

2 Permutaatioryhmät

Rubikin kuution siirrot ovat tietynlaisia permutaatioita. Permutaatiot muodostavat ryhmä, ja tällä tavoin ryhmäteorian työkaluja päästään käyttämään kuutio-ongelman selvittämiseen. Tässä luvussa tutustutaan permutaatioryhmien perusteisiin sekä siihen, millä tavoin kuution siirrot tulkitaan permutaatioiksi.

2.1 Permutaation olemus

Matemaattisen määritelmän mukaan permutaatio on bijektio joukolta itselleen. Näin yksinkertaiselle käsitteelle ei kuitenkaan syyttä ole annettu noin hienoa nimeä. Latiinan sana ”permutatio” tarkoittaa muutosta tai vaihtoa, ja permutaatio kuvaakin joukon sisäistä muutosta, joka kuitenkin säilyttää kaikki joukon alkiot sellaisinaan; yleensä kyseessä on alkioiden järjestyksen vaihtuminen.

Vastaostetussa korttipakassa kortit ovat tietyssä perusjärjestyksessä. Kun korttipakan ensimmäisen kerran sekoittaa, esimerkiksi herttaässä paikalle tulee joku toinen kortti, vaikkapa patakakkonen. Voidaan ajatella, että herttaässä muuttui — tai kuvautui — patakakkoseksi. On siis tapahtunut korttipakan permutaatio, jossa jokainen kortti on voinut vaihtua toiseksi, mutta yksikään kortti ei ole kadonnut eikä kortteja ole myöskään tullut lisää.

Permutaatiota voidaan tarkastella monelta kannalta. Ensinnäkin permutaation voidaan ajatella tarkoittavan operaatiota, joka sekoittaa korttipakan tietyllä tavalla. Toisaalta voidaan ajatella permutaation tarkoittavan sitä *lopputulosta*, johon alunperin perusjärjestyksessä oleva korttipakka asettuu tietyn sekoittamisen jälkeen. Toisinaan toinen tulkinta on sopivampi, toisinaan toinen.

Vielä yksi ajattelutapa on syytä mainita. Jos kuvitellaan kaikki uuden korttipakan kortit numeroiduiksi juoksevalla järjestysnumerolla, voidaan permutaation ajatella *muuttavan näitä järjestysnumeroita*, sen sijaan että se muuttaisi itse kortteja. Tämä helpottaa matemaattista tarkastelua, kun voidaan aina rajoittaa johonkin standardiin lukujoukkoon ja sen bijektioihin tarvitsematta määritellä erikseen korttien tai muiden esineiden joukkoja.

2.2 Permutaatioilla laskeminen

Permutaatiot ovat kuvauksia, joten niiden laskutoimitukseksi on luontevaa valita kuvauksen yhdistäminen. Kahden permutaation tulo on siis $\sigma\tau = \sigma \circ \tau$, ja tuloksena on kuvaus, jossa suoritetaan *ensin oikeanpuoleinen* permutaatio τ , sitten vasemmanpuoleinen permutaatio σ . Laskutoimituksen neutraalialkioksi tulee identtinen kuvaus id , joka ei muuta alkioiden järjestystä mitenkään. Toisaalta permutaation σ käänteisalkioksi tulee käänteiskuvaus σ^{-1} , joka vaihtaa alkioiden järjestyksen takaisin siksi, mikä se olisi ollut ennen permutaation σ soveltamista. Käänteisfunktio on aina olemassa, koska permutaatiot ovat bijektioita.

Rajoitetaan nyt tarkastelemaan vain lukujoukkojen $N_n = \{1, 2, \dots, n\}$ permutaatioita. Joukolla N_n on yhteensä $n!$ permutaatiota, mikä nähdään tuloperiaatteen avulla:

ensimmäiselle alkionle voidaan valita uusi paikka n :llä tavalla, tämän jälkeen toiselle voidaan valita uusi paikka $(n - 1)$:llä tavalla jne.

Määritelmä 2.1. *Symmetrinen ryhmä* S_n on kaikkien joukon N_n permutaatioiden muodostama ryhmä. Ryhmän laskutoimituksena on kuvausten yhdistäminen, neutraalialkiona identtinen kuvaus id ja alkion $\sigma \in S_n$ käänteisalkio on käänteiskuvaus σ^{-1} .

Kuten aiemmin mainittiin, jokaisen äärellisen joukon alkio voidaan varustaa järjestysnumerolla, jolloin joukon permutaatioiden voidaan ajatella olevan jonkin joukon N_n permutaatioita. Tämän vuoksi voidaan äärellisessä tapauksessa aina rajoittua tutkimaan symmetristen ryhmien S_n ominaisuuksia. Tällaisten ryhmien alkioita (mikäli n ei ole kohtuuttoman suuri) voidaan merkitä seuraavalla tavalla:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Esimerkki 2.2. Olkoon permutaatio $\sigma \in S_4$ sellainen, että $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ ja $\sigma(4) = 4$. Tätä permutaatiota voidaan nyt merkitä seuraavasti:

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

Kun tämä permutaatio kerrotaan vasemmalta eräällä toisella permutaatiolla, tuloksena on

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

Toisaalta permutaation σ käänteisalkio on

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

2.3 Rubikin ryhmä

Perusasemassa olevan Rubikin kuution kukin sivu on tietyn värinen ja jaettu yhdeksään ruutuun. Kun Rubikin kuution tahkoja pyörittää, näiden ruutujen paikat sekoittuvat. Jos ajatellaan jokainen ruutu keskiruutuja lukuunottamatta numeroiduksi tietyllä järjestysluvulla, voidaan kuutiota tarkastella joukkona N_{48} . Jokainen kuution siirto siis vastaa tiettyä joukon N_{48} permutaatiota eli symmetrisen ryhmän S_{48} alkioita. (Keskitalojen ajatellaan pysyvän aina paikoillaan.) Näitä alkioita on yhteensä $48! \approx 1,24 \cdot 10^{61}$ kappaletta. Kuitenkaan kaikkia joukon S_{48} permutaatioita ei voida muodostaa kuution siirroilla. Esimerkiksi punaisen ja sinisen sivun reunassa olevan särmäpalan punaista ruutua ei voi vaihtaa sinisen ja keltaisen sivun reunan särmäpalan sinisen sivun ruudun kanssa. Tällöin nimittäin kuutioon tulisi särmäpala, jolla olisi kaksi sinistä ruutua. Tällaista palaa ei alkuperäisessä kuutiossa kuitenkaan ole, eivätkä siirrot voi muuttaa

palojen rakennetta. Toisaalta on paljon muitakin siirtoja, jotka eivät ole mahdollisia. Esimerkiksi minkään särmäpalan kahta ruutua ei voi vaihtaa keskenään ilman että muutkin ruudut muuttuisivat. Syy tähän nähdään myöhemmin.

Rubikin kuution mahdolliset siirrot muodostavat ryhmän. Jos nimittäin tehdään kaksi mahdollista siirtoa peräkkäin, tulos on edelleen mahdollinen siirto. Toisaalta se, ettei tee mitään, on myös mahdollinen siirto, ja tämä siirto vastaa identtistä permutaatiota. Edelleen minkä tahansa siirron voi peruuttaa kääntämällä tahkoja päinvastaisessa järjestyksessä toiseen suuntaan, joten minkä tahansa mahdollisen siirron käänteissiirto on myös mahdollinen.

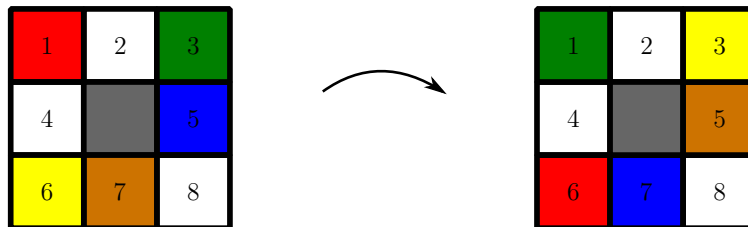
Määritelmä 2.3. Olkoon X joukko, johon kuuluvat kaikki Rubikin kuution ruudut keskiruutuja lukuunottamatta. *Rubikin ryhmä* \mathbb{R} on sellainen joukon X permutaatioiden joukko, jonka jokainen alkio vastaa jotakin Rubikin kuution laillista siirtoa. Rubikin ryhmä voidaan tulkita symmetrisen ryhmän S_{48} aliryhmäksi.

Kun konkreettisten objektien järjestyksen muutos tulkitaan permutaatioksi, tulkinassa on aina useita kaksi vaihtoehtoja. Jotta välttyttäisiin ristiriidoilta, on kiinnitettävä jokin Rubikin ryhmän siirtojen tulkinta, jota tullaan jatkossa käyttämään.

Tarkastellaan yksinkertaisuuden vuoksi vain yhtä sivua ja sen ruutuja. Kuvassa 3 näkyy eräs siirto, joka permutoi ruutuja. Kuvassa ruutujen paikat on numeroitu vapaavaltaisella tavalla, ja valkoisten ruutujen oletetaan pysyvän paikallaan. Siirron permutaatioesitys saadaan nyt seuraavasti:

- 1) Katsotaan, mikä ruutu on paikalla i .
- 2) Katsotaan, millä paikalla j kyseinen ruutu on siirron jälkeen.
- 3) Sanotaan, että etsittävä permutaatio kuvaa luvun i luvuksi j .

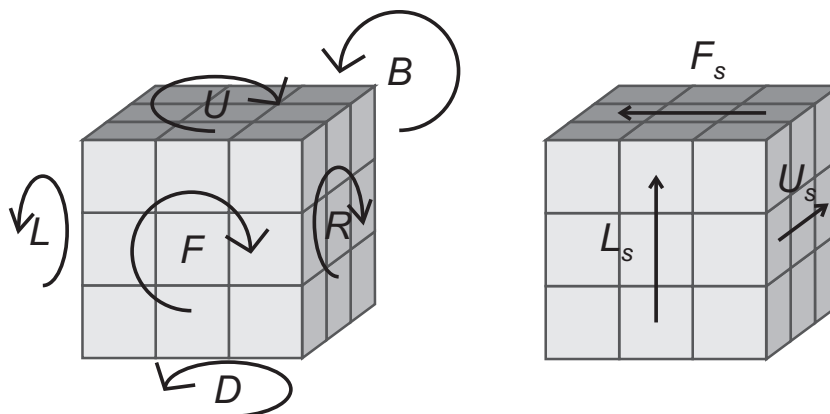
Tällä tavalla tulkittuna kuvan siirto on permutaatio $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 1 & 4 & 7 & 3 & 5 & 8 \end{pmatrix}$.



Kuva 3: Eräs Rubikin ryhmän siirto.

Rubikin ryhmän keskeisimmät alkio ovat niin sanotut *perussiirrot*, joilla tarkoitetaan kunkin tahkon neljännesympyrän suuruista pyörähdystä myötapäivään. Näitä siirtoja merkitään kirjaimilla U , D , F , B , L ja R seuraavan kuvan mukaisesti. (Tämä on yleisesti käytetty merkintätapa, jonka esitteli David Singmaster.) Kuvassa sininen sivu on ylhäällä ja keltainen sivu osoittaa katsojaan päin.

Keskitalahkojen pyöritys vastaa sitä, että pyöritetään molempia rinnakkaisia sivutahkoja vastakkaiseen suuntaan ja sitten käännetään koko kuutiota takaisinpäin. Tämän



Kuva 4: Kuution perussiirrot ja keskitahkojen siirrot.

vuoksi keskitahkojen pyöritystä ei tarvitse ottaa erikseen huomioon. Merkintöjen helpottamiseksi voidaan näitä ”näennäisperussiirtoja” kuitenkin merkitä kirjaimilla U_S , F_S ja L_S oheisen kuvan mukaisesti. (Alaindeksi tulee englannin sanasta ”slice”.) Oikeastaan siis $U_S = UD^{-1}$, $F_S = FB^{-1}$ ja $L_S = LR^{-1}$, ja näihin on vielä lisättävä koko kuution kääntäminen.

Rubikin ryhmä on määritelmänsä mukaisesti perussiirtojen virittämä, eli jokainen Rubikin ryhmän alkio voidaan muodostaa äärellisenä tulona perussiirroista tai niiden käänteisalkioista.

Sitä ruutujen järjestystä, johon perusjärjestyksessä oleva Rubikin kuutio joutuu tietyn laillisen permutaation jälkeen, kutsutaan *kuution tilaksi*. Jokaista tilaa vastaa siis tietty permutaatio, ja monesti tiloja nimitetäänkin myös permutaatioiksi. Jos mihin tahansa tilaan sovelletaan kyseistä tilaa vastaavan permutaation käänteisalkiota, saadaan kuutio palautetuksi perusjärjestykseen. Ongelmana on vain se, että kyseistä käänteisalkiota ei ole helppo palauttaa perussiirroiksi.

Määritelmä 2.4. Olkoon kuution tilaa vastaava permutaatio σ . Kyseisen tilan *ratkaiseminen* tarkoittaa käänteispermutaation σ^{-1} ilmaisemista perussiirtojen ja niiden käänteisalkioiden avulla.

Rubikin kuution ratkaisualgoritmi on jokin menetelmä, jolla mikä tahansa tila voidaan ratkaista. Ratkaisualgoritmin löytämiseksi tullaan jatkossa syventymään Rubikin ryhmän rakenteeseen. Sitä varten täytyy kuitenkin ensin tutustua eräisiin permutaatio-ryhmiä koskeviin käsitteisiin.

2.4 Syklit

Syklit ovat permutaatioita, jotka kuvaavat joitain alkioita kehässä toinen toisilleen:

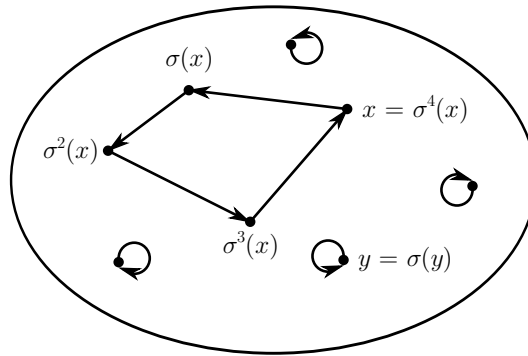
$$x_1 \mapsto x_2 \mapsto x_3 \mapsto \cdots \mapsto x_n \mapsto x_1.$$

Muut alkioit sykli pitää paikallaan.

Määritelmä 2.5. Olkoon X jokin äärellinen joukko. Joukon X permutaatiota σ nimitetään *sykliseksi*, jos löytyy sellainen $x \in X$, että kaikilla $y \in X$ pätee

$$y = \sigma^k(x) \quad \text{jollain } k \in \mathbb{N} \quad \text{tai} \quad \sigma(y) = y.$$

Koska joukko X on äärellinen ja permutaatiot ovat bijektioita, voidaan todistaa, että jollain $n > 0$ pätee $\sigma^n(x) = x$. Pienintä tällaista lukua n kutsutaan syklin *pituudeksi*. Toisaalta sykliä, jonka pituus on n , kutsutaan *n -sykliseksi*.



Kuva 5: Eräs 4-sykli.

Sykliä, jonka pituus on n , voidaan merkitä seuraavasti:

$$(x \ \sigma(x) \ \sigma^2(x) \ \dots \ \sigma^{n-1}(x)).$$

Jos $n = 2$, sykliä nimitetään *vaihdoksi* tai *transpositioksi*.

Esimerkki 2.6. Permutaatio

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

on 4-sykli, sillä $3 = \sigma(2)$, $6 = \sigma^2(2)$, $4 = \sigma^3(2)$, $2 = \sigma^4(2)$ ja toisaalta $\sigma(1) = 1$ ja $\sigma(5) = 5$. Voidaan merkitä $\sigma = (2364)$ tai yhtä hyvin esimerkiksi $\sigma = (3642)$ tai $\sigma = (4236)$. Sen sijaan permutaatio

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

ei ole sykli, koska $3 = \sigma(2)$ ja $2 = \sigma^2(2)$, mutta $\sigma(4) \neq 4$.

Jokainen permutaatio voidaan kirjoittaa erillisten syklien tulona. Tämä merkintätapa on yksikäsitteinen lukuunottamatta sitä, että jokainen n -sykli voidaan kirjoittaa n :llä eri tavalla ja lisäksi syklit voidaan kirjoittaa tuloksi missä järjestyksessä tahansa (erilliset syklit ovat keskenään vaihdannaisia). Sykliesitys löydetään lähtemällä jostain alkioista x ja muodostamalla siitä lähtevä sykli $(x \ \sigma(x) \ \dots)$. Sen jälkeen otetaan jokin alkio y , joka ei esiinny jo muodostetussa syklissä ja muodostetaan siitä lähtevä sykli $(y \ \sigma(y) \ \dots)$. Näin jatketaan, kunnes uusia alkioita ei enää löydy.

Esimerkki 2.7. Edellisen esimerkin permutaatio τ voidaan kirjoittaa syklien tulona muodossa $\tau = (1)(23)(456)$.

Yhden alkion syklejä ei tarvitse merkitä sykliesitykseen. Tällöin edellisen esimerkin sykliesitys olisi yksinkertaisemmin kirjoitettuna $\tau = (23)(456)$. Jos sykliesityksessä on vain yhden alkion syklejä eli kyseessä on identtinen permutaatio, niin tällöin yksi 1-sykli on kuitenkin merkittävä.

Jotta kuvauksen arvoa merkittäessä eivät sulut menisi sekaisin 1-syklin kanssa, merkitään toisinaan selvyuden vuoksi kuvaussulkuja hakasuluilla esimerkiksi seuraavasti: $\tau(4) = (23)(456)[4] = 5$.

2.5 Permutaation etumerkki

Permutaatiot voidaan jakaa ns. *parillisiin* ja *parittomiin* permutaatioihin sen mukaan, koostuvatko ne parillisesta vai parittomasta määrästä 2-syklejä eli vaihtoja. Seuraavaksi on tarkoitus osoittaa, että jokainen permutaatio voidaan kirjoittaa vaihtojen tulona ja että vaikka tietty permutaatio voidaan kirjoittaa tällaisena tulona usealla eri tavalla, vaihtoja tulee kuitenkin joka tapauksessa joko parillinen tai pariton määrä.

Lause 2.8. *Jokainen äärellisen joukon permutaatio voidaan muodostaa 2-syklien tulona. Toisin sanoen 2-syklit virittävät ryhmän S_n .*

Todistus. Lähdetään liikkeelle permutaation sykliesityksestä. Jos permutaatiossa esiintyy n -sykli $\tau = (x_1x_2 \dots x_n)$, korvataan tämä vaihtojen tulolla

$$\tau' = (x_1x_2)(x_2x_3) \cdots (x_{n-1}x_n).$$

Helposti nähdään, että $\tau = \tau'$. Jos nimittäin $y \neq x_k$ kaikilla k , niin $\tau(y) = y = \tau'(y)$. Toisaalta jos $1 \leq k < n$, niin $\tau(x_k) = x_{k+1}$, ja tällöin

$$\begin{aligned} \tau'(x_k) &= (x_1x_2)(x_2x_3) \cdots (x_{k-1}x_k)(x_kx_{k+1}) \cdots (x_{n-1}x_n)[x_k] \\ &= (x_1x_2)(x_2x_3) \cdots (x_{k-1}x_k)(x_kx_{k+1})[x_k] \\ &= (x_1x_2)(x_2x_3) \cdots (x_{k-1}x_k)[x_{k+1}] = x_{k+1}. \end{aligned}$$

Edelleen $\tau(x_n) = x_1$, ja

$$\begin{aligned} \tau'(x_n) &= (x_1x_2)(x_2x_3) \cdots (x_{n-2}x_{n-1})(x_{n-1}x_n)[x_n] \\ &= (x_1x_2)(x_2x_3) \cdots (x_{n-2}x_{n-1})[x_{n-1}] \\ &\quad \vdots \\ &= (x_1x_2)[x_2] = x_1. \end{aligned}$$

Kun jokainen sykliesityksen sykli korvataan edellä mainitulla tavalla, saadaan permutaatio esitettyksi vaihtojen tulona. \square

Olkoon $\sigma \in S_n$. Merkitään

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

Merkitään lisäksi $\Delta(\text{id}) = \Delta_n$.

Esimerkki 2.9. Jos $\sigma \in S_3$, niin

$$\Delta(\sigma) = (\sigma(2) - \sigma(1))(\sigma(3) - \sigma(1))(\sigma(3) - \sigma(2)).$$

Tällöin erityisesti

$$\Delta(\text{id}) = \Delta_3 = (2-1)(3-1)(3-2) = 1 \cdot 2 \cdot 1 = 2,$$

$$\Delta((12)) = (1-2)(3-2)(3-1) = -1 \cdot 1 \cdot 2 = -2,$$

$$\text{ja } \Delta((123)) = (3-2)(1-2)(1-3) = 1 \cdot (-1) \cdot (-2) = 2.$$

Huomaa, että tulon $\Delta(\sigma)$ eri arvot poikkeavat toisistaan vain etumerkiltään.

Tulon $\Delta(\sigma)$ avulla voidaan määritellä permutaation *etumerkki*. Osoitetaan kuitenkin sitä ennen eräs tekninen aputuloks. Tämä tulos selittää samalla edellisessä esimerkissä havaitun tulon etumerkkiin liittyvän ilmiön.

Lemma 2.10. *Kaikilla $\sigma, \tau \in S_n$ pätee $\Delta(\sigma\tau) = (-1)^k \cdot \Delta(\sigma)$, missä k on sellaisten parien $i, j \in N_n$ lukumäärä, joilla $j < i$ mutta $\tau(j) > \tau(i)$. Erityisesti, jos $\sigma = \text{id}$, väite pätee muodossa $\Delta(\tau) = (-1)^k \cdot \Delta_n$.*

Todistus. Todistus perustuu seuraavaan havaintoon: koska τ on bijektio, lukujen i ja j käydessä kertaalleen joukon N_n parit läpi, myös arvot $\tau(i)$ ja $\tau(j)$ käyvät kertaalleen läpi samat parit, joskin eri järjestyksessä. Tämän tiedon perusteella voidaan luvuilla i ja j indeksöityjä tuloja indeksöidä yhtä hyvin luvuilla $\tau(i)$ ja $\tau(j)$.

Aina kun $i < j$, pätee joko $\tau(i) < \tau(j)$ tai $\tau(j) < \tau(i)$, koska τ on injektio. Näin ollen tulo $\Delta(\sigma\tau)$ voidaan aluksi jakaa kahteen osaan:

$$\Delta(\sigma\tau) = \prod_{1 \leq i < j \leq n} (\sigma\tau(j) - \sigma\tau(i)) = \prod_{\substack{1 \leq i < j \leq n \\ \tau(i) < \tau(j)}} (\sigma\tau(j) - \sigma\tau(i)) \cdot \prod_{\substack{1 \leq i < j \leq n \\ \tau(j) < \tau(i)}} (\sigma\tau(j) - \sigma\tau(i)).$$

Käännetään jälkimmäisen tulon tekijät ympäri kertomalla ne luvulla -1 , ja vaihdetaan sitten samassa tulossa kertomisindeksit i ja j päittäin:

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

Jos nyt merkitään kirjaimella k niiden parien $i, j \in N_n$ lukumäärää, joille pätee $j < i$ ja $\tau(j) > \tau(i)$, näyttää kokonaistulo tältä:

$$\begin{aligned} \Delta(\sigma\tau) &= \prod_{\substack{1 \leq i < j \leq n \\ \tau(i) < \tau(j)}} (\sigma\tau(j) - \sigma\tau(i)) \cdot \prod_{\substack{1 \leq j < i \leq n \\ \tau(i) < \tau(j)}} -(\sigma\tau(j) - \sigma\tau(i)) \\ &= (-1)^k \cdot \prod_{\substack{1 \leq i < j \leq n \\ \tau(i) < \tau(j)}} (\sigma\tau(j) - \sigma\tau(i)) \cdot \prod_{\substack{1 \leq j < i \leq n \\ \tau(i) < \tau(j)}} (\sigma\tau(j) - \sigma\tau(i)). \end{aligned}$$

Ensimmäisessä tulossa esiintyy nyt sellaisia tekijöitä, joilla $i < j$, toisessa sellaisia, joilla $j < i$. Muita vaihtoehtoja ei kuitenkaan ole niin kauan kuin $\tau(i) < \tau(j)$. Näin ollen tulot voidaan yhdistää, jolloin saadaan

$$\Delta(\sigma\tau) = (-1)^k \cdot \prod_{\substack{i,j \in N_n \\ \tau(i) < \tau(j)}} (\sigma\tau(j) - \sigma\tau(i)).$$

Lopulta voidaan käyttää hyväksi alussa tehtyä havaintoa. Yllä olevassa tulossa luvut $\tau(i)$ ja $\tau(j)$ käyvät kerran läpi kaikki sellaiset joukon N_n parit, joille pätee $\tau(i) < \tau(j)$. Täten tulo voidaan kirjoittaa vielä kerran uudelleen korvaamalla $\tau(i) = i'$ ja $\tau(j) = j'$:

$$\Delta(\sigma\tau) = (-1)^k \cdot \prod_{0 \leq i' < j' \leq n} (\sigma(j') - \sigma(i')) = (-1)^k \cdot \Delta(\sigma).$$

Näin on väite todistettu. □

Määritelmä 2.11. Permutaation $\sigma \in S_n$ *etumerkki* on

$$\text{sign}(\sigma) = \frac{\Delta(\sigma)}{\Delta_n}.$$

Edellisen lemmän perusteella kaikilla $\sigma \in S_n$ pätee $\text{sign}(\sigma) = \pm 1$. Permutaatiota kutsutaan *parilliseksi*, jos sen etumerkki on 1, ja *parittomaksi*, jos etumerkki on -1 .

Aputuloksesta 2.10 saadaan tulkinta permutaation σ etumerkille: se kertoo, onko sellaisia pareja $i < j$, joille pätee $\sigma(i) > \sigma(j)$ (eli jotka vaihtavat järjestystä), parillinen vai pariton määrä. Aputuloksen avulla voidaan helposti todistaa myös eräs tärkeä etumerkin ominaisuus.

Lemma 2.12. *Kaikilla $\sigma, \tau \in S_n$ pätee $\text{sign}(\sigma\tau) = \text{sign}(\sigma) \text{sign}(\tau)$.*

Todistus. Olkoon k niiden parien $i, j \in N_n$ lukumäärä, joilla $i < j$ mutta $\tau(j) < \tau(i)$. Lemman 2.10 perusteella pätee

$$\Delta(\tau) = (-1)^k \cdot \Delta_n,$$

joten $(-1)^k = \text{sign}(\tau)$. Nyt voidaan laskea samaisen lemmän avulla

$$\Delta(\sigma\tau) = (-1)^k \cdot \Delta(\sigma) = \text{sign}(\tau) \cdot \Delta(\sigma).$$

Jakamalla tämän yhtälön molemmat puolet luvulla Δ_n saadaan

$$\text{sign}(\sigma\tau) = \text{sign}(\tau) \cdot \text{sign}(\sigma),$$

kuten haluttiin. □

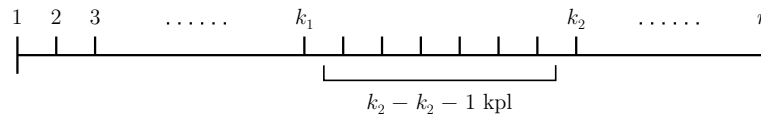
Permutaation etumerkin laskeminen määritelmän 2.11 perusteella on työlästä. Seuraavan lauseen avulla etumerkki voidaan laskea helposti sykliesityksestä lähtien.

Lause 2.13. Olkoon $\sigma \in S_n$. Jos $\text{sign}(\sigma) = 1$ eli σ on parillinen, jokainen σ :n esitys 2-syklien tulona sisältää parillisen määrän tekijöitä. Jos taas $\text{sign}(\sigma) = -1$, niin tekijöitä on pariton määrä.

Todistus. Lasketaan ensin mielivaltaisen vaihdon etumerkki käyttämällä lemmaa 2.10. Olkoon $\tau = (k_1 k_2) \in S_n$ jokin vaihto. Lisäksi voidaan olettaa, että $k_1 < k_2$. Lasketaan, kuinka monella parilla $i, j \in N_n$ pätee $i < j$ mutta $\tau(i) > \tau(j)$, eli kuinka monen parin järjestys kääntyy vaihdossa toisin päin.

Olkoon siis $i < j$. Käydään läpi eri tapaukset.

- 1) Mikäli $i \notin \{k_1, k_2\}$ ja $j \notin \{k_1, k_2\}$, niin $\tau(i) = i$ ja $\tau(j) = j$, joten $\tau(i) < \tau(j)$. Järjestys ei siis vaihdu.
- 2) Jos $i = k_2$, täytyy olla $j > k_2$. Tällöin $\tau(i) = k_1 < k_2 < j = \tau(j)$, joten järjestys ei vaihdu.
- 3) Jos $j = k_1$, täytyy olla $i < k_1$, ja tilanne on samanlainen kuin edellisessä tapauksessa. Järjestys ei vaihdu.
- 4) Jos $i = k_1$ ja $j = k_2$, niin $\tau(i) = j > i = \tau(j)$. Tästä tulee siis yksi pari, jonka järjestys kääntyy.
- 5) Jos $i = k_1$ ja $j \neq k_2$, niin $\tau(i) = k_2$ ja $\tau(j) = j$. Parin järjestys kääntyy siis täsmälleen silloin, kun $k_1 < j < k_2$. Tällaisia tapauksia on $k_2 - k_1 - 1$ kappaletta (ks. kuva 6).
- 6) Jos $j = k_2$ ja $i \neq k_1$, tilanne on samanlainen kuin edellisessä tapauksessa. Pareja, joiden järjestys vaihtuu, on $k_2 - k_1 - 1$ kappaletta.



Kuva 6: Vaihdon etumerkin laskeminen.

Yhteensä järjestyksen kääntäviä pareja on $1 + 2(k_2 - k_1 - 1) = 2(k_2 - k_1) + 1$ kappaletta. Näin ollen lemmän 2.10 mukaan

$$\Delta(\tau) = (-1)^{2(k_2 - k_1) + 1} \cdot \Delta_n = -\Delta_n,$$

joten $\text{sign}(\tau) = -1$.

Olkoon sitten $\sigma = \tau_1 \tau_2 \cdots \tau_m$, missä jokainen τ_k on vaihto. Yllä suoritetun laskun sekä lemmän 2.10 perusteella

$$\text{sign}(\sigma) = \text{sign}(\tau_1) \text{sign}(\tau_2) \cdots \text{sign}(\tau_m) = (-1)^m.$$

Siispä vaihtojen määrä m on pariton, jos ja vain jos $\text{sign}(\sigma) = -1$. □

Korollaari 2.14. Olkoon $\sigma = \tau_1 \tau_2 \cdots \tau_m \in S_n$, missä jokainen τ_k on n_k -sykli. Permutaatio σ on pariton, jos ja vain jos summa $(n_1 - 1) + (n_2 - 1) + \cdots + (n_m - 1)$ on pariton.

Todistus. Koska lauseen 2.8 perusteella jokainen n -sykli voidaan kirjoittaa $n-1$ vaihdon tulona, permutaatio σ voidaan kirjoittaa tulona, joka sisältää $(n_1 - 1) + \dots + (n_m - 1)$ vaihtoa. \square

Esimerkki 2.15. Permutaatio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 10 & 5 & 6 & 9 & 3 & 2 & 4 & 7 \end{pmatrix} \in S_{10}$$

voidaan kirjoittaa syklien tulona muodossa $\sigma = (2\ 8)(3\ 10\ 7)(4\ 5\ 6\ 9)$. Syklien pituuden ovat 2, 3 ja 4. Koska summa $(2 - 1) + (3 - 1) + (4 - 1) = 1 + 2 + 3 = 6$ on parillinen, niin $\text{sign}(\sigma) = 1$.

Lopuksi voidaan vielä mainita, että etumerkki on itse asiassa ryhmähomomorfismi.

Lause 2.16. Kuvaus $\sigma \mapsto \text{sign}(\sigma)$ on homomorfismi ryhmältä (S_n, \circ) kertolaskuryhmälle $(\{1, -1\}, \cdot)$.

Todistus. Koska jokaisella σ pätee $\text{sign}(\sigma) = 1$ tai $\text{sign}(\sigma) = -1$, niin sign on kuvaus $S_n \rightarrow \{-1, 1\}$. Toisaalta lemmän 2.12 perusteella sign on homomorfismi. \square