TAMPEREEN YLIOPISTO

Kandidaattitutkielma

Marika Lähteenmäki

Permutaatioryhmät

Informaatioteknologian ja viestinnän tiedekunta

Matematiikka

Tammikuu 2019

Sisältö

1 Johdanto

Permutaatio on bijektio joukosta joukkoon itseensä. Joukon permutaatioiden joukko varustettuna kuvausten yhdistämisellä on symmetrinen ryhmä. Sen aliryhmiä kutsutaan permutaatioryhmiksi.

Tämän tutkielman luvussa 3 määrittelemme algebran rakenteen permutaatioryhmä, sekä annamme notaation permutaation käsittelyyn. Käsittelemme permutaatioiden yhdistettujä funktioita aliluvussa 3.2, jossa määrittelemme tavan yhdistää permutaatioita sekä tuomme esiin yhdistettyjen permutaatioihin päteviä laskusääntöjä.

Luvussa 4 esittelemme yksinkertaisemman sekä informatiivisemman tavan merkitä permutaatioita, syklit. Käsittelemme erillisiä permutaatioita ja esittelemme niihin kuuluvia lauseita aliluvussa 4.2.

Luvussa 5 käsittelemme parillisia ja parittomia permutaatioita, joihin liittyen esittelemme diskriminantin, transposition sekä alternoivan ryhmän käsitteet, sekä niihin liittyviä lauseita.

Luvussa 2 esittelemme esitietoina ryhmän ja Abelin ryhmän määritelmät sekä muutaman lauseen bijektioiden ominaisuuksista.

Lukijalle on avuksi algebran peruskurssien tiedot ryhmistä, sekä algebrallisten laskujen hallitseminen. Tutkielmassa pyrimme kuitenkin mahdollisimman perusteellisesti tukemaan algebran peruskurssien tietoja kuten ryhmän määritelmän ja yhdistettyjen funktioiden ratkaisun sekä bijektioiden todistamisen.

2 Esitietoja

2.1 Ryhmät

Ryhmä on algebran rakenne, jossa joukkoon on liitetty operaatio, joka toteuttaa tietyt aksioomat. Periaatteena on siis, että kaksi asiaa yhdistämällä voimme muodostaa kolmannen samankaltaisen asian [3, s. 121].

Ryhmäteoria sai alkunsa 1800-luvulla, kun matemaatikot olivat kolmen vuosisadan ajan yrittäneet löytää viidennen ja korkeamman asteen polynomien ratkaisukaavaa. Vuonna 1824 N. H. Abel todisti, että tällaista yleistä ratkaisukaavaa ei ole viidennen asteen polynomeille. Vuonna 1831 E. Galois löysi ne tietyt polynomit, joilla on tällainen kaava juuriensa ratkaisemiseen. Hänen keskeinen ideansa sisälsi hänen keksintönsä ryhmän käsitteestä. [3, s. 121]

Määritelmä 2.1 (Vrt. [1, s. 48])**.** Ryhmä $(G, \cdot)$ on pari, joka koostuu joukosta G ja binäärioperaatiosta $\cdot$, jolle pätee seuraavat aksioomat:

(i) joukko G on suljettu operaation $\cdot$ suhteen, siis pätee $a \cdot b \in G$ aina, kun $a, b \in G$,

(ii) operaatio $\cdot$ on assosiatiivinen eli liitännäinen, siis $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ aina, kun $a, b \in G$,

(iii) joukossa G on neutraalialkio e, jolle pätee $e \cdot a = a \cdot e = a$ aina, kun $a \in G$,

(iv) joukossa G on käänteisalkio a^{-1} jokaiselle joukon G alkiolle a, jolloin pätee $a^{-1} \cdot a = a \cdot a^{-1} = e$.

Määritelmä 2.2 (Vrt. [3, s. 122])**.** Ryhmää G kutsutaan Abelin ryhmäksi, jos se on kommutatiivinen eli vaihdannainen, eli $a * b = b * a$ pätee kaikille $a, b \in G$.

2.2 Bijektioiden ominaisuuksia

Apulause 2.1. *Olkoot $f\colon X \to Y$ ja $g\colon Y \to Z$ kuvauksia. Merkitään kuvausten yhdistämistä symbolilla $\circ$. Silloin pätevät seuraavat kohdat:*

(i) Jos f ja g ovat injektioita, niin $g \circ f$ on injektio.

(ii) Jos f ja g ovat surjektioita, niin $g \circ f$ on surjektio.

(iii) Jos f ja g ovat bijektioita, niin $g \circ f$ on bijektio.

Todistus (vrt. [1, s. 50]). (i) Oletamme, että $(g \circ f)(x_1) = (g \circ f)(x_2)$. Silloin $g(f(x_1)) = g(f(x_2))$. Nyt koska g on injektio, jossa jokainen joukon Y alkio kuvautuu joukon Z eri alkiolle, on silloin oltava $f(x_1) = f(x_2)$. Taas edelleen, koska f on injektio, seuraa, että $x_1 = x_2$. Siis $g \circ f$ on injektio.

(ii) Olkoon $z \in Z$. Koska g on surjektio, on olemassa $y \in Y$, jolle pätee $g(y) = z$. Vastaavasti, koska f on surjektio, on olemassa $x \in X$, jolle pätee $f(x) = y$. Täten $(g \circ f)(x) = g(f(x)) = g(y) = z$. Siis $g \circ f$ on surjektio.

(iii) Kohdista (i) ja (ii) seuraa, että $g \circ f$ on bijektio.

Olemme siis todistaneet apulauseen 2.1. □

Lause 2.2. *Funktiolla $f\colon X \to Y$ on käänteisfunktio, jos ja vain jos f on bijektio.*

Todistus (vrt. [1, s. 50]). Oletamme ensin, että $h\colon Y \to X$ on funktion f käänteisfunktio. Funktio f on injektio, koska jos pätee, että $f(x_1) = f(x_2)$, niin silloin pätee myös, että $(h \circ f)(x_1) = (h \circ f)(x_2)$, jolloin $x_1 = x_2$. Funktio f on surjektio, koska jos alkio y kuuluu joukkoon Y ja $x = h(y)$, niin $f(x) = f(h(y)) = y$. Funktio f on siis bijektio.

Käänteisesti oletamme, että f on bijektio. Määrittelemme funktion $h\colon Y \to X$ seuraavasti: jokaiselle alkiolle $y \in Y$ on olemassa alkio $x \in X$, jolle $y = f(x)$. Koska f on injektio, on olemassa vain yksi sellainen x, jolle ehto $y = f(x)$ pätee. Määrittelemme $h(y) = x$. Funktio h on funktion f käänteisfunktio, koska $f(h(y)) = f(x) = y$, ja $h(f(x)) = h(y) = x$. Täten olemme siis todistaneet lauseen 2.2. □

Lause 2.3. *Olkoon $S(X)$ bijektioiden joukko jostakin joukosta X joukkoon X. Silloin $(S(X), \circ)$ on ryhmä yhdistetyn funktion suhteen. Tällaista ryhmää kutsutaan joukon X symmetriseksi ryhmäksi.*

Todistus (vrt. [1, s. 50]). Ensin toteamme, että apulauseen 2.1 nojalla kahden bijektion yhdistelmä on bijektio, jolloin $S(X)$ on suljettu yhdistetyn funktion nojalla.

Seuraavaksi olkoot funktiot $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$. Nyt saamme

$$(h \circ (g \circ f))(x) = (h \circ (g(f(x)))) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x),$$

kaikilla $x \in X$. Siis yhdistetty funktio on aina liitännäinen.

Kolmanneksi joukon $S(X)$ identiteetti operaation $\circ$ suhteen on identiteettifunktio $1_X = X \to X$, jossa jokainen alkio kuvautuu itselleen, ja neljänneksi, lauseesta 2.2 seuraa, että jokaisella bijektiolla $f \in F$ on käänteisfunktio $f^{-1} \in S(X)$.

Täten $(S(X), \circ)$ toteuttaa siis kaikki ryhmän aksioomat, jolloin $(S(X), \circ)$ on siis ryhmä ja olemme todistaneet lauseen 2.3. □

3 Permutaatio

3.1 Määritelmä ja notaatio

Määritelmä 3.1 (Vrt. [3, s. 103])**.** Joukon X permutaatio on bijektio $\alpha\colon X \to X$.

Permutaatioita voidaan bijektioina yhdistää [3, s. 103] ja apulauseen 2.1 nojalla permutaatioiden yhdiste on myös permutaatio.

Merkitsemme joukon $X = \{1, 2, \ldots, n\}$ symmetristäryhmää notaatiolla $(S_n, \circ)$ ja kutsumme sitä n alkion symmetriseksi ryhmäksi.

Määritelmä 3.2. Permutaatioryhmä on symmetrisen ryhmän aliryhmä.

Lause 3.1. $|S_n| = n!$.

Todistus (vrt. [1, s. 63]). Gilbert ja Nicholson todistavat lauseen 3.1 seuraavalla tavalla. Nyt $|S_n|$ on ryhmän S_n bijektioiden lukumäärä joukosta $\{1, 2, \ldots, n\}$ joukkoon itseensä. Alkion 1 kuvaukselle on bijektion nojalla n kappaletta mahdollisia vaihtoehtoja. Kun alkion 1 kuvaus on valittu, alkion 2 kuvaukselle on $n - 1$ kappaletta vaihtoehtoja. Edelleen alkion 3 kuvaukselle on $n - 2$ vaihtoehtoa. Kun jatketaan vastaavasti, huomaamme, että $|S_n| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$. □

Otamme permutaatioiden merkitsemisessä käyttöön Rotmanin [3, s. 103] käyttämän tavan: Olkoon $X = \{1, 2, \ldots, n\}$. Silloin permutaatio $\alpha\colon X \to X$ tuottaa listan $\alpha(1) = i_1$, $\alpha(2) = i_2$, $\ldots$, $\alpha(n) = i_n$. Voimme esittää tämän permutaation kaksirivisenä matriisina: olkoon $\alpha(j)$ listan j. alkio, siis

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & j & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(j) & \ldots & \alpha(n) \end{pmatrix}.$$

Tällä tavalla meidän on myös helppo ymmärtää permutaatiota. Seuraavaksi annamme esimerkin tällaisesta permutaation esitystavasta konkreettisen joukon permutaatiolla.

Esimerkki 3.1. Tarkastellaan joukon $\{0, 1, 2\}$ permutaatiota, jossa alkiot kuvautuvat seuraavasti: $0 \to 1$, $1 \to 2$, $2 \to 0$. Esitetään se muodossa

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}.$$

Ajattelemme tämän siis kaaviona

$$\begin{bmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 0 \end{bmatrix}.$$

Vastaavasti kirjoitamme ryhmät S_1, S_2 ja S_3 seuraavasti:

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Nyt näemme, että ryhmässä S_1 on yksi alkio, ryhmässä S_2 on kaksi alkiota ja ryhmässä S_3 alkioita on $6 = 3!$, joka on bijektioiden lukumäärä ryhmässä.

3.2 Permutaatioiden yhdistetyt funktiot

Määritelmä 3.3 (Vrt. [1, s. 63])**.** Gilbert ja Nicholson määrittelevät permutaatioiden yhdistetyn funktion seuraavasti: Olkoon permutaatiot $\alpha, \beta \in S_n$. Niiden yhdiste $\alpha \circ \beta$ muodostaa permutaation, jossa ensin käytämme permutaatiota β ja sitten permutaatiota α.

Tämä myös vastaa yhdistetyn funktion merkintätapaa, sillä $(\alpha \circ \beta)(x) = \alpha(\beta(x))$.

Seuraavaksi annamme esimerkin permutaatioiden yhdistämisestä.

Esimerkki 3.2. Ratkaistaan yhdistetyt funktiot $\alpha \circ \beta$ ja $\beta \circ \alpha$. Olkoot

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \in S_4.$$

Ensin ratkaisemme funktion

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Funktio ratkaistaan seuraamalla yhdistetyn funktion alkion kuvauksia.

Lähdemme ratkaisemaan funktiota oikean puoleisen permutaation β ensimmäisestä alkiosta 1, joka kuvautuu alkiolle 4. Siis $\beta(1) = 4$. Seuraavaksi siirrymme vasemman puoleisen permutaation α alkioon 4, joka kuvautuu alkiolle 3. Siis $\alpha(4) = 3$. Siis saamme tulokseksi, että yhdistetyssä kuvauksessa alkio 1 kuvautuu alkiolle 3, $(\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(4) = 3$. Näin ollen

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ & & & \downarrow \\ 2 & 1 & 4 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 4 & 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 3 & & & \end{bmatrix}.$$

Vastaavasti etsimme alkion 2 kuvan seuraamalla ensin permutaation β sisällä alkion 2 kuvaan 1, $\beta(2) = 1$, ja permutaation α alkion 1 kuvaan 2, $\alpha(1) = 2$. Siis alkio 2 kuvatuu alkiolle 2, $\alpha(\beta(2)) = \alpha(1) = 2$. Etsimällä jokaiselle alkiolle kuva vastaavalla tavalla, saamme yhdistetyn funktion tulokseksi:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Samalla tavalla ratkaisemme myös yhdistetyn funktion $\beta \circ \alpha$. Aloitamme oikeanpuoleisesta permutaatiosta α, josta seuraamme alkion kuvaa vasemmanpuoleisen permutaatioon β. Siis saamme ratkaisuksi:

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Näin saimme ratkaistuksi yhdistetyt permutaatiot $\alpha \circ \beta$ ja $\beta \circ \alpha$.

Kuten esimerkistä 3.2 huomaamme, nyt $\alpha \circ \beta \neq \beta \circ \alpha$. Siis S_4 ei ole vaihdannainen. Kuitenkin, kuten Rotman [3, s. 104] huomauttaa, jotkut permutaatiot ovat vaihdannaisia. Esimerkiksi permutaatiot

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ ja } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

ovat vaihdannaisia, kuten näemme seuraavasta:

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

$$\text{ja } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Esimerkki 3.3. Ratkaistaan yhdistetty permutaatio $\sigma \circ \tau$, kun σ on identiteettipermutaatio, eli se kuvaa kaikki alkiot itselleen. Siis olkoot

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

Saadaan siis

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

joka matriisinotaationa on muotoa

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

Ratkaisu on siis sama kuin permutaatio τ. Identiteettipermutaatio kuvaa yhdistettynä permutaationa kaikki permutaatiot itselleen.

Rotman [3, s. 104] esittää permutaatioryhmässä pätevän supistussäännön:

(3.1) $$\text{jos } \gamma \circ \alpha = \gamma \circ \beta, \text{ niin } \alpha = \beta.$$

Osoitamme tämän seuraavalla:

$$\begin{aligned} \alpha &= 1_X \circ \alpha \\ &= (\gamma^{-1} \circ \gamma) \circ \alpha && \text{(identiteettifunktio)} \\ &= \gamma^{-1} \circ (\gamma \circ \alpha) && \text{(liitännäisyys)} \\ &= \gamma^{-1} \circ (\gamma \circ \beta) && \text{(oletus)} \\ &= (\gamma^{-1} \circ \gamma) \circ \beta && \text{(liitännäisyys)} \\ &= 1_X \circ \beta && \text{(identiteettifunktio)} \\ &= \beta. \end{aligned}$$

Vastaavasti voimme myös osoittaa, että kun $\alpha \circ \gamma = \beta \circ \gamma, \text{ niin } \alpha = \beta$.

4 Syklit

Rotman [3, s. 104] tuo esille, kuinka edellisessä luvussa käyttämämme kaksirivinen merkintätapa permutaatiolle on hankala. Lisäksi se ei myöskään paljasta vastauksia peruskysymyksiin, kuten onko permutaation neliö sen identiteetti, tai voidaanko permutaatio jakaa yksinkertaisempiin permutaatioihin?

Seuraavaksi käsittelemme erityisiä permutaatioita, joiden avulla voimme vastata yllämainittuihin kysymyksiin.

Ensin yksinkertaistamme merkintää $\beta \circ \alpha$ kirjoittamalla se $\beta\alpha$, sekä merkintää 1_X kirjoittamalla se (1).

Määritelmä 4.1. (Vrt. [1, s. 64], [2, s. 78-79]) Permutaatio $\alpha \in S_n$ on r alkion pituinen sykli, jota kutsutaan myös r-sykliksi, jos on olemassa alkiot $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, n\}$, joille pätee

$$\begin{aligned} \alpha(i_1) &= i_2 \\ \alpha(i_2) &= i_3 \\ &\vdots \\ \alpha(i_r) &= i_1 \end{aligned}$$

ja $\alpha(x) = x$ kaikille muille alkioille $x \in 1, 2, \ldots, n$. Merkitsemme sykliä α kirjoittamalla $(\, i_1 \; i_2 \; \ldots \; i_r \,)$.

Kaikki permutaatiot muodostuvat sykleistä. 2-syklissä alkiot i_1 ja i_2 kuvautuvat toisilleen ja muut alkiot kuvautuvat itselleen. 2-sykliä kutsutaan myös transpositioksi tai vaihdokseksi. 1-sykli on identiteetti, sillä jokainen alkio kuvautuu itselleen. Siitä syystä kaikki 1-syklit ovat samanarvoisia: $(i) = (1)$ kaikille i. [3, s. 105].

Seuraavaksi annamme esimerkin permutaation merkitsemisestä syklinä.

Esimerkki 4.1. Permutaatio $\pi \in S_4$ on syklinen, kun

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

Merkitsemme sitä lyhyemmin

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

Ajattelemme syklin kaaviona

$$1 \to 4 \to 3 \to 2 \to 1.$$

Voimme myös merkitä permutaatiota π seuraavasti

$$\begin{pmatrix} 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 & 4 \end{pmatrix} \text{ tai } \begin{pmatrix} 2 & 1 & 4 & 3 \end{pmatrix}.$$

Termi sykli (englanniksi cycle) tulee kreikan kielen sanasta ympyrälle (englanniksi circle). Voimme kuvitella syklin $(\, i_1\ i_2\ \cdots\ i_r\,)$ myötäpäiväisenä ympyrän kiertona. Mikä tahansa i_j voidaan ottaa aloituspisteeksi, jolloin r-syklille on r kappaletta erilaisia syklimerkintöjä. [3, s. 105]

Huomautus (vrt. [1, s. 64]). Luvun n arvo ei esiinny syklissä.

Annamme esimerkin permutaation syklien pituuksien selvittämisestä.

Esimerkki 4.2. Selvitetään permutaatioiden α ja β syklien pituudet.

Permutaatio $\alpha \in S_5$ on 5-sykli:

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

Permutaatio $\beta \in S_5$ taas on 3-sykli:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}.$$

Kuten Judson [2, s. 79] huomauttaa, kaikki permutaatiot eivät ole syklejä: Permutaatiossa $\gamma \in S_5$ on 2-sykli ja 3-sykli:

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}.$$

4.1 Syklin kertaluku

Lause 4.1. *Ryhmään S_n kuuluvan r-syklin kertaluku on r.*

Todistus (vrt. [1, s. 64-65]). Olkoon permutaatio

$$\pi = \begin{pmatrix} i_1 & i_2 & \cdots & i_r \end{pmatrix}$$

ryhmän S_n r-sykli, jolloin

$$\begin{aligned}
\pi(i_1) &= i_2,\\
\pi^2(i_1) &= \pi(\pi(i_1)) = \pi(i_2) = i_3,\\
\pi^3(i_1) &= i_4,\\
&\vdots\\
\pi^r(i_1) &= i_1.
\end{aligned}$$

Vastaavasti $\pi^r(i_j) = i_j$, kun $j = 1, 2, \ldots, r$.

Koska π^r kuvaa kaikki alkiot itselleen, se on identiteettipermutaatio. Mikään permutaatioista $\pi, \pi^2, \ldots, \pi^{r-1}$ ei vastaa identiteettipermutaatiota, koska ne kuvaavat alkion i_1 muille alkioille. Täten permutaation π kertaluku on r. □

Esimerkki 4.3. Olkoon permutaatio $\alpha \in S_4$ 3-sykli:

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

Saadaan $\alpha(1) = 4$, $\alpha^2(1) = \alpha(\alpha(1)) = \alpha(4) = 2$ ja $\alpha^3(1) = \cdots = \alpha(2) = 1$. Silloin permutaation α kertaluku on 3.

4.2 Erilliset permutaatiot

Määritelmä 4.2. (Vrt. [3, s. 108]) Permutaatiot α ja β ovat erilliset, jos jokaiselle alkiolle i, j pätee: jos $\alpha(i) \neq i$, niin $\beta(i) = i$, ja jos $\beta(j) \neq j$, niin $\alpha(j) = j$. Permutaatioperhe $\beta_1, \ldots, \beta_t$ on erillinen, jos jokainen permutaatiopari on keskenään erillinen.

Määritelmää selventääksemme annamme esimerkin erillisistä permutaatioista:

Esimerkki 4.4. Osoitetaan, että permutaatiot α ja β ovat erilliset.

Olkoot

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 3 & 5 & 4 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix} \in S_6.$$

Voimme kirjoittaa permutaatiot sykleinä, jolloin saamme

$$\alpha = \begin{pmatrix} 1 & 6 & 4 & 3 \end{pmatrix} \text{ ja } \beta = \begin{pmatrix} 2 & 5 \end{pmatrix}.$$

Sykleistä näemme, että ne koostuvat eri alkioista. Nyt syklissä α esiintyvät alkiot kuvautuvat permutaatiossa β itselleen, ja päinvastoin syklissä β esiintyvät alkiot kuvautuvat permutaatiossa α itselleen:

$$\begin{aligned} & & \beta(1) &= 1 \\ \alpha(2) &= 2 & \beta(3) &= 3 \\ \alpha(5) &= 5 & \beta(4) &= 4 \\ & & \beta(6) &= 6. \end{aligned}$$

Määritelmän 4.2 nojalla permutaatiot α ja β ovat siis erilliset permutaatiot.

Erillisillä permutaatioilla on useita ominaisuuksia, kuten seuraavan lauseen tulos, kommutointi:

Apulause 4.2. *Olkoot permutaatiot $\alpha, \beta \in S_X$ erillisiä. Silloin $\alpha\beta = \beta\alpha$.*

Todistus (vrt. [2, s. 80]). Olkoon

$$\alpha = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \text{ ja } \beta = \begin{pmatrix} b_1 & b_2 & \dots & b_l \end{pmatrix}.$$

Osoitamme, että $\alpha\beta = \beta\alpha$ pätee kaikille $x \in X$. Jos x ei kuulu kumpaankaan joukkoon $\{a_1, a_2, \dots, a_k\}$ tai $\{b_1, b_2, \dots, b_l\}$, niin $\alpha(x) = x$ ja $\beta(x) = x$. Täten

$$\alpha\beta(x) = \alpha(\beta(x)) = \alpha(x) = x = \beta(x) = \beta(\alpha(x)) = \beta\alpha(x).$$

Oletamme nyt, että $x \in \{b_1, b_2, \dots, b_l\}$. Silloin $\beta(b_i) = b_{(i \bmod l)+1}$, missä $i \mod l$ on luvun i jakojäännös jaettaessa luvulla l. Siis

$$\begin{aligned} b_1 &\to b_2, \\ b_2 &\to b_3, \\ &\vdots \\ b_{l-1} &\to b_l, \\ b_l &\to b_1. \end{aligned}$$

Nyt kuitenkin $\alpha(b_i) = b_i$, koska α ja β ovat erilliset permutaatiot. Siis saamme

tuloksen

$$\begin{aligned}\alpha\beta(b_i) &= \alpha(\beta(b_i)) \\ &= \alpha\left(b_{(i \bmod l)+1}\right) \\ &= b_{(i \bmod l)+1} \\ &= \beta(b_i) \\ &= \beta(\alpha(b_i)) \\ &= \beta\alpha(b_i).\end{aligned}$$

Samalla tavalla voimme osoittaa, jos $x \in \{a_1, a_2, \ldots, a_k\}$, niin α ja β kommutoivat.

□

Esimerkki 4.5. Osoitamme, että esimerkin 4.4 erilliset permutaatiot α ja β kommutoivat, siis $\alpha\beta = \beta\alpha$. Nyt

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

$$\text{ja } \beta = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 5 & 3 & 4 & 2 & 6\end{pmatrix} = \begin{pmatrix}2 & 5\end{pmatrix}.$$

Ratkaisemme ensin $\alpha \circ \beta$, joksi saamme

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

Ratkaisemme sitten $\beta \circ \alpha$, joksi saamme

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

Siis nyt $\alpha \circ \beta = \beta \circ \alpha$.

Huomaamme lopuksi, että

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

Permutaatiot, jotka eivät ole syklejä, voidaan jakaa kahteen tai useampaan sykliin seuraavasti: Jos π on permutaatio ryhmässä S_n ja $a \in \{1, 2, \ldots, n\}$, alkion a niin sanottu rata permutaatiossa π koostuu erisuurista alkioista $a, \pi(a), \pi^2(a) = \pi(\pi(a)), \pi^3(a), \ldots$. Voimme jakaa permutaation sen eri ratoihin ja jokainen rata muodostaa syklin. [1, s. 65-66]

Esimerkki 4.6. Olkoon permutaatio $\pi \in S_7$ määritelty kaavalle

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

Jaetaan permutaatio π ratoihin.

Nyt

$$\pi(1) = 3,\ \pi^2(1) = \pi(\pi(1)) = 5,\ \pi^3(1) = \pi(\pi(\pi(1))) = 4,\ \pi^4(1) = 1.$$

Siis alkion 1 rata on $\{1, 3, 5, 4\}$. Tämä on myös alkioiden 3, 4 ja 5 rata, ja se muodostaa syklin $(1\ 3\ 5\ 4)$. Alkion 2 rata on $\{2, 7\}$, joka muodostaa 2-syklin $(2\ 7)$. Alkio 6 kuvautuu itselleen, joten sen rata on $\{6\}$. Se muodostaa 1-syklin (6).

Permutaatio π on siis $\pi = (1\ 3\ 5\ 4) \circ (2\ 7) \circ (6)$. Määritelmän 4.2 mukaan ratojen muodostavat syklit ovat keskenään erillisiä. Jos permutaatio merkitään erillisten syklien yhdisteenä, niin apulauseen 4.2 nojalla ei ole väliä, missä järjestyksessä kirjoitamme syklit. Siis voimme myös kirjoittaa $\pi = (6) \circ (2\ 7) \circ (1\ 3\ 5\ 4)$. Usein jätämme kirjoittamatta 1-syklit ja kirjoitamme vain $\pi = (2\ 7) \circ (1\ 3\ 5\ 4)$ [1, s. 66].

Tästä pääsemmekin seuraavaan lauseeseen:

Lause 4.3. *Jokainen permutaatio voidaan kirjoittaa erillisten syklien yhdistelmänä.*

Todistus (vrt. [1, s. 66]). Olkoon π permutaatio ja olkoot $\gamma_1, \gamma_2, \ldots, \gamma_k$ permutaation π radoista muodostuneet syklit. Oletamme, että alkio a_1 kuuluu permutaation π määrittelyjoukkoon ja että $\pi(a_1) = a_2$.

Jos sykli γ_1 sisältää alkion a_1, voimme kirjoittaa syklin $\gamma_1 = (a_1\ a_2\ \cdots\ a_r)$. Nyt muut syklit $\gamma_2, \gamma_3, \ldots, \gamma_k$, eivät sisällä alkioita $a_1, a_2, \ldots, a_r$, eli alkiot kuvautuvat niissä itselleen.

Siis yhdiste $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$ kuvaa alkion a_1 alkiolle a_2, koska γ_1 on ainoa sykli, joka ei kuvaa alkioita a_1 ja a_2 itselleen. Täten $\pi = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$, sillä π ja $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$ kuvaavat kaikki permutaation π määrittelyjoukon alkiot samalla tavalla. □

Kirjoittaessamme permutaation erillisten syklien yhdisteenä saamme hyödyllisen tavan määrittää permutaation bijektioiden lukumäärä yhdestä erillisten syklien ominaisuudesta, jonka seuraava lause esittää:

Lause 4.4. *Permutaation kertaluku on sen erillisten syklien pituuksien pienin yhteinen jaettava.*

Todistus (vrt. [1, s. 66]). Kun kirjoitamme permutaation π sen erillisinä sykleinä $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_k$, voimme vaihtaa syklien järjestystä, koska ne ovat erillisiä. Siis myös $\gamma^m = {\gamma_1}^m \circ {\gamma_2}^m \circ \ldots {\gamma_k}^m$, mille tahansa positiiviselle kokonaisluvulle m.

Koska syklit ovat erillisiä, γ^m on identiteettipermutaatio, jos ja vain jos ${\gamma_i}^m$ on identiteettipermutaatio jokaiselle $i \in \{1, 2, \ldots, k\}$. Pienin tällainen positiivinen kokonaisluku m on permutaation syklien kertalukujen, siis myös syklien pituuksien, pienin yhteinen jaettava. □

Lauseen 4.4 avulla saamme siis selvitettyä myös permutaation identiteettipermutaation. Teemme nyt esimerkin selventääksemme lauseen 4.4 todistusta, sekä yksinkertaistaaksemme lauseen merkitystä.

Esimerkki 4.7. Selvitetään permutaation $\pi \in S_5$ bijektioiden lukumäärä. Olkoon

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}.$$

Permutaatio voidaan jakaa sykleihin seuraavasti:

$$\pi = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 & 4 \end{pmatrix}.$$

Selvittääksemme permutaation π identiteettipermutaation, pitää meidän selvittää ensin sen muodostavien syklien identiteettipermutaatiot. Merkitään syklejä $\gamma = \gamma_1 \circ \gamma_2 = (1\ 3) \circ (2\ 5\ 4)$. Nyt syklin γ_1 identiteettipermutaatio on ${\gamma_1}^2$, siis kertaluku on 2:

$$\gamma_1(1) = 3$$
$${\gamma_1}^2(1) = 1$$

ja syklin γ_2 identiteettipermutaatio on ${\gamma_2}^3$, siis kertaluku on 3:

$$\gamma_2(2) = 5$$
$${\gamma_2}^2(2) = 4$$
$${\gamma_2}^3(2) = 2.$$

Saadaan $\mathrm{pyj}(2, 3) = 6$, joten permutaation π identiteettipermutaatio on γ^6. Näemme myös, että $\gamma^6(1) = 1$ ja $\gamma^6(2) = 2$. Vastaavasti siis permutaation π kertaluku on 6.

5 Parilliset ja parittomat permutaatiot

Permutaatiot voivat olla joko parillisia tai parittomia. Parillisuus johdetaan siitä, miten permutaatio $\sigma \in S_n$ vaikuttaa n muuttujan polynomiin $f(x_1, x_2, \ldots, x_n)$, kun σ permutoi muuttujat seuraavasti

$$\sigma f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

[1, s. 67-68]

Esimerkki 5.1. Permutoidaan polynomin f muuttujat.

Olkoot

$$\sigma = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \in S_5 \text{ ja}$$

$$f(x_1, x_2, \ldots, x_5) = x_1x_2 + 7x_3x_5 - 9x_1x_4.$$

Nyt $x_{\sigma(1)} = x_3$, $x_{\sigma(3)} = x_5$ ja $x_{\sigma(5)} = x_1$, joten saadaan

$$\sigma f(x_1, x_2, \ldots, x_5) = x_3x_2 + 7x_5x_1 - 9x_3x_4.$$

5.1 Diskriminantti

Määritelmä 5.1. (Vrt. [1, s. 68]) Diskriminantti on polynomi $D(x_1, x_2, \ldots, x_n)$, joka on kaikkien termien $(x_i - x_j)$ tulo, missä $i < j$. Toisin sanoen

$$D = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Esimerkki 5.2. Permutoidaan diskriminantin $D(x_1, x_2, \ldots, x_n)$ muuttujat.

Olkoon $n = 4$. Tällöin

$$D = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Nyt permutaatio $\sigma \in S_n$, jolloin saamme

$$\sigma D = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

[1, s. 68]

Olkoon $\sigma = (\begin{smallmatrix} 1 & 3 & 4 & 2 \end{smallmatrix})$. Tällöin permutoimalla diskriminantin muuttujat saamme

$$\sigma D = (x_3 - x_1)(x_3 - x_4)(x_3 - x_2)(x_1 - x_4)(x_1 - x_2)(x_4 - x_2).$$

Kun järjestelemme termit, saamme

$$\begin{aligned}\sigma D &= (x_1 - x_2)(x_3 - x_1)(x_1 - x_4)(x_3 - x_2)(x_4 - x_2)(x_3 - x_4) \\ &= (x_1 - x_2)(-(x_1 - x_3))(x_1 - x_4)(-(x_2 - x_3))(-(x_2 - x_4))(x_3 - x_4) \\ &= -((x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)),\end{aligned}$$

josta voimme nähdä, että

$$\sigma D = -D.$$

Määritelmä 5.2. (Vrt. [1, s. 68]) Jokaiselle $\sigma \in S_n$ pätee, että $\sigma D = \pm D$. Jos $\sigma D = D$, niin sanomme, että σ on parillinen, ja jos $\sigma D = -D$, niin sanomme, että σ on pariton.

Esimerkin 5.2 permutaatio σ on siis pariton.

Määritelmä 5.3. (Vrt. [1, s. 68]) Olkoon D muuttujien $x_1, x_2, \ldots, x_n$ diskriminantti.

Merkitään symbolilla $D_{k/m}$ kaikkien niiden polynomin D termien tuloa, joissa esiintyy muuttuja x_k, paitsi $(x_k - x_m)$.

Merkitään symbolilla $D_{k,m}$ kaikkien niiden polynomin D termien tuloa, joissa ei esiinny kumpikaan muuttujista x_k tai x_m.

Esimerkki 5.3. Olkoon $n = 6$. Nyt saamme

$$\begin{aligned}D_{3/5} &= (x_1 - x_3)(x_2 - x_3)(x_3 - x_4)(x_3 - x_6) \\ D_{5/3} &= (x_1 - x_5)(x_2 - x_5)(x_4 - x_5)(x_5 - x_6) \\ D_{3,5} &= (x_1 - x_2)(x_1 - x_4)(x_1 - x_6)(x_2 - x_4)(x_2 - x_6)(x_4 - x_6).\end{aligned}$$

Määritelmän 5.3 avulla voimme nyt siis muodostaa diskriminantin D seuraavasti tekijöistään:

$$D = (x_k - x_m)D_{k/m}D_{m/k}D_{k,m}.$$

[1, s. 68]

5.2 Transpositio

Kuten olemme jo aiemmin kertoneet, 2-sykliä kutsutaan transpositioksi, koska se vaihtaa kaksi alkiota keskenään. Transpositioiden parillisuuden selvittäminen on olennaista, kun selvitämme, onko permutaatio parillinen vai pariton.

Lause 5.1. *Kaikki transpositiot ovat parittomia.*

Todistus (vrt. [1, s. 68-69]). Olkoon transpositio $\tau = (k\ m) \in S_n$, missä $k < m$. Koska τ vaihtaa keskenään alkiot k ja m, saamme, että

$$\begin{aligned}
\tau D_{k/m} &= \tau\big((x_1 - x_k)\cdots(x_{k-1} - x_k)(x_k - x_{k+1})\cdots(x_k - x_{m-1})(x_k - x_{m+1})\cdots(x_k - x_n)\big) \\
&= (x_1 - x_m)\cdots(x_{k-1} - x_m)(x_m - x_{k+1})\cdots(x_m - x_{m-1})(x_m - x_{m+1})\cdots(x_m - x_n) \\
&= (x_1 - x_m)\cdots(x_{k-1} - x_m)\underbrace{[-(x_{k+1} - x_m)]\cdots[-(x_{m-1} - x_m)]}_{\text{lkm määrittää muuttujan } u}(x_m - x_{m+1})\cdots(x_m - x_n) \\
&= u(x_1 - x_m)\cdots u(x_{k-1} - x_m)u\big[(x_{k+1} - x_m)\cdots(x_{m-1} - x_m)\big]u(x_m - x_{m+1})\cdots u(x_m - x_n) \\
&= u\big[(x_1 - x_m)\cdots(x_{k-1} - x_m)(x_{k+1} - x_m)\cdots(x_{m-1} - x_m)(x_m - x_{m+1})\cdots(x_m - x_n)\big] \\
&= uD_{m/k}, \qquad \text{missä } u = 1 \text{ tai } u = -1.
\end{aligned}$$

Koska τ^2 on identiteettipermutaatio, saamme

$$D_{k/m} = \tau^2 D_{k/m} = \tau(\tau D_{k/m}) = \tau(uD_{m/k}) = u(\tau D_{m/k}).$$

Kerrotaan puolittain muuttujalla u. Koska $u^2 = 1$, seuraa, että

$$uD_{k/m} = \tau D_{m/k}.$$

Koska $\tau D_{k,m} = D_{k,m}$, kertomalla polynomi D transpositiolla τ saadaan

$$\begin{aligned}
\tau D &= \tau(x_k - x_m)\cdot\tau D_{k/m}\cdot\tau D_{m/k}\cdot\tau D_{k,m} \\
&= (x_m - x_k)\cdot uD_{m/k}\cdot uD_{k/m}\cdot D_{k,m} \\
&= -(x_k - x_m)\cdot u^2\cdot D_{m/k}\cdot D_{k/m}\cdot D_{k,m} \\
&= -D,
\end{aligned}$$

koska $u^2 = 1$. Siis olemme todistaneet, että τ on pariton. Näin ollen kaikki transpositiot ovat parittomia. □

Konkreettistamme lauseen todistusta antamalla siitä esimerkin:

Esimerkki 5.4. Olkoon transpositio

$$\tau = \begin{pmatrix} 1 & 5 \end{pmatrix} \in S_6.$$

Nyt saamme

$$\begin{aligned} D_{1/5} &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_6), \\ D_{5/1} &= (x_2 - x_5)(x_3 - x_5)(x_4 - x_5)(x_5 - x_6) \text{ ja} \\ D_{1,5} &= (x_2 - x_3)(x_2 - x_4)(x_2 - x_6)(x_3 - x_4)(x_3 - x_6)(x_4 - x_6). \end{aligned}$$

Määritämme nyt

$$\tau D = \tau(x_1 - x_5) \cdot \tau D_{1/5} \cdot \tau D_{5/1} \cdot \tau D_{1,5}$$

$$\begin{aligned} \tau(x_1 - x_5) &= (x_5 - x_1) \\ \tau D_{1/5} &= (x_5 - x_2)(x_5 - x_3)(x_5 - x_4)(x_5 - x_6) \\ &= -D_{1/5} \\ \tau D_{5/1} &= (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_1 - x_6) \\ &= -D_{5/1} \\ \tau D_{1,5} &= (x_2 - x_3)(x_2 - x_4)(x_2 - x_6)(x_3 - x_4)(x_3 - x_6)(x_4 - x_6) \\ &= D_{1,5} \end{aligned}$$

$$\tau D = -(x_1 - x_5) \cdot -D_{1/5} \cdot -D_{5/1} \cdot D_{1,5} = -D.$$

Siis transpositio τ on pariton.

Nyt voimme määrittää, onko mielivaltainen permutaatio $\sigma \in S_n$ parillinen vai pariton, jakamalla se tekijöihinsä transpositioiden tuloksi [1, s. 69].

Lause 5.2. *Kaikki r-syklit ovat $r - 1$ transposition yhdisteitä (eivät välttämättä erillisten transpositioiden).*

Todistus (vrt. [1, s. 69]). Jaetaan r-sykli transpositioihin. Saamme

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_r \end{pmatrix} = \underbrace{\begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_{r-1} & a_r \end{pmatrix}}_{r-1 \text{ kpl}}.$$

□

Ja koska lauseen 4.3 nojalla jokainen permutaatio σ on erillisten permutaatioiden yhdiste, seuraa, että σ on transpositioiden yhdiste.[1, s. 69]

Lause 5.3. *Kaikki permutaatiot $\sigma \in S_n$ ovat transpositioiden yhdistettyjä permutaatioita. Lisäksi, jos σ on m transposition yhdiste, σ on parillinen, jos m on parillinen, ja σ on pariton, jos m on pariton.*

Todistus (vrt. [1, s. 69]). Kirjoitamme $\sigma = \tau_1\tau_2\cdots\tau_m$, missä τ_i ovat transpositioita. Olkoon D n muuttujan diskriminantti. Tällöin $\tau_i D = -D$, kaikilla $i = 1, 2, \ldots, m$, lauseen 5.1 nojalla. Siis permutaation $\sigma = \tau_1\tau_2\cdots\tau_m$ vaikutus diskriminanttiin D on vaihtaa etumerkkiä m kertaa. Siis $\sigma D = (-1)^m D$, josta seuraa lauseen väite. □

Gilbert [1, s. 69] tuo esille, että nyt lauseen 5.2 seurauksena syntyy seuraava lause:

Lause 5.4. *Permutaatio n-sykli on pariton permutaatio, jos n on parillinen, ja se on parillinen permutaatio, jos n on pariton.*

Esimerkki 5.5. Kirjoita permutaatio

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

erillisten syklien yhdisteenä ja määritä permutaation kertaluku ja onko permutaatio parillinen vai pariton.

Permutaatio τ muodostuu kahdesta erillisestä syklistä, sillä

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

Saamme siis syklien pituuksilla permutaation τ kertaluvuksi $\operatorname{pyj}(4, 3) = 12$. Sykleistä 4-sykli on pariton ja 3-sykli on parillinen, josta saamme, että τ on pariton.

5.3 Alternoiva ryhmä

Merkitsemme n alkion parillisten permutaatioiden joukkoa notaatiolla A_n. Lauseesta 5.3 seuraa, että A_n on ryhmän S_n aliryhmä, jota kutsutaan n alkion alternoivaksi ryhmäksi. Esimerkiksi

$$A_4 = \left\{ \begin{array}{l} (1), \\ \\ \end{array} \begin{array}{l} (1\ \ 2) \circ (3\ \ 4), \\ (1\ \ 3) \circ (2\ \ 4), \\ (1\ \ 4) \circ (2\ \ 3), \end{array} \begin{array}{l} (1\ \ 2\ \ 3), \ (1\ \ 2\ \ 4), \ (1\ \ 3\ \ 4), \ (2\ \ 3\ \ 4), \\ (1\ \ 3\ \ 2), \ (1\ \ 4\ \ 2), \ (1\ \ 4\ \ 3) \ \ (2\ \ 4\ \ 3) \end{array} \right\}$$

on 12 alkion ryhmä. [1, s. 70] Ryhmän alkioiden lukumäärä määräytyykin seuraavan lauseen mukaisesti:

Lause 5.5. $|A_n| = \frac{1}{2}n!$ *kaikilla* $n \geq 2$.

Todistus (vrt. [1, s.70]). Olkoon O_n parittomien permutaatioiden joukko ryhmässä S_n. Näin ollen $S_n = A_n \cup O_n$ ja $A_n \cap O_n = \varnothing$. Siis $n! = |S_n| = |A_n| + |O_n|$, joten meidän tulee osoittaa, että $|A_n| = |O_n|$. Osoittaaksemme tämän etsimme bijektion $f\colon A_n \to O_n$.

Olkoon $\tau = (1\ 2)$ ja määritellään f siten, että $f(\sigma) = \tau \circ \sigma$ kaikille $\sigma \in A_n$. Tässä $\tau \circ \sigma$ on pariton, koska σ on parillinen ja τ on pariton. Näin ollen f on kuvaus $A_n \to O_n$.

Funktio f on injektio, koska jos $f(\sigma) = f(\sigma_1)$, niin $\tau \circ \sigma = \tau \circ \sigma_1$, joten ryhmän S_n supistussäännöllä (kaava (3.1) sivulla 10) saadaan, että $\sigma = \sigma_1$.

Oletetaan nyt, että $\lambda \in O_n$. Siis $\tau \circ \lambda \in A_n$ ja $f(\tau \circ \lambda) = \tau \circ (\tau \circ \lambda) = (\tau \circ \tau) \circ \lambda = \lambda$, koska $\tau \circ \tau = \mathrm{id}$. Täten f on surjektio. □

Lause 5.6. *Kaikki parilliset permutaatiot voidaan kirjoittaa* 3*-syklien yhdisteenä (jotka eivät välttämättä ole erillisiä).*

Todistus (vrt. [1, s.70]). Lauseen 5.3 mukaan parillinen permutaatio voidaan kirjoittaa transpositioiden parillisen määrän yhdisteenä. Osoitamme nyt, että kahden transposition yhdiste on 3-syklien yhdiste.

Jos kaksi transpositiota ovat samat, niiden yhdiste on identiteettipermutaatio. Jos transpositioilla on yksi yhteinen alkio, esimerkiksi $(a\ b)$ ja $(b\ c)$, niiden yhdiste on $(a\ b) \circ (b\ c) = (abc)$, joka on 3-sykli. Jos transpositioilla ei ole yhteisiä alkioita, esimerkiksi $(a\ b)$ ja $(c\ d)$, voimme kirjoittaa niiden yhdisteen muodossa

$$\begin{pmatrix} a & b \end{pmatrix} \circ \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \circ \underbrace{\begin{pmatrix} b & c \end{pmatrix} \circ \begin{pmatrix} b & c \end{pmatrix}}_{=\,\mathrm{id}} \circ \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a & b & c \end{pmatrix} \circ \begin{pmatrix} b & c & d \end{pmatrix},$$

joka on 3-syklien yhdiste. □

Lauseet 5.3 ja 5.6 osoittavat, että S_n koostuu 2-sykleistä ja A_n koostuu 3-sykleistä.

Esimerkki 5.6. Kirjoitetaan permutaatio $\gamma \in S_6$ 3-syklien yhdisteenä. Olkoon permutaatio

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 6 & 2 & 5 \end{pmatrix} \in S_6,$$

joka kirjoitetaan sykli notaationa

$$(1 \quad 4 \quad 6 \quad 5 \quad 2).$$

Siis γ on 5-sykli. Lauseen 5.4 nojalla permutaatio on siis parillinen. Nyt siis lauseen 5.6 mukaan voimme kirjoittaa permutaation γ 3-syklien yhdisteenä. Kirjoitetaan γ ensin transpositioiden yhdisteenä:

$$(1 \quad 4) \circ (4 \quad 6) \circ (6 \quad 5) \circ (5 \quad 2),$$

josta voimme kirjoittaa sen sitten 3-syklien yhdisteenä:

$$(1 \quad 4 \quad 6) \circ (6 \quad 5 \quad 2).$$

Lähteet

[1] Gilbert, W. ja Nicholson, W. *Modern Algebra with Applications*. 2. painos. New Jersey: John Wiley and Sons, Inc., Hoboken, 2004.

[2] Judson, T. *Abstract Algebra: Theory and Applications*. 2014 vuoden painos. [Verkkopainos] Abstract Algebra -kirjan kotisivu, 2018 [Viitattu 22.11.2018] URL http://abstract.ups.edu/download.html

[3] Rotman, J. *A First Course in Abstract Algebra*. 3. painos. New Jersey: Prentice Hall, 2006