Permutaatioista alternoivaan ryhmään

Pro Gradu-tutkielma
Sini-Susanna Fetula
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2014

Sisältö

1 Johdanto

Tutkielmani aihe liittyy ryhmäteoriaan ja on mielestäni yksi sen mielenkiintoisimmista aihealueista. Ryhmäteoriassa ei tarvita (ainakaan tällä tasolla) kovin pitkälle meneviä matemaattisia laskutekniikoita, vaan se vaatii uudenlaisen ajatusmaailman sisäistämistä. Siinä onkin sen haastavuus, sekä helppous ja mielenkiintoisuus.

Tässä työssä en lähde aivan ryhmäteorian alkeista, tai ainakaan käy niitä tarkemmin läpi. Esitietoja käsittelevässä osiosta löytyy muutama esimerkki ja määritelmä, jotka katsoin hyväksi laittaa muistin virkistämiseksi ja selkiyttämiseksi. Sekä tämän tutkielman aiheen teoria, että ryhmäteorian alkeet löytyy päälähteenä käyttämästäni I.N Hersteinin kirjasta Abstract Algebra. Lisäksi itse olen käyttänyt myös Algebra II - kurssin luentomonistetta ja luentomuistiinpanoja apuna.

Esitietoja kappaleessa on ryhmäteorian alkeisiin kuuluvia määritelmiä, lauseita ja joitain todistuksia. Kaikkia lauseita ei ole todistettu, vaan ne otetaan pelkkänä tuloksena, jotta fokus säilyisi olennaisessa. Nämä tiedot ovat kuitenkin olennaisia ja niitä käytetään moneen kertaan tutkielman aikana ja liittyvät sinänsä tiiviisti tutkielman aiheeseen.

Luvussa 3 käsitellään tutkielman aiheen perusteita, eli permutaatioita ja niiden ominaisuuksia. Luvun kahdessa ensimmäisessä kappaleessa määritellään permutaatiot, esitetään niille muutama esitystapa ja havainnollistetaan niiden käyttöä esimerkein. Luvussa 3.3 keskitytään permutaatioiden esitykseen muiden permutaatioiden avulla eli esitykseen erillisten syklien tulona. Luvun viimeisessä kappaleessa tarkastellaan permutaatioiden pariteettia, joka on yksi permutaatioiden käytetyimmistä ominaisuuksista.

Neljännessä luvussa käsitellään permutaatioryhmiä, niiden ratoja sekä permutaatioiden käyttöä käytännön sovelluksissa. Lisäksi todistetaan muutama ominaisuus permutaatioryhmälle ja sen radoille. Tämän kaappaleen tarkoitus on esitellä permutaatioiden syvempää, soveltavampaa puolta ja näyttää, että niitä voidaan hyödyntää myös käytännössä.

Luvussa 5 päästään sitten käsiksi alternoivaan ryhmään. Ensimmäisessä kappaleessa luonnollisesti esitellään miten alternoiva ryhmä A_n määritellään ja mitä se käytännössä tarkoittaa. Kappaleessa 5.2 lähdetään vähän kiertotietä tutkimaan alternoivan ryhmän ominaisuuksia. Jotta näitä ominaisuuksia pääsisi tutkimaan, täytyy ensin perehtyä hieman permutaatioiden konjugointiin. Tämän kappaleen päämäärä ja koko tutkielman yksi päätuloksista on alternoivan ryhmän A_n yksinkertaisuus, kun $n \geq 5$.

2 Esitietoja

Määritelmä 2.1. Olkoon G epätyhjä joukko ja kuvaus $\bullet: G \times G \to G$, $\bullet(a,b) = a \bullet b$. Nyt pari $(G, \bullet)$ on *ryhmä* mikäli

1. $(\bullet)$ on joukon G *binäärinen operaatio*, eli $\bullet(a,b) = a \bullet b \in G$ kaikilla $a, b \in G$.

2. $(\bullet)$ on *assosiatiivinen operaatio* joukossa G eli $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ kaikilla $a, b, c \in G$.

3. Joukossa G on *neutraalialkio* e, jolle pätee $a \bullet e = e \bullet a = a$ kaikilla $a \in G$.

4. Jokaiselle alkiolle $a \in G$ on olemassa joukossa G *käänteisalkio* a^{-1}, jolle pätee $a^{-1} \bullet a = a \bullet a^{-1} = e$, missä e on siis joukon G neutraalialkio.

Esimerkki 2.2. Tutkitaan onko pari $(\{1, -1\}, \cdot)$, missä $(\cdot)$ on kokonaislukujen kertolasku ryhmä: Nyt

1) $a \cdot b \in \{1, -1\}$ kaikilla $a, b \in \{1, -1\}$

2) kokonaislukujen kertolaskulle pätee assosiatiivisuus, joten
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ kaikilla $a, b, c \in \{1, -1\}$

3) neutraalialkio $i = 1 \in \{1, -1\}$

4) $-1 \cdot -1 = 1 = i$ ja $1 \cdot 1 = 1 = i$,joten $a^{-1} \in \{1, -1\}$ kaikilla $a \in \{1, -1\}$

kohtien 1) , 2) , 3) ja 4) nojalla pari $(\{1, -1\}, \cdot)$ on ryhmä.

Määritelmä 2.3. Olkoon pari $(G, \bullet)$ ryhmä (toteuttaa edellä mainitut ehdot). Jos pari toteuttaa lisäksi ehdon $a \bullet b = b \bullet a$ kaikilla $a, b \in G$, eli $(\bullet)$ on kommutatiivinen operaatio G:ssä, niin pari $(G, \bullet)$ on *Abelin ryhmä.*

Määritelmä 2.4. Olkoon $(G, \bullet)$ ryhmä ja $H \subseteq G$, $H \neq \emptyset$, eli H on joukon G epätyhjä osajoukko. Nyt $(H, \bullet)$ on ryhmän $(G, \bullet)$ *aliryhmä*, mikäli pari $(H, \bullet)$ on ryhmä. Tällöin merkitään $(H, \bullet) \leq (G, \bullet)$, tai lyhemmin $H \leq G$.

Määritelmä 2.5. Olkoon $(G, \bullet)$ ryhmä ja $(H, \bullet)$ sen aliryhmä. Nyt $(H, \bullet)$ on ryhmän $(G, \bullet)$ *normaali aliryhmä*, jos $Ha = \{h \bullet a | h \in H\} = \{a \bullet h | h \in H\} = aH$ kaikilla $a \in G$. Joukkoa Ha kutsutaan *alkion a määräämäksi aliryhmän $(H, \bullet)$ oikeaksi sivuluokaksi* ja joukkoa aH kutsutaan vastaavasti *alkion a määräämäksi aliryhmän $(H, \bullet)$ vasemmaksi sivuluokaksi.*

Lause 2.6 (normaalisuuskriteeri)**.** *Olkoon* $(G, \bullet)$ *ryhmä ja* $(H, \bullet)$ *sen aliryhmä. Nyt* $(H, \bullet)$ *on normaali jos ja vain jos* $aHa^{-1} \subseteq H$ *aina, kun* $a \in G$*.*

Määritelmä 2.7. Olkoot $(G, \bullet)$ ja $(G', *)$ ryhmiä ja kuvaus $f : G \to G'$. Nyt kuvaus f on *homomorfismi*, jos $f(a \bullet b) = f(a) * f(b)$ kaikilla $a, b \in G$. Eli kuvaus f niin sanotusti säilyttää operaation.

Määritelmä 2.8. Olkoot $(G, \bullet)$ ja $(G', *)$ ryhmiä ja $\rho : G \to G'$ homomorfismi. Kuvauksen ρ *kuvaksi* sanotaan joukkoa $Im(\rho) = \{\rho(a) | a \in G\}$. Eli joukkoa johon kuuluu kaikki ne ryhmän $(G', *)$ alkiot, jotka saadaan kuvauksella ρ.

Joukkoa $Ker(\rho) = \{a \in G | \rho(a) = e'\}$, missä e' on ryhmän $(G', *)$ neutraalialkio, sanotaan kuvauksen ρ *ytimeksi*. Ytimeen siis kuuluu kaikki ne ryhmän $(G, \bullet)$ alkiot, jotka ρ kuvaa maaliryhmän $(G', *)$ neutraalialkioksi.

Lause 2.9 (Homomorfismin peruslause, hpl)**.** *Olkoot* $(G, \bullet)$ *ja* $(G', *)$ *ryhmiä ja homomorfismi* $g : G \to G'$ *surjektio,eli* $Im(g) = G'$*. Olkoon lisäksi* $Ker(g) = K$ *Nyt* $G' = Im(g) \cong G/K$*.*

Määritelmä 2.10. Kuvausten yhdistämisoperaatio ($\circ$) määritellään seuraavasti: $f \circ g(x) = f(g(x))$, missä f ja g ovat siis kuvauksia.

Lause 2.11. *Kuvausten yhdistämisoperaatio* ($\circ$) *on assosiatiivinen.*

Todistus. Olkoon f, g ja h kuvauksia, joiden lähtö- ja maalijoukot ovat sopivat. Nyt $[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x))) = f(g \circ h(x)) = [f \circ (g \circ h)](x)$. □

Määritelmä 2.12. Olkoon G ryhmä ja $\alpha \in G$. Nyt *alkion* α *kertaluku* $|\alpha| = s$, missä s on pienin kokonaisluku s, jolle pätee $\alpha^s = (i)$.

Määritelmä 2.13. Ryhmän G *keskus* $Z(G) = \{\sigma \in G | g\sigma = \sigma g, g \in G\}$ sisältää kaikki ne ryhmän alkiot σ, jotka kommutoivat ryhmän muiden alkioioden kanssa.

Lause 2.14. *Jos* $(i) \neq \sigma \in A_n$*, niin on olemassa 3-sykli* τ*, jolle pätee* $\sigma\tau \neq \tau\sigma$*.*

Todistus. Vastaoletus: Olkoon $\alpha \in A_n$ 3-sykli. Tällöin $\sigma\alpha = \alpha\sigma$. Olkoon sitten $g \in A_n$. Nyt voidaan kirjoittaa $g = \alpha_1\alpha_2 \cdots \alpha_r$, missä α_i, $i = 1, ..., r$ on 3-syklejä, sillä 3-syklit generoivat A_n:n. Tällöin vastaoletuksen nojalla $g\sigma = \sigma\alpha_1\alpha_2 \cdots \alpha_r = \alpha_1\alpha_2 \cdots \alpha_r\sigma = \sigma g$. Tällöin $(i) \neq \sigma \in Z(A_n) = \{(i)\}$, mikä on ristiriita. Täten vastaoletus on siis väärä ja väite tosi. □

Lause 2.15. *Olkoon G ryhmä ja $H \leq G$ sekä N ryhmän G normaali aliryhmä. Tällöin $N \cap H$ on normaali ryhmässä H.*

Todistus. Nyt $N \cap H = \{x | x \in N \text{ ja } x \in H\}$. Joten $N \cap H \subset H$,$N \cap H$ on ryhmä (N ja H ovat ryhmiä) ja lisäksi normaalius ehto toteutuu, sillä N on normaali. Tästä seuraa, että $N \cap H$ on normaali aliryhmä H:ssa. □

3 Permutaatioista.

Tässä kappaleessa määritellään mitä permutaatio tarkoittaa, esitetään niille muutamakin erilainen esitystapa. Lisäksi tarkastellaan permutaatioiden ominaisuuksia, kuten pariteettia ja esitystä erillisten syklien tulona.

3.1 Symmetrinen ryhmä ja permutaation määritys.

Määritelmä 3.1. Merkitään joukkoa $\{x_1, ..., x_n\} = X$ Jos kuvaus $\sigma : X \to X$ on bijektio, niin sitä kutsutaan joukon X *permutaatioksi.*

Merkitään lisäksi joukon $X = \{x_1, ..., x_n\}$ kaikkien permutaatioiden joukkoa S_n:llä.

Lause 3.2. *Pari* $(S_n, \circ)$*, missä* $(\circ)$ *on kuvausten yhdistämisoperaatio, on ryhmä.*

Todistus. Olkoon $\alpha, \beta, \gamma \in S_n$. Nyt

1) $\alpha \circ \beta : X \to X$ on bijektio,eli $\alpha \circ \beta \in S_n$, sillä $\alpha : X \to X$ ja $\beta : X \to X$ ovat bijektioita.

2) Kuvaus $i(x) = x$, $x \in X$ kuuluu joukkoon S_n. Lisäksi $\alpha \circ i = i \circ \alpha = \alpha$, joten neutraalialkio $i \in S_n$.

3) Kuvausten yhdistämis operaatiolle pätee assosiatiivisuus, joten $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.

4) $\alpha^{-1} : X \to X$ on bijektio, sillä $\alpha : X \to X$ on bijektio. Lisäksi $\alpha^{-1} \circ \alpha = \alpha \circ \alpha^{-1} = i$, joten käänteisalkio ehto toteutuu.

kohtien 1) , 2) , 3) ja 4) nojalla pari $(S_n, \circ)$ on ryhmä. □

Määritelmä 3.3. Ryhmää $(S_n, \circ)$ sanotaan *astetta n olevaksi symmetriseksi ryhmäksi.*

Ryhmäteoriassa on usein tapana jättää tunnettujen ryhmien operaatio merkitsemättä käytännön syistä, joten jatkossa merkitään $(S_n, \circ) = S_n$.

Voidaan todeta päättelemällä, että astetta n olevan symmetrisen ryhmän S_n kertaluku $|S_n| = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1 = n!$.

3.2 Permutaatioiden esitystavoista.

Kun jatketaan permutaatioiden ja permutaatioryhmien käsittelyä, tarvitaan jokin kätevä tapa kuvata permutaatioita ja miten ne kuvaavat kunkin joukon X alkion. Tässä luvussa esitellään kolme erilaista tapaa merkitä/kuvata permutaatioita.

Olkoon siis joukko $X = \{x_1, x_2, ..., x_n\}$ ja annettu permutaatio $\sigma \in S_n$ sellainen, että $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$,...,$\sigma(x_{n-1}) = x_n$ ja $\sigma(x_n) = x_1$. Permutaatiota voidaan havainnollistaa esimerkiksi siten, että kirjoitetaan riviin kaikki joukon X alkiot ja niiden alapuolelle niiden kuvat vastaavassa järjestyksessä. Tällöin esitys näyttäisi seuraavalta:

$$\sigma = \begin{pmatrix} x_1 & x_2 & ... & x_{n-1} & x_n \\ x_2 & x_3 & ... & x_n & x_1 \end{pmatrix}$$

Tätä merkintätapaa voidaan vielä yksinkertaistaa samaistamalla kaikki joukot X, joissa on n kappaletta elementtejä/alkioita. Samaistaminen onnistuu numeroimalla alkiot ja käsittelemällä niitä vain lukuina.

Tällöin $X = \{1, 2, ..., n\}$ ja $\sigma = \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ 2 & 3 & ... & n & 1 \end{pmatrix}$

Esimerkki 3.4. Olkoon $X = \{1, 2, 3, 4\}$ ja $\sigma \in S_4$ seuraavanlainen permuutaatio: $\sigma(1) = 3$,$\sigma(2) = 2$,$\sigma(3) = 1$ ja $\sigma(4) = 4$. Tällöin $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

Huomautus 3.5. Edellä esitetyssä kaksirivisessä esitystavassa ei ole välttämätöntä kirjoittaa yläriville joukon X alkioita järjestyksessä, vaan sama permutaatio voidaan kirjoittaa useammalla eri tavalla. Esimerkiksi edellisen esimerkin permutaatio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = ...$$

Tästä kaksirivisestä esitystavasta on myös helppo saada selville annetun permutaatiokuvauksen käänteiskuvaus. Jos esimerkiksi $\sigma(1) = 2$, niin $\sigma^{-1}(2) = 1$. Kun tämä tehdään kaikille alkioille, niin käytännössä rivien paikat vain vaihtuu.

Esimerkki 3.6. Jos $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, niin $\tau^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Jos $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, niin $\sigma^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

Huomautus 3.7. Kuvaus voi siis olla myös itsensä käänteiskuvaus, kuten edellisen esimerkin σ.

Entäpä sitten yhdistetyn kuvauksen laskeminen kaksirivisen esitystavan avulla? Kuvausten yhdistämisoperaation määrittelyn nojalla yhdistetty kuvaus saadaan kertomalla permutaatiot oikealta vasemmalle. Jos esimerkiksi $\tau(3) = 2$ ja $\sigma(2) = 2$, niin $\sigma \circ \tau(3) = 2$. Seuraavassa esimerkissä on pyritty havainnollistamaan tätä käytännössä.

Esimerkki 3.8. Olkoon $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ ja $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ Nyt

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Edellä käytetyssä kaksirivisessä esitystavassa on usein tapana kirjoittaa ylemmälle riville alkiot järjestyksessä, joten se voidaan jossain tapauksissa jättää kirjoittamatta. Esimerkiksi $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 & 4 \end{pmatrix}$.

Huom! Tätä yksirivistä esitystapaa ei kuitenkaan pidä sekoittaa seuraavaksi käsiteltävään sykliesitykseen.

Jatketaan siis edelleen permutaatioiden käsittelyä ja vieläkin yksinkertaisemman esitystavan hakemista.

Olkoon edelleen $X = \{1, 2, ..., (n-1), n\}$. Nyt permutaatio σ säilyttää alkion $i \in X$, jos ja vain jos $\sigma(i) = i$. Vastaavasti σ siirtää alkion $j \in X$, jos ja vain jos $\sigma(j) \neq j$. Merkintä $\sigma = \begin{pmatrix} i_1 & i_2 & ... & i_r \end{pmatrix}$, missä $i_k \in X, 1 \leq k \leq n$ tarkoittaa, että $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, ... , $\sigma(i_{r-1}) = i_r$ ja $\sigma(i_r) = i_1$ ja lisäksi σ säilyttää muut joukon X alkiot.

Määritelmä 3.9. Permutaatiota $\sigma = \begin{pmatrix} i_1 & i_2 & ... & i_r \end{pmatrix}$, jonka pituus on r sanotaan *r-sykliksi*

Esimerkki 3.10. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \end{pmatrix}$ ja

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 4 & 3 \end{pmatrix}$$

Seuraavassa vielä muutama asia, jotka on syytä mainita sykliesityksen yhteydessä.

1) Identiteettikuvausta, joka säilyttää kaikki alkiot merkitään usein
   $i = \begin{pmatrix} 1 \end{pmatrix}$

2) 2-syklejä $\sigma = \begin{pmatrix} i_1 & i_2 \end{pmatrix}$ kutsutaan transpooseiksi

3) k-syklin kertaluku on k.

perustellaan vielä kohta 3): Olkoon $\sigma = \begin{pmatrix} 1 & 2 & ... & k \end{pmatrix} \in S_n$. Nyt
$\sigma(1) = 2$, $\sigma^2(1) = \sigma(\sigma(1)) = \sigma(2) = 3$, ..., $\sigma^k(1) = 1$.

Vastaavasti $\sigma(i)^k = i$ kaikilla $i \in \{1, 2, ..., k\}$. Lisäksi σ säilyttää ne joukon X alkiot, jotka eivät kuulu joukkoon $\{1, 2, ..., k\}$, joten saadaan että $\sigma(i)^k = i$ kaikilla $i \in \{1, 2, ..., n\} = X$. Täten σ:n kertaluku $|\sigma| = k$.

Myös sykliesityksestä saadaan kätevästi annetun permutaation käänteiskuvaus kirjoittamalla annetun syklin elementit käänteisessä järjestyksessä. Jos esimerkiksi $\sigma = \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix}$, niin $\sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \end{pmatrix}$.

Sykliesityksessä on helppouden ja yksinkertaisuuden lisäksi yksi iso etu verrattuna aikaisempiin esitystapoihin. Sykliesityksen avulla voidaan nimittäin kirjoittaa pitkät ja hankalat permutaatiokuvaukset lyhyempien ja selkeämpien syklien avulla. Seuraavassa luvussa käydäänkin tätä asiaa läpi.

3.3 Permutaatiot erillisten syklien tulona

Määritelmä 3.11. Kaksi sykliä ovat erilliset, mikäli niillä ei ole yhtään samaa elementtiä, eli ne eivät siirrä yhtään samaa alkiota.

Esimerkiksi $\begin{pmatrix} 1 & 3 & 4 \end{pmatrix} \in S_7$ ja $\begin{pmatrix} 2 & 7 \end{pmatrix} \in S_7$ ovat erillisiä syklejä, mutta $\begin{pmatrix} 1 & 3 & 4 \end{pmatrix} \in S_7$ ja $\begin{pmatrix} 3 & 5 & 6 \end{pmatrix} \in S_7$ eivät ole erillisiä.

Lause 3.12. *Mikäli $\sigma, \tau \in S_n$ ovat erillisiä, niin niille pätee $\tau\sigma = \sigma\tau$.*

Todistus. Olkoon $i \in X$.

1. Olkoon lisäksi $\sigma(i) = i$ sekä $\tau(i) = i$. Nyt
   $\sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i)) = \tau\sigma(i)$

2. Olkoon sitten $\sigma(i) \neq i$, tällöin $\tau(i) = i$, sillä σ ja τ ovat erillisiä. Nyt
   $\sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) \overset{(*)}{=} \tau(\sigma(i)) = \tau\sigma(i)$.
   (*)= τ ei siirrä alkiota $\sigma(i)$, koska σ ja τ ovat erillisiä.

3. Tapaus, jossa $\tau(i) \neq i$, ja $\sigma(i) = i$ toimii vastaavasti kuin kohta 2.

Näistä kolmesta kohdasta saadaan, että $\sigma\tau(i) = \tau\sigma(i)$ kaikilla $i \in S_n$ ja väite on todistettu. □

Vähän myöhemmin tullaan todistamaan, että jokainen permutaatio voidaan esittää erillisten syklien tulona. Tarkastellaan nyt ensin, miten ylipäätään voidaan löytää "osasyklejä" annetun syklin sisältä.

Määritelmä 3.13. *alkion $i \in X$ määräämä sykli permutaatiossa $\sigma \in S_n$* on $\begin{pmatrix} \sigma(i) & \sigma^2(i) & ... & \sigma^{s-1}(i) \end{pmatrix}$, missä s on pienin kokonaisluku, joka toteuttaa ehdon $\sigma^s(i) = i$.

Esimerkki 3.14. Jos $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 4 & 6 \end{pmatrix}$, niin 1. määräämä sykli σ:ssa on $\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}$.

Lause 3.15. *Jokainen permutaatio voidaan esittää erillisten syklien tulona.*

Todistus. Olkoon $\sigma \in S_n$ sellainen permutaatio, joka siirtää k alkiota. Todistetaan väite induktiolla K:n suhteen.

1) Jos $k = 0$, niin $\sigma = i = \begin{pmatrix} 1 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \cdots \begin{pmatrix} n \end{pmatrix}$. Olkoon siis jatkossa $k > 0$.

2) Induktio-oletus: Jos σ:n siirtämien alkioiden lukumäärä on pienempi kuin k, niin se voidaan esittää erillesten syklien tulona.

3) Olkoon nyt $\sigma \in S_n$ sellainen permutaatio, joka siirtää k alkiota ja i_1 eräs alkio, jonka σ siirtää. Merkitään i_1:n määräämää sykliä σ:ssa $\alpha = \begin{pmatrix} i_1 & i_2 & ...i_r \end{pmatrix}$. Luonnollisesti $r \leq k$, jos $r = k$, niin $\sigma = \alpha$ ja σ on itsessään sykli. Oletetaan siis seuraavaksi, että $r < k$ ja tarkastellaan permutaatiota $\sigma\alpha^{-1}$. Nyt $\sigma\alpha^{-1}$:n kertaluku on korkeintaan k ja se säilyttää alkiot $i_1, i_2, ..., i_r$, joten sen siirtämien alkioiden lukumäärä on pienempi kuin k. Induktio-oletuksen nojalla siis $\sigma\alpha^{-1} = \beta_1\beta_2...\beta_t$, missä $\beta_1, \beta_2, ..., \beta_t$ ovat erillisiä. Lisäksi $\beta_1, \beta_2, ..., \beta_t$ ovat erillisiä α:n kanssa, sillä $\sigma\alpha^{-1}$ säilyttää kaikki α:n alkiot, joten ne eivät ole mukana syklissä $\sigma\alpha^{-1}$. Olemme siis saaneet seuraavan yhtälön

$$\sigma\alpha^{-1} = \beta_1\beta_2...\beta_t \Leftrightarrow \sigma = \beta_1\beta_2...\beta_t\alpha$$

, jossa σ on erillisten syklien tulo.

Induktioperiaatteen nojalla väite on nyt todistettu. □

Lause 3.16. *Jokainen sykli voidaan esittää transpoosien tulona.*

Todistus. Nyt $\sigma = \begin{pmatrix} 1 & 2 & ... & k \end{pmatrix} = \begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 1 & k-1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$, joten jokainen permutaatio voidaan esittää transpoosien (Ei välttämättä erillisiä!) tulona. □

Seuraus 3.17. Kahden edellisen lauseen nojalla jokainen permutaatio voidaan esittää transpoosien tulona.

Esimerkki 3.18. Esitetään $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 5 & 1 & 7 & 6 \end{pmatrix}$ erillisten syklien tulona.

Nyt $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 5 & 1 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 3 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 3 & 7 & 6 \end{pmatrix}$.

Lause 3.19. *Jos $\sigma = \alpha_1\alpha_2...\alpha_t$ on permutaation σ esitys erillisten syklien tulona ja $|\alpha_i| = k_i$, $1 \leq i \leq k$, niin $|\sigma| = pyj(k_1, k_2, ..., k_t)$.*

Todistus. Merkitään $pyj(k_1, k_2, ..., k_t) = M$. Nyt $\sigma^M = \alpha_1^M\alpha_2^M...\alpha_t^M$. Koska $M = pyj(k_1, k_2, ..., k_t)$, niin $\alpha_i^M = i$, kaikilla $1 \leq i \leq k$ ja siten $\sigma^M = i$. Toisaalta, jos $\sigma^N = i$, niin vastaavasti $\alpha_i^N = i$, kaikilla $1 \leq i \leq k$. Syklin kertaluvun määritelmän nojalla $k_i|N$ kaikilla $1 \leq i \leq k$. Siten myös $M = pyj(k_1, k_2, ..., k_t)|N$ ja $|\sigma| = M = pyj(k_1, k_2, ..., k_t)$. □

Tämän kappaleen tärkein tulos on, että jokainen permutaatio voidaan esittää erillisten (eivät siirrä yhtään samaa alkiota)syklien tulona ja kertaluku saadaan esityksen erillisten syklien kertalukujen pienimmästä yhteisestä jaettavasta.

3.4 Parilliset ja parittomat permutaatiot.

Permutaation esitys transpoosien tulona ei ole yksikäsitteinen, mutta tietyt ominaisuudet määräytyvät yksiselitteisesti annetusta permutaatiosta. Lähdetään seuraavaksi tarkastelemaan permutaatioiden pariteettia. Tarkastelussa täytyy lähteä liikkeelle hieman mutkan kautta ja ensin määritelläänkin kaksi uutta kuvausta.

Olkoon

$$N = \prod_{1 \leq i < j \leq n} (j - i).$$

Jos $\sigma \in S_n$, niin merkitään

$$\sigma N = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)).$$

Kuvaukselle N pätee myös $\sigma N = N$ tai $\sigma N = -N$ kaikilla $\sigma \in S_n$. Tätä ominaisuutta en perustele tarkemmin tässä työssä, vaan otan sen pelkkänä tuloksena. Katsotaan seuraavaksi kuitenkin pari esimerkkiä, jotka tukevat väitettä.

Esimerkki 3.20. Olkoon n=3, $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix} \in S_3$, $\tau = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in S_3$. Nyt $N = (2-1)(3-2)(3-1) = 2$ ja

$$\sigma N = (\sigma(2)-\sigma(1))(\sigma(3)-\sigma(2))(\sigma(3)-\sigma(1)) = (1-2)(3-1)(3-2) = -2 = -N$$

sekä

$$\tau N = (\tau(2)-\tau(1))(\tau(3)-\tau(2))(\tau(3)-\tau(1)) = (3-2)(1-3)(1-2) = 2 = N.$$

Määritellään seuraavaksi kuvaus $F : S_n \to (\{1,-1\},\cdot)$, $(\cdot)$ on kokonais lukujen kertolasku ja pari $(\{1,-1\},\cdot)$ on ryhmä (todistus esitietoja käsittelevässä osiossa) seuraavasti:

$$F(\sigma) = \begin{cases} 1 & ,\text{kun } \sigma N = N \\ -1 & ,\text{kun } \sigma N = -N \end{cases}.$$

Kuvauksien σN ja F avulla määritellään permutaation pariteetti seuraavalla tavalla:

Määritelmä 3.21. Kuvausta $\sigma \in S_n$ sanotaan *parittomaksi permutaatioksi*, jos $F(\sigma) = -1$. Vastaavasti sitä kutsutaan *parilliseksi permutaatioksi*, jos $F(\sigma) = 1$.

Esimerkki 3.22. Edellisen esimerkin $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix} \in S_3$ on pariton permutaatio, sillä $\sigma N = -2 = -N \Rightarrow F(\sigma) = -1$ ja $\tau = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in S_3$ on parillinen, sillä $\tau N = 2 = N \Rightarrow F(\tau) = 1$.

Lause 3.23. *Jos $\sigma \in S_n$ on transpoosi, niin σ on pariton permutaatio.*

Todistus. Olkoon $\sigma = \begin{pmatrix} i & j \end{pmatrix}$,missä $1 \leq i < j \leq n$. Laskettaessa tuloa σN lasketaan lukujen $(\sigma(u) - \sigma(v))$, missä $1 \leq v < u \leq n$ tuloa. Huomataan, että negatiivisia tulontekijöitä tässä tulossa on $2(j-i-1)+1 = 2j-2i-1 = 2(j-i)-1$ kappaletta. Koska $1 \leq i < j \leq n$ ja j ja i ovat kokonaislukuja, niin $2(j-i)$ on parillinen kokonaisluku. Täten negatiivisten tulontekijöiden lukumäärä $2(j-i)-1$ on pariton kokonaisluku ja tulo $\sigma N < 0$. Tulon ominaisuuden perusteella $\sigma N = -N$ ja σ on pariton. □

Jotta kuvauksien σN ja F avulla saataisiin selville muidenkin kuin transpoosien pariteetti, tarkastellaan miten kuvaus F toimii yhdistetylle kuvaukselle.

Olkoon $\sigma, \tau \in S_n$. Tällöin

$$(\tau\sigma)N = \prod_{1 \leq i < j \leq n} (\tau\sigma(j) - \tau\sigma(i)) = \prod (\tau(j') - \tau(i')).$$

Kun tähän lisätään ehto $\tau(j') - \tau(i') = -[\tau(i') - \tau(j')]$ kaikilla $i' > j'$, niin saadaan

$$(\tau\sigma)N = F(\sigma) \prod_{1 \le i < j \le n} (\tau(j) - \tau(i)) = F(\sigma)\tau N = F(\sigma)F(\tau)N.$$

Tästä saadaan kuvauksen F määritelmä huomioiden tulos $F(\tau\sigma) = F(\tau)F(\sigma)$, eli F on ryhmähomomorfismi.

Tiedetään lisäksi, että $F(\sigma) = -1$, kun σ on transpoosi. Tämän ja edellä todistetun ominaisuuden $F(\tau\sigma) = F(\tau)F(\sigma)$ nojalla voidaan suoraan päätellä, että permutaatio $\alpha \in S_n$ on pariton jos ja vain jos sen esityksessä transpoosien tulona on pariton määrä transpooseja.

Edellisessä luvussa todettiin, että k-sykli $\sigma = \begin{pmatrix} 1 & 2 & \dots & k \end{pmatrix} \in S_n$ voidaan esittää transpoosien tulona seuraavasti:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k \end{pmatrix} = \begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 1 & k-1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

Tässä esityksessä transpooseja on k-1 kappaletta ja voidaan suoraan päätellä, että jos k on parillinen, niin k-1 on pariton luku ja k-syklit ovat parittomia permutaatioita. Vastaavasti, jos k on pariton ,niin k-1 on parillinen ja k-syklit ovat parillisia permutaatioita. Syklin pariteetin näkee siis kätevästi suoraan syklin pituudesta/kertaluvusta.

Esimerkki 3.24. 3-syklit $\sigma = \begin{pmatrix} i & j & k \end{pmatrix}$ ovat parillisia, sillä k=3 on pariton. 6-syklit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ ovat parittomia, sillä k=6 on parillinen.

Kuvauksen F homomorfisuudesta voidaan myös päätellä seuraavat "pariteetti laskusäännöt":

1) parillinen· parillinen=parillinen

2) parillinen· pariton=pariton

3) pariton· pariton=parillinen.

Esimerkki 3.25. Olkoon

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 5 & 2 & 3 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 8 & 6 \end{pmatrix} \begin{pmatrix} 7 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 4 & 5 & 2 \end{pmatrix}}_{pariton} \underbrace{\begin{pmatrix} 3 & 8 & 6 \end{pmatrix}}_{parillinen}.$$

Nyt $F(\sigma) = F(\begin{pmatrix} 1 & 4 & 5 & 2 \end{pmatrix})F(\begin{pmatrix} 3 & 8 & 6 \end{pmatrix}) = -1 \cdot 1 = -1$

Huomautus 3.26. Symmetrisen ryhmän S_n permutaatio σ on joko pariton tai parillinen, mutta ei voi olla molempia.

Lause 3.27. *Permutaatiolla σ ja sen käänteiskuvauksella σ^{-1} on sama pariteetti.*

Todistus. Olkoon $\sigma = \alpha_1\alpha_2\cdots\alpha_k$ permutaation esitys transpoosien tulona. Nyt $\sigma^{-1} = (\alpha_1\alpha_2\cdots\alpha_k)^{-1} \overset{(*)}{=} \alpha_k^{-1}\alpha_{k-1}^{-1}\cdots\alpha_1^{-1} \overset{(**)}{=} \alpha_k\alpha_{k-1}\cdots\alpha_1$. Joten kuvauksilla σ ja σ^{-1} on sama pariteetti.

$(*)$ = yhdistetyn kuvauksen käänteiskuvaus.

$(**)$ = transpoosit ovat itsensä käänteiskuvauksia. □

Tiivistettynä tämän kappaleen tärkeimmät tulokset ovat 1) k-sykli on parillinen, jos k on pariton, ja päinvastoin. 2) pariteetti laskusäännöt 3) permutaatiolla ja sen käänteiskuvauksella on sama pariteetti.

Tästä onkin hyvä jatkaa eteenpäin permutaatioryhmiin.

4 Permutaatioryhmistä ja niiden käytöstä.

Permutaatioilla on myös tiettyjä käytännön soveluksia. Tässä luvussa tarkastellaan miten permutaatioryhmä on määritelty ja mitä tarkoittaa permutaatioryhmän rata. Lisäksi tutkitaan muutamia soveltavia esimerkkejä, joissa hyödynnetään juuri permutaatioryhmän ratoja.

Määritelmä 4.1. Olkoon $X = \{1, 2, ..., n\}$ ja $G \leq S_n$. Aliryhmää G sanotaan *antetta n olevaksi permutaatioryhmäksi.*

Merkitään lisäksi relaatio $(\sim)$: $i \sim j \Leftrightarrow$ on olemassa $g \in G$ siten, että $g(i) = j$. Nyt $(\sim)$ on ekvivalenssirelaatio joukossa X ja jakaa siis kyseisen joukon pistevieraisiin ekvivalenssiluokkiin. Näitä ekvivalenssilokkia voidaan merkitä $T_1, T_2, ...T_r$ ja tällöin sanotaan, että ne ovat permutaatioryhmän G *radat joukossa X.*

Huomautus 4.2. Seuraavassa pari huomautusta permutaatioryhmän radoista.

1) Joukko $X = T_i \cup T_2 \cup ... \cup T_r$ voidaan kirjoittaa ratojen unionina ja $T_i \cap T_j = \emptyset$, kun $i \neq j$. Tästä seuraa myös, että $n = |X| = \sum_{i=1}^{r} |T_i|$.

2) *Alkion i määräämä rata G:ssä* $T_i = \{g(i) | g \in G\}$, missä G siis on permutaatioryhmä.

3) Jos permutaatioryhmällä on vain yksi rata, sitä kutsutaan *transitiiviseksi.*

Esimerkki 4.3. Olkoon $N = \{1, 2, 3, 4, 5\}$ ja

$$G = \{ \begin{pmatrix} 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 5 & 4 \end{pmatrix}, \\ \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 5 & 4 \end{pmatrix} \} \leq S_5.$$

Tällöin $T_1 = \{g(1) | g \in G\} = \{1, 3\} = T_3$ ja $T_2 = \{2, 4, 5\} = T_4 = T_5$

Määritelmä 4.4. Alkion *i stabiloija* ryhmässä G on $G_i = \{g \in G |\ g(i) = i\}$.

Lause 4.5. *Olkoon G permutaatioryhmä, T sen rata ja $k \in T$. Tällöin $|T| = [G : G_k]$.*

Todistus. Olkoon $G = \bigcup_{i=1}^{r} g_i G_k$.

1) Jos $x \in g_i G_k$, niin $x = g_i g$, missä $g \in G_k$. Tällöin $x(k) = g_i g(k) \overset{(*)}{=} g_i(k)$.

2) Jos, jollakin $h \in G$ $h(k) = g_i(k)$, niin $g_i^{-1} h(k) = k$. Joten $g_i^{-1} h(k) \in G_k$ ja $h \in g_i G_k$. Täten siis $|\{g(k) | g \in G\}| = |T| = |\{g_i G_k |\ i = 1, ..r\}| = [G : G_k]$.

□

Huomautus 4.6. Transitiivisessa ryhmässä $|G| = |T||G_k| = |X||G_k|$.

Määritelmä 4.7. Merkitään $fix_X(g) = \{i \in X | g(i) = i\}$, missä G on permutaatioryhmä joukossa X.

Lemma 4.8. (Ei-Burnsiden lemma) Olkoon G permutaatioryhmä joukossa X. Tällöin ryhmän G ratojen lukumäärä joukossa $X = \frac{1}{|G|} \cdot \sum_{g \in G} |fix_X(g)|$.

Todistus. Olkoot $T_1, ...T_r$ permutaatioryhmän G radat joukon X suhteen. Merkitään $S_j = \{(i, g) \in T_j \, x \, G | g(i) = i\}$. Nyt $|S_j| = \sum_{g \in G} |fix_{T_j}(g)|$ ja toisaalta $|S_j| = \sum_{l \in T_j} |G_l|$, missä G_l on alkion $l \in T_j$ stabiloija. Nyt $|T_j| = \frac{|G|}{|G_l|} \Leftrightarrow |G_l| = \frac{|G|}{|T_j|}$. Tällöin $|S_j| = \sum_{l \in T_j} |G_l| = \sum_{l \in T_j} \frac{|G|}{|T_j|} = |T_j| \cdot \frac{|G|}{|T_j|} = |G|$. Edelleen $\sum_{g \in G} |fix_X(g)| = \sum_{j=1}^{r} (\sum_{g \in G} |fix_{T_j}(g)|) = \sum_{j=1}^{r} |S_j| = \sum_{j=1}^{r} |G| = r|G| \Leftrightarrow r = |T_j| = \frac{1}{|G|} \cdot \sum_{g \in G} |fix_X(g)|$. □

Esimerkki 4.9. (Kuution tahkojen erilaiset väritykset)

Kuution tahkot väritetään käyttäen kolmea väriä. Kuinka monta erilaista väritystä saadaan? Värityksiä pidetään samoina, jos ne saadaan toisistaan kuution kiertojen avulla.

Ratk. Kuution värityksiä on kaiken kaikkiaan $3^6 = 729$ kappaletta. Kuution kierrot muodostaa permutaatioryhmän G, joka permutoi kuution kaikkien väritysten joukkoa. Tällöin samanlaiset väritykset ovat G:n samalla radalla. On siis määritettävä kuinka monta rataa G:llä on kaikkien väritysten joukossa. Merkataan kuution tahkoja ja kulmia seuraavasti: etutahko T_1,vasen sivutahko T_2, takatahko T_3, oikea sivutahko T_4, ylätahko T_5 ja alatahko T_6. Etu vasen ylä-kulma=evy=1, ovy=2, eva=3, eoa=4, tvy=5, toy=6, tva=7, toa=8. Tällöin saadaan:

1) Kierto 90° myötäpäivään ylä- ja alatahkon keskipisteiden kautta kulkevan akselin suhteen. $R_1 = (T_1 \quad T_2 \quad T_3 \quad T_4)\,(T_5)\,(T_6)$. Tyyppiä R_1 olevia ratoja on 3 kpl (ylä- ja alatahkoina oleva tahkopari voidaan valita kolmella tavalla).

2) Kierto 180° saman akselin suhteen. Tällöin $R_2 = R_1^2 = (T_1 \quad T_3)\,(T_2 \quad T_4)\,(T_5)\,(T_6)$. Kuten tyyppiä R_1, myös tyyppiä R_2 olevia kiertoja on 3 kappaletta.

3) Kierto 270° saman akselin suhteen. Tällöin $R_3 = R_1^3 = (T_1 \quad T_4 \quad T_3 \quad T_2)\,(T_5)\,(T_6)$. Kuten tyyppiä R_1, myös tyyppiä R_3 olevia kiertoja on 3 kappaletta.

4) Kierto 120° kärkien 1 ja 8 määräämän akselin suhteen. $R_4 = (T_1 \quad T_5 \quad T_2)\,(T_3 \quad T_6 \quad T_4)$. (Kulmat siirtyvät $2 \to 5$,$5 \to 3$, $3 \to 2$, $6 \to 7$, $7 \to 4$, $4 \to 6$.) Tyyppiä R_4 olevia kiertoja on 4 kpl, koska akselin määräävä kulmapari voidaan valita neljällä eri tavalla.

5) Kierto 240° saman akselin suhteen. $R_5 = R_4^2 = (T_1 \quad T_2 \quad T_5)\,(T_3 \quad T_4 \quad T_6)$. (Kulmat siirtyvät $2 \to 5$,$5 \to 3$, $3 \to 2$, $6 \to 7$, $7 \to 4$, $4 \to 6$.) Samoin kuin tyyppiä R_4 myös tyyppiä R_5 olevia kiertoja on 4 kpl.

6) Kierto 180° vastakkaisten särmien (esim 3-7 ; 2-6) keskipisteiden kautta kulkevan akselin suhteen. $R_6 = (T_1 \quad T_3)\,(T_2 \quad T_6)\,(T_4 \quad T_5)$.Kulmat siirtyvät seuraavasti: $3 \leftrightarrow 7$, $2 \leftrightarrow 6$, $1 \leftrightarrow 8$, $4 \leftrightarrow 5$. Vastakkaisia särmäpareja on kuusi, joten tyyppiä R_6 olevia kiertoja on 6kpl.

kiertotyyppi	lkm	säilyvien väritysten lkm	lisäys lausekkeeseen $\sum_{g\in G}\lvert fix_x(g)\rvert$
(i)	1	$3^6 = 729$	729
R_1	3	$3^3 = 27$	$3 \cdot 3^3 = 81$
R_2	3	$3^3 = 27$	$3 \cdot 3^4 = 243$
R_3	3	$3^3 = 27$	$3 \cdot 3^3 = 81$
R_4	4	$3^2 = 9$	$4 \cdot 9 = 36$
R_5	4	$3^2 = 9$	$4 \cdot 9 = 36$
R_6	6	$3^3 = 27$	$6 \cdot 27 = 162$
			$\sum g \in G\lvert fix_x(g)\rvert = 1368$

Täten erilaisten väritysten lukumäärä= ryhmän G ratojen lukumäärä= $\frac{1}{|G|} \cdot \sum g \in G|fix_x(g)| = \frac{1}{24} \cdot 1368 = 57$.
Vastaus on siis 57 erilaista väritystä.

Esimerkki 4.10. Tarkastellaan leimauskorttia, joka on 3x3-ruudukko. Tehdään leima/reikä kahteen ruutuun. Kuinka monta erilaista rei'itystä on mahdollista tehdä? Rei'ityksiä pidetään samoina, jos ne saadaan toisistaan kiertämällä korttia. Merkitään kaikkien rei'itysten joukkoa X:llä. Nyt $|X| = \binom{9}{2} = \frac{9!}{2!7!} = 36$. Numeroivaan ruudut edeten vasemmasta ylänurkasta oikeaan alanurkkaan, ylhäältä alas ja vasemmalta oikealle. Tällöin:

1) 90° kiertoa myötäpäivään vastaa permutaatio $\alpha = \big(1 \quad 3 \quad 9 \quad 7\big)\big(2 \quad 6 \quad 8 \quad 4\big)\big(5\big)$.

2) 180° kiertoa myötäpäivään vastaa permutaatio $\alpha^2 = \big(1 \quad 9\big)\big(3 \quad 7\big)\big(2 \quad 8 \quad 6 \quad 4\big)\big(5\big)$.

3) 270° kiertoa myötäpäivään vastaa permutaatio $\alpha^3 = \big(1 \quad 7 \quad 9 \quad 3\big)\big(2 \quad 4 \quad 8 \quad 6\big)\big(5\big)$.

Nyt $< \alpha >= \{(i), \alpha, \alpha^2, \alpha^3\}$ on permutaatioryhmä joukon X suhteen ja samat rei'itykset ovat ovat $< \alpha >$:n samalla radalla tässä joukossa. Täten erilaisten rei'itysten lukumäärä= $< \alpha >$:n ratojen lukumäärä joukossa $X = \frac{1}{|<\alpha>|} \cdot \sum_{g\in<\alpha>} |fix_X(g)| = \frac{1}{4} \cdot (|fix_X((i))| + |fix_X(\alpha)| + |fix_X(\alpha^2)| + |fix_X(\alpha^3)|) = \frac{1}{4} \cdot (36 + 0 + 4 + 0) = 10$.

Lause 4.11. *(Caychy'n lause) Olkoon G äärellinen ryhmä, p alkuluku ja $p \mid |G|$. Tällöin G:llä on sellainen alkio a, jolle pätee $|a| = p$.*

Todistus. Merkitään $X = \{(g_1, g_2, ..., g_p) \mid g_i \in G, g_1 g_2 ... g_p = 1\}$. Nyt $X \neq \emptyset$, sillä $(1, 1, ..., 1) \in X$. Kuinka monta alkiota joukossa X sitten on? Alkiot $g_1, ..., g_{p-1}$ voidaan valita vapaasti ryhmästä G ja alkio g_p valitaan niin, että näiden tuloksi tulee yksi($g_p = (g_1 ... g_{p-1})^{-1}$). Tästä saadaan,että $|X| = |G|^{p-1}$. Määritellään seuraavaksi kuvaus $\alpha : X \to X$, $\alpha((g_1, g_2, ..., g_p)) = (g_2, g_3, ..., g_p, g_1)$. Nyt kuvaus α on bijektio, eli se on permutaatio joukon X suhteen. Nyt $\alpha^2((g_1, g_2, ..., g_p)) = (g_3, g_4, ..., g_p, g_1 g_2), ..., \alpha^p((g_1, g_2, ..., g_p)) = (g_1 g_2 ... g_p) = (i)$. Siten $|\alpha| = p$ ja $< \alpha >$ on kertalukua p oleva permutaatioryhmä joukossa X. Koska p on alkuluku, niin $< \alpha >$:n radat sisältävät, joko yhden tai p alkiota. Oletetaan, että yhden kappaleen ratoja on s kappaletta ja p alkion ratoja r kappaletta. Täten $s \cdot 1 + r \cdot p = |X| = |G|^{p-1} \overset{(*)}{=} (pt)^{p-1} \Leftrightarrow s = (pt)^{p-1} - rp \Rightarrow p \mid s$. Nyt $(1, 1, ..., 1) \in X$ muodostaa yhden alkion radan, joten $s \geq 1$. Koska $p \geq 2$,$p \mid s$, niin $s \geq 2$. Täten on olemassa alkio $a = (a, ...a) \in X$, missä $a = (a, ...a) \neq (1, ..., 1)$. Tällöin $\underbrace{a..a}_{p\ kpl} = 1 \Leftrightarrow a^p = 1 \Leftrightarrow |a| = p$. □

Tämän luvun sisältämän teorian ydinkohdat ovat permutaatioryhmän ja sen radan määritteleminen sekä lausekkeet joiden avulla voidaan laskea ratojen lukumäärä ja radan pituus, kun tunnetaan yksi alkio, joka kuuluu kyseenomaiseen rataan. Ja toki sovellus esimerkit ovat myös luvun yksi pääkohdista.

5 Alternoivasta ryhmästä.

Tässä luvussa keskitytään alternoivan ryhmän määrittelemiseen ja sen ominaisuuksiin.

5.1 Alternoivan ryhmän A_n määritteleminen.

Edellisessä luvussa määriteltiin kuvaukset σN ja F. Niiden avulla määritellään myös alternoiva ryhmä A_n seuraavasti:

Määritelmä 5.1. Paria $(A_n, \circ)$, missä $A_n = \{\sigma \in S_n | F(\sigma) = 1\}$ ja $(\circ)$ on kuvausten yhdistämisoperaatio, kutsutaan *astetta n olevaksi alternoivaksi ryhmäksi*. Se sisältää siis kaikki symmetrisen ryhmän S_n parilliset permutaatiot ja sitä merkitään jo otsikossakin löytyvällä tavalla A_n.

Todistetaan vielä, että pari $(A_n, \circ)$ todella on ryhmä: Olkoon $\sigma, \tau, \alpha \in A_n$. Nyt

1) $\sigma\tau \in A_n$, sillä $F(\sigma\tau) = F(\sigma)F(\tau) = 1 \cdot 1 = 1$

2) $(\sigma\tau)\alpha = \sigma(\tau\alpha)$, sillä $\sigma, \tau, \alpha \in S_n$ $(A_n \subset S_n)$ ja S_n on ryhmä.

3) $i \in A_n$, sillä $iN = N \to F(i) = 1$, koska i on identiteettikuvaus eikä muuta kuvausta N mitenkään.

4) jos$\sigma \in A_n$, niin $\sigma^{-1} \in A_n$, sillä aikaisemmin todettiin kuvauksella ja sen käänteiskuvauksella olevan sama paritetti. Lisäksi σ^{-1} on olemassa, koska $\sigma^{-1} \in S_n$.

Nyt kohtien 1), 2), 3) ja 4) nojalla $(A_n, \circ) = A_n$ on ryhmä.

Lisäksi huomataan, että jos $\rho \in S_n$ ja $\sigma \in A_n$, niin $\rho^{-1}\sigma\rho \in A_n$, sillä σ on parillinen ja kuvauksilla ρ^{-1}, ρ on sama pariteetti, joten paritetti laskusääntöjen mukaan tulo $\rho^{-1}\sigma\rho$ on parillinen ja kuuluu siten ryhmään A_n, jossa siis tämän nojalla toteutuu normaalisuuskriteeri. Saadaan siis, että alternoiva ryhmä A_n on symmetrisen ryhmän S_n normaali aliryhmä.

Toisessa luvussa pääteltiin, että symmetrisen ryhmän kertaluku $|S_n| = n!$. Alternoivan ryhmän A_n kertaluvun määrittelemiseksi täytyy tutkia edellisessä luvussa määriteltyä kuvausta F hieman tarkemmin.

Tutkittava kuvaus määriteltiin seuraavasti: $F : S_n \to (\{1, -1\}, \cdot)$,

$$F(\sigma) = \begin{cases} 1 & , \text{kun } \sigma N = N \\ -1 & , \text{kun } \sigma N = -N \end{cases}.$$

Samalla todettiin myös, että kaikille $\sigma \in S_n$ pätee, että $\sigma N = N$ tai $\sigma N = -N$, joten kuvauksen F kuvajoukko $im(F) = \{1, -1\}$ ja F on näin ollen surjektio. Lisäksi kuvauksen F ydin $Ker(F) = \{\sigma \in S_n | F(\sigma) = 1\} = A_n$. Nyt kuvaukselle F pätee homomorfismien peruslause, jonka mukaan $Im(F) \cong S_n/Ker(F)$. Eli $\{1, -1\} \cong S_n/A_n$, josta saadaan ryhmän ominaisuuksien nojalla $\frac{|S_n|}{|A_n|} = |\{1, -1\}| \Leftrightarrow \frac{n!}{|A_n|} = 2 \Leftrightarrow |A_n| = \frac{n!}{2}$.

Tämän kappaleen yhteenvetona ollaan siis saatu, että alternoiva ryhmä A_n on symmetrisen ryhmän S_n normaali aliryhmä, joka sisältää kaikki S_n:n parilliset permutaatiot ja jonka kertaluku on $\frac{|S_n|}{2}$.

5.2 Alternoivan ryhmän ominaisuuksia.

Lähdetään seuraavaksi tutkimaan alternoivaa ryhmää tarkemmin. Tämän kappaleen ja koko tutkielman yksi pää tavoitteista on todistaa seuraava tulos: Kun $n \geq 5$, niin alternoiva ryhmä A_n on yksinkertainen. Ennen kuin tähän päästään tutkitaan hieman permutaatioiden konjugointia ja todistetaan muutama muu ominaisuus alternoivalle ryhmälle A_n. Lähdetään liikeelle transpooseeja koskevasta lauseesta, jota käytetään myöhemmin hyödyksi.

Lause 5.2. *Jos $n \geq 3$ ja $\tau_1, \tau_2 \in S_n$ ovat transpooseja, niin $\tau_1\tau_2$ on 3-sykli tai kahden 3-syklin tulo.*

Todistus. 1) Olkoon $\tau_1 = \tau_2$, niin $\tau_1\tau_2 = \tau_1^2 = i = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$

2) Jos $\tau_1 \neq \tau_2$ ja permutaatioilla yksi yhteinen alkio/elementti, jota ne siirtää. Tällöin voidaan merkitä, että $\tau_1 = \begin{pmatrix} 1 & 2 \end{pmatrix}$ ja $\tau_2 = \begin{pmatrix} 1 & 3 \end{pmatrix}$. Jolloin $\tau_1\tau_2 = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$.

3) Olkoon $\tau_1 \neq \tau_2$ ja permutaatioilla ei ole yhtään yhteistä alkiota/elementtiä, jota ne siirtävät. Tällöin voidaan merkitä, että $\tau_1 = \begin{pmatrix} 1 & 2 \end{pmatrix}$ ja $\tau_2 = \begin{pmatrix} 3 & 4 \end{pmatrix}$. Nyt $\tau_1\tau_2 = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 4 & 3 \end{pmatrix}$

Kohtien 1), 2), 3) nojalla väite on todistettu. □

Lause 5.3. *3-syklit generoivat alternoivan ryhmän A_n, kun $n \geq 3$.*

Todistus. Olkoon $\sigma \in A_n$ jokin parillinen permutaatio. Nyt σ voidaan esittää transpoosien tulona, jossa on parillinen määrä transpooseja. Voidaan kirjoitaa $\sigma = \alpha_1\alpha_2 \cdots \alpha_{2m}$, $m \geq 1 \in \mathbb{Z}$. Nyt transpoosit voidaan siis jakaa pareihin ja edellisen lauseen nojalla jokainen transpoosipari $\alpha_{2i-1}\alpha_{2i}$, missä $1 \leq i \leq m$ on 3-sykli tai kahden 3-syklin tulo. Joten nyt σ on 3-sykli tai jokin korkeintaan $2m$:n 3-syklin tulo. Ollaan siis todistettu, että mielivaltainen alternoivan ryhmän permutaatio voidaan esittää 3-syklien avulla, mikä tarkoittaa, että 3-syklit generoivat altenoivan ryhmän A_n. □

Tarkastellaan seuraavaksi permutaatioiden konjugointia ja edetään tutkimaan alternoivaa ryhmää. Ja todistetaan ryhmälle A_n ominaisuus: 3-syklit konjugoivat ryhmässä. Määritellään kuitenkin ensin, mitä tarkoitetaan sillä, että kaksi alkiota konjugoivat keskenään.

Määritelmä 5.4. Olkoon G ryhmä sekä $x, y \in G$. Jos on olemassa $a \in G$, jolle $a^{-1}xa = y$, niin *x ja y konjugoivat G:ssä.*

Seuraavassa esimerkki kahdesta permutaatiosta, jotka konjugoivat. Nyt $\sigma = \begin{pmatrix} 2 & 5 & 6 \end{pmatrix}$ ja $\tau = \begin{pmatrix} 3 & 4 & 1 \end{pmatrix}$ konjugoivat ryhmässä S_6, sillä

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix}^{-1}}_{\in S_n} \begin{pmatrix} 3 & 4 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix}}_{\in S_n} = \begin{pmatrix} 2 & 5 & 6 \end{pmatrix}$$

.

Lause 5.5. *Konjugointikuvaus $K : S_n \to S_n$, $K(x) = \rho^{-1}x\rho$, $\rho \in S_n$ on homomorfismi.*

Todistus. Nyt $K(\sigma\tau) = \rho^{-1}\sigma\tau\rho = \rho^{-1}\sigma(\rho\rho^{-1})\tau\rho = (\rho^{-1}\sigma\rho)(\rho^{-1}\tau\rho) = K(\sigma)K(\tau)$, joten kuvaus K on ryhmähomomorfismi. □

Lause 5.6. *k-syklin konjugaatti on k-sykli.*

Todistus. Olkoon $\alpha = \begin{pmatrix} a_1 & a_2 & ... & a_k \end{pmatrix} \in S_n$, $\beta \in S_n$ ja lisäksi

1) Olkoon $x \in S_n$ sellainen, että $\beta(x) \notin \{a_1, a_2, ..., a_k\}$. Nyt $\beta^{-1}\alpha\beta(x) = \beta^{-1}\alpha(\beta(x)) = \beta^{-1}(\beta(x)) = x$, eli $\beta^{-1}\alpha\beta(x)$ ei siirrä alkiota x.

2) Olkoon sitten $x \in S_n$ sellainen, että $\beta(x) \in \{a_1, a_2, ..., a_k\}$. Nyt

$$\beta^{-1}\alpha\beta(x) = \beta^{-1}\alpha(\beta(x)) \overset{merk.\beta(x)=a_r}{=} \beta^{-1}\alpha(a_r) = \begin{cases} \beta^{-1}(a_{r+1}) & , kun\ 1 \leq r \leq k-1 \\ \beta^{-1}(a_1) & , kun\ r = k \end{cases}.$$

Kohdat 1) ja 2) yhdistämällä saadaan, että

$$\beta^{-1}\alpha\beta = \begin{pmatrix} \beta^{-1}(a_2) & \beta^{-1}(a_3) & ... & \beta^{-1}(a_k) & \beta^{-1}(a_1) \end{pmatrix} = \begin{pmatrix} \beta^{-1}(a_1) & \beta^{-1}(a_2) & ... & \beta^{-1}(a_k) \end{pmatrix}.$$

Joka on k-sykli.

□

Esimerkki 5.7. Edellisen esimerkin permutaation $\tau = \begin{pmatrix} 3 & 4 & 1 \end{pmatrix}$ konjugaatti $\sigma = \begin{pmatrix} 2 & 5 & 6 \end{pmatrix}$ on 3-sykli, samoin kuin τ itse.

Pohditaan seuraavaksi, miten saadaan selville konjugoivatko, jotkin kaksi annettua permutaatiota. Väitetään, että kaksi permutaatiota konjugoivat, jos ja vain jos niillä on sama syklirakenne. Samalla syklirakenteella tarkoitetaan seuraavaa:

Määritelmä 5.8. kahdella syklillä $\sigma, \tau \in S_n$ on sama syklirakenne, jos niiden esitykset erillisten syklien tulona vastaavat toisiaan kun otetaan huomioon syklien pituudet ja lukumäärät.

Esimerkki 5.9. Sykleillä

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

ja

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

on sama syklirakenne.

Lause 5.10. *Kaksi sykliä $\sigma, \tau \in S_n$ konjugoivat, jos ja vain jos niillä on sama syklirakenne.*

Todistus. ” $\Rightarrow$ ” Olkoon $\sigma = \alpha_1 \alpha_2 \cdots \alpha_k$ permutaation esitys erillisten syklien tulona ja $\tau = \rho^{-1}\sigma\rho$, $\rho \in S_n$ eräs permutaation σ konjugaatti. Nyt

$$\begin{aligned} \tau = \rho^{-1}\sigma\rho &= \rho^{-1}(\alpha_1\alpha_2\cdots\alpha_k)\rho = \rho^{-1}\alpha_1(\rho\rho^{-1})\alpha_2(\rho\rho^{-1})\cdots(\rho\rho^{-1})\alpha_k\rho \\ &= \underbrace{(\rho^{-1}\alpha_1\rho)}_{\alpha_1 : n\text{konjugaatti}} \ (\rho^{-1}\alpha_2\rho)\cdots(\rho^{-1}\alpha_k\rho) = \alpha_1'\alpha_2'\cdots\alpha_k' \end{aligned}$$

ja sykleillä σ, τ on sama syklirakenne, sillä k-syklin konjugaatti on k-sykli.

” $\Leftarrow$ ” Olkoon $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_{k_1} \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \dots & b_{k_2} \end{pmatrix} \cdots \begin{pmatrix} x_1 & x_2 & \dots & x_{k_r} \end{pmatrix}$ ja

$$\tau = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{k_1} \end{pmatrix} \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_{k_2} \end{pmatrix} \cdots \begin{pmatrix} \chi_1 & \chi_2 & \dots & \chi_{k_r} \end{pmatrix}$$

kaksi symmetrisen ryhmän S_n permutaatiota, joilla on sama syklirakenne. Nyt, jos

$$\rho = \begin{pmatrix} a_1 & a_2 & \dots & a_{k_1} & b_1 & b_2 & \dots & b_{k_2} & x_1 & x_2 & \dots & x_{k_r} \\ \alpha_1 & \alpha_2 & \dots & \alpha_{k_1} & \beta_1 & \beta_2 & \dots & \beta_{k_2} & \chi_1 & \chi_2 & \dots & \chi_{k_r} \end{pmatrix} \in S_n$$

, niin $\rho^{-1}\tau\rho = \sigma$ ja τ ja σ konjugoivat.

Katsotaan edellä olevan permutaation ρ valinnan tueksi, miten $\rho^{-1}\tau\rho$ kuvaa alkion a_1. Nyt $\rho^{-1}\tau\rho(a_1) = \rho^{-1}\tau(\rho(a_1)) = \rho^{-1}\tau(\alpha_1) = \rho^{-1}(\alpha_2) = a_2 = \sigma(a_1)$. □

Määritelmä 5.11. Kokonaisluvun n jaotuksella tarkoitetaan luvun n esitystä kokonaislukujen summana seuraavasti: $n = n_1 + n_2 + ... + n_k$, missä $0 \leq n_1 \leq n_2 \leq ... \leq n_k \leq n$ ja n_i, $1 \leq i \leq k$ ovat kokonaislukuja.

Lause 5.12. *Konjugointiluokkien lukumäärä symmetrisessä ryhmässä S_n on samalla myös kokonaisluvun n jaotuksien lukumäärä.*

Todistus. Nyt kaksi sykliä konjugoivat jos ja vain jos niillä on sama syklirakenne, joten konjugointi luokkien lukumäärä ryhmässä S_n on myös ryhmässä S_n olevien erilaisten syklirakenteiden lukumäärä. Koska symmetrisen ryhmän permutaatiot kuvaavat alkioita $1, 2, ..., n$, niin erilaiset syklirakenteet voidaan samaistaa kokonaisluvun n jaotuksiksi seuraavasti: Olkoon $\sigma = \alpha_1\alpha_2 \cdots \alpha_k \in S_n$ permutaation esitys erillisten syklien tulona ja r_i syklin α_i, $1 \leq i \leq k$ kertaluku. Samaistetaan tämä syklirakenne jaotukseksi

$$n = \underbrace{1 + 1 + .. + 1}_{(n - \Sigma_{1 \leq i \leq k} r_i) kpl} + \Sigma_{1 \leq i \leq k} r_i,$$

missä kokonaisluvut r_i ovat suuruusjärjestyksessä ja kirjoittamattomat 1-syklit on "luettu"kokonaisluvuksi 1 ja lisätty summaan. Näin ollen kokonaisluvun n jaotusten lukumäärä = S_n:n erilaisten sykliesitysten lukumäärä = S_n:n konjugointiluokkien lukumäärä. □

Esimerkki 5.13. Nyt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 8 & 2 & 7 & 6 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 8 \end{pmatrix} \in S_8$$

voidaan samaistaan kokonaisluvun 8 jaotukseen $8 = 1 + 1 + 1 + 2 + 2 + 3$

Lause 5.14. *Jos $n \geq 5$, niin 3-syklit konjugoivat alternoivassa ryhmässä A_n.*

Todistus. Olkoon σ_1 ja s_2 kaksi 3-sykliä S_n:ssä. Nyt ne konjugoivat ryhmässä S_n ja voidaan kirjoittaa $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ ja $\sigma_2 = \rho \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rho^{-1}$, jollakin $\rho \in S_n$. Jos ρ on pariton, niin $\tau = \rho \begin{pmatrix} 4 & 5 \end{pmatrix} \in A_n$ on parillinen. Tällöin

$$\tau\sigma_1\tau^{-1} = \tau \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \tau^{-1} = \rho \begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix}^{-1} \rho^{-1} = \rho \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rho^{-1} = \sigma_2$$

, eli σ_1 ja σ_2 konjugoivat myös alternoivassa ryhmässä A_n. □

Lause 5.15. *Jos $n \geq 5$, niin symmetrisen ryhmän S_n ainoa ei-triviaali normaali aliryhmä on alternoiva ryhmä A_n.*

Todistus. Olkoon N symmetrisen ryhmän S_n normaali aliryhmä, joka on ei-triviaali. Eli $N \neq \{i\}$ ja $N \neq S_n$. Olkoon sitten $\sigma \neq i \in N$. Nyt S_n:n keskus on $\{i\}$ ja transpoosit generoivat ryhmän S_n, joten on olemassa transpoosi $\tau \in S_n$ siten, että $\sigma\tau \neq \tau\sigma$. Aiemmin todistettiin, että k-syklin konjugaatti on myös k-sykli, joten $\tau_1 = \sigma\tau\sigma^{-1}$ on myös transpoosi. Tällöin $\tau\tau_1 = \tau\sigma\tau\sigma^{-1} = (\tau\sigma\tau)\sigma^{-1} = (\tau\sigma\tau^{-1})\sigma^{-1} \neq i$ on normaaliuskriteerin nojalla myös joukossa N. Nyt joukko N sisältää siis elementin, joka on kahden transpoosin tulo. Lauseen (4.2) nojalla voidaan todeta: 1) Jos transpooseilla τ ja τ_1 on yksi yhteinen elementti, niin $\tau\tau_1$ on 3-sykli. Täten joukko N sisältää 3-syklin ja koska 3-syklit konjugoivat joukossa S_n ja N on sen normaali aliryhmä, niin joukko N sisältää kaikki 3-syklit. Tästä taas voidaan päätellä, että $A_n \subset N$, sillä 3-syklit generoivat ryhmän A_n. 2) Jos transpooseilla τ ja τ_1 on yksi yhteinen elementti, niin voidaan merkitä $\tau = \begin{pmatrix}1 & 2\end{pmatrix}$ ja $\tau_1 = \begin{pmatrix}3 & 4\end{pmatrix}$ ja tiedetään $\tau\tau_1 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \in N$. Koska $n \geq 5$, niin $\begin{pmatrix}1 & 5\end{pmatrix} \in S_n$ ja tällöin $\begin{pmatrix}1 & 5\end{pmatrix}\underbrace{\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}}_{\in N}\begin{pmatrix}1 & 5\end{pmatrix}^{-1} = \begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \in N$, sillä N on S_n:n normaali aliryhmä. Tästä saadaan edelleen N:n normaaliuden nojalla, että $\underbrace{\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}}_{\in N}\underbrace{\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}}_{\in N} \in N$. Joukko N sisältää siis tässäkin tapauksessa 3-syklin ja normaaliuden nojalla kaikki 3-syklit kuuluvat sinne. Tällöin pätee $A_n \subset N$.

Koska symmetrisellä ryhmällä S_n ei ole aliryhmiä, joiden kertalu olisi alternoivan ryhmän kertaluvun $|A_n|$ ja symmetrisen ryhmän kertaluvun $|S_n|$ välissä, niin täytyy olla, että $N = A_n$ ja väite on tosi. □

Lause 5.16. *A_5 on kertalukua 60 oleva yksinkertainen ryhmä.*

Todistus. Oletetaan, että A_n ei ole yksinkertainen. Tällöin on olemassa sellainen ryhmän A_5 normaali aliryhmä N, jolle pätee $|\{i\}| < |N| < |A_5|$ ja $|N|$ on pienin mahdollinen. Olkoon sitten $T = \{\sigma \in S_n | \sigma N \sigma^{-1} \subset N\}$ merkintä aliryhmän N normalisoijalle ryhmässä S_5. Koska N on normaali aliryhmä ryhmässä A_5, niin normalisoijan ehto toteutuu kaikilla $\sigma \in A_5$. Eli $A_5 \subset T$ ja koska lisäksi $T \leq S_n$, niin täytyy olla joko $T = A_5$ tai $T = S_5$. Jos $T = S_5$, niin se tarkoittaisi, että N olisi normaali aliryhmä myös joukossa S_n, mikä on edellisen lauseen nojalla ristiriita. Täytyy siis olla $T = A_5$. Tällöin

$\begin{pmatrix}1 & 2\end{pmatrix} \notin T = A_5$ ja näin ollen $M \overset{merk.}{=} \begin{pmatrix}1 & 2\end{pmatrix} N \begin{pmatrix}1 & 2\end{pmatrix}^{-1} \neq N$. Nyt

$$\begin{aligned}\sigma M \sigma^{-1} &= \sigma \begin{pmatrix}1 & 2\end{pmatrix} N \begin{pmatrix}1 & 2\end{pmatrix}^{-1} \sigma^{-1} \\ &= \begin{pmatrix}1 & 2\end{pmatrix} [\underbrace{\begin{pmatrix}1 & 2\end{pmatrix}^{-1} \sigma \begin{pmatrix}1 & 2\end{pmatrix}}_{\in A_5 = T} N \underbrace{\begin{pmatrix}1 & 2\end{pmatrix}^{-1} \sigma^{-1} \begin{pmatrix}1 & 2\end{pmatrix}}_{\in A_5 = T}] \begin{pmatrix}1 & 2\end{pmatrix}^{-1} \\ &\overset{NnormaaliA_5:ss}{=} \begin{pmatrix}1 & 2\end{pmatrix} N \begin{pmatrix}1 & 2\end{pmatrix}^{-1}\end{aligned}$$

Siis myös M on ryhmän A_5 normaali aliryhmä ja aliryhmien ominaisuuksista voidaan suoraan päätellä, että myös $M \cap N = \{a | a \in M \text{ja } a \in N\}$ ja $MN = \{mn | m \in M \text{ja } n \in N\}$ ovat ryhmän A_5 normaaleja aliryhmiä. Nyt $M = \begin{pmatrix}1 & 2\end{pmatrix} N \begin{pmatrix}1 & 2\end{pmatrix}^{-1} \neq N$, joten myös $M \cap N \neq N$. Tällöin $|M \cap N| < |N|$ ja koska N valittiin minimaaliseksi normaaliksi aliryhmäksi ryhmässä A_5, niin täytyy olla $M \cap N = \{(i)\}$ Tutkimalla joukkoa $\begin{pmatrix}1 & 2\end{pmatrix} MN \begin{pmatrix}1 & 2\end{pmatrix}^{-1} = \underbrace{\begin{pmatrix}1 & 2\end{pmatrix} M \begin{pmatrix}1 & 2\end{pmatrix}^{-1}}_{=N} \underbrace{\begin{pmatrix}1 & 2\end{pmatrix} N \begin{pmatrix}1 & 2\end{pmatrix}^{-1}}_{=M} = NM \overset{N,Mnormaaleja}{=} MN$ huomataan, että $\begin{pmatrix}1 & 2\end{pmatrix}$ kuuluu joukon MN normalisoijaan joukossa S_5. Koska normalisoija on S_5:n aliryhmä, sekä A_5 ja $\begin{pmatrix}1 & 2\end{pmatrix}$ kuuluvat normalisoijaan, täytyy olla $MN = A_5$. Tutkitaan seuraavaksi ryhmän MN kertalukua. Tiedetään, että $|M| = |N|$ (k-syklin konjugaatti on k-sykli) ja $MN = A_5$ sekä $M \cap N = \{(i)\}$. Nämä yhdistämällä voidaan päätellä, että $|N|^2 = |MN| = |A_5| = 60$, mikä ei voi pitää paikkaansa, sillä 60 ei ole minkään kokonaisluvun neliö. Täten vastaoletus on siis väärä ja väite tosi. □

Edellä esitetty todistus on esitetty I.N Hersteinin kirjassa Abstract Algebra s. 219. Algebra II kurssin luentomuistiinpanoissa on toisenlainen versio todistuksesta. Tämä versio on mielestäni selkeämpi, joten haluan esittää myös sen tässä.

Todistus. Oletetaan, että N on alternoivan ryhmän A_5 normaali aliryhmä ja $N \neq \{(i)\}$. Tällöin on olemassa $\sigma \in N$, $\sigma \neq (i)$. Nyt koska $N = 5$, niin $\sigma = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$, $\sigma = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$ tai $\sigma = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}$. Tutkitaan tilanne näissä jokaisessa tapauksessa erikseen.

1) Olkoon $\sigma = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$. Nyt permutaation σ konjugaatti $\alpha\sigma\alpha^{-1}$, $\alpha \in A_5$ on 3-sykli ja kuuluu ryhmän N normaliuden nojalla joukkoon N. On siis osoitettu, että normaali aliryhmä N sisältää 3-syklin, koska 3-syklit konjugoivat ryhmässä A_5, niin kaikki 3-syklit kuuluvat joukkoon N. Lisäksi 3-syklit generoivat ryhmän A_5, joten $A_5 \subset N$. Nyt $N \subseteq A_5$ ja $A_5 \subseteq N$, joten täytyy olla $N = A_5$.

2) Olkoon $\sigma = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$. Nyt $\tau = \begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} \in A_5$ ja $\tau\sigma\tau^{-1} \in N$. Täten $\tau^{-1}\sigma\tau\sigma = \begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} = \begin{pmatrix}3 & 5 & 4\end{pmatrix} \in N$. Päädytään siis 1)-kohdan tilanteeseen, jossa joukko N sisältää 3-syklin. Kuten 1)-kohdassakin, voidaan päätellä, että $N = A_5$.

3) Olkoon $\sigma = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}$ ja $\tau = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \in A_5$. Nyt $\tau^{-1}\sigma\tau \in N$ ja $\tau^{-1}\sigma\tau\sigma^{-1} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} = \begin{pmatrix}1 & 3 & 4\end{pmatrix} \in N$. Saadaan siis tässäkin tapauksessa, että N sisältää 3-syklin ja 1)-kohdan nojalla $N = A_5$. Kohdat 1), 2) ja 3) yhdistämällä ollaan siis saatu: N on normaali aliryhmä A_5:ssä $\Leftrightarrow N = \{(i)\}$ tai $N = A_5$. Joten A_5 on yksinkertainen.

□

Edellisen todistuksen mekaanisissa laskuissa on hypätty monta välivaihetta pois, jotta todistus pysyisi selkeänä. Katsotaan tässä todistuksen jälkeen toinen näistä laskuista välivaiheineen, jotta laskut eivät jää epäselviksi. Toinen laskuista menee vastaavasti.

$$\begin{aligned}\tau^{-1}\sigma\tau\sigma &= (\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix})^{-1}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \\ &= \begin{pmatrix}1 & 2\end{pmatrix}^{-1}\begin{pmatrix}3 & 5\end{pmatrix}^{-1}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \\ &= \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \\ &= \begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} = \begin{pmatrix}3 & 5 & 4\end{pmatrix}\end{aligned}$$

Lause 5.17. *Alternoiva ryhmä A_6 on yksinkertainen.*

Todistus. Aiemmin todistettiin, että alternoiva ryhmä A_5 on yksinkertainen. Todistuksessa tehtiin vastaoletus. Joka päättyi ristiriitaan, missä alternoivan ryhmän A_5 kertaluku $|A_5| = \frac{5!}{2} = 60$ pitäisi olla jonkin kokonaisluvun neliö N^2. Samaa päättelyä voidaan käyttää myös A_6:n tapauksessa. Myöskään $|A_6| = \frac{6!}{2} = 360$ ei ole minkään kokonaisluvun neliö, joten A_6 on yksinkertainen. □

Lause 5.18. *Alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$*

Todistus. Aiemmin todistettiin tapaus n=5, joten jatkossa voidaan olettaa $n \geq 6$. Olkoon sitten $N \neq \{(i)\}$ ryhmän A_n normaali aliryhmä. Tällöin on siis olemassa $\sigma \neq (i) \in N \subseteq A_n$. Lisäksi alternoivan ryhmän keskus $Z(A_n) = \{(i)\}$, kun $n > 3$ ja 3-syklit generoivat ryhmän A_n, joten on olemassa 3-sykli τ, jolle pätee $\sigma\tau \neq \tau\sigma$ (Lause (2.14)). Tällöin $\sigma\tau\sigma^{-1}\tau^{-1} \neq (i)$. Lisäksi koska N on normaali aliryhmä ryhmässä A_n, niin $\sigma\tau\sigma^{-1}\tau^{-1} \in N$. Nyt koska τ on 3-sykli, niin sen konjugaatti $\sigma\tau\sigma^{-1}$ ja käänteiskuvaus τ^{-1} ja $\sigma\tau\sigma^{-1}\tau^{-1} \neq (i) \in N$ on kahden 3-syklin tulo. Tämä tulo siirtää korkeintaan kuutta alkiota, joten voidaan ajatella, että $\sigma\tau\sigma^{-1}\tau^{-1} \neq (i) \in H \cong A_6 \subset A_n$ Täten $N \cap H \neq (i)$ ja esitietoja käsittelevässä kappaleessa olevan lauseen (2.15) nojalla $N \cap H \neq (i)$ ryhmän A_6 normaali aliryhmä. Koska A_6 on yksinkertainen niin täytyy olla $N \cap H = H$. Koska 3-syklit generoivat ryhmän $H \cong A_6$, niin joukon N täytyy myös sisältää 3-sykli. Aiemmin todistettiin, että 3-syklit gonjugoivat ryhmässä S_n ja koska N on normaali A_n:ssä, niin se sisältää kaikki 3-syklit ja näin ollen $N = A_n$ (3-syklit generoivat A_n:n)ja väite on todistettu. □

6 Yhteenveto ja loppusanat.

Tämän tutkielman aikana on käyty läpi ryhmäteorian perusteita ja permutaatioilla laskemista sekä niiden ominaisuuksia ja vähän sovelluksiakin. Kokonaisuudessaan siis melko laaja katsaus ryhmäteorian ja permutaatioiden maailman ytimeen.

Esitietoja käsittelevässä kappaleessa on kerätty yhteen tärkeimmät asiat aivan ryhmäteorian alkeista, mutta esimerkkejä ei pahemmin ole ja osan perusteluistakin jätin pois. Tämä siksi, että tutkielman fokus pysyisi paremmin sen ytimessä. Tämän kappaleen teoriasta ja muusta esimerkkeineen saisi aivan oman minitutkielman, jos lähtisi tarkasti käymään läpi.

Kolmannessa luvussa käydään läpi perustietoja permutaatioista. Tärkeimpinä voisi mainita ainakin kuvausten sykliesityksen ja sykleillä laskemisen ja laskusäännöt. Sekä permutaatioiden esityksen erillisten syklien tulona ja pariteetin päättelyn + pariteettilaskusäännöt. Pyrin laittamaan paljon esimerkkejä tähän kappaleeseen, jotta lukija saisi harjoitusta ja ymmärrystä siitä, miten laskeminen tapahtuu käytännössä. Esimerkit kannattaakin käydä läpi, niin että lukee tehtävänannon ja laskee sitten itse paperille ja tarkistaa vastauksen.

Neljännessä luvussa käsitellään permutaatioiden sovelluksia ja käyttöä. Kappaleen teoria menee vähän syvemmälle aiheeseen ja on astetta vaativampaa. Päälimmäisenä tästä kappaleesta olisi varmaan hyvä jäädä mieleen permutaatioryhmä ja sen rata, sekä se miten ratojen lukumäärä tietyssä joukossa ja radan pituus(kun tiedetään yksi alkio, joka kuuluu ko. rataan) voidaan laskea. Ja tietenkin myös se, että käytäntöön permutaatioita ja ratoja voidaan soveltaa tapauksissa, jossa pitää ottaa huomioon kappaleen kierrot.

Viimeisessä luvussa palataan taas enemmän ryhmäteorian pariin ja lähdetään tarkastelemaan alternoivaa ryhmää. Liikkeelle lähdetään aivan alusta, eli määritelmästä ja edetään konjugoinnin kautta todistamaan muutama ominaisuus alternoivalle ryhmälle. Kappaleen päätulos on sen viimeinen lause, jonka väite on: Kun $n \geq 5$, niin alternoiva ryhmä A_n on yksinkertainen.

Viitteet

[1] I.N. Herstein: *Abstract Algebra*, Prentice-Hall,1996

[2] M. Niemenmaa ; K. Myllylä ; J-M. Tirilä: Algebra 1, luentorunko, Oulun yliopisto, 2010

[3] K. Myllylä ; *Algebra 1*, luennot ja muistiinpanot, Oulun yliopisto, kevät 2010

[4] M. Niemenmaa ; *Algebra 2*, luennot ja muistiinpanot, Oulun yliopisto, kevät 2011