lähteenä on käytetty kirjaa [2].

1 Permutaatiot

Tässä luvussa tutustutaan permutaatioihin ja niihin liittyviin perustuloksiin. Lauseet ja lemmat, jotka jätetään tässä yhteydessä todistamatta, on todistettu kurssilla Permutaatiot, kunnat ja Galois'n teoria.

Määritelmä 1.1. Olkoon $X = \{1, 2, ..., n\}$. Jos $\alpha : X \to X$ on bijektio, niin α on ***permutaatio*** joukon X suhteen.

Määritelmä 1.2. Joukon X kaikkien permutaatioiden muodostamaa joukkoa kutsutaan ***symmetriseksi ryhmäksi*** S_X. Kun $X = \{1, 2, ..., n\}$, ryhmästä S_X käytetään usein merkintää S_n ja sitä kutsutaan ***astetta n olevaksi symmetriseksi ryhmäksi***.

Huomautus 1.3. Symmetrisen ryhmän S_n kertaluku on $n!$.

Esimerkki 1.4. Olkoot $X = \{1, 2, 3\}$ ja α permutaatio joukon X suhteen. Jos $\alpha \in S_3$ ja $\alpha(1) = 2$, $\alpha(2) = 3$ ja $\alpha(3) = 1$, niin merkitään

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Jos lisäksi

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3,$$

niin

$$\alpha \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Toisaalta

$$\sigma \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Näin ollen $\alpha \circ \sigma \neq \sigma \circ \alpha$. Voidaan siis päätellä, että permutaatiot eivät kommutoi symmetrisessä ryhmässä S_3.

Määritelmä 1.5. Olkoot $i_1, i_2, ..., i_r \in \{1, 2, ..., n\}$ eri alkioita. Jos permutaatio $\alpha \in S_n$ säilyttää kaikki muut alkiot ja

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, ..., \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

niin tällöin permutaatiota α kutsutaan ***r-sykliksi*** tai r:n pituiseksi sykliksi ja sitä merkitään

$$\alpha = (i_1\ i_2\ ...\ i_r).$$

Huomautus 1.6. 1. $e = (1)$ on 1-sykli, joka pitää kaikki alkiot paikoillaan.

2. 2-sykli $(j\ k)$ vaihtaa alkioiden j ja k paikkaa keskenään ja säilyttää kaikki muut alkiot. 2-sykliä kutsutaan ***transpoosiksi***.

Esimerkki 1.7. Edellä esitelty permutaatioiden kaksirivinen esitystapa ei ole kätevin mahdollinen. Mikä tahansa permutaatio voidaankin ilmoittaa syklien tulona. Olkoon esimerkiksi $\alpha \in S_9$,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}.$$

Permutaation syklimuotoon saattaminen aloitetaan katsomalla mihin alkio 1 kuvautuu. Koska permutaatio α kuvaa alkion 1 alkiolle 6 ja alkio 6 kuvautuu edelleen alkiolle 1, on permutaation α sykliesityksen ensimmäinen sykli (1 6). Seuraavaksi katsotaan mihin alkio 2 kuvautuu ja näin jatketaan kunnes jokainen alkio on ilmaantunut johonkin sykliin. Permutaation α esitykseksi syklien tulona saadaan:

$$\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5).$$

Usein 1-syklit jätetään kuitenkin merkitsemättä. Tällöin on kuitenkin hyvä mainita symmetrinen ryhmä, johon kyseinen permutaatio kuuluu;

$$\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9) \in S_9.$$

Määritelmä 1.8. Permutaatiot/syklit $\alpha, \beta \in S_n$ ovat ***erillisiä***, mikäli ne eivät siirrä yhtään samaa alkiota. Toisin sanoen jos $\alpha(i) \neq i$, niin $\beta(i) = i$ ja jos $\beta(j) \neq j$, niin $\alpha(j) = j$. Joukko permutaatioita/syklejä $\beta_1, ..., \beta_t$ on erillisiä, jos joukon permutaatiot/syklit ovat pareittain erillisiä.

Esimerkki 1.9. Permutaatiot

$$(1\ 2\ 6\ 3)(4\ 12),\ (11\ 5\ 7) \in S_{12}$$

ovat erillisiä.

Lemma 1.10. *Erilliset permutaatiot $\alpha, \beta \in S_n$ kommutoivat keskenään.*

Lause 1.11. *Jokainen permutaatio $\alpha \in S_n$ on joko sykli tai se voidaan esittää erillisten syklien tulona.*

Muuttamalla permutaatio kaksirivisestä esitystavasta syklimuotoon esimerkissä 1.7 esitetyllä tavalla, syntyy automaattisesti esitys erillisten syklien tulona. Syklien tulona esitetty permutaatio saadaan erillisten syklien tuloksi niin ikään helposti. Esimerkiksi transpoosien tulo

$$(1\ 7)(1\ 4)(3\ 9)(3\ 5)(3\ 11)(3\ 12)(6\ 10)$$

on erillisten syklien tulona ilmaistuna

$$(1\ 4\ 7)(3\ 12\ 11\ 5\ 9)(6\ 10) \in S_{12}.$$

Muutoksessa jokainen alkio käydään erikseen läpi aloittaen aina oikeanpuoleisimmasta syklistä, joka siirtää kyseistä alkiota ja edeten siitä vasemmalle. Tässä esimerkissä transpoosi (1 4) on oikeanpuoleisin sykli, joka siirtää alkiota 1, joten alkion 1 kuvautumisen tarkastelu aloitetaan siitä. Kyseinen sykli kuvaa siis alkion 1 alkiolle 4, mutta alkio 4 ei kuvaudu tämän syklin vasemmalla puolella enää mihinkään, joten alkio 1 todellakin kuvautuu alkiolle 4.

Sama sykli on vasemmanpuoleisin, joka kuvaa alkiota 4. Siinä alkio 4 kuvautuu alkiolle 1 ja seuraavassa syklissä vasemmalla alkio 1 kuvautuu alkiolle 7, joten alkio 4 kuvautuu alkiolle 7. Edelleen samalla metodilla alkio 7 kuvautuu alkiolle 1. Saatiin siis aikaan sykli (1 4 7). Näin jatketaan kunnes kaikki alkiot on käyty läpi ja lopulta saadaan esitys erillisten syklien tulona.

Lause 1.12. *Olkoot $\alpha \in S_n$. Permutaation α esitys erillisten syklien tulona $\alpha = \beta_1 \cdots \beta_t$ on yksikäsitteinen lukuunottamatta syklien $\beta_1, ..., \beta_t$ järjestystä.*

Lause 1.13. *1. Syklin* $(i_1\, i_2 \ldots i_r)$ *käänteissykli on sykli* $(i_r\, i_{r-1} \ldots i_1)$*. Tällöin merkitään:*

$$(i_1\, i_2 \ldots i_r)^{-1} = (i_r\, i_{r-1} \ldots i_1).$$

2. Jos $\gamma \in S_n$ *ja* $\gamma = \beta_1 \cdots \beta_k$*, niin*

$$\gamma^{-1} = \beta_k^{-1} \cdots \beta_1^{-1}.$$

Määritelmä 1.14. Permutaatioilla $\alpha, \beta \in S_n$ on sama ***syklirakenne***, jos niiden esitykset erillisten syklien tulona sisältävät yhtä monta r-sykliä kaikilla luvun r arvoilla.

Esimerkki 1.15. Permutaatioilla

$$(1\ 2)(4\ 11\ 8)(3\ 10\ 6)(5\ 7),\ (1\ 11\ 3)(2\ 9)(4\ 7\ 5)(8\ 10) \in S_{11}$$

on sama syklirakenne, sillä molemmissa on yksi 1-sykli, kaksi transpoosia, kaksi 3-sykliä, eikä kummassakaan ole mitään muita syklejä.

Esimerkki 1.16. Symmetrisessä ryhmässä S_5 on syklirakenteeltaan seitsemää erilaista permutaatiota. Alla olevassa taulukossa on esiteltynä symmetrisen ryhmän S_5 permutaatioiden kaikki mahdolliset syklirakenteet ja laskettu kunkin syklirakenteen omaavien permutaatioiden lukumäärät symmetrisessä ryhmässä S_5.

Syklirakenne	lukumäärä
(1)	1
$(1\ 2)$	$\frac{5\cdot 4}{2} = 10$
$(1\ 2\ 3)$	$\frac{5\cdot 4\cdot 3}{3} = 20$
$(1\ 2\ 3\ 4)$	$\frac{5\cdot 4\cdot 3\cdot 2}{4} = 30$
$(1\ 2\ 3\ 4\ 5)$	$\frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{5} = 24$
$(1\ 2)(3\ 4\ 5)$	$\frac{5\cdot 4}{2} \cdot \frac{3\cdot 2\cdot 1}{3} = 20$
$(1\ 2)(3\ 4)$	$\frac{5\cdot 4}{2} \cdot \frac{3\cdot 2}{2} \cdot \frac{1}{2} = 15$
Σ	$5\,! = 120$

Lemma 1.17. *Jos* $\gamma, \alpha \in S_n$, *niin permutaatiolla* $\alpha\gamma\alpha^{-1}$ *on sama syklirakenne kuin permutaatiolla* γ. *Erityisesti, jos permutaatiolla* γ *on esitys*

$$\gamma = (a_1 \ldots a_s) \cdots (x_1 \ldots x_t)$$

erillisten syklien tulona, niin permutaatio $\alpha\gamma\alpha^{-1}$ *saadaan permutaatiosta* γ *siirtämällä permutaation* γ *alkioita permutaation* α *määrämällä tavalla, eli*

$$\alpha\gamma\alpha^{-1} = (\alpha(a_1) \ldots \alpha(a_s)) \cdots (\alpha(x_1) \ldots \alpha(x_t)).$$

Todistus. Olkoon σ permutaatio, joka saadaan permutaation α avulla permutaatiosta γ lemmassa määritellyllä tavalla, eli

$$\sigma = (\alpha(a_1) \ldots \alpha(a_s)) \cdots (\alpha(x_1) \ldots \alpha(x_t)).$$

Nyt on osoitettava, että

$$\sigma = \alpha\gamma\alpha^{-1}.$$

Jaetaan tarkastelu kahteen osaan sen perusteella, siirtääkö γ jotain permutoitavan joukon alkiota.

1) Jos γ säilyttää alkion i, niin σ säilyttää alkion $\alpha(i)$. Toisaalta myös permutaatio $\alpha\gamma\alpha^{-1}$ säilyttää alkion $\alpha(i)$:

$$\alpha\gamma\alpha^{-1}(\alpha(i)) = \alpha\gamma(i) = \alpha(i),$$

koska γ säilyttää alkion i.

2) Oletetaan seuraavaksi, että γ siirtää alkiota i_1. Olkoot $\gamma(i_1) = i_2$ ja

$$(i_1\ i_2 \ldots)$$

jokin sykli permutaation γ esityksessä erillisten syklien tulona.

Tällöin permutaation σ määritelmän mukaan, yksi sen sykleistä on

$$(k\ l \ldots),$$

missä $\alpha(i_1) = k$ ja $\alpha(i_2) = l$. Nyt

$$\alpha\gamma\alpha^{-1}(k) = \alpha\gamma(i_1) = \alpha(i_2) = l = \sigma(k).$$

Kohtien 1) ja 2) perusteella permutaatiot σ ja $\alpha\gamma\alpha^{-1}$ liikuttavat samalla tavalla jokaista muotoa $k = \alpha(i_j)$ olevaa alkiota. Permutaatioiden bijektiivisyydestä johtuen erityisesti α on surjektio, mistä seuraa, että jokainen alkio k on muotoa $\alpha(i_j)$, missä i_j on permutaation γ jossakin syklissä oleva alkio.

Näin ollen $\sigma = \alpha\gamma\alpha^{-1}$.

Nyt selvästi permutaatioilla γ ja σ on sama syklirakenne. Lisäksi lauseen 1.11 nojalla γ voidaan aina esittää erillisten syklien tulona. Näin ollen myös lemman ensimmäinen väite pitää paikkansa. □

Esimerkki 1.18. Olkoot $\gamma = (1\ 3)(2\ 4\ 7)(5)(6) \in S_7$ ja $\alpha = (2\ 5\ 6)(1\ 4\ 3) \in S_7$. Tällöin lemman 1.17 nojalla

$$\alpha\gamma\alpha^{-1} = (\alpha(1)\ \alpha(3))(\alpha(2)\ \alpha(4)\ \alpha(7))(\alpha(5))(\alpha(6)) = (4\ 1)(5\ 3\ 7)(6)(2).$$

Lause 1.19. *Permutaatioilla γ, $\sigma \in S_n$ on sama syklirakenne jos ja vain jos on olemassa sellainen $\tau \in S_n$, että $\sigma = \tau\gamma\tau^{-1}$.*

Todistus. Olkoon permutaatioilla $\gamma, \sigma \in S_n$ sama syklirakenne. On osoitettava, että on olemassa sellainen permutaatio $\tau \in S_n$, että $\sigma = \tau\gamma\tau^{-1}$.

Olkoot

$$\sigma = (a_1\ a_2\ ...\ a_{n_1})(b_1\ b_2\ ...\ b_{n_2})...(x_1\ x_2\ ...\ x_{n_r})$$

ja

$$\gamma = (\alpha_1\ \alpha_2\ ...\ \alpha_{n_1})(\beta_1\ \beta_2\ ...\ \beta_{n_2})...(\chi_1\ \chi_2\ ...\ \chi_{n_r})$$

permutaatioiden σ ja γ esitykset erillisten syklien tulona. Tällöin

$$\tau = \begin{pmatrix} \alpha_1 & \alpha_2 & ... & \alpha_{n_1} & \beta_1 & \beta_2 & ... & \beta_{n_2} & ... & \chi_1 & \chi_2 & ... & \chi_{n_r} \\ a_1 & a_2 & ... & a_{n_1} & b_1 & b_2 & ... & b_{n_2} & ... & x_1 & x_2 & ... & x_{n_r} \end{pmatrix} \in S_n.$$

Näistä esityksistä on helppo nähdä, että $\sigma = \tau\gamma\tau^{-1}$. Esimerkiksi

$$\sigma(a_1) = a_2$$

ja

$$\tau\gamma\tau^{-1}(a_1) = \tau\gamma(\alpha_1) = \tau(\alpha_2) = a_2.$$

Näin ollen saman syklirakenteen omaaville permutaatioille $\gamma, \sigma \in S_n$ löytyy aina sellainen permutaatio $\tau \in S_n$, että $\sigma = \tau\gamma\tau^{-1}$.

Lause on todistettu toiseen suuntaan lemmassa 1.17. □

Lause 1.20. *Jos $n \geq 2$, niin jokainen permutaatio $\alpha \in S_n$ voidaan esittää transpoosien tulona.*

Määritelmä 1.21. Permutaation ***pariteetti*** kuvaa permutaation parillisuutta. Permutaatio $\alpha \in S_n$ on ***parillinen***, jos sen esitys transpoosien tulona sisältää parillisen määrän transpooseja ja muulloin α on ***pariton***.

Esimerkki 1.22. Olkoon

$$\alpha = (1\ 7\ 2\ 6)(3\ 9\ 5)(4)(8) \in S_9.$$

Permutaation α esitys transpoosien tulona on

$$\alpha = (1\ 6)(1\ 2)(1\ 7)(3\ 5)(3\ 9).$$

Tämä ei sisällä parillista määrää transpooseja, joten permutaatio α on pariton.

Määritelmä 1.23. Olkoot $\alpha \in S_n$ ja $\alpha = \beta_1 \cdots \beta_t$ permutaation α esitys erillisten syklien tulona. Tällöin ***signum*** α, joka on permutaation α etumerkkifunktion arvo, on määritelty seuraavasti:

$$sgn(\alpha) = (-1)^{n-t}.$$

Esimerkki 1.24. Olkoon

$$\alpha = (1\ 11\ 3)(2\ 9)(4\ 7\ 5)(8\ 10)(6) \in S_{11}.$$

Nyt permutaation α esityksessä erillisten syklien tulona on 5 sykliä, joten

$$sgn(\alpha) = (-1)^{11-5} = (-1)^6 = 1.$$

Esimerkki 1.25. Olkoon $\alpha \in S_n$ mikä tahansa transpoosi. Tällöin α siirtää kahta alkiota ja säilyttää muut $n-2$ alkiota. Näin ollen

$$t = (n-2) + 1 = n - 1$$

ja

$$sgn(\alpha) = (-1)^{n-(n-1)} = -1.$$

Lause 1.26. *Kaikille permutaatioille* α, $\beta \in S_n$

$$sgn(\alpha\beta) = sgn(\alpha)\, sgn(\beta).$$

Todistus. Nyt jokainen permutaatio $\alpha \in S_n$ voidaan lauseen 1.20 nojalla esittää transpoosien tulona. Olkoon permutaation α esitys transpoosien tulona $\alpha = \tau_1 ... \tau_m$. Todistetaan induktiolla luvun m suhteen, että $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$.

1. Tapaus $m = 1$;

   Olkoon permutaation β esitys erillisten syklien tulona

   $$\beta = \underbrace{(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)}_{r\ kpl}.$$

   Tällöin

   $$\beta = (a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n),$$

   missä $k, l \geq 0$. Kertomalla yhtälöä vasemmalta puolittain transpoosilla $\alpha_1 = (a\ b)$ saadaan

   $$\alpha_1\beta = (a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)$$

   $$= (a\ b)(a\ b)(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)$$

   eli

   $$(a\ b)(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)$$

   $$= \underbrace{(a\ c_1\ ...\ c_k\ b\ d_1\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)}_{r-1\ kpl}.$$

Transpoosilla kertominen siis tässä tapauksessa vähentää syklien määrää erillisten syklien esityksessä yhdellä. Koska $sgn(\beta) = (-1)^{n-r}$, niin

$$sgn(\alpha_1\beta) = (-1)^{n-(r-1)} = (-1)^{n-r+1} = -(-1)^{n-r} = sgn(\alpha_1)sgn(\beta).$$

Edellinen tarkastelu sisältää tilanteen, että permutaatio β säilyttää toisen tai molemmat transpoosin siirtämistä alkioista a ja b, johtuen oletuksesta $k, l \geq 0$.

Mikäli transpoosi α_1 on sellainen, että sen siirtämät alkiot ovat samassa syklissä permutaatiossa β, niin tällöin transpoosin ja permutaation β tulossa on yksi sykli enemmän kuin permutaatiossa β. Signumien kannalta päädytään kuitenkin samaan lopputulokseen.

Olkoon esimerkiksi transpoosi $\alpha_1 = (b\ d_i)$, missä $1 \leq i \leq l$. Tällöin

$$\begin{aligned}
\alpha_1\beta &= (b\ d_i)\underbrace{(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_i\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)}_{r\ kpl} \\
&= (b\ d_i)(b\ d_1\ ...\ d_i\ ...\ d_l)(a\ c_1\ ...\ c_k)\ ...\ (x_1\ ...\ x_n) \\
&= (b\ d_1\ ...\ d_{i-1})(d_i\ ...\ d_l)(a\ c_1\ ...\ c_k)\ ...\ (x_1\ ...\ x_n) \\
&= \underbrace{(a\ c_1\ ...\ c_k)(b\ d_1\ ...\ d_{i-1})(d_i\ ...\ d_l)\ ...\ (x_1\ ...\ x_n)}_{r+1\ kpl}
\end{aligned}$$

ja

$$sgn(\alpha_1\beta) = (-1)^{n-(r+1)} = (-1)^{n-r-1} = -(-1)^{n-r} = sgn(\alpha_1)sgn(\beta).$$

Transpoosin α_1 valinnalla ei siis ole merkitystä.

2. Induktio-oletus: Jos $m = k$, niin $\alpha_k = \tau_1...\tau_k$ ja oletetaan, että

$$sgn(\alpha_k\beta) = sgn(\alpha_k)\, sgn(\beta)$$

kaikilla permutaatioilla $\beta \in S_n$.

3. Olkoon $m = k + 1$. Tällöin $\alpha_{k+1} = \tau_1...\tau_k\tau_{k+1} = \alpha_k\tau_{k+1}$.

Nyt

$$sgn(\alpha_{k+1}\beta) = sgn(\alpha_k\tau_{k+1}\beta) = sgn(\alpha_k\beta^*),$$

missä $\beta^* = \tau_{k+1}\beta$.

Kohdan 1. nojalla

$$sgn(\beta^*) = sgn(\tau_{k+1})sgn(\beta) = -sgn(\beta).$$

Lisäksi induktio-oletuksen nojalla

$$sgn(\alpha_{k+1}) = sgn(\alpha_k)sgn(\tau_{k+1}) = -sgn(\alpha_k)$$

ja

$$sgn(\alpha_k\beta^*) = sgn(\alpha_k)\, sgn(\beta^*).$$

Yhdistämällä yllä olevat tiedot, saadaan

$$sgn(\alpha_{k+1}\beta) = sgn(\alpha_k\beta^*) = sgn(\alpha_k)\,(-sgn(\beta))$$

$$= -sgn(\alpha_k)\, sgn(\beta) = sgn(\alpha_{k+1})\, sgn(\beta).$$

Induktioperiaatteen nojalla $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$ kaikilla permutaatioilla $\alpha, \beta \in S_n$. □

Lause 1.27. *Olkoon $\alpha \in S_n$. Jos $sgn(\alpha) = 1$, niin α on parillinen ja jos $sgn(\alpha) = -1$, niin α on pariton.*

Todistus. Olkoon $\alpha = \tau_1 \cdots \tau_q$ permutaation α esitys transpoosien tulona. Lauseen 1.26 ja esimerkin 1.25 nojalla

$$sgn(\alpha) = sgn(\tau_1) \cdots sgn(\tau_q) = (-1)^q.$$

Jos $sgn(\alpha) = 1$, niin luvun q täytyy olla parillinen ja määritelmän 1.21 mukaan permutaatio α on tällöin parillinen. Toisaalta, jos $sgn(\alpha) = -1$, niin luvun q täytyy olla pariton, jolloin myös permutaatio α on pariton. □

Lause 1.28. *Olkoon $\alpha \in S_n$ sykli. Jos syklissä α on pariton määrä alkioita, niin α on parillinen ja jos taas syklissä α on parillinen määrä alkioita, niin α on pariton.*

Todistus. Olkoon syklissä $\alpha = (a_1 \quad a_2 \quad ... \quad a_{r-1} \quad a_r) \in S_n$ pariton määrä alkoita. Syklin α esitys transpoosien tulona on

$$\alpha = (a_1 \quad a_2 \quad ... \quad a_{r-1} \quad a_r) = (a_1 \quad a_r)(a_1 \quad a_{r-1})...(a_1 \quad a_2).$$

Tämä sisältää siis $r-1$ kappaletta transpooseja ja $r-1$ on parillinen luku, koska r on pariton. Parillisuuden määritelmän mukaan sykli α on siis parillinen.

Olkoon sitten syklissä $\alpha = (a_1 \quad a_2 \quad ... \quad a_{k-1} \quad a_k) \in S_n$ parillinen määrä alkoita. Syklin α esitys transpoosien tulona on

$$\alpha = (a_1 \quad a_2 \quad ... \quad a_{k-1} \quad a_k) = (a_1 \quad a_k)(a_1 \quad a_{k-1})...(a_1 \quad a_2).$$

Tämä sisältää siis $k-1$ kappaletta transpooseja, mikä on pariton luku, koska k on parillinen. Parillisuuden määritelmän mukaan sykli α on siis pariton. □

Seuraus 1.29. *Olkoot α, $\beta \in S_n$. Jos permutaatioilla α ja β on sama pariteetti, niin permutaatio $\alpha\beta$ on parillinen ja jos permutaatioilla α ja β on eri pariteetti, niin permutaatio $\alpha\beta$ on pariton.*

2 Ryhmistä

Tässä luvussa otetaan esiin myöhemmin tarvittavia ryhmiin liittyviä asioita. Tässä yhteydessä todistamatta jätetyt tulokset on todistettu algebran peruskursseilla.

Määritelmä 2.1. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Pari $(G, *)$ on ***ryhmä***, mikäli seuraavat kolme ehtoa toteutuvat:

1. Operaatio $(*)$ on ***binäärinen*** joukossa G eli

$$a * b \in G$$

   aina, kun $a, b \in G$;

2. Operaatio $(*)$ on ***assosiatiivinen*** eli

$$(a * b) * c = a * (b * c)$$

   aina, kun $a, b, c \in G$;

3. Joukossa G on sellainen alkio e, että

$$a * e = e * a = a$$

   aina, kun $a \in G$. Alkiota e kutsutaan ***neutraali-*** tai ***ykkösalkioksi***;

4. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että

$$a * a^{-1} = a^{-1} * a = e.$$

   Alkiota a^{-1} kutsutaan alkion a ***käänteisalkioksi***.

Lause 2.2. *Symmetriseksi ryhmäksi S_n nimetty joukko, joka koostuu joukon $X = \{1, 2, ..., n\}$ permutaatioista, on ryhmä, kun se varustetaan permutaatioiden yhdistämisoperaatiolla $(\circ)$.*

Todistus. Tehdään todistus osoittamalla, että ryhmän määritelmässä vaaditut asiat täyttyvät.

1. Jos $\alpha, \beta \in S_n$, niin sekä α että β permutoivat n kappaletta alkioita siirtäen niitä tai pitäen ne paikoillaan. Tällöin myös näiden permutaatioiden yhdistelmä $\alpha \circ \beta$ permutoi n kappaletta alkioita, koska permutoitavaan joukkoon ei synny mistään uusia alkioita.

   Siispä $\alpha \circ \beta \in S_n$ ja $(\circ)$ on binäärinen operaatio joukossa S_n.

2. Tarkistetaan toisena assosiatiivisuuden voimassaolo.

   Permutaatioiden yhdistäminen tarkoittaa permutaatioiden syklien laittamista peräkkäin muuttamatta niiden järjestystä. Esimerkiksi permutaatiossa $\alpha \circ \beta$ on joukko syklejä järjestäytyneenä siten, että ensin ovat permutaation α syklit ja niiden perässä permutaation β syklit. Kun permutaatiota $\gamma \in S_n$ operoidaan vasemmalta permutaatiolla $\alpha \circ \beta$, lisätään permutaatioden α ja β syklit permutaation γ syklien eteen.

   Vastaavasti permutaatiossa $\beta \circ \gamma$ on joukko syklejä siten, että vasemmalla puolella ovat permutaation β syklit ja oikealla puolella ovat permutaation γ syklit. Kun permutaatiota α operoidaan oikealta permutaatiolla $\beta \circ \gamma$, lisätään permutaation $\beta \circ \gamma$ syklit permutaation α syklien jatkeeksi.

   Täten

   $$(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$$

   kaikilla $\alpha, \beta, \gamma \in S_n$. Siispä $(\circ)$ on assosiatiivinen operaatio joukossa S_n.

3. Identiteettikuvaus e, $e(x) = x$ kaikilla $x \in X$, kuvaa jokaisen joukon X alkion itselleen, joten se on bijektio ja täten myös permutaatio. Koska permutaatio e ei siirrä mitään permutoitavan joukon alkiota, niin

   $$e \circ \alpha = \alpha = \alpha \circ e$$

   kaikilla $\alpha \in S_n$, . Täten e on neutraalialkio.

4. Jos $\alpha : X \to X$ on bijektio eli $\alpha \in S_n$, niin myös $\alpha^{-1} : X \to X$ on bijektio, eli $\alpha^{-1} \in S_n$. Nyt

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

kaikilla $\alpha \in S_n$. Siis α^{-1} on permutaation α käänteisalkio.

Täten pari $(S_n, \circ)$ on ryhmä. □

Määritelmä 2.3. Ryhmää G kutsutaan ***Abelin ryhmäksi***, jos tässä ryhmässä on voimassa ***kommutatiivisuus***:

$$x * y = y * x \quad \textit{kaikilla } x, y \in G.$$

Lemma 2.4. *Olkoot G ryhmä ja $a, b \in G$. Tällöin*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Määritelmä 2.5. Olkoon $(G, *)$ ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan ryhmän $(G, *)$ ***aliryhmäksi***; merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Lause 2.6 (Aliryhmäkriteeri)**.** *Olkoot $(G, *)$ ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraavat ehdot toteutuvat:*

1. $a, b \in H \Rightarrow a * b \in H$;
2. $a \in H \Rightarrow a^{-1} \in H$.

Lause 2.7. *Olkoot G ryhmä ja H ryhmän G äärellinen epätyhjä osajoukko. Tällöin $H \leq G$ jos ja vain jos $ab \in H$ aina kun $a, b \in H$.*

Esimerkki 2.8. Neljän permutaation joukko

$$V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

muodostaa ryhmän. Tämä on varsin helppo todistaa osoittamalla, että V on ryhmän S_4 aliryhmä lausetta 2.7 käyttäen.

Tarkistetaan siis binäärisyyden voimassa olo:

$$(1\ 2)(3\ 4)(1\ 2)(3\ 4) = (1),$$

$$(1\ 3)(2\ 4)(1\ 3)(2\ 4) = (1),$$

$$(1\ 4)(2\ 3)(1\ 4)(2\ 3) = (1),$$

$$(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3) = (1\ 3)(2\ 4)(1\ 2)(3\ 4),$$

$$(1\ 2)(3\ 4)(1\ 4)(2\ 3) = (1\ 3)(2\ 4) = (1\ 4)(2\ 3)(1\ 2)(3\ 4),$$

$$(1\ 3)(2\ 4)(1\ 4)(2\ 3) = (1\ 2)(3\ 4) = (1\ 4)(2\ 3)(1\ 3)(2\ 4).$$

Täten $V \leq S_4$ ja samalla huomataan, että V on myös Abelin ryhmä.

Nimetään ryhmä V ***neliryhmäksi*** myöhempää käyttöä varten.

Määritelmä 2.9. Äärellisen ryhmän G alkioiden lukumäärälle käytetään merkintää $|G|$ ja sitä kutsutaan ryhmän G ***kertaluvuksi***.

Määritelmä 2.10. Olkoot H ryhmän G aliryhmä ja $a \in G$. Ryhmän G osajoukkoa

$$aH = \{ah : h \in H\}$$

kutsutaan alkion a määräämäksi ryhmän H ***vasemmaksi sivuluokaksi***. Vastaavasti

$$Ha = \{ha : h \in H\}$$

on alkion a määräämä ryhmän H ***oikea sivuluokka***.

Huomautus 2.11. Yleisesti vasemmat ja oikeat sivuluokat eivät ole samoja. Lisäksi sivuluokat eivät useimmiten myöskään ole ryhmän G aliryhmiä.

Lause 2.12. *Olkoot G äärellinen ryhmä ja H sen aliryhmä. Tällöin aliryhmän H kertaluku $|H|$ jakaa ryhmän G kertaluvun $|G|$.*

Määritelmä 2.13. Olkoot $(G, *)$ ja $(H, \circ)$ ryhmiä. Kuvaus $f : G \to H$ on ***homomorfismi***, jos

$$f(x * y) = f(x) \circ f(y)$$

kaikilla $x, y \in G$.

Jos lisäksi f on bijektio, niin kuvaus f on ***isomorfismi***. Tällöin ryhmiä G ja H kutsutaan ***isomorfisiksi*** ja merkitään $G \cong H$.

Lause 2.14. *Kuvaus $sgn : S_n \to (\{-1, 1\}, \cdot)$ on homomorfismi.*

Todistus. Koska lauseen 1.26 nojalla kaikille permutaatioille $\alpha, \beta \in S_n$

$$sgn(\alpha\beta) = sgn(\alpha)sgn(\beta),$$

niin määritelmän mukaan $sgn : S_n \to (\{-1, 1\}, \cdot)$ on homomorfismi. □

Lause 2.15. *Olkoon $f : G \to H$ homomorfismi ja alkiot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin*

$$f(e_G) = e_H \quad ja \quad f(a^{-1}) = (f(a))^{-1}$$

aina, kun $a \in G$.

Määritelmä 2.16. Homomorfismin $f : G \to H$ ***ydintä*** merkitään $Ker(f)$ ja se on lähtöryhmän G osajoukko

$$Ker(f) = \{x \in G : f(x) = e_H\}$$

ja ***kuvaa*** merkitään $Im(f)$ ja se on maaliryhmän H osajoukko

$$Im(f) = \{h \in H : h = f(x)\, jollakin\, x \in G\}.$$

Esimerkki 2.17. Homomorfismin $sgn : S_n \to (\{-1, 1\}, \cdot)$ ydin on permutaatioiden joukko

$$Ker(sgn) = \{\alpha \in S_n : sgn(\alpha) = 1\}.$$

Lauseen 1.27 nojalla signumin ytimeen kuuluu kaikki parilliset permutaatiot.

Homomorfismin $sgn : S_n \to (\{-1, 1\}, \cdot)$ kuva on koko maalijoukko, eli se sisältää molemmat maalijoukon alkiot aina, kun $n \geq 2$.

Tällöin $(1), (1\ 2) \in S_n$, joille $sgn((1)) = 1$ ja $sgn((1\ 2)) = -1$.

Määritelmä 2.18. Ryhmän G aliryhmä K on ***normaali aliryhmä***, jos $gkg^{-1} \in K$, kun $k \in K$ ja $g \in G$. Tällöin merkitään $K \lhd G$.

Lemma 2.19. *Jokainen Abelin ryhmän G aliryhmä on normaali.*

Todistus. Olkoot $K \leq G$, $k \in K$ ja $g \in G$. Tällöin

$$gkg^{-1} = kgg^{-1} = k \in K,$$

joten $K \lhd G$. □

Huomautus 2.20. Lemman 2.19 käänteinen väite ei pidä paikkaansa. Eli myös ei-kommutatiivisilla ryhmillä voi olla normaaleja aliryhmiä.

Lause 2.21. *Olkoon $f : (G, \cdot) \to (H, *)$ homomorfismi. Tällöin*

$$Ker(f) \leq G \quad ja \quad Im(f) \leq H.$$

Todistus. Todistetaan molemmat kohdat erikseen käyttämällä aliryhmäkriteeriä.

1. Ytimen määritelmän mukaan $Ker(f) \subseteq G$. Lisäksi $e_G \in Ker(f)$, sillä lauseen 2.15 nojalla $f(e_G) = e_H$, joten $Ker(f) \neq \emptyset$.

   Olkoon $a, b \in Ker(f)$. Tällöin $f(a) = e_H$ ja $f(b) = e_H$.

   Koska f on homomorfismi, niin

   $$f(a \cdot b) = f(a) * f(b) = e_H * e_H = e_H,$$

   eli $a \cdot b \in Ker(f)$.

   Lisäksi

   $$f(a^{-1}) = (f(a))^{-1} = e_H^{-1} = e_H,$$

   joten $a^{-1} \in Ker(f)$ kaikilla $a \in Ker(f)$.

   Näin ollen $Ker(f) \leq G$.

2. Kuvan $Im(f)$ määritelmän mukaan $Im(f) \subseteq H$. Lisäksi $e_H = f(e_G) \in Im(f)$, joten $Im(f) \neq \emptyset$.

   Olkoon nyt $c, d \in Im(f)$. Tällöin on olemassa sellaiset alkiot $a, b \in G$, että $f(a) = c$ ja $f(b) = d$.

   Koska f on homomorfismi, niin

$$c * d = f(a) * f(b) = f(a \cdot b).$$

   Lisäksi, koska G on ryhmä, niin $a \cdot b \in G$.

   Näin ollen $f(a \cdot b) = c * d \in Im(f)$.

   Lisäksi lauseen 2.15 nojalla

$$(f(a))^{-1} = f(a^{-1}) \in Im(f)$$

   aina, kun $a \in G$.

   Siispä $Im(f) \leq H$.

□

Lemma 2.22. *Ryhmän G aliryhmä K on normaali aliryhmä jos ja vain jos*

$$gK = Kg$$

kaikilla $g \in G$. Näin ollen normaalin aliryhmän vasemmat ja oikeat sivuluokat ovat samat.

Todistus. Oletetaan aluksi, että $K \lhd G$. Olkoon $gk \in gK$ ja merkitään $gkg^{-1} = k^* \in K$. Tällöin

$$gk = gke = gkg^{-1}g = (gkg^{-1})g = k^*g \in Kg,$$

joten $gK \subseteq Kg$.

Olkoon sitten $kg \in Kg$. Tällöin

$$(g^{-1})k(g^{-1})^{-1} = g^{-1}kg \in K$$

ja merkitään $g^{-1}kg = k^{**}$. Nyt

$$kg = g(g^{-1}kg) = gk^{**} \in gK$$

ja näin ollen $Kg \subseteq gK$. Siispä $gK = Kg$, kun $K \lhd G$.

Oletetaan nyt, että $gK = Kg$ kaikilla $g \in G$. Tällöin jokaiselle $k \in K$ on olemassa $k^* \in K$ siten että $gk = k^*g$. Operoidaan tätä yhtälöä puolittain oikealta alkion g käänteisalkiolla g^{-1}, jolloin saadaan

$$gkg^{-1} = k^*gg^{-1} = k^* \in K.$$

Täten $gkg^{-1} \in K$ kaikilla $g \in G$ ja siten $K \lhd G$. □

Jos G on ryhmä, niin merkinnällä $S(G)$ tarkoitetaan joukkoa, johon kuuluvat kaikki ryhmän G epätyhjät osajoukot. Jos $X, Y \in S(G)$, määritellään

$$XY = \{xy : x \in X ja\ y \in Y\}.$$

Osoitetaan, että tämä kertolasku on assosiatiivinen.

Nyt $X(YZ)$ on joukko, johon kuuluvat kaikki muotoa $x(yz)$ olevat alkiot, missä $x \in X$, $y \in Y$ ja $z \in Z$. Toisaalta joukkoon $(XY)Z$ kuuluvat kaikki alkiot $(xy)z$. Koska $x, y, z \in G$, niin ryhmän G assosiatiivisuuden nojalla $x(yz) = (xy)z$. Joukot $X(YZ)$ ja $(XY)Z$ ovat samoja, koska niiden kaikki alkiot ovat samoja. Näin ollen yllä määritelty kertolasku on assosiatiivinen myös joukossa $S(G)$.

Lause 2.23. *Olkoot G ryhmä ja K sen aliryhmä. Tällöin merkintä G/K tarkoittaa kaikkia aliryhmän K vasempia sivuluokkia, eli*

$$G/K = \{aK : a \in G\}.$$

Jos K on normaali aliryhmä, niin

$$aKbK = abK$$

kaikilla $a, b \in G$ ja G/K on ryhmä.

Todistus. Sivuluokkien tulo $(aK)(bK)$ voidaan ajatella myös neljän alkion tulona aiemmin tarkastellussa joukossa $S(G)$. Assosiatiivisuuden ja lemman 2.22 nojalla saadaan

$$(aK)(bK) = a(Kb)K = a(bK)K = abKK = abK.$$

Näin ollen normaalin aliryhmän K kahden sivuluokan tulo on edelleen ryhmän K sivuluokka ja binäärisyys on siis voimassa joukossa G/K.

Koska kertolasku on assosiatiivinen joukossa $S(G)$, niin $X(YZ) = (XY)Z$ kaikilla ryhmän G epätyhjillä osajoukoilla X, Y, Z.

Koska myös ryhmän K sivuluokat ovat ryhmän G osajoukkoja, niin assosiatiivisuus on voimassa myös joukossa G/K.

Joukon G/K neutraalialkio on sivuluokka $K = eK$, koska

$$(eK)(bK) = ebK = bK = beK = (bK)(eK)$$

kaikilla $bK \in G/K$.

Jokaiselle alkiolle $aK \in G/K$ löytyy käänteisalkio $a^{-1}K$, koska

$$(a^{-1}K)(aK) = a^{-1}aK = K = aa^{-1}K = (aK)(a^{-1}K),$$

kun alkio a^{-1} on alkion a käänteisalkio ryhmässä G.

Näin ollen G/K on ryhmä. □

Määritelmä 2.24. Edellä esiteltyä ryhmää G/K kutsutaan ryhmän G ***tekijäryhmäksi*** normaalin aliryhmän K suhteen.

Lause 2.25. *Olkoon $f : G \to H$ homomorfismi. Tällöin*

$$Ker(f) \lhd G$$

ja

$$G/Ker(f) \cong Im(f).$$

Erityisesti, jos $Ker(f) = K$ ja kuvaus $\phi : G/K \to Im(f) \leq H$ on määritelty siten, että $\phi : aK \mapsto f(a)$, niin ϕ on isomorfismi.

Todistus. Lauseen 2.21 nojalla $Ker(f) \leq G$. Olkoot $x \in K$ ja $a \in G$. Koska f on homomorfismi, niin tällöin

$$f(axa^{-1}) = f(a)f(x)f(a)^{-1} = f(a)e_H f(a)^{-1} = e_H.$$

Näin ollen $axa^{-1} \in K$ ja määritelmän mukaan $Ker(f) \lhd G$.

Nyt kuvaus ϕ on hyvin määritelty. Olkoon $a, b \in G$. Jos $aK = bK$, niin $a = bk$ jollakin $k \in K$ ja

$$f(a) = f(bk) = f(b)f(k) = f(b)e_H = f(b).$$

Osoitetaan seuraavaksi, että kuvaus ϕ on homomorfismi. Koska kuvaus f on homomorfismi ja määritelmän mukaan $\phi(aK) = f(a)$, niin

$$\phi(aKbK) = \phi(abK) = f(ab) = f(a)f(b) = \phi(aK)\phi(bK).$$

Siispä kuvaus ϕ on homomorfismi.

Selvästi $Im(\phi) \leq Im(f)$. Jos $y \in Im(f)$, niin $y = f(a)$ jollakin $a \in G$ ja täten $y = f(a) = \phi(aK)$. Näin ollen kuvaus ϕ on surjektio.

Osoitetaan lopuksi, että kuvaus ϕ on injektio. Jos $\phi(aK) = \phi(bK)$, niin $f(a) = f(b)$. Tällöin myös pätee, että

$$e_H = f(a)^{-1}f(a) = f(b)^{-1}f(a) = f(b^{-1}a).$$

Täten $b^{-1}a \in Ker(f) = K$, eli

$$e_G K = (b^{-1}a)K = b^{-1}KaK.$$

Operoidaan yllä olevaa yhtälöä puolittain vasemmalta sivuluokalla bK, jolloin saadaan

$$bKe_G K = bKb^{-1}KaK$$

$$\Leftrightarrow bK = aK.$$

Näin ollen kuvaus ϕ on siis injektio.

Koska kuvaus $\phi : G/K \to Im(f)$ on homomorfismi ja bijektio, niin se on näin ollen myös isomorfismi. □

Lemma 2.26. *Olkoon G ryhmä ja $H \lhd G$. Määritellään kuvaus*

$$\pi : G \to G/H, \pi(a) = aH.$$

Tällöin π on surjektiivinen homomorfismi ja $Ker(\pi) = H$.

Määritelmä 2.27. Olkoon G on ryhmä ja $H \lhd G$. Kuvausta

$$\pi : G \to G/H, \pi(a) = aH$$

kutsutaan ***luonnolliseksi homomorfismiksi***.

Lause 2.28. *Olkoon H ja K ryhmän G aliryhmiä, niin että $H \lhd G$. Tällöin $HK \leq G$, $H \cap K \lhd K$ ja*

$$K/(H \cap K) \cong HK/H.$$

Todistus. Jos $kh \in KH$, niin $h^* = khk^{-1} \in H$, koska $H \lhd G$. Tällöin

$$kh = khk^{-1}k = h^*k \in HK,$$

joten $KH \subseteq HK$. Vastaavasti nähdään, että jos $hk \in HK$, niin

$$hk = kk^{-1}hk = kh^{**} \in KH.$$

Näin ollen myös $HK \subseteq KH$ ja siispä $HK = KH$.
Olkoon $hk, h^*k^* \in HK$. Tällöin

$$hkh^*k^* \in HKHK = HHKK = HK.$$

Binäärisyys on siis voimassa. Lisäksi lemman 2.4 nojalla

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK,$$

joten jokaiselle alkiolle löytyy myös käänteisalkio.

Täten lauseen 2.6 nojalla $HK \leq G$.
Koska $H \leq HK \leq G$ ja $H \lhd G$, niin $H \lhd HK$.
Osoitetaan seuraavaksi, että jokainen sivuluokka $xH \in HK/H$ voidaan esittää muodossa kH, missä $k \in K$.

Sivuluokat xH ovat siis muotoa hkH, missä $h \in H$ ja $k \in K$. Koska $H \lhd HK$, niin

$$hk = kk^{-1}hk = kh^*$$

jollakin $h^* \in H$ ja

$$hkH = kh^*H = kH.$$

Näin ollen kuvaus $f : K \to HK/H, f(k) = kH$ on surjektio.

Lisäksi f on homomorfismi, koska se sisältyy määritelmän 2.27 mukaiseen luonnolliseen homomorfismiin $\pi : G \to G/H$. Koska lemman 2.26 nojalla $Ker(\pi) = H$, niin $Ker(f) = H \cap K$ ja $H \cap K$ on lauseen 2.25 nojalla ryhmän K normaali aliryhmä.
Edelleen lauseen 2.25 nojalla $K/(H \cap K) \cong HK/H$. □

Määritelmä 2.29. Ryhmä $G \neq \{e\}$ on ***yksinkertainen***, jos ryhmällä G ei ole muita normaaleja aliryhmiä kuin $\{e\}$ ja G itse.

Lause 2.30. *Symmetrinen ryhmä S_n ei ole yksinkertainen, kun $n \geq 3$.*

Todistus. On siis löydettävä sellainen normaali aliryhmä H, että $H \neq \{(1)\}$ ja $H \neq S_n$.

Kuvaus $sgn : S_n \to (\{-1, 1\}, \cdot)$ on lauseen 2.14 nojalla homomorfismi. Lisäksi lauseen 2.25 nojalla tiedetään, että $Ker(sgn) \lhd S_n$.

Kun $n \geq 3$ niin esimerkiksi 3-sykli $\alpha = (1\ 2\ 3) \in Ker(sgn)$, koska $sgn(\alpha) = 1$. Näin ollen $Ker(sgn) \neq \{(1)\}$.

Toisaalta esimerkiksi transpoosi $\beta = (1\ 2) \in S_n$, mutta $\beta \notin Ker(sgn)$, koska $sgn(\beta) = -1$. Täten $Ker(sgn)$ ei ole myöskään koko symmetrinen ryhmä S_n.

Siispä symmetrinen ryhmä S_n ei ole yksinkertainen, kun $n \geq 3$. □

3 Alternoiva ryhmä

Tässä luvussa määritellään alternoiva ryhmä A_n ja tutkitaan sen yksinkertaisuutta luvun n eri arvoilla. Katsotaan siis, että löytyykö alternoiville ryhmille muita normaaleja aliryhmiä kuin neutraalialkion muodostama yhden alkion ryhmä ja alternoiva ryhmä itse.

Lause 3.1. *Olkoon joukko A_n symmetrisen ryhmän S_n sellainen osajoukko, joka sisältää ainoastaan kaikki joukon S_n parilliset permutaatiot. Tällöin A_n on ryhmä.*

Todistus. Osoitetaan, että A_n on ryhmän S_n aliryhmä käyttäen aliryhmäkriteeriä 2.6.

1. Binäärisyys;

   Seurauksen 1.29 nojalla parillisten permutaatioiden tulo on edelleen parillinen. Näin ollen jos $\alpha,\ \beta \in A_n$, niin $\alpha\beta \in A_n$.

2. Käänteisalkion olemassaolo;

   Lauseen 1.13 nojalla erillisten syklien tulona esitetyn permutaation α käänteispermutaatio α^{-1} sisältää yhtä monta saman pituista sykliä kuin permutaatio α. Tällöin myöskään pariteetti ei muutu ja $\alpha^{-1} \in A_n$, kun $\alpha \in A_n$.

Näin ollen A_n on ryhmä. □

Määritelmä 3.2. Symmetrisen ryhmän S_n parillisten permutaatioiden muodostamaa ryhmää A_n kutsutaan ***alternoivaksi ryhmäksi***.

Lause 3.3. *Alternoiva ryhmä A_n on symmetrisen ryhmän S_n normaali aliryhmä.*

Todistus. Alternoiva ryhmä A_n koostuu siis kaikista symmetrisen ryhmän S_n parillisista permutaatioista. Näin ollen, jos $\alpha \in A_n$, niin lauseen 1.27 nojalla $sgn(\alpha) = 1$ ja homomorfismin $sgn : S_n \to (\{-1, 1\}, \cdot)$ ydin $Ker(sgn) = A_n$. Lauseen 2.25 nojalla $A_n \lhd S_n$. □

Lause 3.4. *Alternoivan ryhmän A_n kertaluku on puolet symmetrisen ryhmän S_n kertaluvusta:*

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Todistus. Lauseen 2.25 nojalla $S_n/Ker(sgn) \cong Im(sgn)$ eli $S_n/A_n \cong (\{-1, 1\}, \cdot)$.

Koska isomorfisten ryhmien kertaluvut ovat samat, niin

$$|S_n/A_n| = 2 \quad eli \quad \frac{|S_n|}{|A_n|} = 2,$$

joten

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

□

Esimerkki 3.5. Lauseen 1.28 ja seurauksen 1.29 nojalla ryhmässä A_6 on syklirakenteeltaan kuutta erilaista permutaatiota. Seuraavassa taulukossa on esiteltynä ryhmän A_6 permutaatioiden kaikki mahdolliset syklirakenteet ja laskettu kunkin syklirakenteen omaavien permutaatioiden lukumäärät ryhmässä A_6.

Syklirakenne	lukumäärä
(1)	1
(1 2 3)	$\frac{6\cdot5\cdot4}{3} = 40$
(1 2 3 4 5)	$\frac{6\cdot5\cdot4\cdot3\cdot2}{5} = 144$
(1 2)(3 4)	$\frac{6\cdot5}{2} \cdot \frac{4\cdot3}{2} \cdot \frac{1}{2} = 45$
(1 2 3)(4 5 6)	$\frac{6\cdot5\cdot4}{3} \cdot \frac{3\cdot2\cdot1}{3} \cdot \frac{1}{2} = 40$
(1 2)(3 4 5 6)	$\frac{6\cdot5}{2} \cdot \frac{4\cdot3\cdot2\cdot1}{4} = 90$
Σ	360

Lemma 3.6. *Olkoon $n \geq 3$. Tällöin jokainen ryhmän A_n alkio on joko 3-sykli tai se voidaan esittää 3-syklien tulona.*

Todistus. Olkoon $\alpha \in A_n$ permutaatio. Parillisuuden määritelmän nojalla permutaation α esitys transpoosien tulona sisältää parillisen määrän transpooseja:

$$\alpha = \tau_1\tau_2 \cdots \tau_{2q-1}\tau_{2q}.$$

Mikäli jokainen kahden transpoosin tulo $\tau_i\tau_{i+1}$ voidaan esittää 3-syklinä tai niiden tulona, niin myös permutaatio α voidaan esittää 3-syklien tulona. Osoitetaan siis, että kaikki kahden transpoosin tulot voidaan esittää 3-syklinä tai niiden tulona.

Olkoot alkiot a, b, c, d erillisiä. Tällöin

1. $(a\ b)(a\ b) = (1) = (a\ b\ c)(a\ b\ c)(a\ b\ c) = (a\ b\ c)(a\ c\ b)$,
2. $(a\ b)(a\ c) = (a\ c\ b)$ ja
3. $(a\ b)(c\ d) = (a\ b)(1)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$.

Näin ollen kaikki kahden transpoosin tulot voidaan esittää 3-syklinä tai niiden tulona ja täten myös permutaatio $\alpha \in A_n$ voidaan esittää 3-syklinä tai niiden tulona. □

Lemma 3.7. *Olkoon $n \geq 5$. Jos ryhmän A_n normaali aliryhmä H sisältää jonkin 3-syklin, niin $H = A_n$.*

Todistus. Olkoot $\alpha = (a_1\ a_2\ a_3) \in H$ ja $\beta = (b_1\ b_2\ b_3) \in A_n$ mikä tahansa 3-sykli. Olkoon lisäksi $\tau_1 \in S_n$ sellainen permutaatio, että $\tau_1(a_1) = b_1$, $\tau_1(a_2) = b_2$ ja $\tau_1(a_3) = b_3$.

Jaetaan nyt tarkastelu kahteen osaan sen mukaan, että onko τ_1 parillinen vai pariton.

1) Jos τ_1 on parillinen, niin $\tau_1 \in A_n$ ja merkitään tällöin $\tau_1 = \tau$. Nyt koska H on ryhmän A_n normaali aliryhmä, niin

$$\tau\alpha\tau^{-1} \in H.$$

2) Jos τ_1 on pariton, niin $\tau = (b_4\ b_5)\tau_1$, missä $b_4 \neq b_5$ ja $b_4, b_5 \notin \{b_1, b_2, b_3\}$, on seurauksen 1.29 nojalla parillinen ja siis $\tau \in A_n$. Edelleen, koska $H \lhd A_n$, niin

$$\tau\alpha\tau^{-1} \in H.$$

Permutaation τ_1 määrittelystä johtuen molemmissa kohdissa 1) ja 2) pätee, että

$$\tau\alpha\tau^{-1} = \beta \in H.$$

Perustellaan tämä väite.

Nyt $\tau^{-1}(b_1) = a_1$, $\alpha(a_1) = a_2$ ja $\tau(a_2) = b_2$. Eli kokonaisuudessaan $\tau\alpha\tau^{-1}(b_1) = (b_2)$.

Vastaavasti nähdään, että $\tau\alpha\tau^{-1}(b_2) = b_3$ ja $\tau\alpha\tau^{-1}(b_3) = b_1$. Yhtälön vasen ja oikea puoli siis siirtävät alkioita b_1, b_2 ja b_3 samalla tavalla. Huomataan, että permutaatio τ voi siirtää alkioiden b_1, b_2 ja b_3 lisäksi myös muita alkioita, mutta τ^{-1} kumoaa nämä siirrot ja yhtälön oikea ja vasen puoli ovat siis todella samat.

Näin ollen ryhmän A_n normaali aliryhmä H sisältää kaikki 3-syklit ja lemman 3.6 nojalla $H = A_n$. □

Lause 3.8. *A_3 on yksinkertainen ryhmä.*

Todistus. Olkoon $H \neq \{(1)\}$ ryhmän A_3 normaali aliryhmä. On osoitettava, että $H = A_3$.

Ryhmässä A_3 on kolme alkiota (1), (1 2 3) ja (1 3 2). Jos kumpi tahansa 3-sykleistä kuuluu normaaliin aliryhmään H, niin tällöin molemmat 3-syklit kuuluvat sinne, koska 3-syklit ovat toistensa käänteisalkioita:

$$(1\ 2\ 3)^{-1} = (1\ 3\ 2).$$

Näin ollen $H = A_3$ ja A_3 on yksinkertainen ryhmä. □

Lause 3.9. *A_4 ei ole yksinkertainen ryhmä.*

Todistus. Ryhmälle A_4 löytyy esimerkiksi esimerkin 2.8 mukainen neljän permutaation normaali aliryhmä.

Lauseen 1.19 nojalla permutaatio $\alpha v \alpha^{-1}$ on kahden erillisen transpoosin tulo, kun $\alpha \in A_4$ ja $v \in V - \{(1)\}$. Nyt kuitenkaan ryhmässä A_4 ei ole muita kahden erillisen transpoosin tuloja, kuin ne jotka kuuluvat ryhmään V. Näin ollen $\alpha v \alpha^{-1} \in V$ ja V on siis ryhmän A_4 normaali aliryhmä. Siispä A_4 ei ole yksinkertainen ryhmä. □

Lause 3.10. *A_5 on yksinkertainen ryhmä.*

Todistus. Olkoon $H \neq \{(1)\}$ ryhmän A_5 normaali aliryhmä. On osoitettava, että $H = A_5$. Lemman 3.7 nojalla riittää kuitenkin osoittaa, että H sisältää jonkin 3-syklin.

Koska $H \neq \{(1)\}$, niin ryhmä H sisältää jonkin permutaation $\sigma \neq (1)$. Lauseen 1.28 ja seurauksen 1.29 nojalla ryhmässä A_5 on permutaation (1) lisäksi 3-syklejä, kahden transpoosin tuloja ja 5-syklejä. Voidaan siis olettaa, että permutaation σ syklirakenne on (1 2 3), (1 2)(3 4) tai (1 2 3 4 5).

Mikäli $\sigma = (1\ 2\ 3)$, niin lause on todistettu.

Jos taas $\sigma = (1\ 2)(3\ 4)$, niin määritellään permutaatio $\tau = (1\ 2)(3\ 5) \in A_5$. Koska H on ryhmän A_5 normaali aliryhmä, niin $(\tau\sigma\tau^{-1})\sigma^{-1} \in H$. Nyt kuitenkin

$$(\tau\sigma\tau^{-1})\sigma^{-1} = (1\ 2)(3\ 5)(1\ 2)(3\ 4)(1\ 2)(3\ 5)(1\ 2)(3\ 4) = (3\ 5\ 4),$$

joten myös tässä tapauksessa H sisältää 3-syklin.

Katsotaan vielä tilanne, jossa $\sigma = (1\ 2\ 3\ 4\ 5)$. Määritellään permutaatio $\rho = (1\ 3\ 2) \in A_5$. Koska edelleen H on ryhmän A_5 normaali aliryhmä, niin $(\rho\sigma\rho^{-1})\sigma^{-1} \in H$. Nyt

$$(\rho\sigma\rho^{-1})\sigma^{-1} = (1\ 3\ 2)(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(1\ 5\ 4\ 3\ 2) = (1\ 3\ 4),$$

joten taas H sisältää 3-syklin.

Täten ryhmän A_5 normaalista aliryhmästä H löytyy aina 3-sykli, joten $H = A_5$ ja A_5 on yksinkertainen ryhmä. □

Lause 3.11. *A_6 on yksinkertainen ryhmä.*

Todistus. Olkoon $H \neq \{(1)\}$ ryhmän A_6 normaali aliryhmä. On osoitettava, että $H = A_6$. Jaetaan tarkastelu kahteen osaan.

1) Oletetaan aluksi, että on olemassa sellainen permutaatio $(1) \neq \alpha \in H$, että $\alpha(i) = i$ jollakin i, missä $1 \leq i \leq 6$. Määritellään permutaatioiden joukko

$$F = \{\sigma \in A_6 : \sigma(i) = i\}.$$

Nyt $(1) \in F$ ja $F \subseteq A_6$. Lisäksi, jos $\alpha, \beta \in F$, niin $\alpha(i) = i$ ja $\beta(i) = i$. Tällöin myös $\alpha\beta(i) = i$, joten $\alpha\beta \in F$. Lauseen 2.7 nojalla F on ryhmän A_6 aliryhmä ja siis myös itse ryhmä.

Nyt tiedetään, että $\alpha \in H \cap F$ ja $H \cap F \neq \{(1)\}$.

Lauseen 2.28 nojalla $H \cap F \lhd F$. Joukon F permutaatiot permutoivat käytännöllisesti katsoen viittä alkiota, koska jokainen joukon F permutaatio säilyttää alkion i. Näin ollen $F \cong A_5$ ja lauseen 3.10 nojalla myös ryhmä F on yksinkertainen. Täten ryhmän F ainoat normaalit aliryhmät ovat $\{(1)\}$ ja F itse.

Koska kuitenkin $H \cap F \neq \{(1)\}$, niin $H \cap F = F$. Tästä seuraa suoraan, että $F \leq H$.

Ryhmän F määrittelystä johtuen se sisältää joitakin ryhmän A_6 3-syklejä. Näin ollen myös ryhmä H sisältää 3-syklejä.

Lemman 3.7 nojalla $H = A_6$.

2) Oletetaan sitten, että ei ole olemassa sellaista permutaatiota $(1) \neq \alpha \in H$, että $\alpha(i) = i$, jollakin $1 \leq i \leq 6$. Tällöin permutaatio $\alpha \in H$ siis siirtää kaikkia permutoitavan joukon alkioita ja sen mahdolliset syklirakenteet ovat esimerkin 3.5 mukaisesti $(1\ 2)(3\ 4\ 5\ 6)$ ja $(1\ 2\ 3)(4\ 5\ 6)$.

Jos permutaatio α on muotoa $(1\ 2)(3\ 4\ 5\ 6)$, niin

$$\alpha^2 = (1\ 2)(3\ 4\ 5\ 6)(1\ 2)(3\ 4\ 5\ 6) = (1)(2)(3\ 5)(4\ 6).$$

Eli tällöin permutaatio $\alpha^2 \in H$ säilyttää alkiot 1 ja 2. Tämä on ristiriidassa oletuksen kanssa, joten permutaation α syklirakenne ei voi olla muotoa $(1\ 2)(3\ 4\ 5\ 6)$.

Oletetaan nyt, että permutaatio α on muotoa $(1\ 2\ 3)(4\ 5\ 6)$.

Koska H on ryhmän A_6 normaali aliryhmä, niin H sisältää alkion $\beta\alpha^{-1}\beta^{-1}$, missä $\beta = (2\ 3\ 4) \in A_6$ ja näin myös $\alpha(\beta\alpha^{-1}\beta^{-1}) \in H$.

Katsotaan miltä tämä permutaatio näyttää:

$$\alpha(\beta\alpha^{-1}\beta^{-1}) = (1\ 2\ 3)(4\ 5\ 6)(2\ 3\ 4)(4\ 6\ 5)(1\ 3\ 2)(2\ 4\ 3)$$

$$= (1\ 5\ 3\ 2\ 4)(6).$$

Eli jälleen löytyi ryhmästä H permutaatio, joka säilyttää jonkin alkion. Tämä on ristiriidassa oletuksen kanssa.

Näin ollen ei löydy sellaista ryhmän A_6 normaalia aliryhmää, jonka kaikki permutaatiot siirtäisivät jokaista permutoitavan joukon alkiota.

Kohtien 1) ja 2) nojalla $H = A_6$ ja ryhmä A_6 on siten yksinkertainen. □

Lause 3.12. *A_n on yksinkertainen ryhmä kaikilla $n \geq 5$.*

Todistus. Koska lauseen 3.10 nojalla tiedetään, että A_5 on yksinkertainen ryhmä, voidaan keskittyä tilanteeseen, jossa $n \geq 6$.

Olkoon H ryhmän A_n sellainen normaali aliryhmä, että $H \neq \{(1)\}$. On osoitettava, että $H = A_n$. Lemman 3.7 nojalla riittää kuitenkin osoittaa, että H sisältää jonkin 3-syklin.

Koska $H \neq \{(1)\}$, niin on olemassa sellainen permutaatio $\beta \in H$, joka siirtää jotain permutoitavan joukon alkiota. Toisin sanoen $\beta(i) = j$ joillakin permutoitavan joukon alkioilla $i \neq j$.

Olkoon nyt $\alpha \in A_n$ sellainen 3-sykli, että se säilyttää alkion i, mutta siirtää alkiota j. Tällöin

$$\beta\alpha(i) = \beta(i) = j,$$

mutta

$$\alpha\beta(i) = \alpha(j) \neq j,$$

joten permutaatiot α ja β eivät kommutoi keskenään.

Koska $H \lhd A_n$, niin $\alpha\beta\alpha^{-1} \in H$ ja myös $\gamma = (\alpha\beta\alpha^{-1})\beta^{-1} \in H$. Permutaatioiden α ja β kommutoimattomuuden nojalla permutaatio $\gamma \neq (1)$. Nyt

lauseen 1.19 nojalla $\beta\alpha^{-1}\beta^{-1}$ on 3-sykli ja permutaatio $\gamma = \alpha(\beta\alpha^{-1}\beta^{-1})$ on siis kahden 3-syklin tulo.

Näin ollen permutaatio γ siirtää enintään kuutta permutoitavan joukon alkiota. Sovitaan, että nämä alkiot löytyvät joukosta $\{i_1, ..., i_6\}$ oli niitä sitten kuusi kappaletta tai vähemmän. Määritellään nyt permutaatioiden joukko

$$F = \{\sigma \in A_n : \sigma(i) = i \; kaikilla \; i \neq i_1, ..., i_6\}.$$

Selvästi $F \cong A_6$ ja $\gamma \in H \cap F$. Täten lauseen 2.28 nojalla $H \cap F$ on ryhmän F sellainen normaali aliryhmä, että $H \cap F \neq \{(1)\}$.

Toisaalta, koska $F \cong A_6$, niin lauseen 3.11 nojalla ryhmä F on yksinkertainen ja täten $H \cap F = F$. Näin ollen $F \leq H$. Koska ryhmässä F on selvästi 3-syklejä, niin myös ryhmässä H on 3-syklejä.

Täten lemman 3.7 nojalla A_n on yksinkertainen ryhmä kaikilla $n \geq 5$. $\square$

4 Ratkeavuus

Tässä luvussa tutustutaan ratkeavuuden käsitteeseen ja tutkitaan alternoivien ja symmetristen ryhmien ratkeavuutta.

Määritelmä 4.1. Ryhmän G ***normaali sarja*** on aliryhmien ketju

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{e\},$$

missä jokainen ryhmä G_{i+1} on ryhmän G_i normaali aliryhmä.

Tämän sarjan tekijäryhmät ovat

$$G_0/G_1, G_1/G_2, ..., G_{t-1}/G_t.$$

Äärellinen ryhmä G on ***ratkeava***, jos sillä on normaali sarja, jonka tekijäryhmien kertaluvut ovat alkulukuja.

Lause 4.2. *Symmetrinen ryhmä S_4 on ratkeava.*

Todistus. Tarkastellaan aliryhmien ketjua

$$S_4 \geq A_4 \geq V \geq W \geq \{(1)\},$$

missä V on esimerkin 2.8 mukainen neljän permutaation ryhmä ja W on jokin kertalukua kaksi oleva ryhmän V normaali aliryhmä.

Ryhmällä V on kolme kertalukua kaksi olevaa normaalia aliryhmää, joihin kuuluu neutraalialkio ja jokin kahden transpoosin tulo. Koska jokainen ryhmän V alkio on itsensä käänteisalkio, on aliryhmyys selvä. Lisäksi lemman 2.19 nojalla Abelin ryhmän V jokainen aliryhmä on normaali.

Lauseen 3.3 nojalla $A_4 \lhd S_4$.

Lisäksi neliryhmä V on alternoivan ryhmän A_4 normaali aliryhmä lauseen 3.9 todistuksen nojalla.

Nyt

$$|S_4/A_4| = |S_4|/|A_4| = 24/12 = 2,$$

$$|A_4/V| = |A_4|/|V| = 12/4 = 3,$$

$$|V/W| = |V|/|W| = 4/2 = 2$$

ja

$$|W/\{(1)\}| = |W|/|\{(1)\}| = 2/1 = 2.$$

Normaali sarjan tekijäryhmien kertaluvut ovat siis alkulukuja, joten S_4 on ratkeava ryhmä. □

Lause 4.3. *Alternoiva ryhmä A_4 on ratkeava.*

Todistus. Lauseen 4.2 todistus osoittaa samalla, että myös alternoiva ryhmä A_4 on ratkeava. □

Lause 4.4. *Alternoiva ryhmä A_3 on ratkeava.*

Todistus. Ryhmässä A_3 on kolme permutaatiota: (1), (1 2 3) ja (1 3 2). Koska ryhmän 3-syklit ovat toistensa käänteispermutaatioita, niin ryhmällä A_3 on vain triviaalit aliryhmät $\{(1)\}$ ja A_3. Näistä saadaan kuitenkin aikaan normaali sarja

$$A_3 = G_0 \geq G_1 = \{(1)\}.$$

Lisäksi

$$|G_0/G_1| = |A_3|/|\{(1)\}| = |A_3| = 3.$$

Koska 3 on alkuluku, niin määritelmän 4.1 mukaan A_3 on ratkeava. □

Lause 4.5. *Olkoon $n \geq 5$. Tällöin alternoiva ryhmä A_n ei ole ratkeava.*

Todistus. Kun $n \geq 5$, niin lauseen 3.12 nojalla ryhmällä A_n on olemassa vain triviaalit normaalit aliryhmät $\{(1)\}$ ja A_n. Tällöin ratkeavuuden määritelmässä esiintyvä ainoa mahdollinen normaalien aliryhmien ketju on

$$A_n = G_0 \geq G_1 = \{(1)\}.$$

Nyt kuitenkin

$$|G_0/G_1| = |A_n|/|\{(1)\}| = |A_n| = n\,!/2,$$

eikä kertaluku $n\,!/2$ ole alkuluku millään $n \geq 5$.

Näin ollen alternoiva ryhmä A_n ei voi olla ratkeava, kun $n \geq 5$. □

Lause 4.6. *Ratkeavan ryhmän G jokainen aliryhmä H on ratkeava.*

Todistus. Koska ryhmä G on ratkeava, niin on olemassa aliryhmien ketju

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{e\},$$

missä jokainen ryhmä G_i on ryhmän G_{i-1} normaali aliryhmä. Lisäksi tekijäryhmien G_{i-1}/G_i kertaluvut ovat alkulukuja kaikilla i.

Muodostetaan aliryhmien ketju aliryhmälle H:

$$H = H \cap G_0 \geq H \cap G_1 \geq H \cap G_2 \geq \cdots \geq H \cap G_t = \{e\}.$$

Jos $h \in H \cap G_i$ ja $g \in H \cap G_{i-1}$, niin $ghg^{-1} \in H$ ja $ghg^{-1} \in G_i$, koska G_i on ryhmän G_{i-1} normaali aliryhmä. Näin ollen $ghg^{-1} \in H \cap G_i$ eli
$H \cap G_i \lhd H \cap G_{i-1}$.

Siispä kyseessä on normaali sarja ja

$$(H \cap G_{i-1})/(H \cap G_i) = (H \cap G_{i-1})/[(H \cap G_{i-1}) \cap G_i].$$

Lisäksi lauseen 2.28 nojalla

$$(H \cap G_{i-1})/[(H \cap G_{i-1}) \cap G_i] \cong G_i(H \cap G_{i-1})/G_i.$$

Nyt kuitenkin ryhmä $G_i(H \cap G_{i-1})/G_i$ on ryhmän G_{i-1}/G_i aliryhmä.

Koska ryhmän G_{i-1}/G_i kertaluku on alkuluku, niin lauseen 2.12 nojalla sillä on vain triviaalit aliryhmät G_{i-1}/G_i ja $\{e\}$, joiden kertaluku on 1 tai jokin alkuluku. Siispä myös tekijäryhmän $(H \cap G_{i-1})/(H \cap G_i)$ kertaluku on isomorfisuuden nojalla 1 tai jokin alkuluku.

Jos tekijäryhmän $(H \cap G_{i-1})/(H \cap G_i)$ kertaluku on 1, niin silloin ryhmät $(H \cap G_{i-1})$ ja $(H \cap G_i)$ ovat samat. Tällöin toinen näistä ryhmistä voidaan jättää pois ja lopulta päädytään tilanteeseen, jossa jokaisen tekijäryhmän kertaluku on alkuluku.

Näin ollen ryhmän G aliryhmälle H muodostettu aliryhmien ketju täyttää ratkeavuuden määritelmässä esitetyt vaatimukset ja aliryhmä H on siis ratkeava. □

Lause 4.7. *Olkoon $n \geq 5$. Tällöin symmetrinen ryhmä S_n ei ole ratkeava.*

Todistus. Jos symmetrinen ryhmä S_n olisi ratkeava, niin lauseen 4.6 nojalla jokaisen sen aliryhmän täytyisi myös olla ratkeava.

Lauseen 4.5 nojalla alternoiva ryhmä A_n ei kuitenkaan ole ratkeava, kun $n \geq 5$. Koska lisäksi $A_n \leq S_n$, niin myöskään symmetrinen ryhmä S_n ei voi olla ratkeava, kun $n \geq 5$. □

Lähdeluettelo

[1] Markku Niemenmaa, Jukka Kauppi: *Algebra 2*, Oulun yliopisto, 2008.

[2] Joseph J. Rotman: *Advanced modern algebra*, University of Illions at Urbana-Champaign, 2002.

[3] Seth Warner: *Modern algebra 2*, Duke University, 1965.