1 Johdanto

1.1 Yleistä

Unkarilainen kuvanveistäjä ja arkkitehtuurin professori Ernő Rubik kehitti maineikkaan kuutionsa vuonna 1974. Hän kehitti kuutionsa alun perin arkkitehtiopiskelijoiden visuaalisen hahmottamisen edistämiseen ja kutsui sitä itse nimellä "Magic Cube". Vuonna 1980, kun Ideal Toys esitteli lelun maailmalle, se nimettiin uudelleen Rubikin kuutioksi.

Rubikin kuutio saavutti lyhyessä ajassa suuren suosion, jota se ei ole vieläkään menettänyt. Siitä on tehty monia muunnelmia: erikokoisia, -värisiä ja -muotoisia. Tietokoneen avulla voidaan tarkastella myös useampiulotteisia Rubikin kuutioita.

Todelliset harrastajat käyttävät itse öljyämiään ja virittelemiään kuutioita saavuttaakseen mahdollisimman nopeita tuloksia. Maailmalla kilpaillaan paitsi perinteisessä pyörittelyssä myös sokkona, jaloilla ja yhdellä kädellä ratkaisemisessa. Tämänhetkinen virallinen nopeusennätys[1] on Edouard Chambonilla, joka vuonna 2008 ratkaisi kuution nopeimmillaan 9,18 sekunnissa ja keskimäärin 11,48 sekunnissa. Erityisen mainittavaa on, että jaloilla ratkaisemisen maailmanennätys, 39,88 sekuntia, kuuluu tällä hetkellä suomalaiselle Anssi Vanhalalle[2].

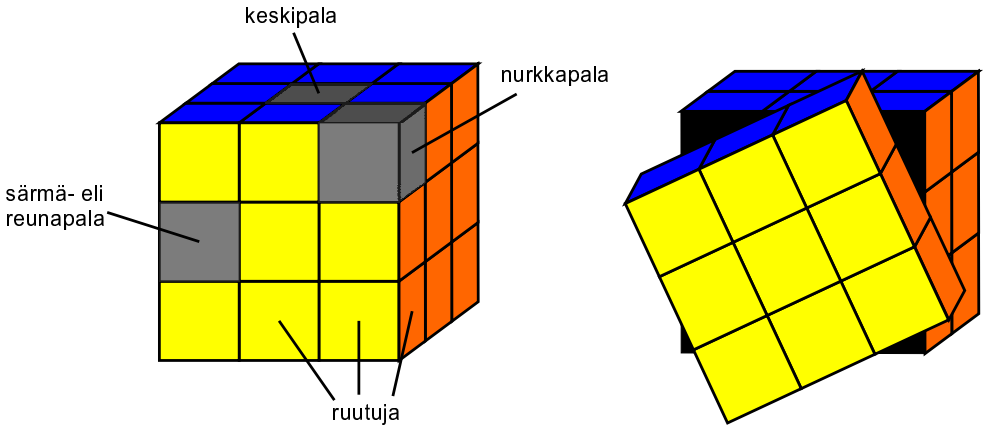
Rubikin kuution ratkaiseminen on päältä katsottuna äärimmäisen monimutkainen ongelma. Erilaisia kombinaatioita tavallisella $3 \times 3 \times 3$-kuutiolla on 43 252 003 274 489 856 000 eli noin $4{,}3 \cdot 10^{19}$ kappaletta. Kuitenkin kuution matemaattinen perusrakenne avautuu melko vähällä vaivalla. Tämän rakenteen selvittämisessä ryhmäteorian perustyökaluista on paljon apua, ja toisaalta kuutio toimii erinomaisena havaintovälineenä abstraktilta tuntuvien algebrallisten käsitteiden oppimisessa.

Ratkaisemiseen tarvittava pyöritysten määrä ei ole vielä täsmällisesti selvinnyt. Vuonna 1998 Michael Reid löysi kombinaation, jonka ratkaisemiseen vaaditaan vähintään 26 kappaletta sivutahkon pyöräytyksiä neljännesympyrän verran. (Tällaista pyöräytystä kutsutaan tässä materiaalissa *perussiirroksi* tai perussiirron käänteissiirroksi.) Toisaalta Silviu Radu osoitti vuonna 2006, että minkä tahansa aseman ratkaisemiseen tarvitaan korkeintaan 35 tällaista siirtoa. Näiden lukumäärien välissä on vielä tilaa tarkennukselle. Jos sen sijaan myös sivutahkon 180 asteen pyöräytys lasketaan siirroksi, tuoreempi tulos löytyy elokuulta 2007, jolloin Daniel Kunkle ja Gene Cooperman osoittivat supertietokoneen avulla, että kaikki kuution kombinaatiot voidaan ratkaista 26 siirrolla. Tällaisilla siirroilla laskettuna alaraja puolestaan on 20 siirtoa.[3]

[1] http://www.worldcubeassociation.org/results/events.php
[2] http://www.worldcubeassociation.org/results/events.php?eventId=333ft
[3] Tilanne 12.3.2008.

1.2 Kuution rakenne

Rubikin kuution jokainen *sivutahko* koostuu yhdekästä kuutionmuotoisesta palasta, joista 4 on *nurkkapaloja*, 2 *särmä- eli reunapaloja* ja 1 *keskipala*. Sivutahkot kääntyvät keskipisteensä ympäri, mutta muuten paloja ei voi liikuttaa toistensa suhteen. Näennäisesti myös *keskitahkoja* voi kiertää keskipisteensä ympäri, mutta tämä liike voidaan nähdä myös niin, että kaksi keskitahkon rinnalla olevaa sivutahkoa kiertyvät vastakkaiseen suuntaan (minkä jälkeen koko kuutiota käännetään vielä liikkeen suuntaan).



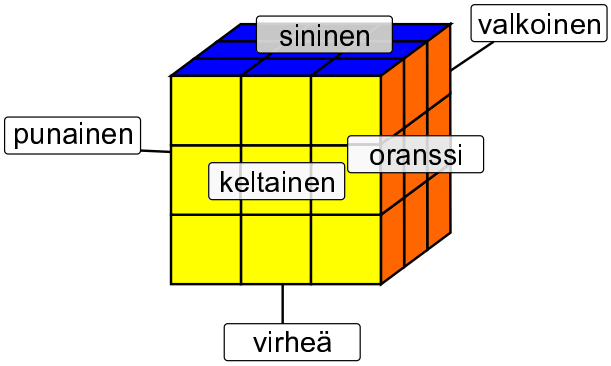
Kuva 1: Kuution rakenne ja sivutahkon pyöritys

Mitä tahansa yhdistelmää kuution sivutahkojen kääntöjä kutsutaan *siirroksi*. Kaksi siirtoa samastetaan, mikäli niillä päästään tietystä alkutilanteesta samaan lopputilanteeseen.

Kuution sivut on väritetty niin, että perusasemassa jokainen sivu on yksivärinen eikä kahdella eri sivulla esiinny samaa väriä. Jokaisella nurkkapalalla on näin ollen kolme värillistä sivua, joita kutsutaan *ruuduiksi*. Särmäpalat puolestaan sisältävät vain kaksi värillistä ruutua ja kukin keskipala yhden. Kun kuution sivutahkoja kierretään, eriväriset ruudut joutuvat eri sivuille, ja kuution värirakenne sekoittuu. Kuution ratkaisemisessa pyritään saamaan jokainen kuution sivu jälleen yhdenväriseksi.

Myynnissä olevien kuutioiden väritykset vaihtelevat. Tämän materiaalin puitteissa oletetaan, että sivujen värit ovat keltainen, sininen, punainen, oranssi, virheä ja valkoinen. Nämä värit sijaitsevat kuutiossa siten, että keltainen on vastapäätä valkoista, ja jos keltainen sivu osoittaa katsojaan päin, muut värit kiertävät sivuja myötäpäivään järjestyksessä sininen, oranssi, virheä, punainen.

On hyödyllistä huomioida heti aluksi, että kuution keskipalojen voidaan olettaa pysyvän paikallaan kuution sivuja pyöritettäessä. Nimittäin, kunkin sivutah-



Kuva 2: Kuution väritys

kon keskipala pysyy paikallaan, kun kyseistä sivua pyöritetään[4], eikä tämä pyöritys tietenkään vaikuta mitenkään muiden sivujen keskipalojen asemiin. Toisaalta keskitahkojen pyörittäminen vastaa kahden rinnakkaisen sivutahkon pyörittämistä, joten sekään ei muuta keskipalojen keskinäisiä asemia. Näin ollen kuution jokaisen sivun alkuperäinen väri voidaan tunnistaa sen keskipalasta. Tämä ei ole mahdollista esimerkiksi $4 \times 4 \times 4$-kuutiossa (nimeltään muuten "Rubikin kosto"), sillä siinä ei ole mitään keskipaloja, jotka pysyisivät paikallaan toistensa suhteen.

2 Permutaatioryhmät

Permutaatioryhmät olivat itse asiassa ensimmäinen ryhmäteorian tutkimuskohde. Tämä johtuu siitä, että permutaatioita esiintyy joka puolella sekä matematiikassa että käytännön elämässä. Toisaalta jokainen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa, joten voidaan ajatella, että permutaatioryhmien tunteminen riittää kaikkien ryhmien tuntemiseen.

2.1 Permutaation olemus

Matemaattisen määritelmän mukaan permutaatio on bijektio joukolta itselleen. Näin yksinkertaiselle käsitteelle ei kuitenkaan syyttä ole annettu noin hienoa nimeä. Latinan 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.

[4]Keskipalat tosin kiertyvät itsensä ympäri, ja jos niiden alkuperäinen suunta merkitään niihin esimerkiksi kynällä, on lisähaaste yrittää ratkaistaessa palauttaa ne alkuperäisiin asentoihinsa. Tämä tunnetaan "superkuutio"-ongelmana.

Vastaostetussa korttipakassa kortit ovat tietyssä perusjärjestyksessä. Kun korttipakan ensimmäisen kerran sekoittaa, esimerkiksi herttaässän 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 (injektiivisyys) eikä kortteja ole myöskään tullut lisää (surjektiivisuus).

Permutaatiota voidaan tarkastella monelta kannalta. Toisaalta voidaan ajatella permutaation 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 rajoittua 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 kuvausten 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.

Rajoitutaan nyt tarkastelemaan vain lukujoukkojen $N_n = \{1, 2, \ldots, n\}$ permutaatioita. Joukolla N_n on yhteensä $n!$ permutaatiota, mikä nähdään helposti tuloperiaatteen avulla: ensimmäiselle alkiolle 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 alkiot 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

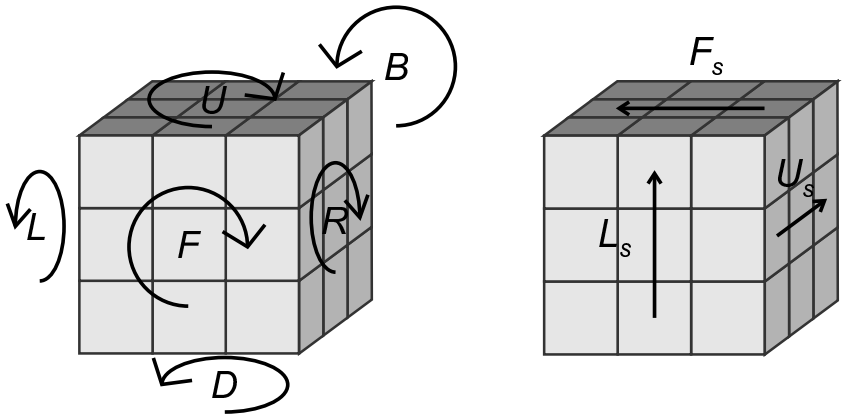
Perusasemassa olevan Rubikin kuution kukin sivu on tietyn värinen ja jaettu yhdeksään ruutuun. Kun Rubikin kuution tahkoja pyörittää, näiden ruutujen paikat sekoittuvat. Jos ajatellaan jokainen ruutu keskiruutuja lukuunottamatta numeroiduksi tietyllä järjestysluvulla, voidaan kuutiota ajatella joukkona N_{48}. Jokainen kuution siirto siis vastaa tiettyä joukon N_{48} permutaatiota eli symmetrisen ryhmän S_{48} alkiota. (Keskipalojen 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 olevaa punaisen sivun yläkulman ruutua ei voi vaihtaa sinisen sivun keskiruudun kanssa. Tällöin nimittäin kuutioon tulisi nurkkapala, 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 sivua ei voi vaihtaa keskenään ilman että muutkin ruudut vaihtuisivat. 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.

Rubikin ryhmän keskeisimmät alkiot ovat niin sanotut *perussiirrot*, jotka vastaavat kunkin tahkon neljännesympyrän suuruista pyörähdystä myötäpäivään. Näitä siirtoja merkitään kirjaimilla U, D, F, B, L ja R seuraavan kuvan mukaisesti. Kuvassa sininen sivu on ylhäällä ja keltainen sivu osoittaa katsojaan päin.



Kuva 3: Kuution perussiirrot ja keskitahkojen siirrot

Keskitahkojen pyöritys vastaa sitä, että pyöritetään molempia rinnakkaisia sivutahkoja vastakkaiseen suuntaan ja sitten käännetään koko kuutiota takaisinpäin. Tämän vuoksi keskitahkojen pyöritystä ei tarvitse ottaa erikseen huomioon. Merkintöjen helpottamiseksi voidaan näitä "valeperussiirtoja" kuitenkin merkitä kirjaimilla U_S, F_S ja L_S oheisen kuvan mukaisesti. 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.

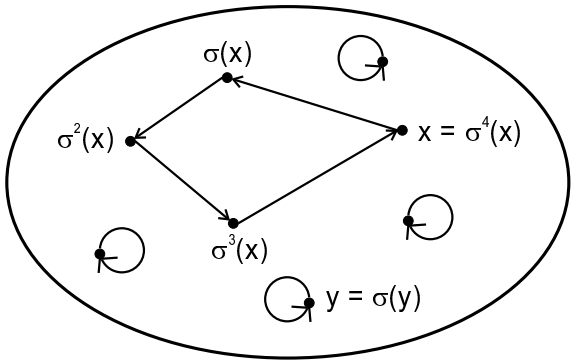
Sitä ruutujen järjestystä, johon perusjärjestyksessä oleva Rubikin kuutio joutuu tietyn laillisen permutaation jälkeen, kutsutaan *kuution tilaksi*. Jokaista tilaa vastaa siis tietty permutaatio, ja monesti tiloja nimitetäänkin myös permutaatioiksi. Jos mihin tahansa tilaan sovelletaan kyseistä tilaa 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. Tehtävän helpottamiseksi tutkitaan Rubikin ryhmän rakennetta, ja sitä varten täytyy ensin tutustua eräisiin permutaatioryhmiä koskeviin käsitteisiin.

2.4 Syklit

Määritelmä 2.5. Olkoon X jokin äärellinen joukko. Joukon X permutaatiota σ nimitetään *sykliksi*, jos löytyy sellainen $x \in X$, että kaikilla $y \in X$ pätee joko $y = \sigma^k(x)$ jollain $k \in \mathbb{N}$ tai $\sigma(y) = y$. Koska X on äärellinen, niin jollain $n > 0$ pätee $\sigma^n(x) = x$. Pienintä tällaista lukua n kutsutaan syklin *pituudeksi*. Toisaalta sykliä, jonka pituus on n, kutsutaan *n-sykliksi*.



Kuva 4: Eräs 4-sykli

Sykliä, jonka pituus on n, voidaan merkitä seuraavasti:

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

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 $3 = \sigma(2)$, $6 = \sigma^2(2)$, $4 = \sigma^3(2)$, $2 = \sigma^5(2)$ 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 alkiosta 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 $\tau = (1)(23)(456)$.

Sopimus. 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.

Huom! Jotta kuvauksen arvoa merkittäessä eivät sulut menisi sekaisin 1-syklin kanssa, merkitään toisinaan selvyyden 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, koostuuvatko se 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 $\tau = (x_1 x_2 \dots x_n)$, niin korvataan tämä vaihtojen tulolla $\tau' = (x_1 x_2)(x_2 x_3) \cdots (x_{n-1} x_n)$. Helposti nähdään, että $\tau = \tau'$. Jos nimittäin $y \neq x_k$ kaikilla k, niin $\tau(y) = y = \tau'(y)$. Toisaalta $\tau(x_k) = x_{k+1}$, mikäli $1 \leq k < n$, ja tällöin

$$\begin{aligned}\tau'(x_k) &= (x_1 x_2)(x_2 x_3) \cdots (x_{k-1} x_k)(x_k x_{k+1}) \cdots (x_{n-1} x_n)[x_k] \\ &= (x_1 x_2)(x_2 x_3) \cdots (x_{k-1} x_k)(x_k x_{k+1})[x_k] \\ &= (x_1 x_2)(x_2 x_3) \cdots (x_{k-1} x_k)[x_{k+1}] = x_{k+1}.\end{aligned}$$

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

$$\begin{aligned}\tau'(x_n) &= (x_1 x_2)(x_2 x_3) \cdots (x_{n-2} x_{n-1})(x_{n-1} x_n)[x_n] \\ &= (x_1 x_2)(x_2 x_3) \cdots (x_{n-2} x_{n-1})[x_{n-1}] \\ &\;\;\vdots \\ &= (x_1 x_2)[x_2] = x_1.\end{aligned}$$

Kun jokainen sykliesityksen sykli korvataan edellä mainitulla tavalla, saadaan permutaatio esitetyksi vaihtojen tulona. □

Olkoon $\sigma \in S_n$. Merkitään

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

Merkitään lisäksi $\Delta(\mathrm{id}) = \Delta_n$. Tämän tulon avulla voidaan määritellä ns. *permutaation etumerkki*. Osoitetaan kuitenkin sitä ennen eräs tekninen aputulos.

Lemma 2.9. *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 $\sigma = \mathrm{id}$, 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:

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

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

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

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

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

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

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

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 $\tau(j) = j'$:

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

Näin on väite todistettu. □

Määritelmä 2.10. Permutaation $\sigma \in S_n$ *etumerkki* on

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

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

Aputuloksen avulla voidaan helposti todistaa eräs tärkeä etumerkin ominaisuus.

Lemma 2.11. *Kaikilla $\sigma, \tau \in S_n$ pätee* $\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$.

Todistus. Olkoon k niiden parien $i, j \in N_n$ lukumäärä, joilla $i < j$, mutta $\tau(j) < \tau(i)$. Lemman 2.9 perusteella pätee

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

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

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

Jakamalla tämän yhtälön molemmat puolet luvulla Δ_n saadaan $\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\tau) \cdot \operatorname{sign}(\sigma)$, kuten haluttiin. □

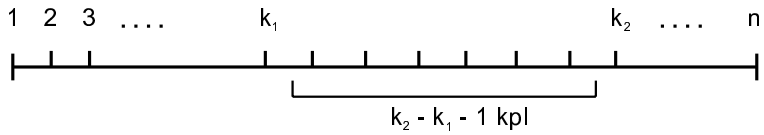
Permutaation etumerkin laskeminen määritelmän avulla on hieman työlästä. Seuraavan lauseen avulla etumerkki voidaan laskea helposti permutaation sykliesityksestä lähtien.

Lause 2.12. *Olkoon $\sigma \in S_n$. Jos* $\operatorname{sign}(\sigma) = 1$ *eli σ on parillinen, niin jokainen σ:n esitys 2-syklien tulona sisältää parillisen määrän tekijöitä. Jos taas* $\operatorname{sign}(\sigma) = -1$, *niin tekijöitä on pariton määrä.*

Todistus. Käytetään jälleen lemmaa 2.9. 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 toisinpäin.

Olkoon siis $i < j$. Aluksi huomataan, että mikäli $i \neq k_1$ ja $j \neq k_2$, niin $\tau(i) = i < j = \tau(j)$. Toisaalta, mikäli $i = k_1$ ja $j = k_2$, niin $\tau(i) = j > i = \tau(j)$. Tästä tulee siis yksi pari, jonka järjestys kääntyy. Jäljelle jäävät tapaukset, joissa $i = k_1$ ja $j \neq k_2$ tai joissa $i \neq k_1$ ja $j = k_2$.

Jos $i = k_1$ ja $j \neq k_2$, niin $\tau(i) = k_2$ ja $\tau(j) = j$. Parien järjestys kääntyy siis täsmälleen silloin, kun $j < k_2$. Tällaisia tapauksia on $k_2 - k_1 - 1$ kappaletta (ks. oheinen kuva). Samoin, jos $i \neq k_1$ ja $j = k_2$, järjestys kääntyy täsmälleen silloin, kun $\tau(i) = i > k_1 = \tau(j)$. Näitä tapauksia on myös $k_2 - k_1 - 1$ kappaletta.



Kuva 5: Vaihdon etumerkin laskeminen

Yhteensä järjestyksen kääntäviä pareja on siis $1+2(k_2-k_1-1) = 2(k_2-k_1)+1$ kappaletta. Näin ollen lemman 2.9 mukaan

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

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

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

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

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

Korollaari 2.13. *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 $(n_1-1)+(n_2-1)+\cdots+(n_m-1)$ vaihtoa. □

Esimerkki 2.14. 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 $\operatorname{sign}(\sigma) = 1$.

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

Lause 2.15. *Kuvaus $\sigma \mapsto \operatorname{sign}(\sigma)$ on homomorfismi ryhmältä $(S_n, \circ)$ ryhmälle $(\{1,-1\}, \cdot)$.*

Todistus. Koska jokaisella σ pätee $\operatorname{sign}(\sigma) = 1$ tai $\operatorname{sign}(\sigma) = -1$, niin sign on kuvaus $S_n \to \{-1, 1\}$. Toisaalta lemman 2.11 perusteella sign on homomorfismi. □