Ryhmäteoreettinen näkökulma Rubikin kuutioon

Jokke Häsä

Matematiikan ja tilastotieteen laitos, kevät 2008

Sisältö

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].

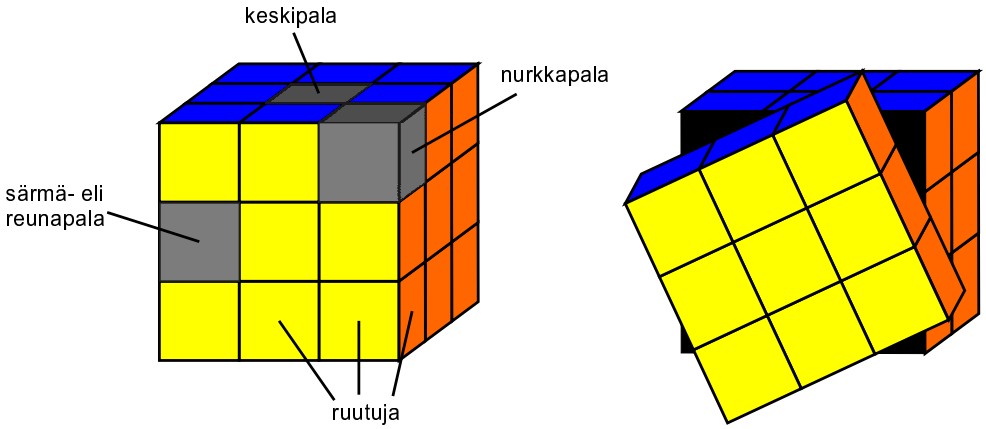
Rubikin kuution ratkaiseminen on päältä katsottuna äärimmäisen monimutkainen ongelma. Erilaisia kombinaatioita tavallisella $3 \times 3 \times 3$-kuutiolla on 43 252 003 274 489 856 000 eli noin $4{,}3 \cdot 10^{19}$ kappaletta. Kuitenkin kuution matemaattinen perusrakenne avautuu melko vähällä vaivalla. 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).



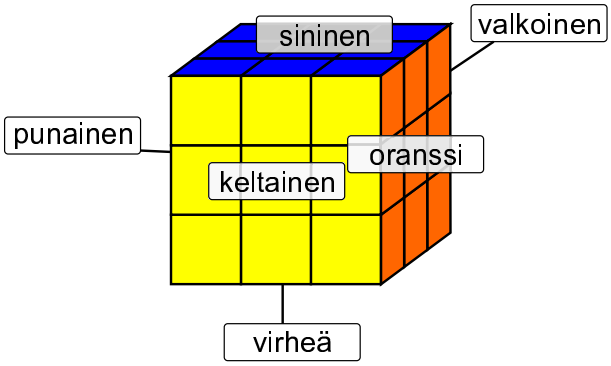
Kuva 1: Kuution rakenne ja sivutahkon pyöritys

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

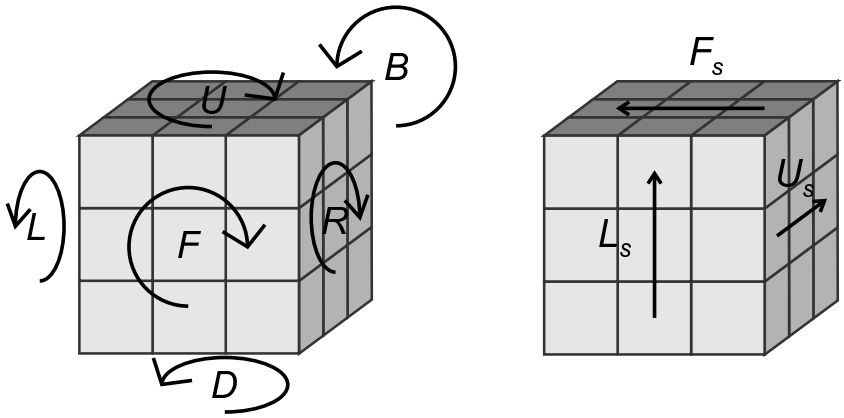
Perusasemassa olevan Rubikin kuution kukin sivu on tietyn värinen ja jaettu yhdeksään ruutuun. Kun Rubikin kuution tahkoja pyörittää, näiden ruutujen paikat sekoittuvat. Jos ajatellaan jokainen ruutu keskiruutuja lukuunottamatta numeroiduksi tietyllä järjestysluvulla, voidaan kuutiota ajatella joukkona 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.

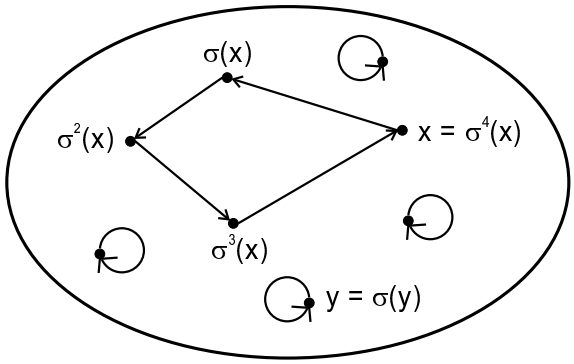
Sitä ruutujen järjestystä, johon perusjärjestyksessä oleva Rubikin kuutio joutuu tietyn laillisen permutaation jälkeen, kutsutaan *kuution tilaksi*. Jokaista tilaa vastaa siis tietty permutaatio, ja monesti tiloja nimitetäänkin myös permutaatioiksi. Jos mihin tahansa tilaan sovelletaan kyseistä tilaa 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. □

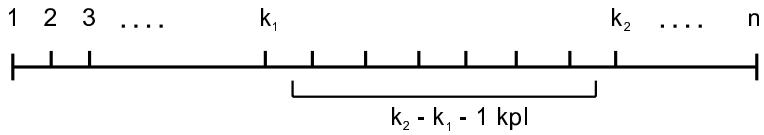
Permutaation etumerkin laskeminen määritelmän avulla on hieman työlästä. Seuraavan lauseen avulla etumerkki voidaan laskea helposti permutaation sykliesityksestä lähtien.

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. □

3 Tekijäryhmät

Tekijäryhmän käsitteen avulla voidaan monimutkainen ryhmä jakaa suuriin, helpommin käsiteltäviin osiin. Tämän jälkeen voidaan erikseen tarkastella, miten laskutoimitus vaikuttaa näihin osiin kokonaisuutena, ja jättää hetkeksi huomiotta se, mitä itse asiassa tapahtuu kunkin tällaisen osan sisällä.

3.1 Tekijäryhmän määritelmä

Tekijäryhmän määrittelemistä varten määritellään aluksi sivuluokat ja normaalit aliryhmät.

Määritelmä 3.1. Olkoon G jokin ryhmä, jolla on aliryhmä H. Kullakin alkiolla $g \in G$ määritellään H:n *vasen sivuluokka*

$$gH = \{gh \mid h \in H\}.$$

Vastaavasti voidaan määritellä *oikea sivuluokka* $Hg = \{hg \mid h \in H\}$.

Sivuluokista voidaan tehdä heti määritelmän perusteella muutamia havaintoja. Ensinnäkin $eH = H$, jos e on ryhmän G neutraalialkio. Aliryhmä on siis itse yksi sivuluokistaan. Toisaalta, koska $e \in H$, kaikilla $g \in G$ pätee $g = g \cdot e \in gH$. Jokainen ryhmän alkio siis kuuluu johonkin sivuluokkaan, eli sivuluokat *peittävät* koko ryhmän G. Nämä havainnot pätevät yhtä hyvin vasemmille kuin oikeillekin sivuluokille.

Esimerkki 3.2. Tarkastellaan ryhmää $(\mathbb{Z}, +)$ ja sen aliryhmää

$$4\mathbb{Z} = \{n \in Z \mid n \text{ on jaollinen 4:llä}\}.$$

Etsitään sivuluokat havainnoimalla. Ensinnäkin yksi sivuluokista on $0 + 4\mathbb{Z} = 4\mathbb{Z} = \{\ldots, -4, 0, 4, 8, 12, \ldots\}$. (Huomaa, että kun ryhmän laskutoimituksena on yhteenlasku, sivuluokkamerkinnässäkin on kertomerkin sijaan +-merkki.)

Muut sivuluokat saadaan lisäämällä eri lukuja aliryhmän $4\mathbb{Z}$ alkioihin:

$$\begin{aligned}
1 + 4\mathbb{Z} &= \{\ldots, -3, 1, 5, 9, 13, \ldots\} \\
2 + 4\mathbb{Z} &= \{\ldots, -2, 2, 6, 10, 14, \ldots\} \\
3 + 4\mathbb{Z} &= \{\ldots, -1, 3, 7, 11, 15, \ldots\} \\
4 + 4\mathbb{Z} &= \{\ldots, 0, 4, 8, 12, 16, \ldots\} \\
&\vdots
\end{aligned}$$

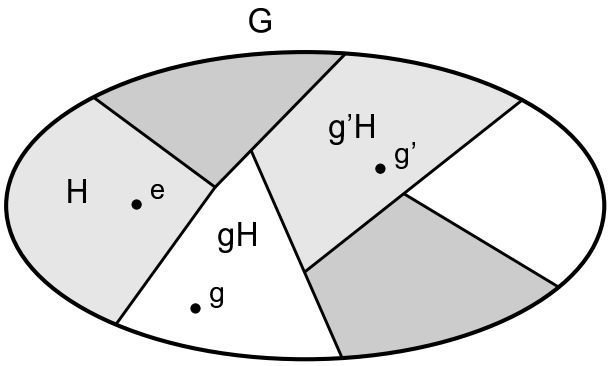
Huomataan, että $4 + 4\mathbb{Z}$ on sama joukko kuin $4\mathbb{Z}$ ja että sivuluokkia ei enää tulee lisää, vaikka kokeiltaisiin uusilla luvuilla: esimerkiksi $13 + \mathbb{Z}$ on sama joukko kuin $1 + \mathbb{Z}$. Jokainen kokonaisluku näyttää nyt kuuluvan johonkin neljästä sivuluokasta $4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$ ja $3 + 4\mathbb{Z}$, ja jokainen näistä sivuluokista sisältää eri lukuja kuin toiset.

Edellisessä esimerkissä huomattiin, että eri sivuluokat eivät sisältäneet samoja alkioita. Tämä on itse asiassa yleinen sääntö, joka voidaan osoittaa esimerkiksi seuraavasti: oletetaan, että $x \in g_1H \cap g_2H$ eli että $x = g_1h_1$ ja $x = g_2h_2$ joillain $h_1, h_2 \in H$. Tällöin $g_1 = xh_1^{-1}$, ja kaikilla $h' \in H$ pätee

$$g_1h' = xh_1^{-1}h' = g_2 \underbrace{h_2h_1^{-1}h'}_{\in H} \in g_2H,$$

joten $g_1H \subset g_2H$. Samalla tavoin nähdään myös, että $g_2H \subset g_1H$. Siispä aina pätee joko $g_1H = g_2H$ tai $g_1H \cap g_2H = \emptyset$.

Jonkin aliryhmän vasemmat tai oikeat sivuluokat muodostavat siis koko ryhmän osituksen (ks. kuva 6). Tarkoituksena olisi nyt unohtaa sivuluokkien varsinainen sisältö ja tutkia sitä, miten laskutoimitus kohtelee näitä sivuluokkina kokonaisuutena. Olisi siis tarkoitus laskea *kokonaisten sivuluokkien tuloja* $g_1H \cdot g_2H$. Tällainen tulo on joukko, joka sisältää kaikki sellaiset alkiot $g_1h_1g_2h_2$, joille pätee $h_1, h_2 \in H$. Kyseessä on sama joukko kuin $g_1 \cdot (Hg_2) \cdot H$, eli H:n *oikean* sivuluokan Hg_2 alkiot kerrottuina vasemmalta alkiolla g_1 ja oikealta kaikilla aliryhmän H alkioilla.



Kuva 6: Aliryhmän H sivuluokat

Ongelmana on nyt se, että joukko $g_1H \cdot g_2H$ ei välttämättä ole itse sivuluokka. Tällaisessa tapauksessa ei kokonaisiin sivuluokkiin rajoittumisesta olisi paljon iloa, kun sivuluokkien joukko ei olisi suljettu niiden laskutoimituksen suhteen. Ongelma kuitenkin ratkeaa, mikäli H:n vasemmat ja oikeat sivuluokat ovat samoja. Tällöin nimittäin pätee

$$g_1H \cdot g_2H = g_1 \cdot (Hg_2) \cdot H = g_1 \cdot (g_2H) \cdot H = (g_1g_2)H \cdot H = (g_1g_2)H,$$

ja näin ollen osien g_1H ja g_2H tuloksi tulee yksinkertaisesti osa $(g_1g_2)H$.

Määritelmä 3.3. Ryhmän G aliryhmää H kutsutaan *normaaliksi aliryhmäksi*, mikäli H:n vasemman- ja oikeanpuoleiset sivuluokat ovat samat eli kaikilla $g \in G$ pätee $gH = Hg$. Jos H on G:n normaali aliryhmä, merkitään $H \trianglelefteq G$.

Huom. Jos ryhmä on vaihdannainen, sen jokainen aliryhmä on normaali, sillä on aivan sama, kertooko g aliryhmän alkioita vasemmalta vai oikealta puolelta.

Seuraava lause antaa helposti tarkistettavan kriteerin sille, onko jokin aliryhmä normaali vai ei.

Lause 3.4. *Olkoon G ryhmä ja H sen aliryhmä. Aliryhmä H on normaali täsmälleen silloin, kun kaikilla $g \in G$ pätee $gHg^{-1} \subset H$ eli*

$$ghg^{-1} \in H \quad \textit{jokaisella } h \in H.$$

Todistus. Ryhmä on normaali, jos kaikilla $g \in G$ pätee $gH = Hg$. Kun yhtälön molemmilla puolilla olevien joukkojen alkiot kerrotaan oikealta g:n käänteisalkiolla, saadaan joukkoyhtälö $H = gHg^{-1}$. Tämä yhtälö pätee siis kaikilla $g \in G$ täsmälleen silloin, kun H on normaali. Tästä nähdään heti, että jos H on normaali, niin myös $gHg^{-1} \subset H$ pätee kaikilla $g \in G$.

Oletetaan sitten, että $g^{-1}Hg \subset H$ pätee kaikilla $g \in G$. Olkoot $h \in H$ ja $g \in G$. Nyt myös $g^{-1} \in G$, joten oletuksen mukaan $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$. Edelleen

$$h = g\underbrace{g^{-1}hg}_{\in H}g^{-1} \in gHg^{-1},$$

mistä seuraa, että $H \subset gHg^{-1}$. Näin ollen $H = gHg^{-1}$ kaikilla $g \in G$, ja H on normaali. □

Esimerkki 3.5. Ryhmä S_3 koostuu kuudesta alkiosta: (12), (23), (13), (123), (132) ja id. Tarkistetaan, onko aliryhmä $H = \langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$ normaali. Lasketaan sitä varten muotoa ghg^{-1} olevat tulot, missä $h \in H$. Niissä tapauksissa, joissa $g \in H$ tai $h = \mathrm{id}$, tulo kuuluu selvästi aliryhmään H. Toisaalta silloin, kun $g \notin H$, alkio g on vaihto, joten $g^{-1} = g$. Laskettavat tulot ovat siis itse asiassa muotoa ghg. Saadaan

$$\begin{aligned} (12)(123)(12) &= (132), & (12)(132)(12) &= (123) \\ (23)(123)(23) &= (132), & (23)(132)(23) &= (123) \\ (13)(123)(13) &= (132), & (13)(132)(13) &= (123). \end{aligned}$$

Koska jokainen tulo ghg^{-1} kuuluu aliryhmään H, kyseinen aliryhmä on normaali.

Olkoon nyt $H' = \langle(12)\rangle = \{\mathrm{id}, (12)\}$. Tämä aliryhmä ei ole normaali, sillä esimerkiksi

$$(123)(12)(123)^{-1} = (123)(12)(321) = (23) \notin H'.$$

Määritelmä 3.6. Olkoon $H \trianglelefteq G$. Ryhmää, jonka alkioita ovat sivuluokat gH, missä $g \in G$, kutsutaan *tekijäryhmäksi*. Tekijäryhmää merkitään G/H, ja sen laskutoimitus noudattaa sääntöä $g_1H \cdot g_2H = (g_1g_2)H$. Tekijäryhmän alkioita voidaan merkitä myös $gH = [g]$, jolloin laskusäännöksi tulee $[g_1][g_2] = [g_1g_2]$.

Esimerkki 3.7. Koska ryhmä $(\mathbb{Z}, +)$ on vaihdannainen, sen kaikki aliryhmät ovat normaaleja. Tutkitaan tekijäryhmää $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$. Tämän tekijäryhmän alkiot ovat aiemmassa esimerkissä määritetyt neljä sivuluokkaa $\mathbb{Z} = [0]$, $1 + \mathbb{Z} = [1]$, $2 + \mathbb{Z} = [2]$ ja $3 + \mathbb{Z} = [3]$. Kyseessä on siis äärellinen 4 alkion ryhmä. Tekijäryhmän laskutoimituksen määritelmän mukaan esimerkiksi $[1] + [2] = [1 + 2] = [3]$ ja $[3] + [4] = [7] = [3]$, missä viimeinen yhtäsuuruus tulee siitä, että sivuluokat $7 + \mathbb{Z}$ ja $3 + \mathbb{Z}$ ovat sama joukko. Laskemalla kaikki mahdolliset summat voidaan muodostaa tekijäryhmän *laskutoimitustaulu*:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

.

3.2 Rubikin ryhmä jako paikkojen ja asentojen mukaan

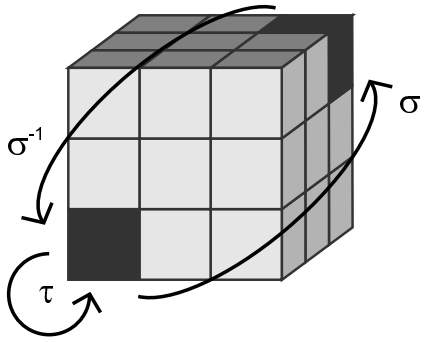
Tarkastellaan sellaista Rubikin ryhmän osajoukkoa $\mathbb{R}_a$, jonka permutaatiot pitävät kuution jokaisen palan paikallaan, vaikka voivatkin muuttaa niiden asentoa.

Lause 3.8. *Osajoukko $\mathbb{R}_a$ on Rubikin ryhmän normaali aliryhmä.*

Todistus. Helposti nähdään, että $\mathbb{R}_a$ on Rubikin ryhmän aliryhmä. Jos nimittäin permutaatiot σ ja τ pitävät kaikki kuution palat paikoillaan, myös niiden yhdistelmä $\sigma\tau$ pitää palat paikoillaan. Toisaalta identtinen permutaatio pitää palat paikoillaan, ja jos σ ei liikuta paloja, ei myöskään käänteiskuvaus σ^{-1} liikuta niitä.

Osoitetaan sitten, että aliryhmä $\mathbb{R}_a$ on normaali käyttämällä aiemmin todistettua kriteeriä 3.4. Olkoot $\tau \in \mathbb{R}_a$ ja $\sigma \in \mathbb{R}$. Tarkastellaan yhdistelmää $\sigma\tau\sigma^{-1}$ siltä kannalta, liikuttaako se paloja vai ei.

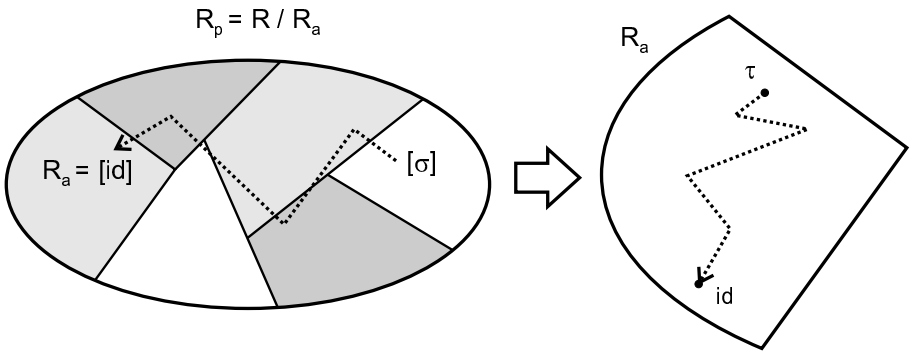
Jos σ siirtää jonkin palan paikasta A paikkaan B, niin σ^{-1} siirtää kyseisen palan takaisin paikasta B paikkaan A. Koska τ puolestaan pitää tuon palan paikallaan kohdassa A, ei yhdistelmä liikuta lainkaan kyseistä palaa (ks. oheinen kuva). Sama päättely voidaan tehdä jokaisen palan kohdalla, joten yhdistelmä ei liikuta paloja. Näin ollen $\sigma\tau\sigma^{-1} \in \mathbb{R}_a$, ja $\mathbb{R}_a$ on normaali. □



Kuva 7: Yhdistelmä $\sigma\tau\sigma^{-1}$ ei siirrä paloja

Kutsutaan aliryhmää $\mathbb{R}_a$ *Rubikin asentoryhmäksi*. Koska asentoryhmä on normaali, voidaan määritellä tekijäryhmä $\mathbb{R}_p = \mathbb{R}/\mathbb{R}_a$. Tätä tekijäryhmää kutsutaan puolestaan *Rubikin paikkaryhmäksi*. Tekijäryhmän alkiot ovat sivuluokkia $[\sigma]$. Aina kun $[\sigma_1] = [\sigma_2]$, täytyy päteä $\sigma_1 = \sigma_2 \circ \tau$ jollain $\tau \in \mathbb{R}_a$. Tämä tarkoittaa sitä, että saman sivuluokan alkiot eroavat toisistaan vain jonkin sellaisen siirron verran, joka ei muuta palojen paikkoja. Tekijäryhmä voidaan nähdä permutaatioryhmänä, jonka alkiot permutoivat kuution *paloja* niiden asennoista välittämättä.

Yllä kuvatun jaon merkitys on siinä, että sen avulla voidaan hetkeksi unohtaa, missä asennoissa kuution palat ovat, ja keskittyä palojen liikuttamiseen. Kuution ratkaisemiseksi olisi annetusta asemasta σ lähtien löydettävä perussiirtojen ketju, joka palauttaisi kuution perusasemaan id. Edetään ratkaisussa nyt niin, että yritetään ensin palauttaa *paikkaryhmässä* asema $[\sigma]$ asemaksi [id]. Koska $[\mathrm{id}] = \mathbb{R}_a$, niin tässä asemassa kaikki palat ovat jo oikeilla paikoillaan, mutta ne voivat olla vielä väärissä asennoissa. Tämän jälkeen katsotaan tarkemmin, mihin asemaan τ aliryhmässä $\mathbb{R}_a$ ollaan päädytty, ja yritetään palauttaa tämä asema vielä perusasemaksi id. Nämä vaiheet näkyvät kuvassa 8.



Kuva 8: Ratkaisun vaiheet

3.3 Algoritmi 1: nurkkapalojen 3-sykli

Kuten yllä todettiin, paikkaryhmää $\mathbb{R}_p$ voidaan ajatella kuution palojen permutaatioryhmänä. Kukin sivuluokka $[\sigma]$ vastaa sitä palojen permutaatiota, jonka σ aiheuttaa. Jos kaksi permutaatiota siirtävät paloja samalla tavalla, ne kuuluvat samaan sivuluokkaan.

Seuraavaksi kuvattava algoritmi tuottaa 3-syklin palojen paikkoja permutoivassa ryhmässä $\mathbb{R}_p$. Jos kuutio asetetaan siten, että keltainen sivu on katsojaan päin ja sininen sivu ylöspäin, ja keltaisen sivun palat numeroidaan vasemmalta oikealle ja ylhäältä alas keskipalaa lukuunottamatta numeroilla $\{1, \ldots, 8\}$, niin saatava 3-sykli on (316). Se koostuu kahdenlaisista siirroista: ensimmäinen on perussiirto $\sigma = U$ ja toinen kolmen perussiirron yhdistelmä $\tau = RD^{-1}R^{-1}$. Näistä kootaan lopuksi yhdistelmä $\sigma\tau\sigma^{-1}\tau^{-1}$. Kokonaisuudessa siirtosarja on siis seuraavanlainen:

$$(316) = URD^{-1}R^{-1}U^{-1}RDR^{-1}.$$

Tämä siirtosarja, kuten kaikki permutaatioiden yhdistelmät, suoritetaan oikealta vasemmalle.

Kuvassa 9 esitetään koko siirtosarja vaihe kerrallaan. Huomaa erityisesti, miten yhdistelmät $\sigma\tau$ ja $\sigma^{-1}\tau^{-1}$ käsittelevät 3-sykliin kuulumattomia paloja. Nämä palat siirtyvät ensin permutaatiossa $\sigma^{-1}\tau^{-1}$ jonnekin, mistä ne sitten palaavat takaisin permutaatiossa $\sigma\tau$. Näiden palojen osalta siis näyttäisi siltä, että kyseiset permutaatiot olisivat toistensa käänteissiirtoja, vaikka tosiasiassa $\sigma^{-1}\tau^{-1} = (\tau\sigma)^{-1} \neq (\sigma\tau)^{-1}$. Permutaatioiden $\tau\sigma$ ja $\sigma\tau$ (tai niiden käänteisalkioiden) ero tulee näkyviin vain 3-sykliin osallistuvissa paloissa. Tästä puhutaan lisää myöhemmin.

Huomaa myös, että permutaatio τ eroaa permutaatiosta τ^{-1} vain siinä, että jälkimmäisessä on perussiirto D, edellisessä D^{-1}. Samaten koko 3-syklin käänteisalkio on

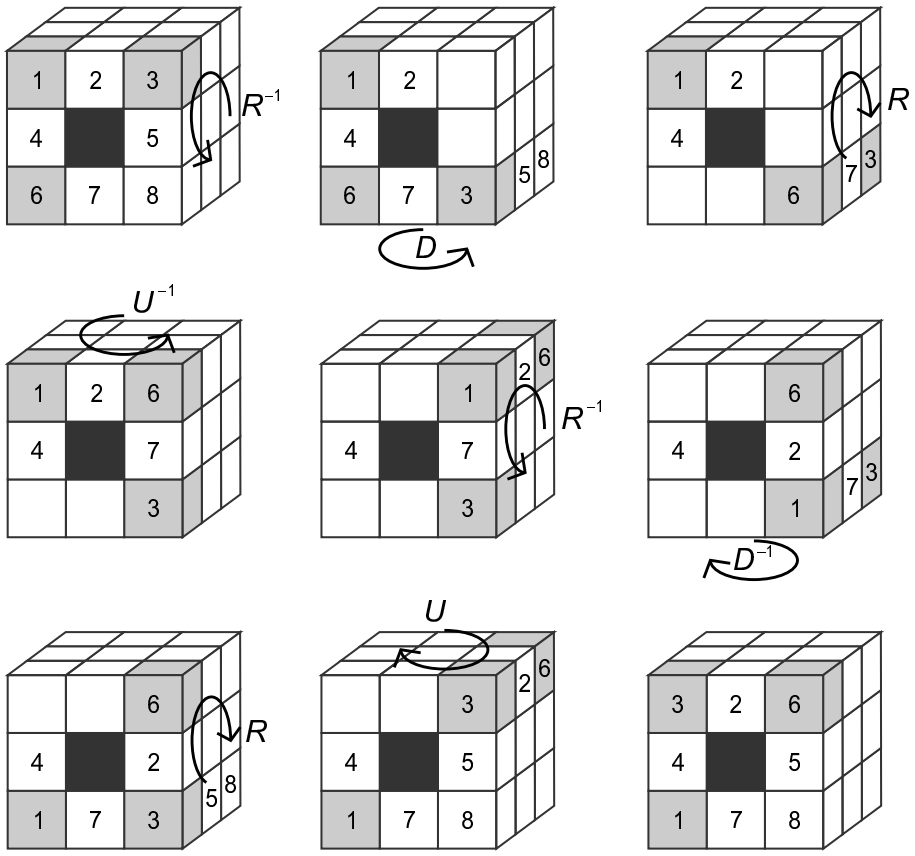
$$(\sigma\tau\sigma^{-1}\tau^{-1})^{-1} = (\tau^{-1})^{-1}(\sigma^{-1})^{-1}\tau^{-1}\sigma^{-1} = \tau\sigma\tau^{-1}\sigma^{-1}.$$

Käänteisalkiossa tehdään siis edelleen ensin käänteispermutaatiot; eroa alkuperäiseen 3-sykliin on siis vain siinä, että σ-permutaatiot tehdään ennen τ-permutaatioita.

3.4 Alternoivat ryhmät

On helppo todeta, että parilliset permutaatiot muodostavat symmetrisen ryhmän S_n aliryhmän. Tätä aliryhmää nimitetään *alternoivaksi ryhmäksi* ja merkitään

$$A_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\}.$$



Kuva 9: Nurkkapalojen 3-sykli

Tässä luvussa osoitetaan, että alternoiva ryhmä on normaali ja että se jakaa symmetrisen ryhmän kahteen yhtä suureen sivuluokkaan, joista toinen siis sisältää kaikki parittomat permutaatiot.

Lause 3.9. *Alternoiva ryhmä A_n on normaali ryhmässä S_n.*

Todistus. Käytetään lauseen 3.4 normaalisuuskriteeriä. Olkoot $\tau \in A_n$ ja $\sigma \in S_n$ mielivaltaisia. Tarkastellaan yhdistelmän $\sigma\tau\sigma^{-1}$ etumerkkiä. Ensinnäkin havaitaan, että

$$\operatorname{sign}(\sigma) \cdot \operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma \circ \sigma^{-1}) = \operatorname{sign}(\mathrm{id}) = 1,$$

joten $\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)$. Näin ollen

$$\operatorname{sign}(\sigma\tau\sigma^{-1}) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)^2 \operatorname{sign}(\tau) = 1 \cdot 1 = 1.$$

Nähdään, että $\sigma\tau\sigma^{-1} \in A_n$, jolloin voidaan päätellä, että $\sigma A_n \sigma^{-1} \subset A_n$. Aliryhmä A_n on siis normaali. □

Seuraavaksi ryhdytään tutkimaan, kuinka monesta alkiosta alternoiva ryhmä koostuu. Apuna käytetään algebran kurssilta tuttua *Lagrangen lausetta*, joka muistin virkistämiseksi mainitaan tässä ilman todistusta.

Lause 3.10 (Lagrange). *Olkoon G äärellinen ryhmä, ja $H \leq G$. Tällöin aliryhmän alkioiden lukumäärä $|H|$ jakaa koko ryhmän alkioiden lukumäärän $|G|$. Lisäksi aliryhmän H vasemman- ja oikeanpuoleisia sivuluokkia on yhtä paljon, ja niiden lukumäärä on $|G|/|H|$.*

Lagrangen lause sanoo siis, että sivuluokat jakavat ryhmän *tasan* yhtä suuriin osiin. Sivuluokkien lukumäärään nimitetään aliryhmän *indeksiksi* ja merkitään $[G : H]$.

Jotta voitaisiin päätellä alternoivan ryhmän koko, tarvitsee siis vain selvittää, kuinka monta sivuluokkaa sillä on. Koska parilliset permutaatiot sisältyvät kaikki yhteen sivuluokkaan, muissa sivuluokissa voi olla vain parittomia permutaatioita. Osoittautuu, että myös parittomat permutaatiot muodostavat yhden ainoan sivuluokan, jolloin Lagrangen lauseesta seuraa, että kumpikin sivuluokka sisältää täsmälleen puolet ryhmän alkioista.

Lause 3.11. *Alternoivalla ryhmällä A_n on täsmälleen kaksi sivuluokkaa, jos $n \geq 2$. Toisin sanoen alternoivan ryhmän indeksi $[S_n : A_n]$ on 2, jos $n \geq 2$.*

Huom. Todistus seuraisi suoraan nk. *homomorfialauseesta*, koska kuvaus $\operatorname{sign} : S_n \to \{-1, 1\}$ on homomorfismi, jonka ydin on A_n ja joka on surjektiivinen, jos $n \geq 2$. Homomorfialauseen mukaan nimittäin tekijäryhmä S_n/A_n on tällöin isomorfinen kahden alkion ryhmän $\{-1, 1\}$ kanssa. Seuraavassa annetaan kuitenkin suora todistus, joka ei käytä homomorfialausetta.

Todistus. Ensimmäiseksi havaitaan, että jos $n \geq 2$, niin ryhmä S_n sisältää vaihdon (12). Vaihto on pariton, joten $(12) \notin A_n$, ja näin ollen sivuluokkia on vähintään kaksi.

Olkoon sitten edelleen $n \geq 2$ ja olkoon σ jokin pariton permutaatio. Osoitetaan, että $\sigma \in (12) \circ A_n$. Ensinnäkin

$$\operatorname{sign}((12)^{-1}\sigma) = \operatorname{sign}((12)) \cdot \operatorname{sign}(\sigma) = -1 \cdot (-1) = 1,$$

joten $(12)^{-1}\sigma \in A_n$. Täten

$$\sigma = (12) \circ \underbrace{(12)^{-1}\sigma}_{\in A_n} \in (12) \circ A_n.$$

Koska σ oli mielivaltainen pariton permutaatio, nähdään, että jokainen pariton permutaatio kuuluu samaan sivuluokkaan. Siispä sivuluokkia on tasan kaksi. □

Symmetrinen ryhmä jakautuu siis tasan kahteen sivuluokkaan, joista toinen sisältää kaikki parilliset permutaatiot ja toinen kaikki parittomat. Sivuluokasta toiseen voidaan siirtyä kertomalla annettu permutaatio millä tahansa parittomalla permutaatiolla.

Pienimpiä parillisia permutaatioita ovat 3-syklit. Todistetaan vielä luvun lopuksi, että 3-syklien avulla voidaan muodostaa kaikki muutkin parilliset permutaatiot.

Lause 3.12. *Syklit, joiden pituus on 3, virittävät alternoivan ryhmän.*

Todistus. Tarkastellaan mielivaltaista identtisestä kuvauksesta poikkeavaa permutaatiota $\sigma \in A_n$. Koska σ on parillinen, se voidaan kirjoittaa tulona

$$\pi_1\rho_1 \circ \pi_2\rho_2 \circ \cdots \circ \pi_m\rho_m,$$

missä jokainen π_k ja jokainen ρ_k on vaihto. Osoitetaan, että jokainen yhdistelmä $\pi_k\rho_k$ voidaan korvata joko 3-syklien tulolla tai neutraalialkiolla. Kun muistetaan, että $(ab) = (ba)$ kaikilla $a, b \in N_n$, saadaan kolme tapausta:

1) jos $\pi_k\rho_k$ on muotoa $(ab)(ab)$, niin $\pi_k\rho_k = \mathrm{id}$

2) jos $\pi_k\rho_k$ on muotoa $(ab)(bc)$, niin $\pi_k\rho_k = (abc)$

3) jos $\pi_k\rho_k$ on muotoa $(ab)(cd)$, niin $\pi_k\rho_k = (abc)(bcd)$.

Näin ollen σ voidaan kirjoittaa 3-syklien tulona. □

4 Konjugointi

4.1 Konjugoinnin määritelmä

Usein ryhmän alkiot kuvaavat operaatioita jossain joukossa. Permutaatiot ovat tästä hyvä esimerkki. Tällaisessa tapauksessa voidaan konjugoinnilla siirtää jossain joukon osassa toimiva operaatio toiseen osaan. Tästä on hyötyä varsinkin, jos edellä mainittu operaatio on erityisen helppo hahmottaa ja sitä halutaan käyttää uudelleen jossain toisessa kohdassa.

Määritelmä 4.1. Olkoon G ryhmä ja olkoon $g \in G$. Ryhmän G sisäistä kuvausta

$$x \mapsto gxg^{-1}$$

nimitetään *konjugoinniksi* ja tulosalkiota gxg^{-1} alkion x *konjugaatiksi*. Konjugaattia merkitään myös $gxg^{-1} = {}^g x$. Jos X on ryhmän G osajoukko, niin joukko

$$^g X = gXg^{-1} = \{gxg^{-1} \mid x \in X\}$$

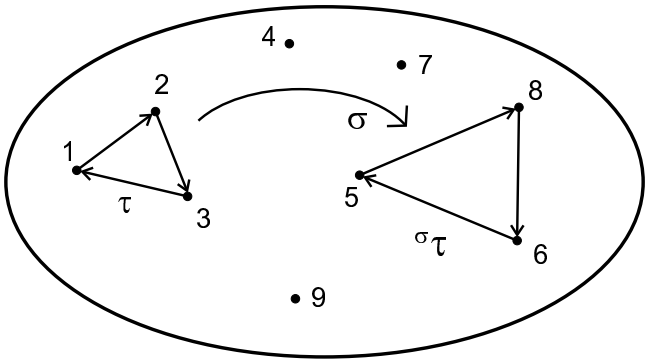
on *joukon X konjugaattijoukko*.

Konjugointi on kääntyvä operaatio: kun konjugoitu alkio ${}^g x$ konjugoidaan uudestaan alkiolla g^{-1}, saadaan alkuperäinen alkio x. Jos ryhmä on vaihdannainen, niin kullakin alkiolla on ainoana konjugaattinaan vain alkio itse, sillä $gxg^{-1} = gg^{-1}x = x$. Toisaalta ei-vaihdannaisissa ryhmissä konjugointi on hyvin yleinen työkalu. Esimerkiksi lauseen 3.4 normaalisuuskriteeri voidaan lausua muodossa: H on normaali jos ja vain jos se sisältää kaikkien alkioidensa konjugaatit.

Esimerkki 4.2. Olkoon $\tau = (123) \in S_9$ ja olkoon $\sigma = (167)(259)(38)$. Nyt $\sigma^{-1} = (83)(952)(761)$, ja

$$^\sigma\tau = \underbrace{(167)(259)(89)}_{\sigma}(123)\underbrace{(83)(952)(761)}_{\sigma^{-1}} = (586).$$

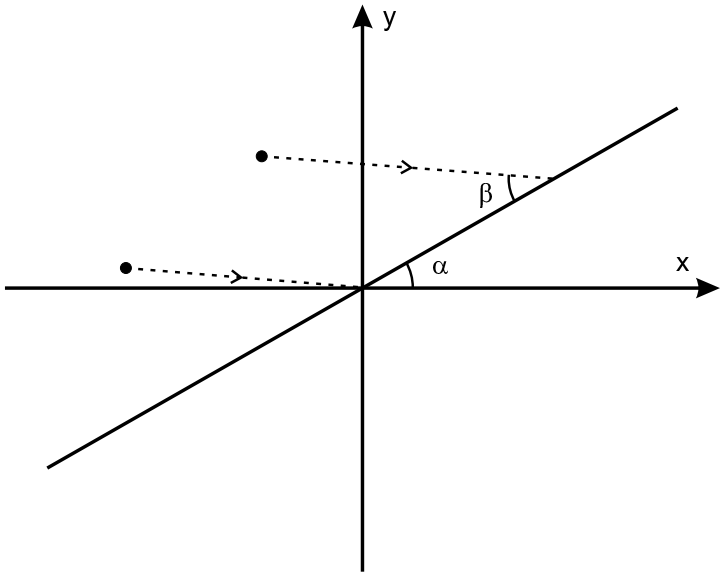
Esimerkin 3-sykli saatiin siis konjugoimalla siirretyksi toimimaan lukujen 1, 2 ja 3 sijasta luvuilla 5, 8 ja 6.



Kuva 10: Syklin siirto konjugoimalla

Vaikka konjugointi on tässä määritelty vain ryhmän sisäiseksi operaatioksi, kyse on oikeastaan yleisemmästä periaatteesta. Jos esimerkiksi f on topologisten avaruuksien X ja Y välinen homomorfismi ja g_Y on jatkuva kuvaus joukolta Y itselleen, voidaan konjugoimalla muodostaa jatkuva kuvaus $g_X = f \circ g_Y \circ f^{-1}$ joukolta X itselleen. Konjugointia vastaava operaatio on tuttu myös lineaarialgebrasta, kuten seuraava esimerkki osoittaa.

Esimerkki 4.3. Olkoon annettu tasossa origon kautta kulkeva nouseva suora, jonka x-akselin kanssa muodostama kulma on α astetta. Tarkastellaan lineaarikuvausta L, joka projisoi minkä tahansa tason pisteen kulmassa β annetulle suoralle (ks. kuva 11).



Kuva 11: Projisointikuvaus

Mainitun lineaarikuvauksen matriisia ei ole ihan helppo muodostaa, vaikka kuvaus on geometrisesti yksinkertainen. Tiedetään kuitenkin, että kuvauksella on kaksi ominaisarvoa: suoran suunnassa olevilla vektoreilla x pätee $Lx = x$ ja projektiosuunnassa olevilla vektoreilla puolestaan $Lx = 0$. Ominaisarvot ovat siis 1 ja 0. Lineaarikuvauksen matriisi voidaan näin ollen diagonalisoida niin, että se on muotoa $D = P^{-1}LP$, missä P on *kannanvaihtomatriisi*, joka vaihtaa kantavektoreiksi suoran ja projisoinnin suuntaiset vektorit. Tässä uudessa kannassa ilmoitettuna kuvaus ainoastaan projisoi kohtisuoraan jälkimmäisen koordinaatin suhteen, joten sen matriisiksi tulee diagonaalimatriisi

$$D = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Kannanvaihtomatriisi P puolestaan on helppo muodostaa, koska se vain kiertää kantavektoreita $(1, 0)$ ja $(0, 1)$ niin, että ne tulevat suoran ja projisoinnin suuntaisiksi. Tällöin $P(1, 0) = (\cos\alpha, \sin\alpha)$ ja $P(0, 1) = (-\cos(\beta - \alpha), \sin(\beta - \alpha))$, joten kannanvaihtomatriisiksi tulee

$$P = \begin{bmatrix} \cos\alpha & -\cos(\beta - \alpha) \\ \sin\alpha & \sin(\beta - \alpha) \end{bmatrix}.$$

Nyt siis alkuperäinen lineaarikuvaus on saadun diagonaalimatriisin konjugaatti: $L = PDP^{-1}$, ja sen matriisi voitaisiin tästä yhtälöstä myös helposti laskea.

Edellisestä esimerkistä näkyy hyvin konjugoinnin yleinen periaate. Tarkasteltava lineaarikuvaus on vaikeasti hahmotettava luonnollisessa kannassa, ja sen matriisi on monimutkainen. Kannanvaihdolla voidaan siirtää lineaarikuvauksen kuvailema operaatio helpompaan koordinaatistoon, jolloin matriisistakin tulee selkeä. Operaation suorittamisen jälkeen voidaan sitten palata taas alkuperäiseen kantaan.

Esimerkki 4.4. Määritellään jokaisella $n \in \mathbb{Z}$ kokonaislukuja permutoiva kuvaus σ_n seuraavasti: jos $n \in Z$, niin $\sigma_n(x) = n + x$ kaikilla $x \in \mathbb{Z}$. Nämä kuvaukset muodostavat ryhmän $T = \{\sigma_n \mid n \in \mathbb{Z}\}$, jossa $\mathrm{id} = \sigma_0$, $\sigma_m \circ \sigma_n = \sigma_{m+n}$ ja $\sigma_n^{-1} = \sigma_{-n}$. Ryhmä T on vaihdannainen, sillä

$$\sigma_m \circ \sigma_n = \sigma_{m+n} = \sigma_{n+m} = \sigma_n \circ \sigma_m.$$

Näin ollen konjugointi ryhmässä T ei muuta alkioita lainkaan. Asia voidaan kuitenkin nähdä myös toisella tavalla.

Mikäli ryhmän alkiot nimittäin toimivat jossain joukossa, niiden konjugoiminen siirtää kyseisen toiminnan johonkin toisaalle samassa joukossa. Jos nyt pätee ${}^{\sigma}\tau = \tau$, tämä tarkoittaa sitä, että alkio τ toimi *jo alun perinkin* siellä, mihin σ sen toiminnan siirtää. Vaihdannaisen ryhmän jokaisen alkion toiminta ulottuu siis joka puolelle joukkoa, eikä konjugointia siksi tarvita mihinkään. Tämä nähdään hyvin esimerkin ryhmässä T, sillä jokainen T:n alkio siirtää kaikkia kokonaislukuja samalla tavalla, ja siksi alkion konjugoiminen on tarpeetonta.

Koska konjugointi on saman operaation siirtämistä paikasta toiseen, voi olla toisinaan hyödyllistä tarkastella, mitkä operaatiot voidaan tässä mielessä samankaltaisia.

Määritelmä 4.5. Olkoon G ryhmä ja olkoon $x \in G$. Alkion x *konjugaattiluokka* on niiden alkioiden joukko, jotka saadaan konjugoimalla alkiota x. Kyseinen joukko on siis $\{gxg^{-1} \mid g \in G\}$.

Koska konjugointi on kääntyvä operaatio, x kuuluu y:n konjugaattiluokkaan jos ja vain jos y kuuluu x:n konjugaattiluokkaan. Toisaalta x kuuluu omaan konjugaattiluokkaansa, sillä ${}^{\mathrm{id}}x = x$. Voidaan myös helposti osoittaa, että eri konjugaattiluokat ovat aina erillisiä. Konjugaattiluokat muodostavat siis koko ryhmän osituksen samalla tavoin kuin aliryhmien sivuluokat. Konjugaattiluokat voivat kuitenkin olla keskenään hyvinkin eri kokoisia.

4.2 Konjugointi permutaatioryhmissä

Permutaatioiden konjugoiminen on helppoa ja symmetrisessä ryhmässä konjugaattiluokille saadaan yksinkertainen sääntö.

Lause 4.6. *Olkoot $\sigma, \tau \in S_n$. Oletetaan, että τ:n esitys erillisten syklien tulona on*

$$\tau = (x_{1,1} \dots x_{1,k_1}) \cdots (x_{m,1} \dots x_{m,k_m}).$$

Merkitään $\sigma(x_{i,j}) = x'_{i,j}$ kaikilla i ja j. Tällöin τ:n konjugaatille pätee

$${}^{\sigma}\tau = (x'_{1,1} \dots x'_{1,k_1}) \cdots (x'_{m,1} \dots x'_{m,k_m}).$$

Todistus. Merkitään väitteessä esiintyvää tuloa

$$\tau' = (x'_{1,1} \dots x'_{1,k_1}) \cdots (x'_{m,1} \dots x'_{m,k_m})$$

ja osoitetaan, että $\sigma\tau\sigma^{-1} = \tau'$. Olkoon sitä varten $y \in N_n$ mielivaltainen. Koska σ on bijektio, löydetään jokin $x \in N_n$, jolle $y = \sigma(x)$. Jos x ei esiinny τ:n sykliesityksessä, ei myöskään y esiinny τ':n sykliesityksessä. Tässä tapauksessa $\tau'(y) = y$, ja $\sigma\tau\sigma^{-1}(y) = \sigma\tau(x) = \sigma(x) = y$.

Oletetaan sitten, että x esiintyy τ:n sykliesityksessä eli että $x = x_{r,s}$ joillain r ja s. Tällöin pätee

$$\tau\sigma^{-1}(y) = \tau(x) = (x_{r,1} \dots x_{r,s} \dots x_{r,k_r})[x_{r,s}] = x_{r,s+1}.$$

(Huomaa, että sykliesitys voidaan valita siten, että $s \neq k_r$, kun 1-syklit jätetään merkitsemättä.) Lisäksi nähdään, että $y = x'_{r,s}$, joten

$$\tau'(y) = (x'_{r,1} \dots x'_{r,s} \dots x'_{r,k_r})[x'_{r,s}] = [x'_{r,s+1}] = \sigma(x_{r,s+1}).$$

Saatiin, että mielivaltaisella alkiolla $y \in N_n$ pätee $\tau'(y) = \sigma(x_{r,s+1}) = \sigma\tau\sigma^{-1}(y)$. Siispä väite on todistettu. □

Jonoa $(n_1, n_2, \dots, n_m)$, missä jokainen n_m on permutaation σ sykliesityksessä esiintyvien erillisten m-syklien määrä, nimitetään permutaation *syklityypiksi*. Edellä olevasta lauseesta saadaan suoraan seuraava seuraus.

Korollaari 4.7. *Permutaatiot voivat kuulua samaan konjugaattiluokkaan vain jos niillä on sama syklityyppi.*

Esimerkki 4.8. Valitaan jokin n-sykli $\tau = (x_1\ x_2 \dots x_n)$ ryhmästä S_n, missä $n > 3$. Tämä n-sykli virittää aliryhmän $H = \{\mathrm{id}, \tau, \tau^2, \dots, \tau^{n-1}\}$. Osoitetaan, että H ei voi olla normaali.

Jotta H olisi normaali, sen täytyy sisältää kaikkien alkioidensa konjugaatit. Kuitenkin, jos $\sigma = (x_1\ x_2)$, niin edellisen lauseen mukaan

$$^{\sigma}\tau = (x_2\ x_1\ x_3 \dots x_n).$$

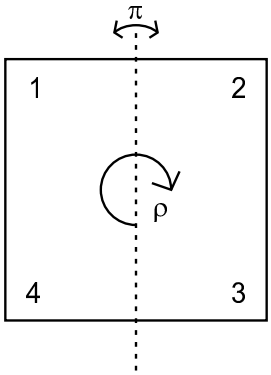
Helposti nähdään, että $\tau^k(x_2) = x_1$ vain, jos $k = n-1$, mutta toisaalta $\tau^{n-1}(x_1) = x_n$. Näin ollen $^{\sigma}\tau$ on eri permutaatio kuin τ^k kaikilla k, joten $^{\sigma}\tau$ ei kuulu aliryhmään H.

Kun käytettävissä ovat kaikki symmetrisen ryhmän permutaatiot, myös kaikki mahdolliset konjugoinnit onnistuvat, ja konjugaattiluokat muodostuvat täsmälleen niistä permutaatioista, joilla on sama syklityyppi. Jos sen sijaan rajoitutaan johonkin ryhmän S_n aliryhmään, konjugaattiluokat voivat hajota pienempiin osiin, kun konjugoivaa alkiota ei enää löydykään.

Esimerkki 4.9. Tarkastellaan ryhmän S_4 aliryhmää

$$\begin{aligned} D_8 = \{&\mathrm{id},\ (1234),\ (13)(24),\ (1432),\\ &(12)(34),\ (24),\ (14)(32),\ (13)\}, \end{aligned}$$

jota nimitetään *neliön symmetriaryhmäksi*. Nimitys johtuu siitä, että jos neliön nurkat numeroidaan kuvan 12 mukaisesti, jokainen ryhmän D_8 permutaatio vastaa sellaista nurkkien siirtoa, joka säilyttää neliön rakenteen. Toisin sanoen, jos neliötä käännellään niin, että nurkat palautetaan lopulta alkuperäisten nurkkien paikoille, saadaan niiden numeroinnin muuttumisesta ryhmän D_8 permutaatio.



Kuva 12: Neliön kierto ja peilaus

Neliötä voidaan käännellä pääasiassa kahdella tavalla. Ensimmäinen tapa on neljännesympyrän kierto myötäpäivään, joka vastaa permutaatiota $\rho = (1234)$. Tämä kierto voidaan suorittaa neljä kertaa, minkä jälkeen neliö palaa alkuperäiseen asentoonsa, ja näin saadaan kierron virittämä aliryhmä

$$R = \langle \rho \rangle = \{\mathrm{id}, (1234), \underbrace{(13)(24)}_{\rho^2}, \underbrace{(1423)}_{\rho^3}\}.$$

Toinen tapa on esimerkiksi pystyakselin varassa suoritettu peilaus $\pi = (12)(34)$. Neliötä voi peilata myös vaaka-akselin sekä eri lävistäjien suhteen, mutta nämä kaikki peilaukset saadaan myös yhdistämällä jokin kierroista peilaukseen π:

$$\pi = (12)(34), \quad \pi\rho = (24), \quad \pi\rho^2 = (14)(23) \quad \text{ja} \quad \pi\rho^3 = (13).$$

Alkiot ρ ja π siis virittävät neliön symmetriaryhmän.

Etsitään ryhmän D_8 jako konjugaattiluokkiin. Oman konjugaattiluokkansa muodostaa aina neutraalialkion yksiö $\{\mathrm{id}\}$. Toisaalta syklityyppi rajoittaa sitä, mitkä alkiot voidaan saada toisistaan konjugoimalla. Kokeilemalla nähdään esimerkiksi, että

$$^{\pi}(1234) = (1432),$$

joten yhden konjugaattiluokan muodostavat 4-syklit (1234) ja (1423). Konjugoinnilla on tässä erityinen geometrinen merkitys. Kun neliöön käytetään peilausta, neliö ikään kuin kääntyy nurin päin, taustapuoli eteen. Tällöin neljänneskierto myötäpäivään muuttuukin alkuperäisessä neliössä neljänneskierroksi vastapäivään. Sama toimii millä tahansa peilauksella, ja kaikki nämä tuottavatkin saman konjugaatin.

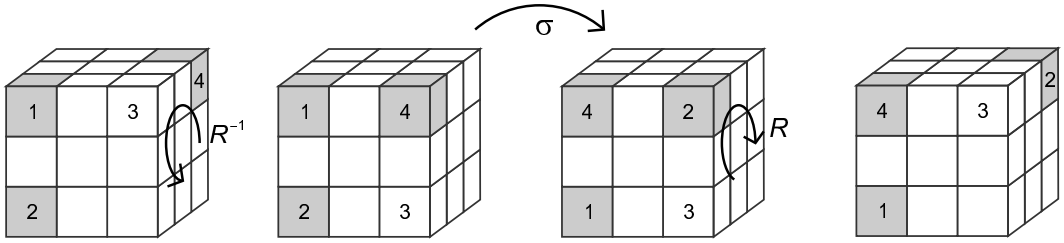
Pystypeilaus $(12)(34)$ taas voidaan muuttaa vaakapeilaukseksi $(14)(23)$ kiertämällä neliötä ensin neljänneskierroksen verran. Niinpä $^{\rho}(12)(34) = (14)(23)$. Myös diagonaalipeilaukset (24) ja (13) toimivat tässä konjugoivina alkioina. Samalla tavoin nähdään vielä, että esimerkiksi $^{\rho}(13) = (24)$.

Jäljelle jää vielä kiertoalkio $\rho^2 = (13)(24)$, joka on samaa syklityyppiä kuin vaaka- ja pystypeilaukset. Kierrolla konjugoiminen tuottaisi kuitenkin vain uuden kierron. Jos taas konjugoitaisiin jollain peilausalkiolla τ, tulisi neliö käännetyksi ensin nurin päin ja sitten kierron jälkeen jälleen oikein päin. Niinpä tuloksena ei voi olla peilausta, jossa neliö jäisi loppujen lopuksi nurin päin.

Algebrallisesti sama voidaan todeta, kun huomataan, että kiertoryhmä R on itse asiassa normaali aliryhmä. Sen indeksi on nimittäin $[D_8 : R] = |D_8|/|R| = 8/4 = 2$. Näin ollen se sisältää kaikki konjugaattinsa, joten kierto ρ^2 ei voi konjugoitua ryhmän ulkopuolella olevaksi peilaukseksi. Konjugaattiluokiksi saadaan siis lopulta seuraavat joukot: $\{\mathrm{id}\}$, $\{(1234), (1432)\}$, $\{(13), (24)\}$, $\{(12)(34), (14)(23)\}$ ja $\{(13)(24)\}$.

4.3 Konjugointi Rubikin ryhmässä

Konjugointi auttaa Rubikin kuution ratkaisussa merkittävästi, sillä sen avulla voidaan opittu siirtosarja siirtää kuution toiseen osaan. Jos esimerkiksi halutaan suorittaa paikkaryhmässä $\mathbb{R}_p$ kuvan 13 mukainen 3-sykli (124) aiemmin opitun syklin $\sigma = (123)$ asemesta, voidaan ensin suorittaa perussiirto R^{-1}, joka tuo palan 4 palan 3 paikalle (ja liikuttaa toki samalla muitakin paloja). Tämän jälkeen suoritetaan opittu siirto σ, ja lopuksi palautetaan pala 4 paikalleen perussiirrolla R. On siis suoritettu konjugaattisiirto ${}^R\sigma$. Aiemman teoreettisen tarkastelun perusteella tiedetään, että kyseinen konjugaatti todella on 3-sykli eikä liikuta muita kuin haluttuja paloja.



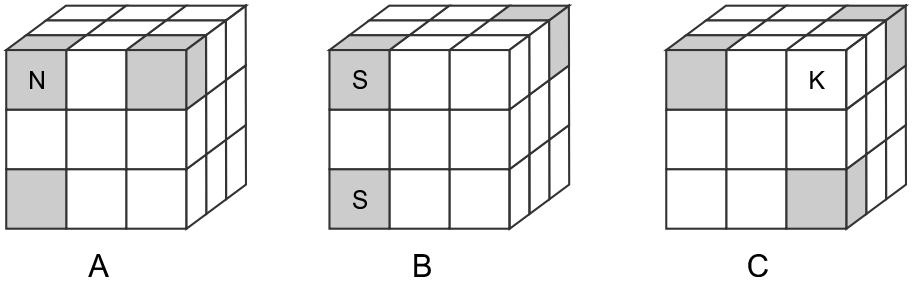
Kuva 13: Opitun siirron konjugointi

Jotta kaikki nurkkapalat saataisiin paikoilleen tunnettua 3-sykliä ja sen konjugaatteja soveltamalla, täytyisi kahden ehdon täyttyä: ensinnäkin nurkkapalojen permutaation pitäisi aina olla parillinen. Toiseksi kaikkien konjugointiin tarvittavien permutaatioiden pitäisi olla laillisia siirtoja.

Ensimmäinen ehto ei kuitenkaan päde, koska mikä tahansa perussiirto on nurkkapalojen kannalta 4-sykli, joka ei ole parillinen. Toisaalta, jos nurkkapalat ovat asennossa, joka vastaa paritonta permutaatiota, tekemällä mikä tahansa perussiirto (missä tahansa vaiheessa) saa tilanteen jälleen vastaamaan parillista permutaatiota. Tällöin se on periaatteessa mahdollista ratkaista 3-syklien avulla.

Käydään nyt läpi kaikki mahdolliset kolmen nurkkapalan kombinaatiot ja osoitetaan, että jokaista näistä kohti löytyy permutaatio σ, joka vie opittuun 3-sykliin τ osallistuvat palat noiden kolmen nurkkapalan paikalle. Tällöin voidaan mikä tahansa 3-sykli suorittaa konjugaattina ${}^\sigma\tau$.

Lasketaan ensin, kuinka monta erilaista kolmen nurkkapalan kombinaatiota kuutiosta yhteensä löytyy. Koska nurkkapaloja on yhteensä kahdeksan, lukumäärä on $\binom{8}{3} = 56$. Nämä kombinaatiot jakautuvat kolmeen joukkoon A, B ja C, jotka näkyvät kuvassa 14. Jokaisen joukon sisällä kombinaatiot saadaan toisistaan koko kuutiota kiertämällä.



Kuva 14: Kolmen nurkkapalan kombinaatiot

Lasketaan nyt kussakin joukossa A, B ja C olevien kombinaatioiden lukumäärä, jotta varmistutaan siitä, että nämä joukot todella sisältävät kaikki mahdolliset kombinaatiot.

A: Tämä on ainoa joukko, jossa kaikki nurkkapalat ovat samalla sivulla. Sivuvaihtoehtoja on kuusi, ja jokaisella sivulla kirjaimella N merkitty pala voi olla neljässä eri nurkassa. Näin saadaan yhteensä $6 \cdot 4 = 24$ eri kombinaatiota.

B: Kirjaimilla S merkityt palat ovat samalla särmällä. Tämä särmä voidaan valita 12 eri särmän joukosta. Kolmanneksi palaksi voidaan sitten valita jompi kumpi vastakkaisen särmän nurkkapaloista. (Nämä kombinaatiot saadaan toisistaan kiertämällä kuutio ylösalaisin.) Yhteensä saadaan siis 24 kombinaatiota.

C: Nämä kombinaatiot koostuvat kirjaimella K merkityn nurkkapalan viereisten nurkkien paloista. Nurkan K valinta määrää koko kombinaation täysin, ja se voidaan valita vapaasti kaikkien kahdeksan nurkan joukosta. Kombinaatioita on siis 8.

Yhteensä edellä laskettuja kombinaatioita on juuri $24 + 24 + 8 = 56$, joten kaikki kombinaatiot kuuluvat johonkin luetelluista joukoista.

Oletetaan, että jokin asema saadaan toisesta kiertämällä kuutiota neljänneskierros jonkin keskiakselinsa ympäri. Nurkkapalojen kannalta sama tulos saadaan, jos pidetään keskitahko paikallaan ja kierretään vain sivutahkoja. Tällöin keskipalat eivät liiku, joten kuution sivut säilyvät samassa asennossa. Jos siis ajatellaan kuvassa 14 keltaisen sivun olevan katsojaan päin ja sinisen ylöspäin, voidaan mikä tahansa kombinaatio palauttaa kuvan kaltaiseen asemaan vain sivutahkoja liikuttamalla.

Lause 4.10. *Mikä tahansa ryhmän $\mathbb{R}_p$ 3-sykli, joka liikuttaa vain nurkkapaloja, on mahdollinen siirto.*

Todistus. Merkitään luvussa 3.3 opittua nurkkapalojen 3-sykliä kirjaimella τ. Valitaan jokin kuution palojen numerointi, jossa $\tau = (123)$. Osoitetaan, että mitä tahansa kolmea nurkkapalaa a, b ja c kohti voidaan löytää siirto $\sigma \in \mathbb{R}_p$, jolle $\sigma\{1,2,3\} = \{a,b,c\}$. Tällöin pätee joko ${}^{\sigma}\tau = (abc)$ tai ${}^{\sigma}\tau = (acb)$. Koska joka tapauksessa $(abc)^2 = (acb)$, niin kumpikin 3-sykli voidaan muodostaa.

Olkoot siis a, b ja c jotkin kolme nurkkapalaa. Etsitään konjugoivan siirron σ sijasta sen käänteissiirto σ^{-1}. Tämän muodostaminen koostuu seuraavista vaiheista:

1. Saatetaan sivutahkoja kiertämällä kuutio johonkin kuvan 14 kolmesta asemasta, joista jokaisessa keltainen sivu osoittaa katsojaan päin ja sininen ylöspäin.

2A. Jos päädyttiin asemaan A, siirto σ^{-1} on valmis.

2B. Jos päädyttiin asemaan B, kierretään oikeaa tahkoa neljänneskierros vastapäivään siirrolla R^{-1}.

2C. Jos päädyttiin asemaan C, kierretään ensin alatahkoa vastapäivään, sitten oikeaa tahkoa vastapäivään, eli suoritetaan siirto $R^{-1}D^{-1}$.

Kaikissa tapauksissa saadaan konjugoiva siirto σ^{-1}, joka siirtää nurkat a, b ja c nurkiksi 1, 2 ja 3. Tämän käänteissiirto on etsitty σ. □

Huom. Kuutiota ratkaistaessa ei tarvitse suorittaa edellisessä todistuksessa mainittua vaihetta 1 vaan riittää, että kääntää kuution ympäri ja nimeää uudelleen perussiirrot niin, että edessä olevan uuden tahkon kierto on F, ylätahkon kierto U jne. Myöskään vaiheiden 2A, 2B ja 2C konjugointeja ei tarvitse muistaa ulkoa vaan niiden sijaan voi keksiä kuhunkin tilanteeseen sopivan konjugointisiirron.

4.4 Ryhmän keskus

Usein on hyödyllistä tarkastella niiden alkioiden joukkoa, joilla konjugoiminen ei vaikuta muihin alkioihin.

Määritelmä 4.11. Olkoon G ryhmä ja olkoon $x \in G$. Alkion x *keskittäjä* on joukko

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Ryhmän G *keskus* on niiden alkioiden joukko, jotka eivät konjugoitaessa liikuta mitään alkioita:

$$\zeta G = \{g \in G \mid gx = xg \text{ kaikilla } x \in G\} = \bigcap_{x \in G} C_G(x).$$

Voidaan myös sanoa, että keskus on niiden alkioiden joukko, jotka kommutoivat kaikkien alkioiden kanssa.

On helppo nähdä, että sekä keskus että jokainen keskittäjä ovat koko ryhmän aliryhmiä. Keskus on lisäksi vaihdannainen ja normaali.

Vaikka keskittäjän määritelmä on annettu siinä muodossa, että sen alkioilla konjugoiminen ei vaikuta alkioon x, voidaan sama ajatella myös niin, että x:llä konjugoiminen ei vaikuta keskittäjän alkioihin. Jos nimittäin ${}^{g}x = x$, niin myös ${}^{g^{-1}}x = x$, ja

$$ {}^{x}g = (gg^{-1})(xgx^{-1}) = g \cdot {}^{g^{-1}}x \cdot x^{-1} = gxx^{-1} = g. $$

Samaten keskus voidaan määritellä niiden alkioiden joukkona, joihin mikään konjugointi ei vaikuta. Tästä seuraa tietysti suoraan keskuksen normaalisuus.

Tarkastellaan seuraavaksi hieman keskittäjäaliryhmien $C_G(x)$ sivuluokkia. Keskittäjän alkioilla konjugoitaessa x pysyy paikallaan, joten voisi olettaa, että kaikki samaan sivuluokkaan kuuluvat alkiot tuottavat konjugoitaessa x:stä saman konjugaatin. Tästä havainnosta saadaan seuraava lause.

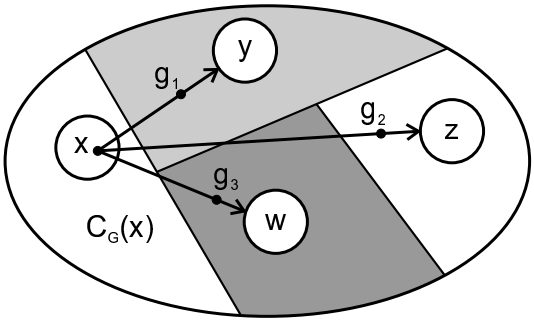
Lause 4.12. *Olkoon G äärellinen ryhmä ja olkoon $x \in G$. Keskittäjän $C_G(x)$ sivuluokkien lukumäärä $[G : C_G(x)]$ on sama kuin alkion x konjugaattiluokan koko.*

Todistus. Osoitetaan edellä mainittu seikka, eli että kaksi alkion x konjugaattia ovat samat jos ja vain jos niitä konjugoivat alkiot kuuluvat samaan keskittäjän sivuluokkaan. Tällöin konjugaatteja täytyy olla yhtä paljon kuin sivuluokkia. Olkoot siis $g_1, g_2 \in G$. Tällöin

$$ \begin{aligned} {}^{g_1}x = {}^{g_1}x &\iff {}^{g_2^{-1}}({}^{g_1}x) = {}^{g_2^{-1}}({}^{g_2}x) \\ &\iff {}^{(g_2^{-1}g_1)}x = {}^{(g_2^{-1}g_2)}x = x \\ &\iff g_2^{-1}g_1 \in C_G(x). \end{aligned} $$

Saatiin siis, että kaksi konjugaattia ovat samat jos ja vain jos alkio $g_2^{-1}g_1$ kuuluu keskittäjään. Tällöin kuitenkin g_1 ja g_2 kuuluvat samaan sivuluokkaan, joten väite on todistettu. □

Oheisessa kuvassa on havainnollistettu keskittäjäaliryhmän ja konjugaattiluokan suhdetta. Alkion x konjugaattiluokka on neljän alkion joukko $\{x, y, z, w\}$. Saman alkion keskittäjällä puolestaan on neljä sivuluokkaa $C_G(x)$, $g_1 \cdot C_G(x)$, $g_2 \cdot C_G(x)$ ja $g_3 \cdot C_G(x)$. Kustakin eri sivuluokasta otettu alkio tuottaa eri konjugaatin, esimerkiksi ${}^{g_1}x = y$, toisaalta saman sivuluokan alkiot tuottavat aina saman konjugaatin. Huomaa, että konjugaatin sijaintia ryhmässä ei tunneta; ei esimerkiksi päde välttämättä $y \in g_1 \cdot C_G(x)$.



Kuva 15: Keskittäjän sivuluokat ja konjugaatit

Esimerkki 4.13. Tarkastellaan permutaation $\tau = (123)$ keskittäjää ryhmässä S_3. Koska permutaatiolla σ konjugoiminen tuottaa τ:sta syklin $(\sigma(1)\ \sigma(2)\ \sigma(3))$, täytyy tutkia, missä tapauksissa tämä tulossykli on sama permutaatio kuin τ. Permutaatio τ voidaan kirjoittaa kolmella eri tavalla: (123), (231) tai (312). Näitä vastaavat konjugoivat permutaatiot id, (123) ja (132). Muut ryhmän S_3 permutaatiot eivät pidä konjugoinnissa τ:ta paikallaan; esimerkiksi ${}^{(12)}(123) = (213) \neq (123)$.

Syklin τ keskittäjä on siis $C_G(\tau) = \{\mathrm{id}, (123), (132)\}$. Sen indeksi on

$$[S_3 : C_G(\tau)] = |S_3|/|C_G(\tau)| = 6/3 = 2,$$

joten sillä on itsensä lisäksi vain yksi sivuluokka. Tämä on 2-syklien muodostama joukko $(12) \circ \tau = \{(12), (23), (13)\}$.

Edellä todistetun lauseen mukaan jokaista keskittäjän $C_G(\tau)$ sivuluokkaa vastaa jokin τ:n konjugaatti. Koska symmetrisessä ryhmässä konjugaattiluokat määräytyvät syklityypin mukaan, on τ:n konjugaattiluokka kahden 3-syklin joukko $\{(123), (132)\}$. Keskittäjä vastaa itse tietysti 3-sykliä $\tau = (123)$. Toinen sivuluokka vastaa tällöin 3-sykliä (132), ja konjugoimalla permutaatiota τ tuon sivuluokan alkioilla saadaankin seuraavat tulokset:

$$\begin{aligned} & {}^{(12)}(123) = (213) = (132), \\ & {}^{(23)}(123) = (132) \\ \text{ja} \quad & {}^{(13)}(123) = (321) = (132). \end{aligned}$$

Nähdään siis, että sivuluokan alkiot tuottavat kaikki saman 3-syklin.

Todistetun lauseen seurauksena saadaan nk. *luokkayhtälö*. Numeroidaan äärellisen ryhmän G konjugaattiluokat $A_1, A_2, \ldots, A_m$ ja valitaan jokaisesta luokasta edustaja $x_i \in A_i$. Koska konjugaattiluokan A_i koko on edellisen lauseen mukaan

$[G : C_G(x_i)]$ ja konjugaattiluokat muodostavat toisaalta koko ryhmän osituksen, pätee yhtälö

$$|G| = \sum_{k=1}^{m} [G : C_G(x_i)].$$

Koska $\zeta G \leq C_G(x_i)$ kaikilla i, luku $|\zeta G|$ jakaa jokaisen luvun $|C_G(x_i)|$ Lagrangen lauseen mukaisesti. Löytyy siis luvut $k_i \in \mathbb{Z}$, joille $|C_G(x_i)| = k_i \cdot |\zeta G|$ kaikilla i. Nyt kaikilla i pätee

$$[G : \zeta G] = \frac{|G|}{|\zeta G|} = \frac{k_i \cdot |G|}{|C_G(x_i)|} = k_i \cdot [G : C_G(x_i)].$$

Siispä jokainen luku $[G : C_G(x_i)]$ jakaa keskuksen indeksin $[G : \zeta G]$. Lisäksi $x_i \in \zeta G$ jos ja vain jos $G = C_G(x_i)$, jolloin $[G : C_G(x_i)] = 1$. Keskukseen kuuluvat siis täsmälleen ne alkiot, joilla indeksi $[G : C_G(x_i)]$ on 1.

Esitetään luvun lopuksi eräs luokkayhtälön sovellus.

Lemma 4.14. *Jos ryhmän G koko on p^m, missä p on alkuluku ja m nollaa suurempi kokonaisluku, niin G:llä on epätriviaali keskus.*

Todistus. Olkoon ryhmän G konjugaattiluokkien määrä r. Valitaan jokaisesta konjugaattiluokasta edustaja x_i ja merkitään $n_i = [G : C_G(x_i)]$ kaikilla i. Luokkayhtälön mukaan

$$p^m = \sum_{i=1}^{r} n_i.$$

Lagrangen lauseen perusteella jokainen indeksi n_i jakaa koko ryhmän koon p^m. Koska p on alkuluku, täytyy jokaisen luvun n_i olla muotoa p^{k_i} jollain $k_i \in \mathbb{N}$. Jos nyt keskus olisi triviaali, niin löytyisi vain yksi indeksi i, jolla $k_i = 1$. Voidaan olettaa, että kyseinen indeksi on m. Saadaan yhtälö

$$p^m = p \cdot \left(p^{k_1 - 1} + p^{k_2 - 1} + \cdots + p^{k_{r-1} - 1}\right) + 1.$$

Kyseisen yhtälön vasen puoli on jaollinen p:llä mutta oikea puoli ei. Keskus ei siis voi olla triviaali. □

Lause 4.15. *Jos G on ryhmä ja $|G| = p^2$, missä p on alkuluku, G on vaihdannainen.*

Todistus. Olkoon p alkuluku ja olkoon $|G| = p^2$. Koska G:n keskus on G:n aliryhmä, niin Lagrangen lauseen mukaan $|\zeta G| \in \{1, p, p^2\}$. Edellisen lemman mukaan $|\zeta G| \neq 1$. Täten keskuksen indeksi eli tekijäryhmän $G/\zeta G$ koko on joko 1 tai p. Kummassakin tapauksessa tekijäryhmä on syklinen. Tästä seuraa (todistus harjoitustehtävänä), että G on vaihdannainen. □

5 Tuloryhmät

Jotkin ryhmät voidaan jakaa toisistaan riippumattomiin osiin niin, että jokainen ryhmän alkio saadaan tulona eri osista valituista alkioista. Tällöin ryhmää voidaan käsitellä osiensa tulona eli tuloryhmänä.

5.1 Suorat tulot

Tarkastellaan aluksi permutaatioryhmiin liittyvää esimerkkiä.

Esimerkki 5.1. Symmetrisestä ryhmästä S_4 löytyy muun muassa syklien virittämät aliryhmät

$$\begin{aligned} & H = \langle (1234) \rangle = \{\mathrm{id}, (1234), (13)(24), (1432)\} \\ \text{ja} \quad & K = \langle (123) \rangle = \{\mathrm{id}, (123), (132)\}. \end{aligned}$$

Näiden aliryhmien alkioista voidaan muodostaa tulojoukko HK, johon kuuluvat kaikki muotoa hk olevat alkiot, missä $h \in H$ ja $k \in K$. Laskemalla kukin näistä 12 tulosta nähdään, että

$$\begin{aligned} HK = \{ & \mathrm{id},\ (1234),\ (13)(24),\ (1423), \\ & (123),\ (1324),\ (142),\ (34), \\ & (132),\ (14),\ (234),\ (1243)\ \}. \end{aligned}$$

Saatu tulojoukko ei kuitenkaan ole ryhmän S_4 aliryhmä, koska esimerkiksi $(1324) \in HK$, mutta $(1324)^2 = (12)(34) \notin HK$.

Etsitään nyt jokin ehto, jolla aliryhmien tulosta HK tulisi ryhmä. Kahden tulojoukosta valitun alkion h_1k_1 ja h_2k_2 tulo on $h_1k_1h_2k_2$, joka ei välttämättä kuulu joukkoon HK. Jos kuitenkin vaaditaan, että aliryhmien H ja K alkiot olisivat *keskenään vaihdannaisia*, pätee edellä mainitussa tulossa

$$h_1 \underbrace{k_1 h_2}_{\text{vaihd.}} k_2 = h_1 h_2 k_1 k_2,$$

ja oikeanpuoleinen tulo kuuluu nyt joukkoon HK. Myös minkä tahansa alkion $hk \in HK$ käänteisalkio kuuluu joukkoon HK, sillä $h^{-1} \in H$, $k^{-1} \in K$ ja näin ollen $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$. Joukosta HK tulee tällöin aliryhmä, sillä myös neutraalialkiolle pätee $e = e \times e \in HK$.

Määritelmä 5.2. Olkoot H ja K ryhmän G aliryhmiä. Joukkoa HK kutsutaan aliryhmien H ja K *sisäiseksi suoraksi tuloksi*, jos se toteuttaa seuraavat ehdot:

1) $hk = kh$ kaikilla $h \in H$ ja $k \in K$

2) $H \cap K = \{e\}$, missä e on ryhmän G neutraalialkio.

Sisäistä suoraa tuloa merkitään $HK = H \times K$ tai toisinaan (sisäisyyttä korostaen) myös $(H \times K)_s$. Jos ryhmässä G on laskutoimituksena yhteenlasku, tuloa kutsutaan *sisäiseksi suoraksi summaksi* ja merkitään $H \oplus K$.

Edellä havaittiin, että kahden aliryhmän sisäinen suora tulo $H \times K$ on itsekin aliryhmä.

Esimerkki 5.3. Tarkastellaan symmetrisen ryhmän S_5 aliryhmiä

$$H = \{\mathrm{id}, (123), (132)\} \quad \text{ja} \quad K = \{\mathrm{id}, (45)\}.$$

Koska erilliset syklit kommutoivat keskenään, pätee $hk = kh$ kaikille $h \in H$ ja $k \in K$. Lisäksi $H \cap K = \{\mathrm{id}\}$, joten joukko

$$HK = \{\mathrm{id}, (123), (132), (45), (123)(45), (132)(45)\}$$

on aliryhmien H ja K suora tulo eli $HK = H \times K$. Lisäksi $H \times K \leq S_5$.

Esimerkki 5.4. Tarkastellaan yhteenlaskuryhmää $\mathbb{Z}_{15} = \{[0], [1], [2], \ldots, [14]\}$, missä $[n] = [m]$ aina kun $m - n$ on jaollinen 15:llä. Tällä ryhmällä on aliryhmät $H = \langle [5] \rangle = \{[0], [5], [10]\}$ ja $K = \langle [3] \rangle = \{[0], [3], [6], [9], [12]\}$. Koska ryhmä $\mathbb{Z}_{15}$ on vaihdannainen ja $H \cap K = \{[0]\}$, voidaan muodostaa aliryhmien H ja K suora summa $H \oplus K$. Lasketaan summa-alkiot oheiseen taulukkoon. (Jätetään taulukon alkioista hakasulut selvyyden vuoksi merkitsemättä.)

$H \oplus K$	$[0]$	$[5]$	$[10]$
$[0]$	0	5	10
$[3]$	3	8	13
$[6]$	6	11	1
$[9]$	9	14	4
$[12]$	12	2	7

Taulukosta huomataan, että $H \oplus K = \mathbb{Z}_{15}$. Lisäksi kukin ryhmän $\mathbb{Z}_{15}$ alkio esiintyy taulukossa täsmälleen kerran.

Todistetaan seuraavassa lemmassa kaksi hyödyllistä ehtoa, jotka pätevät kaikille ryhmille, jotka voidaan esittää aliryhmiensä suorana summana.

Lemma 5.5. *Oletetaan, että H ja K ovat ryhmän G aliryhmiä ja että $G = H \times K$. Tällöin seuraavat ehdot pätevät:*

1) *H ja K ovat G:n normaaleja aliryhmiä*

2) *jokaisella alkiolla $g \in G$ on yksikäsitteinen esitys $g = hk$, missä $h \in H$ ja $k \in K$.*

Todistus. Osoitetaan ensin, että ehto 1) pätee. Olkoot sitä varten $h' \in H$, $k' \in K$ ja $g \in G$. Osoitetaan, että konjugaatit ${}^g h'$ ja ${}^g k'$ kuuluvat edelleen aliryhmiin H ja K. Koska $G = H \times K$, voidaan kirjoittaa $g = hk$ joillain $h \in H$ ja $k \in K$. Nyt pätee $kh' = h'k$, joten

$$gh'g^{-1} = h(kh')k^{-1}h^{-1} = h(h'k)k^{-1}h^{-1} = hh'h^{-1} \in H.$$

Toisaalta myös $h(kk'k^{-1}) = (kk'k^{-1})h$, joten

$$gk'g^{-1} = h(kk'k^{-1})h^{-1} = (kk'k^{-1})hh^{-1} = kk'k^{-1} \in K.$$

Siispä ${}^g h' \in H$ ja ${}^g k' \in K$, joten aliryhmät H ja K ovat normaaleja.

Todistetaan sitten ehto 2). Oletetaan, että alkiolla $g \in G$ on esitykset tuloina h_1k_1 ja h_2k_2, missä $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Siispä $h_1k_1 = h_2k_2$, josta saadaan

$$h_2^{-1}h_1 = k_2k_1^{-1}.$$

Yllä olevan yhtälön vasemman puolen alkio kuuluu joukkoon H ja oikean puolen alkio joukkoon K, joten molemmat alkiot kuuluvat itse asiassa leikkausjoukkoon $H \cap K$. Toisaalta suoran tulon määritelmän mukaan $H \cap K = \{e\}$, missä e on ryhmän G neutraalialkio. Näin ollen $h_2^{-1}h_1 = e$ ja $k_2k_1^{-1} = e$, mistä nähdään, että $h_1 = h_2$ ja $k_1 = k_2$. Nähtiin, että alkion g esitys on yksikäsitteinen. □

Huomautus 5.6. Aliryhmien sisäinen suora tulo voidaan määritellä myös usemmalle kuin kahdelle aliryhmälle. Määritelmä on aivan samanlainen kuin kahden aliryhmän tapauksessa, ja ehdoiksi tulee

1) $h_ih_j = h_jh_i$ aina, kun $i \neq i$ ja alkiot h_i ja h_j kuuluvat aliryhmiin H_i ja H_j

2) $H_i \cap H_j = \{e\}$ kaikilla aliryhmillä H_i ja H_j, kun $i \neq j$.

Suoraa tuloa voidaan tällöin merkitä $H_1 \times H_2 \times \cdots \times H_n$ tai tulomerkinnällä $\prod_{i=1}^{n} H_i$. Määritelmä toimii myös äärettömän monen aliryhmän tapauksessa. Tällöin kuitenkin kaikilla suoran tulon $\prod_{i=1}^{\infty} H_i$ alkioilla on *äärelliset* esitykset $h_{i_1}h_{i_2}\cdots h_{i_n}$, missä $h_{i_k} \in H_{i_k}$ kaikilla k. Ääretöntä tuloa ei nimittäin voida ryhmässä yleensä määritellä.

Sisäinen suora tulo määritellään jonkin ryhmän G sisältämien aliryhmien välillä. Koska kuitenkin osoittautuu, että nämä aliryhmät ovat täysin riippumattomia toisistaan, ei uloimmaista ryhmää G oikeastaan tarvita mihinkään, vaan suora tulo voidaan itse asiassa määritellä minkä tahansa kahden ryhmän välillä. Se, että ryhmissä on mahdollisesti täysin erilaiset alkiot ja laskutoimitukset, ei tuota estettä.

Määritelmä 5.7. Ryhmien $(G_1, \circ)$ ja $(G_2, *)$ *ulkoinen suora tulo* on ryhmä, jonka alkioina ovat parit (g_1, g_2), missä $g_1 \in G_1$ ja $g_2 \in G_2$, ja laskutoimituksena

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \circ g_1', g_2 * g_2').$$

Ulkoista suoraa tuloa merkitään $G_1 \times G_2$ ja toisinaan $(G_1 \times G_2)_u$. Jos molemmissa ryhmissä käytetään laskutoimituksena yhteenlaskua, voidaan ulkoista suoraa tuloa kutsua myös *ulkoiseksi suoraksi summaksi* ja merkitä $G_1 \oplus G_2$.

Ulkoisessa suorassa tulossa neutraalialkiona toimii pari (e_1, e_2), missä e_1 ja e_2 ovat ryhmien G_1 ja G_2 neutraalialkiot. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on puolestaan (g_1^{-1}, g_2^{-1}).

Esimerkki 5.8. Muodostetaan ryhmien

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} \quad \text{ja} \quad \mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

ulkoinen suora summa. Tulo koostuu pareista $([m]_3, [n]_5)$, jotka voidaan kirjoittaa oheisen taulukon muotoon. (Jätetään jälleen taulukosta pois hakasulut alkioiden ympäriltä.)

$\mathbb{Z}_3 \oplus \mathbb{Z}_5$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_5$	$(0_3, 0_5)$	$(1_3, 0_5)$	$(2_3, 0_5)$
$[1]_5$	$(0_3, 1_5)$	$(1_3, 1_5)$	$(2_3, 1_5)$
$[2]_5$	$(0_3, 2_5)$	$(1_3, 2_5)$	$(2_3, 2_5)$
$[3]_5$	$(0_3, 3_5)$	$(1_3, 3_5)$	$(2_3, 3_5)$
$[4]_5$	$(0_3, 4_5)$	$(1_3, 4_5)$	$(2_3, 4_5)$

Kun verrataan saatua taulukkoa aikaisempaan esimerkkiin 5.4, huomataan, että aikaisemman taulukon lukua $[k]_{15}$ vastaa tässä taulukossa aina sellainen pari $([m]_3, [n]_5)$, jolle pätee $[m \cdot 5 + n \cdot 3]_{15} = [k]_{15}$. Ryhmän $\mathbb{Z}_{15}$ virittää alkio $[1]_{15}$, sillä kaikki ryhmän alkiot saadaan sen monikertoina. Taulukkoesityksestä päätellen tätä alkiota vastaa pari $([2]_3, [2]_5)$, ja jos lasketaan kyseisen parin monikerrat

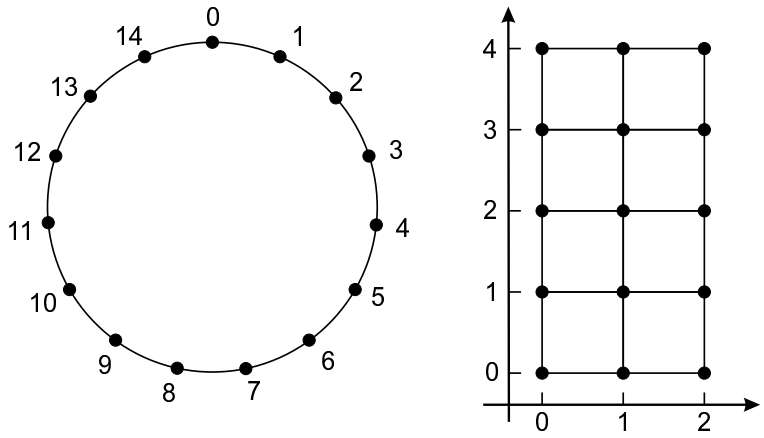
summaryhmässä $\mathbb{Z}_3 \oplus \mathbb{Z}_5$, saadaan

$$\begin{aligned} 2 \cdot (2_3, 2_5) &= (4_3, 4_5) = (1_3, 4_5), \\ 3 \cdot (2_3, 2_5) &= (6_3, 6_5) = (0_3, 1_5), \\ 4 \cdot (2_3, 2_5) &= (8_3, 8_5) = (2_3, 3_5), \\ 5 \cdot (2_3, 2_5) &= (10_3, 10_5) = (1_3, 0_5) \end{aligned}$$

jne.

Laskemalla kaikki monikerrat huomataan, että pari $([2]_3, [2]_5)$ virittää summaryhmän $\mathbb{Z}_3 \oplus \mathbb{Z}_5$. Näin voidaan lopulta todeta, että ryhmät $\mathbb{Z}_{15}$ ja $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ ovat isomorfiset, sillä ne ovat samankokoiset ja molemmat erään alkionsa virittämiä.

Kuvassa 16 on piirretty syklinen ryhmä $\mathbb{Z}_{15}$ kahdella tavalla: yhtenä pitkänä syklinä ja kahden ryhmän tulona.



Kuva 16: Kaksi tapaa hahmottaa 15 alkion syklinen ryhmä

Esimerkki 5.9. Muodostetaan ryhmien A_n ja $(\{1, -1\}, \cdot)$ ulkoinen suora tulo. Tulo koostuu pareista (σ, k), missä σ on joku parillinen permutaatio ja $k = \pm 1$. Merkitään tällaista paria yksinkertaisesti σ, jos $k = 1$, ja $-\sigma$, jos $k = -1$. Tuloryhmän koko on $2 \cdot |A_n| = |S_n|$, ja houkutus olisi samastaa se symmetrisen ryhmän kanssa niin, että miinusmerkkiset alkiot vastaisivat parittomia permutaatioita. Päteehän tuloryhmässä myös

$$(-\sigma) \cdot (-\tau) = (\sigma, -1) \cdot (\tau, -1) = (\sigma \circ \tau, 1) = \sigma\tau,$$

eli kahden "parittoman" permutaation tulo on jälleen parillinen. Tällainen samastus ei kuitenkaan onnistu, sillä esimerkiksi ryhmän S_3 kaikki parittomat permutaatiot ovat vaihtoja, joten niiden toinen potenssi on identtinen kuvaus, mutta $(-(123))^2 = (132)$. Yleisesti voidaankin osoittaa, että ryhmät $A_n \times (\{1, -1\}, \cdot)$ ja S_n eivät ole isomorfisia paitsi tapauksessa $n = 2$.

Jos H_1 ja H_2 ovat ryhmien G_1 ja G_2 aliryhmiä, niin niiden ulkoinen suora tulo on ryhmä, joka sisältyy ryhmään $G_1 \times G_2$. Se on siis kyseisen ryhmän aliryhmä. Osoitetaan seuraavassa lemmassa, että kahden normaalin aliryhmän tulo on myös normaali koko ryhmien tulossa.

Lemma 5.10. *Jos H_1 ja H_2 ovat ryhmien G_1 ja G_2 normaaleja aliryhmiä, niin ryhmä $(H_1 \times H_2)_u$ on normaali ryhmässä $(G_1 \times G_2)_u$.*

Todistus. Olkoot $(h_1, h_2) \in H_1 \times H_2$ ja $(g_1, g_2) \in G_1 \times G_2$. Tällöin pätee

$$(g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}),$$

ja koska H_1 ja H_2 ovat normaaleja, konjugaateille pätee $g_1 h_1 g_1^{-1} \in H_1$ ja $g_2 h_2 g_2^{-1} \in H_2$. Siispä ${}^{(g_1,g_2)}(h_1, h_2) \in H_1 \times H_2$, joten $H_1 \times H_2$ on normaali. □

Aliryhmien sisäinen tulo poikkeaa ulkoisesta tulosta oikeastaan vain teknisiltä yksityiskohdiltaan. Seuraava lause osoittaa, että nämä käsitteet voidaan samastaa.

Lause 5.11. *Olkoot G_1 ja G_2 ryhmiä. Tällöin $(G_1 \times G_2)_u = (H \times K)_s$ eräillä aliryhmillä $H, K \leq (G_1 \times G_2)_u$. Toisaalta, jos H ja K ovat ryhmän G aliryhmiä, niin $(H \times K)_s \cong (H \times K)_u$.*

Todistus. Todistetaan aluksi ensimmäinen väite. Olkoot siis G_1 ja G_2 jotkin kaksi ryhmää, joiden neutraalialkiot ovat e_1 ja e_2. Tarkastellaan tuloryhmän $(G_1 \times G_2)_u$ aliryhmiä $H = (G_1 \times \{e_1\})_u$ ja $K = (\{e_1\} \times G_2)_u$. Selvästikin $H \cap K = \{(e_1, e_2)\}$. Lisäksi kaikilla $g_1 \in G_1$ ja $g_2 \in G_2$ pätee

$$(g_1, e_2)(e_1, g_2) = (g_1, g_2) = (e_1, g_2)(g_1, e_2),$$

joten aliryhmän H alkiot kommutoivat aliryhmän K alkioiden kanssa. Näin ollen voidaan muodostaa sisäinen suora tulo $(H \times K)_s$. Lisäksi nähdään, että jos $(g_1, g_2) \in (G_1 \times G_2)_u$, niin $(g_1, g_2) = (g_1, e_2)(e_1, g_2)$, missä $(g_1, e_2) \in H$ ja $(e_1, g_2) \in K$. Täten $(H \times K)_s = (G_1 \times G_2)_u$.

Todistetaan sitten toinen väite. Olkoot H ja K ryhmän G aliryhmiä. Määritellään kuvaus $\varphi : (H \times K)_u \to (H \times K)_s$ kaavalla $\varphi(h, k) = hk$ ja osoitetaan, että se on isomorfismi. Jokainen sisäisen suoran tulon alkio on muotoa hk, missä $h \in H$ ja $k \in K$, ja $\varphi(h, k) = hk$, joten kuvaus φ on surjektio. Oletetaan sitten, että $\varphi(h_1, k_1) = \varphi(h_2, k_2)$ joillain $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Tällöin siis $h_1 k_1 = h_2 k_2 \in (H \times K)_s$, ja koska lemman 5.5 mukaan jokaisen sisäisen suoran tulon alkion esitys tällaisena tulona on yksikäsitteinen, täytyy olla $(h_1, k_1) = (h_2, k_2)$. Kuvaus φ on siis injektio. Homomorfisuus seuraa siitä, että yhtälö

$$\begin{aligned}\varphi(h_1, k_1) \cdot \varphi(h_2, k_2) &= h_1 k_1 h_2 k_2 = h_1 h_2 k_1 k_2 = \varphi(h_1 h_2, k_1 k_2) \\ &= \varphi\big((h_1, k_1)(h_2, k_2)\big)\end{aligned}$$

pätee kaikilla $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. □

Jos ryhmä G on joidenkin aliryhmiensä H ja K sisäinen suora tulo, sitä voidaan edellisen lauseen nojalla ajatella tuloryhmänä $H \times K$, jonka alkiot ovat pareja (h, k), missä $h \in H$ ja $k \in K$. Jokainen pari (h, k) samastetaan tällöin ryhmän G alkioon hk.

Esimerkki 5.12. Osoitetaan, että jos $n > 2$, ryhmä $A_n \times (\{1, -1\}, \cdot)$ ei ole isomorfinen ryhmän S_n kanssa. Jos näin nimittäin olisi, niin S_n olisi edellisen lauseen nojalla esitettävissä kahden aliryhmänsä B ja C suorana tulona. Nämä aliryhmät ovat molemmat normaaleja, ja toinen niistä sisältää neutraalialkion lisäksi vain yhden alkion: olkoon esimerkiksi $C = \{\mathrm{id}, \sigma\}$. Näytetään, että C ei voi olla normaali.

Koska $\sigma^2 = \mathrm{id}$, koostuu σ:n sykliesitys kokonaan erillisistä vaihdoista. Olkoon yksi näistä vaihdoista (ab). Kun $n > 2$, löydetään joukosta N_n jokin kolmaskin alkio c. Nyt konjugaatin ${}^{(bc)}\sigma$ sykliesityksessä esiintyy vaihto (ac), jota ei ollut σ:n sykliesityksessä. Näin ollen $\sigma \neq {}^{(bc)}\sigma$, joten ${}^{(bc)}\sigma \notin C$. Tästä seuraa, että C ei ole normaali.

Koska ryhmä S_n ei siis sisällä kaksialkioista normaalia aliryhmää, se ei voi olla isomorfinen suoran tulon $A_n \times (\{1, -1\}, \cdot)$ kanssa.

5.2 Tuloryhmät Rubikin ryhmässä

Rubikin kuution rakenteesta johtuen mitkään lailliset permutaatiot eivät voi siirtää nurkkapalaan kiinnitettyä ruutua särmäpalaan tai päinvastoin. Siistä sellaiset siirrot, jotka koskevat vain nurkkaruutuja ovat täysin riippumattomia särmäruutuja liikuttavista siirroitsta, ja on samantekevää, missä järjestyksessä erityyppisiin ruutuihin liittyvät siirrot suoritetaan. Tällaisten siirtojen joukot muodostavat Rubikin ryhmän sisäisen suoran tulon.

Tässä luvussa osoitetaan muutama Rubikin ryhmän rakenteeseen liittyvä lause, joiden avulla voidaan myöhemmin ratkaista kaikki paikkojen ryhmän $\mathbb{R}_p$ asemat. Tehtävän helpottamiseksi tarkastellaan myös Rubikin ryhmän ulkopuolisia ruutujen permutaatioryhmän aliryhmiä. Merkitään kirjaimella N kaikkien nurkkapalojen ruutujen joukkoa ja kirjaimella S kaikkien särmäruutujen joukkoa. Olkoon edelleen S_N kaikkien nurkkaruutujen permutaatioiden ryhmää ja symbolilla S_S vastaavasti kaikkien särmäruutujen permutaatioiden ryhmä. Jos kaikki ruudut numeroidaan luvuilla $1, \ldots, 48$, näiden permutaatioryhmien voidaan ajatella olevan ryhmän S_{48} aliryhmiä.

Edellä mainittujen ryhmien käsittelyä helpottaa, kun otetaan käyttöön *kantajan* käsite. Jos permutaation σ toimii perusjoukossa X, sen kantaja on

$$\mathrm{supp}(\sigma) = \{x \in X \mid \sigma(x) \neq x\}.$$

Permutaation kantaja on siis niiden alkioiden joukko, joihin permutaatio vaikuttaa. Nyt voidaan määritellä ryhmät S_N ja S_S kantajan avulla esimerkiksi seuraavasti:

$$S_N = \{\sigma \in S_{48} \mid \text{supp}(\sigma) \subset N\} \quad \text{ja} \quad S_S = \{\sigma \in S_{48} \mid \text{supp}(\sigma) \subset S\}.$$

Osoitetaan nyt, että ryhmät S_N ja S_S ovat toisistaan riippumattomia.

Lause 5.13. *Nurkka- ja särmäruutuja liikuttavat ryhmät muodostavat suoran tulon $S_N \times S_S$.*

Todistus. Ensinnäkin huomataan, että jos σ kuuluu molempiin ryhmiin, niin näiden ryhmien määritelmän mukaan $\text{supp}(x) \subset N \cap S$ eli $\sigma(x) = x$ pätee kaikilla ruuduilla x, jotka eivät ole sekä nurkka- että särmäruutuja. Koska mikään ruutu ei ole kiinni sekä nurkka- että särmäpalassa, pätee $\sigma(x) = x$ kaikilla ruuduilla x, joten $\sigma = \text{id}$.

Olkoot sitten x jokin nurkkapalan ruutu ja y jokin särmäpalan ruutu. Rubikin kuution rakenteen perusteella $\sigma(x) \in N$ ja $\sigma(y) \in S$ kaikilla siirroilla $\sigma \in \mathbb{R}$. Jos nyt $\sigma \in S_N$ ja $\tau \in S_S$, niin

$$\sigma\tau(x) = \underbrace{\sigma(x)}_{\in N} = \tau\sigma(x)$$

ja vastaavasti

$$\tau\sigma(y) = \underbrace{\tau(y)}_{\in S} = \sigma\tau(x).$$

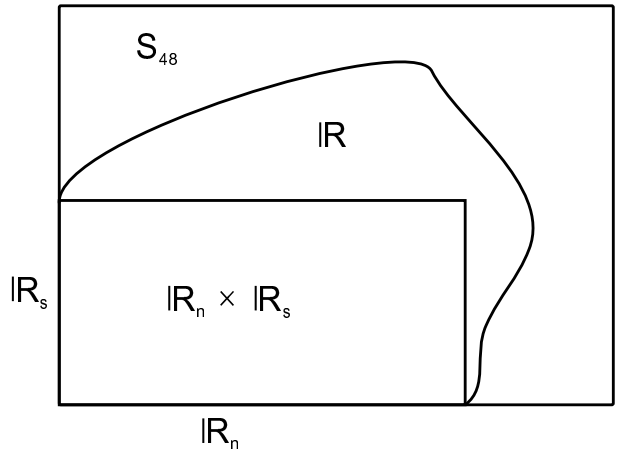
Koska kaikki Rubikin kuution ruudut keskiruutuja lukuunottamatta ovat kiinni joko nurkka- tai särmäpaloissa, nähdään, että $\sigma\tau = \tau\sigma$. Täten S_N ja S_S muodostavat suoran tulon. □

Määritellään vielä erikseen edellä käsiteltyjen ryhmien Rubikin ryhmään sisältyvät osat.

Määritelmä 5.14. Joukkoa $\mathbb{R}_n = \mathbb{R} \cap S_N$ kutsutaan Rubikin *nurkkaryhmäksi* ja joukkoa $\mathbb{R}_s = \mathbb{R} \cap S_S$ puolestaan Rubikin *särmäryhmäksi.*

Koska Rubikin nurkka- ja särmäryhmä ovat kahden ryhmän leikkauksia, ne ovat itsekin ryhmiä ja siten Rubikin ryhmän aliryhmiä, samoin kuin tuloryhmä $\mathbb{R}_n \times \mathbb{R}_s$. Rubikin ryhmässä voidaan siis käsitellä erikseen pelkkiin nurkka- tai pelkkiin reunaruutuihin vaikuttavia siirtoja, mutta näiden yhdistelminä ei välttämättä saada kaikkia mahdollisia siirtoja. Oheisessa kuvassa on esitetty Rubikin ryhmän ja tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ suhde.

Jako nurkka- ja särmäryhmiin heijastuu myös aiemmin esiteltyihin ali- ja tekijäryhmiin, ja Rubikin ryhmää voidaan siten edelleen paloitella pienempiin osiin. Todistetaan ensin eräitä yleishyödyllisiä tuloksia.



Kuva 17: Tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ asema Rubikin ryhmässä

Lemma 5.15. *Oletetaan, että aliryhmät H ja K muodostavat suoran tulon ryhmässä G ja että N normaali G:ssä. Merkitään $N_H = N \cap H$ ja $N_K = N \cap K$. Seuraavat väitteet pätevät:*

1) N_H ja N_K ovat tulon $H \times K$ normaaleja aliryhmiä.

2) Tekijäryhmät H/N_H ja K/N_K ovat isomorfisia joidenkin ryhmän G/N aliryhmien kanssa. Isomorfismeiksi voidaan lisäksi valita kuvaukset, joille pätee $hN_H \mapsto hN$ ja $kN_K \mapsto kN$.

3) Ryhmien H/N_H ja K/N_K kuvat mainitussa isomorfismissa muodostavat suoran tulon ryhmässä G/N.

Todistus. 1) Lemman 5.5 nojalla H on normaali tulossa $H \times K$. Toisaalta $H \times K$ on ryhmän G aliryhmä ja $N \trianglelefteq G$, joten N on myös normaali tulossa $H \times K$. (Jos nimittäin ${}^gH = H$ kaikilla $g \in G$, niin sama pätee myös kaikilla aliryhmän alkioilla $g \in H \times K$.) Kahden normaalin aliryhmän leikkaus on aina normaali, joten $N_H = H \cap N \trianglelefteq H \times K$. Samalla tavoin voidaan osoittaa, että $N_K \trianglelefteq H \times K$.

2) Ensinnäkin on hyvä huomata, että $N_H \trianglelefteq H$ ja $N_K \trianglelefteq K$, sillä H ja K ovat tulon $H \times K$ aliryhmiä. Osoitetaan isomorfismin olemassaolo ensin aliryhmän H tapauksessa. Olkoon $h \in H$. Jos nyt $hN_H = h'N_H$ jollain $h' \in H$, niin $h^{-1}h' \in N_H$. Erityisesti pätee $h^{-1}h' \in N$ eli $hN = h'N$. Siispä jokaista sivuluokkaa $[h] \in H/N_H$ vastaa yksikäsitteinen sivuluokka $[h] \in G/N$, joten voidaan määritellä kuvaus $\varphi : H/N_H \to G/N$, jolle pätee $\varphi(hN_H) = hN$. Tällainen kuvaus on homomorfismi, sillä kaikilla $h_1, h_2 \in H$ pätee

$$\varphi(h_1N_H) \cdot \varphi(h_2N_H) = h_1N \cdot h_2N = (h_1h_2)N = \varphi(h_1N_H \cdot h_2N_H).$$

Osoitetaan, että kuvaus φ on injektio. Oletetaan, että $h_1N = h_2N$ joillain $h_1, h_2 \in H$. Tällöin pätee $h_1^{-1}h_2 \in N$. Toisaalta H on ryhmä, joten pätee myös $h_1^{-1}h_2 \in H$. Siispä $h_1^{-1}h_2 \in N_H$ eli $h_1N_H = h_2N_H$. Kuvaus φ on siis injektiivinen homomorfismi ryhmälle G/N, joten lähtöryhmä H/N_H on isomorfinen kuvaryhmän $\mathrm{Im}(\varphi) \leq G/N$ kanssa. Toisen aliryhmän K tapauksessa todistus etenee samalla tavalla.

3) Osoitetaan, että kuvaryhmät

$$\{[h] \in G/N \mid h \in H\} \quad \text{ja} \quad \{[k] \in G/N \mid k \in K\}$$

muodostavat suoran tulon ryhmässä G/N. Olkoot $h \in H$ ja $k \in K$. Koska H ja K muodostavat suoran tulon, pätee $hk = kh$. Niinpä

$$hN \cdot kN = (hk)N = (kh)N = kN \cdot hN.$$

Lisäksi, jos $h \in H \cap K$, niin $h = e$, missä e on ryhmän G neutraalialkio. Täten mikä tahansa sivuluokka, joka kuuluu kumpaankin edellä mainituista kuvaryhmistä, on välttämättä $[e] = N$. □

Koska asentoryhmä $\mathbb{R}_a$ on Rubikin ryhmän normaali aliryhmä, ovat leikkausryhmät

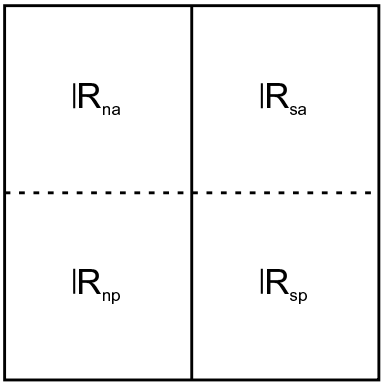
$$\mathbb{R}_{na} = \mathbb{R}_n \cap \mathbb{R}_a \quad \text{ja} \quad \mathbb{R}_{sa} = \mathbb{R}_s \cap \mathbb{R}_a$$

lemman 5.15 kohdan 1) nojalla normaaleja suorassa tulossa $\mathbb{R}_n \times \mathbb{R}_s$. Siispä niiden suhteen voidaan muodostaa tekijäryhmät

$$\mathbb{R}_{np} = \mathbb{R}_n/\mathbb{R}_{na} \quad \text{ja} \quad \mathbb{R}_{sp} = \mathbb{R}_s/\mathbb{R}_{sa}.$$

Näiden tekijäryhmien tulkinta on se, että $\mathbb{R}_{np}$:n alkiot vaihtavat vain *nurkkapalojen paikkoja* ja $\mathbb{R}_{sp}$ alkiot vain *särmäpalojen paikkoja*, niiden asennoista välittämättä. Mainitun lemman kohdan 3) nojalla nämä uudet paikkaryhmät voidaan ajatella Rubikin paikkaryhmän aliryhmiksi, jossa ne muodostavat suoran tulon.

Kuvassa 18 on kaavamaisesti esitetty tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ rakenne. Kullakin rivillä vierekkäiset ryhmät muodostavat suoran tulon. Jos siis annettu Rubikin kuution asema sisältyy tuloryhmään $\mathbb{R}_n \times \mathbb{R}_s$, niin nurkkien palat ja asemat voidaan ratkaista särmäpaloista riippumatta. Edelleen sekä nurkka- että särmäpalojen kohdalla voidaan noudattaa aikaisempaa jakoa, jossa ratkaistaan ensin palojen paikat, sitten niiden asennot. Ensin siis ratkaistaan kuviossa alarivin ryhmä, sitten sen yläpuolella oleva ryhmä. Toisinpäin eteneminen olisi mahdotonta, sillä paloilla ei voi ajatella olevan mitään "oikeita asentoja", elleivät ne ole oikeilla paikoillaan. Viimeksi mainitun seikan algebrallinen tulkinta on se, että aliryhmässä on aina neutraalialkio, mutta muissa sivuluokissa ei ole mitään tähän rinnastettavaa toisista poikkeavaa alkiota.



Kuva 18: Tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ rakenne

Itse asiassa Rubikin ryhmän paloittelua voitaisiin jatkaa samalla tavalla vieläkin pidemmälle, sillä jokaista yksittäistä palaa koskevat permutaatiot ovat riippumattomia muita paloja koskevista permutaatioista. Näin voitaisiin muodostaa eriasteisia tuloryhmiä, joissa keskityttäisiin erilaisiin palajoukkoihin, ja jakaa nämä ryhmät edelleen paikka- ja asentoryhmiin. Rubikin kuutiota ratkaistaessa voidaan saman periaatteen mukaisesti laittaa osa oikealla paikallaan olevista paloista myös oikeaan asentoon ja siirtyä vasta sen jälkeen käsittelemään muita paloja.

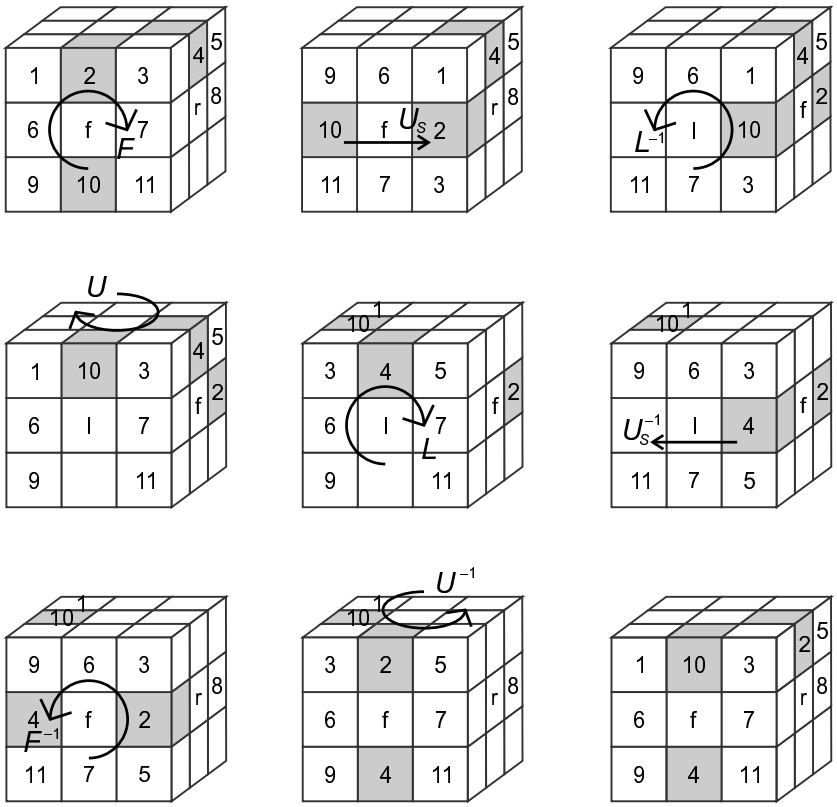
5.3 Algoritmi 2: särmäpalojen 3-sykli

Särmäpaloja kiertävä 3-sykli on samankaltainen kuin aiemmin opittu nurkkapalojen 3-sykli. Se on jälleen muotoa $\sigma\tau\sigma^{-1}\tau^{-1}$, missä σ on perussiirto U^{-1} ja τ kolmen siirron yhdistelmä $F^{-1}U_S^{-1}L$. Yhdessä näistä koostuu siis kuvassa 19 esitetty kahdeksan siirron sarja

$$U^{-1}F^{-1}U_S^{-1}LUL^{-1}U_SF.$$

Tämä siirtosarja suoritetaan tietysti oikealta vasemmalle, aloittaen siirrosta F.

Algoritmi on tässä kirjoitettu siirron U_S avulla, joka on kuution keskitahkon siirto. Tämä on tehty sen takia, että algoritmi olisi helpompi hahmottaa. Toisaalta tästä seuraa, että siirrot F ja L näyttävät nyt kuvassa molemmat pyörittävän etutahkoa, vaikka todellisuudessa kyseinen "etutahko" on kääntynyt oikealle siirron U_S vaikutuksesta siinä vaiheessa, kun käytetään siirtoa L, ja tilalle on tullut aiemmin vasemmalla sivulla ollut tahko. Kuvassa tahkoja merkitään keskipalojen kirjaimilla f, r ja l.



Kuva 19: Särmäpalojen 3-sykli

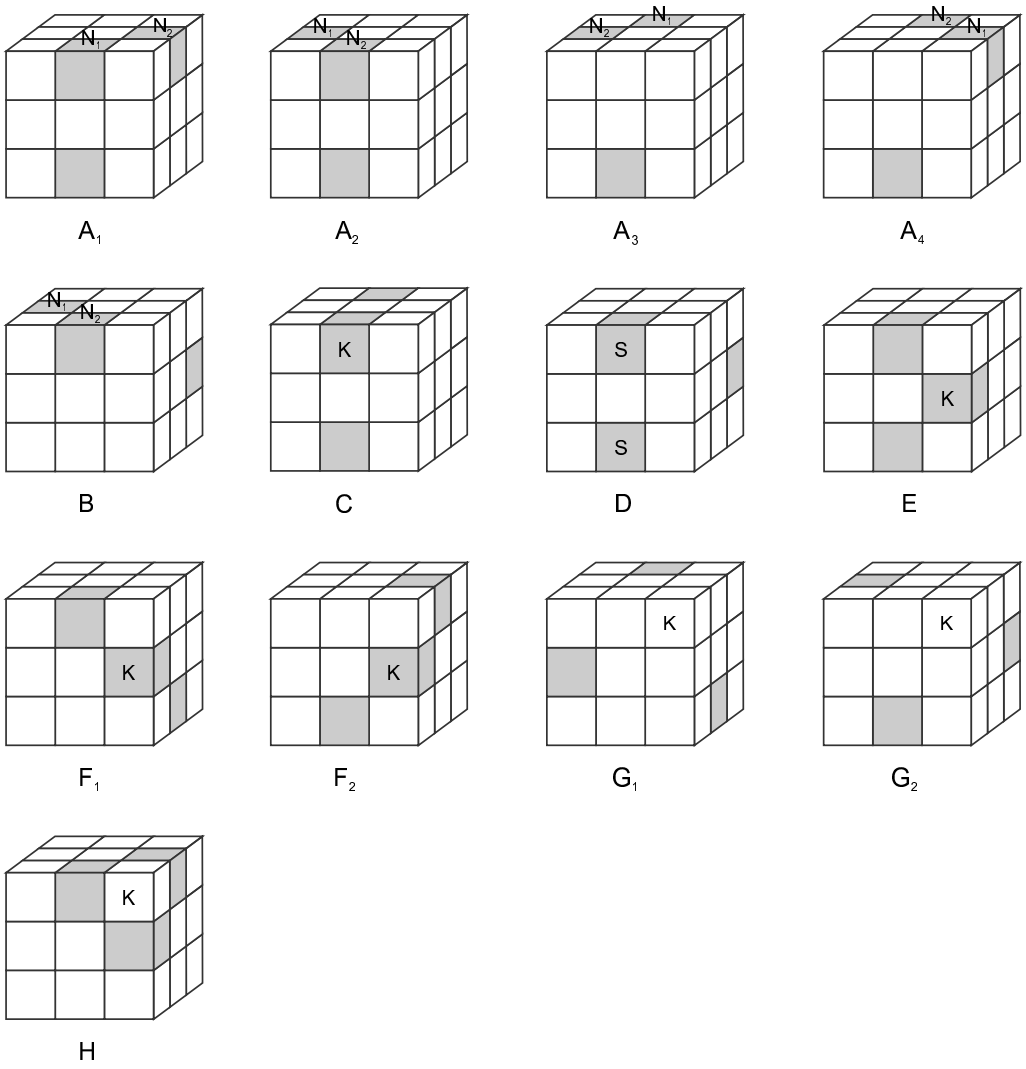
5.4 Rubikin paikkaryhmän ratkaiseminen

Tässä luvussa tarkistetaan ensin, että kaikki särmäpalojen 3-syklit ovat mahdollisia siirtoja. Sen jälkeen tutkitaan Rubikin paikkaryhmän parillisuusominaisuuksia, joita hyväksi käyttäen saadaan lopulta nurkka- ja reunapalat oikeille paikoilleen.

Käydään ensin läpi kaikki kolmen särmäpalan kombinaatiot samalla tavoin kuin aiemmin (luvussa 4.3) tehtiin nurkkapaloille. Tällä kertaa kombinaatioita tulee yhteensä $\binom{12}{3} = 220$ kappaletta, ja ne voidaan jakaa 13 joukkoon kuvan 20 mukaisesti. Kunkin joukon sisällä kombinaatiot saadaan toisistaan koko kuutiota kiertämällä.

Lasketaan kunkin edellä mainituista joukoista sisältämien kombinaatioiden lukumäärä, jotta varmistutaan siitä, että muita kombinaatioita ei ole.

A_1 Kirjaimilla N_1 ja N_2 merkityt palat voivat sijaita millä tahansa kuution kuudesta sivusta neljässä eri nurkassa. Kolmas pala on aina palaa N_1 vastapäätä. Joukossa on siis $6 \cdot 4 = 24$ kombinaatiota.



Kuva 20: Kolmen reunapalan kombinaatiot

A_2, A_3, A_4 Nämä kombinaatiot saadaan joukon A_1 kombinaatioista yksikäsitteisellä tavalla, nimittäin kiertämällä ylätahkoa kussakin tapauksessa tietyn verran. Kusakin joukossa on siis 24 kombinaatiota.

B Kirjaimilla N_1 ja N_2 merkityt palat voivat sijaita millä tahansa kuution kuudesta sivusta neljässä eri nurkassa. Kolmas pala sijaitsee vastakkaisen nurkkasärmän keskellä. Kombinaatioita on $6 \cdot 4 = 24$ kappaletta.

C Kaikki kolme palaa sijaitsevat samalla keskitahkolla. Keskitahkoja on yhteensä kolme, ja kirjaimella K merkitty pala voi olla mikä tahansa keskitahkon neljästä reunapalasta. Vaihtoehtoja on siis yhteensä $3 \cdot 4 = 12$ kappaletta.

D Kirjaimella S merkityt palat voivat sijaita vierekkäin millä tahansa kuution kolmesta keskitahkosta. Vaihtoehtoja niiden sijainnille saadaan yhteensä 12. Kolmas pala voidaan sen jälkeen valita vastakkaisen sivutahkon jommasta kummasta reunasta. Nämä vaihtoehdot saadaan toisistaan kääntämällä kuutio ylösalaisin. Kombinaatioita on siis 24.

E Kaikki palat sijaitsevat samalla sivutahkolla. Sivutahkoja on kuusi, ja kirjaimella K merkitty pala voidaan valita 4 tahkon joukosta. Kombinaatioita on siis 24.

F_1, F_2 Näissä tapauksissa kirjaimella K merkitty pala voidaan valita kunkin särmän keskeltä, ja kaikki kolme palaa määräytyvät sen mukaan. Molemmissa joukoissa on siis 12 kombinaatiota.

G_1, G_2 Kirjaimella K merkitty pala voidaan valita kunkin nurkkapalan joukosta, ja palat määräytyvät sen mukaisesti. Vastakkaisia nurkkia vastaa kuitenkin sama kombinaatio, joten näissä joukoissa on kummassakin $8/2 = 4$ kombinaatiota.

H Kirjaimella K merkitty pala voidaan valita kustakin nurkasta, ja palat sijaitsevat sen vierellä. Kombinaatioita on 8 kappaletta.

Yhteensä luetelluissa joukoissa on $7 \cdot 24 + 3 \cdot 12 + 8 + 2 \cdot 4 = 220$ kombinaatiota.

Lause 5.16. *Mikä tahansa ryhmän $\mathbb{R}_p$ 3-sykli, joka liikuttaa vain särmäpaloja, on mahdollinen siirto.*

Todistus. Kuten luvun 4.3 vastaavassa todistuksessa, jossa tarkasteltiin nurkkapalojen 3-syklejä, tässäkin riittää todistaa, että jokaista kuvassa 20 lueteltua kombinaatioiden joukkoa kohti löytyy siirto, jolla palat saadaan joukon A_1 mukaiseen perusasemaan. Tämän siirron käänteissiirrolla konjugoiminen tuottaa sitten halutun 3-syklin. Nyt tosin joudutaan kunkin kombinaatiojoukon sisällä mahdollisesti käyttämään myös keskitahkojen siirtoja, mikä johtaa siihen, että alla kuvattavien siirtojen merkinnät muuttuvat. Tämä johtuu siitä, että perussiirrot on alun perin nimetty sivujen mukaan ja sivut puolestaan tunnistetaan keskipaloista, joita joudutaan nyt ehkä siirtämään. Koska siirtojen uudelleen merkitseminen on kuitenkin vain tekninen toimenpide, se sivuutetaan tässä kokonaan.

Konjugoivan siirron käänteissiirto löytyy seuraavasti: Ensin saatetaan kuutiota kiertämällä kuutio johonkin kuvan 20 kolmestatoista asemasta, joista jokaisessa ajatellaan sinisen sivun osoittavan ylöspäin ja keltaisen sivun katsojaan päin. Jos päädyttiin asemaan A_1, siirto on valmis. Muuten suoritetaan (uudelleen nimettyjä)

perussiirtoja oheisen taulukon mukaisesti riippuen siitä, mihin asemaan päädyttiin. (Siirrot suoritetaan oikealta vasemmalle.)

asema	siirto	asema	siirto
A_2	U^{-1}	E	R
A_3	U^2	F_1	RD^{-1}
A_4	U	F_2	$F^{-1}D$
B	$U^{-1}D^{-1}R$	G_1	$UF^{-1}R^2$
C	$R^{-1}B^{-1}$	G_2	$R^{-1}U^{-1}$
D	R^{-1}	H	$RD^{-1}R^{-1}$

Kaikissa tapauksissa löytyy siirto, jonka käänteissiirrolla konjugoiminen tuottaa halutun 3-syklin. □

Osoitetaan seuraavaksi lemma, joka liittyy siirtojen parillisuuteen. Merkitään sitä varten kaikkien nurkkapalojen *paikkojen* permutaatioryhmää S_N^p ja samaten kaikkien reunapalojen paikkojen permutaatioryhmää S_S^p. Näitä ryhmiä voidaan ajatella symmetrisen ryhmän S_{20} (kaikkien palojen permutaatiot) aliryhmänä. Helposti nähdään, että nämä ryhmät muodostavat lisäksi suoran tulon ryhmässä S_{20}, sillä $\text{supp}(\nu) \cap \text{supp}(\sigma) = \emptyset$ kaikilla $\nu \in S_N^p$ ja $\sigma \in S_S^p$.

Lemma 5.17. *Jos τ on Rubikin paikkaryhmän siirto, niin sille löytyy yksikäsitteinen esitys tulona $\tau = \nu \circ \sigma$, missä $\nu \in S_N^p$ ja $\sigma \in S_S^p$. Näille permutaatioille pätee* $\text{sign}(\nu) = \text{sign}(\sigma)$.

Todistus. Koska τ on paikkaryhmän siirto, se voidaan esittää paikkaryhmän perussiirtojen $\tau_1, \ldots, \tau_n$ tulona. Kaikkien palojen permutaatioiden ryhmässä S_{20} jokainen perussiirto τ_i on puolestaan kahden erillisen 4-syklin tulo, joista toinen liikuttaa vain nurkkapaloja, toinen vain särmäpaloja. Merkitään näitä 4-syklejä $\nu_i \in S_N^p$ ja $\sigma_i \in S_S^p$. Koska ryhmät S_N^p ja S_S^p muodostavat suoran tulon, voidaan kirjoittaa $\tau_i = (\nu_i, \sigma_i)$ jokaisella i. Näin saadaan siirrolle τ esitys

$$\tau = (\nu_1, \sigma_1) \cdots (\nu_n, \sigma_n) = (\nu_1 \nu_2 \cdots \nu_n,\ \sigma_1 \sigma_2 \cdots \sigma_n).$$

Merkitään nyt $\nu = \nu_1 \cdots \nu_n$ ja $\sigma = \sigma_1 \cdots \sigma_n$. Koska kaikki siirrot ν_i ja σ_i ovat 4-syklejä, pätee

$$\text{sign}(\nu) = (-1)^n = \text{sign}(\sigma).$$

□

Jokainen Rubikin paikkaryhmän siirto $\sigma \in \mathbb{R}_p$ voidaan siis kirjoittaa muodossa $(\nu, \sigma) \in S_N^p \times S_S^p$. Jos myös ν ja σ kuuluvat paikkaryhmään $\mathbb{R}_p$, niin (ν, σ) on tuloryhmässä $\mathbb{R}_{np} \times \mathbb{R}_{sp}$. Edellisen lemman avulla saadaan nyt lause, joka mahdollistaa paikkaryhmän ratkaisemisen.

Lause 5.18. *Oletetaan, että* $\tau = (\nu, \sigma) \in \mathbb{R}_p$. *Jos* $\text{sign}(\nu) = 1$ *tai* $\text{sign}(\sigma) = 1$, *niin* ν *ja* σ *kuuluvat paikkaryhmään* $\mathbb{R}_p$. *Lisäksi tuloryhmän* $\mathbb{R}_{np} \times \mathbb{R}_{sp}$ *indeksille paikkaryhmän aliryhmänä pätee* $[\mathbb{R}_p : \mathbb{R}_{np} \times \mathbb{R}_{sp}] \leq 2$.

Todistus. Oletetaan, että $\text{sign}(\nu) = 1$ tai $\text{sign}(\sigma) = 1$. Edellisen lemman perusteella pätee tällöin $\text{sign}(\nu) = \text{sign}(\sigma) = 1$. Aiemmin on osoitettu, että kaikki nurkkapalojen 3-syklit ovat mahdollisia siirtoja, ja lauseen 3.12 mukaan jokainen parillinen permutaatio saadaan 3-syklien yhdistelmänä. Täten $\nu \in \mathbb{R}_p$, ja sama pätee myös permutaatiolle σ.

Osoitetaan sitten, että $[\mathbb{R}_p : \mathbb{R}_{np} \times \mathbb{R}_{sp}] \leq 2$. Olkoon $\pi = (\pi_1, \pi_2)$ jokin perussiirto. Oletetaan, että $\tau = (\sigma, \nu) \in \mathbb{R}_p$ ei kuulu tuloryhmään $\mathbb{R}_{np} \times \mathbb{R}_{sp}$. Todistuksen alun perusteella joko $\text{sign}(\nu) = -1$ tai $\text{sign}(\sigma) = -1$. Tällöin täytyy kuitenkin edellisen lemman mukaan olla $\text{sign}(\nu) = \text{sign}(\sigma) = -1$, ja koska perussiirrolle pätee $\text{sign}(\pi_1) = \text{sign}(\pi_2) = -1$, saadaan

$$\text{sign}(\pi_1^{-1}\nu) = 1 \quad \text{ja} \quad \text{sign}(\pi_2^{-1}\sigma) = 1.$$

Yllä osoitettiin, että tämän perusteella yhdistelmä $\pi^{-1}\tau = (\pi_1^{-1}\nu, \pi_2^{-1}\sigma)$ kuuluu tuloryhmään $\mathbb{R}_{np} \times \mathbb{R}_{sp}$, joten $\tau \in \pi \cdot (\mathbb{R}_{np} \times \mathbb{R}_{sp})$. Koska mikä tahansa tuloryhmään kuulumaton permutaatio kuuluu yhteen tiettyyn tuloryhmän sivuluokkaan, sivuluokkia voi olla korkeintaan kaksi. □

Edellisen lauseen nojalla Rubikin kuution palat saadaan oikeille paikoilleen seuraavalla tavalla:

1. Kirjoitetaan, onko ratkaistavassa asemassa nurkkapalojen (tai särmäpalojen) permutaatio parillinen. Jos ei ole, tehdään jokin perussiirto. Tämän jälkeen *sekä* nurkkien *että* särmien permutaatio on parillinen.

2. Ratkaistaan nurkat ja särmät erikseen aiemmin opittujen 3-syklien ja niiden konjugaattien avulla.

5.5 Puolisuorat tulot

Kahden aliryhmän suorassa tulossa eri aliryhmien alkiot kommutoivat keskenään. Tällöin aliryhmät ovat toisistaan riippumattomia. Ehtoa voidaan kuitenkin lieventää, jos vain halutaan kahden aliryhmän tulon olevan ryhmä eikä riippumattomuudella ole niin väliä.

Tarkastellaan kahta aliryhmää N ja H jossain ryhmässä G. Tulojoukon alkiot ovat muotoa $nh \in NH$, ja kahden tällaisen alkion tulo on $n_1h_1 \cdot n_2h_2$. Jotta tämä alkio kuuluisi edelleen joukkoon NH, riittää että toinen aliryhmistä, esimerkiksi N, on *normaali*. Tällöin nimittäin nähdään, että N:n vasemman sivuluokan alkio h_1n_2 kuuluu myös vastaavaan oikeanpuoleiseen sivuluokkaan, joten $h_1n_2 = n'h_1$ eräällä $n' \in N$. Näin ollen

$$n_1h_1 \cdot n_2h_2 = n_1n' \cdot h_1h_2 \in NH.$$

Tulojoukko on siis suljettu laskutoimituksen suhteen. Samalla tavoin nähdään myös, että käänteisalkiot ovat mukana tulojoukossa, sillä $(nh)^{-1} = h^{-1}n^{-1} = n'h^{-1}$ eräällä $n' \in N$.

Määritelmä 5.19. Ryhmän G aliryhmät N ja H muodostavat *sisäisen puolisuoran tulon*, jos seuraavat ehdot pätevät:

1) N on normaali G:ssä

2) $N \cap H = \{e\}$, missä e on ryhmän G neutraalialkio.

Puolisuoraa tuloa merkitään $NH = N \rtimes H$ tai $HN = H \ltimes N$.

Esimerkki 5.20. Alternoivalla ryhmällä A_4 on normaali aliryhmä

$$N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

Tarkastellaan tämän lisäksi 3-syklin virittämää aliryhmää $H = \{\mathrm{id}, (123), (132)\}$, joka ei ole normaali (esim. ${}^{(34)}(123) = (124) \notin A_4$). Näiden aliryhmien leikkauksessa on vain identtinen permutaatio, joten ne muodostavat puolisuoran tulon $N \rtimes H$. Kootaan kyseisen tulon alkiot taulukkoon.

$N \rtimes H$	id	(12)(34)	(13)(24)	(14)(23)
id	id	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(243)	(142)	(134)
(123)	(132)	(143)	(234)	(124)

Jokainen alternoivan ryhmän alkio esiintyy taulukossa täsmälleen kerran. Siispä $N \rtimes H = A_4$, ja jokaisella A_4:n alkiolla on yksikäsitteinen esitys tulona $n \circ h$, missä $n \in N$ ja $h \in H$.

Aivan kuten suoran tulon tapauksessa, myös puolisuorassa tulossa $N \rtimes H$ alkioiden esitykset muodossa nh ovat yksikäsitteisiä. Tämä seuraa määritelmän kohdasta 2). Kahden alkion tulon esitys saadaan seuraavasta kaavasta, joka pätee kaikissa ryhmissä:

$$n_1h_1 \cdot n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 = \underbrace{n_1{}^{h_1}n_2}_{\in N} \cdot \underbrace{h_1h_2}_{\in H}. \tag{5.21}$$

Kaavasta nähdään, että ei-normaalin ryhmän H alkiot voidaan jälleen kertoa keskenään N:n alkioista riippumatta, mutta toista normaalin aliryhmän alkiota on kerrottaessa konjugoitava ensin H:n alkiolla. Olennaista on, että konjugaatti kuuluu edelleen ryhmään N, koska N on normaali. Kyseessä on siis eräänlainen puolittainen riippumattomuus.

Huom. Jos normaali aliryhmä on tulossa oikeanpuoleisena, yllä oleva kaava tulee muotoon $h_1n_1 \cdot h_2n_2 = h_1h_2 \cdot {}^{h_2^{-1}}n_1n_2$.

Kaavan (5.21) avulla voidaan määritellä myös kahden erilaisen ryhmän *ulkoinen* puolisuora tulo. Ongelmana on vain se, että alkion n konjugointi alkiolla h ei onnistu, jos n ja h ovat eri ryhmissä. Tällainen ulkoinen konjugointi voidaan kuitenkin määritellä, kun ensin mietitään, minkälainen operaatio konjugointi itse asiassa on.

Konjugoinnissa jokaiseen ryhmän G alkioon g liitetään kuvaus $x \mapsto {}^gx$. Tämä kuvaus on ryhmän G sisäinen automorfismi eli bijektiivinen homomorfismi ryhmältä itselleen. Lisäksi konjugointi toteuttaa ns. *ryhmän toiminnan* ehdot: neutraalialkiota vastaa identtinen kuvaus $x \mapsto x$, ja alkioiden tuloa vastaa yhdistetty kuvaus, nimittäin ${}^{gh}x = {}^g\big({}^hx\big)$. Nämä ominaisuudet huomioiden voidaan määritellä ryhmän konjugointi toisessa ryhmässä.

Määritelmä 5.22. Olkoot G ja H ryhmiä. Kuvausta $g \mapsto \varphi_g$, joka liittää jokaiseen G:n alkioon g jonkin kuvauksen φ_g ryhmältä H itselleen, kutsutaan *konjugoivaksi toiminnaksi*, jos seuraavat ehdot täyttyvät:

1) kuvaus φ_g on isomorfismi (eli automorfismi) jokaisella $g \in G$

2) φ_e on identtinen kuvaus, jos e on G:n neutraalialkio

3) $\varphi_{g_1g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ kaikilla $g_1, g_2 \in G$.

Konjugoivan toiminnan käsitteen sekä kaavan (5.21) avulla voidaan määritellä kahden mielivaltaisen ryhmän puolisuora tulo.

Määritelmä 5.23. Olkoot $(N, \diamond)$ ja $(G, *)$ ryhmiä. Oletetaan, että on määritelty jokin ryhmän G konjugoiva toiminta $g \mapsto \varphi_g$ ryhmässä N. Ryhmien G ja N

ulkoinen puolisuora tulo $N \rtimes G$ muodostuu pareista (n, g), missä $n \in N$ ja $g \in G$. Laskutoimitus määritellään kaavalla

$$(n_1, g_1)(n_2, g_2) = \big(n_1 \diamond \varphi_{g_1}(n_2),\ g_1 * g_2\big).$$

Toisinpäin merkityssä puolisuorassa tulossa $G \ltimes N$ laskutoimitus on vastaavasti

$$(g_1, n_1)(g_2, n_2) = \big(g_1 * g_2,\ \varphi_{g_2}^{-1}(n_1) \diamond n_2\big).$$

Tuloa voidaan merkitä myös ulkoisuutta korostaen $(N \rtimes G)_u$ tai $(G \ltimes N)_u$.

Huom. Ulkoisen suoran tulon rakenne riippuu valitusta konjugoivasta toiminnasta. Toiminnaksi voidaan aina valita $\varphi_g = \mathrm{id}$ kaikilla g, jolloin puolisuorasta tulosta tulee suora tulo. Eri valinnat tuottavat kuitenkin erilaisen tulon.

Toisin kuin suoran tulon tapauksessa, ulkoisesta puolisuorasta tulosta on vaikea äkkiseltään nähdä, että se todella on ryhmä. Todistetaan tämä seuraavaksi.

Lause 5.24. *Ryhmien* $(N, \diamond)$ *ja* $(H, *)$ *puolisuora tulo on ryhmä.*

Todistus. Puolisuora tulo on suljettu laskutoimituksen suhteen, koska konjugaatti $\varphi_{g_1}(n_2)$ on ryhmän N alkio ja siten tulo $n_1 \diamond \varphi_{g_1}(n_2)$ kuuluu ryhmään N. Tarkistetaan ryhmän aksioomat.

1) Laskutoimitus on liitännäinen, sillä kaikilla $n_1, n_2, n_3 \in N$ ja $g_1, g_2, g_3 \in G$ pätee

$$\begin{aligned}
\big((n_1, g_1)(n_2, g_2)\big)(n_3, g_3) &= \big(n_1 \diamond \varphi_{g_1}(n_2),\ g_1 * g_2\big)(n_3, g_3) \\
&= \big(n_1 \diamond \varphi_{g_1}(n_2) \diamond \varphi_{g_1 * g_2}(n_3),\ g_1 * g_2 * g_3\big) \\
&= \big(n_1 \diamond \varphi_{g_1}(n_2) \diamond \varphi_{g_1}(\varphi_{g_2}(n_3)),\ g_1 * g_2 * g_3\big) \\
&= \big(n_1 \diamond \varphi_{g_1}(n_2 \diamond \varphi_{g_2}(n_3),\ g_1 * g_2 * g_3\big) \\
&= (n_1, g_1)\big(n_2 \diamond \varphi_{g_2}(n_3),\ g_2 * g_3\big) \\
&= (n_1, g_1)\big(n_2, g_2)(n_3, g_3)\big).
\end{aligned}$$

Tässä käytettiin hyväksi muun muassa niitä tietoja, että $\varphi_g(n_1 n_2) = \varphi_g(n_1)\varphi_g(n_2)$ ja $\varphi_{g_1 g_2}(n) = \varphi_{g_1}(\varphi_{g_2}(n))$.

2) Puolisuoran tulon neutraalialkio on pari (e_N, e_G), missä e_N on N:n neutraalialkio ja e_G on G:n. Kaikilla $n \in N$ ja $g \in G$ nimittäin pätee

$$(e_N, e_G)(n, g) = (e_N \diamond \varphi_{e_N}(n),\ e_G * g) = (e_N \diamond n,\ g) = (n, g)$$

ja

$$(n, g)(e_N, e_G) = (n \diamond \varphi_g(e_N),\ g * e_G) = (n \diamond e_N,\ g) = (n, g).$$

Yllä käytettiin tietoja $\varphi_{e_N} = \mathrm{id}$ ja $\varphi_g(e_N) = e_N$ (homomorfismi).

3) Alkion (n, g) käänteisalkio puolisuorassa tulossa on $(\varphi_{g^{-1}}(n^{-1}),\, g^{-1})$, sillä

$$\begin{aligned}\big(\varphi_{g^{-1}}(n^{-1}),\, g^{-1}\big)\,(n, g) &= \big(\varphi_{g^{-1}}(n^{-1}) \diamond \varphi_{g^{-1}}(n),\, g^{-1} * g\big) \\ &= \big(\varphi_{g^{-1}}(n^{-1} \diamond n),\, e_G\big) = (\varphi_{g^{-1}}(e_N),\, e_G) \\ &= (e_N,\, e_G)\end{aligned}$$

ja

$$\begin{aligned}(n, g)\,\big(\varphi_{g^{-1}}(n^{-1}),\, g^{-1}\big) &= \big(n \diamond \varphi_g(\varphi_{g^{-1}}(n^{-1})),\, g * g^{-1}\big) \\ &= \big(n \diamond \varphi_{g*g^{-1}}(n^{-1}),\, e_G\big) = \big(n \diamond \varphi_{e_G}(n^{-1}),\, e_G\big) \\ &= \big(n \diamond n^{-1},\, e_G\big) = (e_N, e_G).\end{aligned}$$

Nyt on osoitettu, että puolisuora tulo $N \rtimes G$ on ryhmä. Tapaus $G \ltimes N$ voidaan käsitellä samalla tavalla. Tuossa tapauksessa käänteisalkioksi tulee $(g^{-1},\, \varphi_g(n^{-1}))$. □

Esimerkki 5.25. Tarkastellaan neliön symmetriaryhmän aliryhmää

$$N = \{\mathrm{id}, \pi, \rho^2, \pi \circ \rho^2\},$$

missä π on peilaus pystyakselin suhteen, ρ^2 kierto puolirympyrän verran, ja $\pi \circ \rho^2$ peilaus vaaka-akselin suhteen (vrt. esimerkki 4.9. Tämä ryhmä on vaihdannainen, ja sen kertotaulu näyttää seuraavalta:

$\circ$	id	π	ρ^2	$\pi \circ \rho^2$
id	id	π	ρ^2	$\pi \circ \rho^2$
π	π	id	$\pi \circ \rho^2$	ρ^2
ρ^2	ρ^2	$\pi \circ \rho^2$	id	π
$\pi \circ \rho^2$	$\pi \circ \rho^2$	ρ^2	π	id

.

Muodostetaan nyt ryhmän N puolisuora tulo ryhmän $\mathbb{Z}_3 = \{[0], [2], [3]\}$ kanssa. Sitä varten on ensin määriteltävä ryhmän $\mathbb{Z}_3$ konjugoiva toiminta ryhmässä N.

Konjugoivan toiminnan määritelmän mukaan täytyy olla $\varphi_0 = \mathrm{id}$, ja $\varphi_2 = \varphi_{1+1} = \varphi_1 \circ \varphi_1$. Tarvitsee siis valita vain alkiota $[1] \in \mathbb{Z}_3$ vastaava homomorfismi φ_1. Määritellään se seuraavan taulukon mukaisesti:

σ	id	π	ρ^2	$\pi \circ \rho^2$
$\varphi_1(\sigma)$	id	ρ^2	$\pi \circ \rho^2$	π

.

Taulukosta nähdään suoraan, että φ_1 on bijektio. Homomorfisuuden tarkistamiseksi pitäisi tarkistaa kaikki tulot $\varphi_1(\sigma) \circ \varphi_1(\tau)$, joissa σ ja τ ovat N:n identtisestä poikkeavia permutaatioita. Tyydytään tässä tarkistamaan vain yksi:

$$\varphi(\pi) \circ \varphi(\rho^2) = \rho^2 \circ (\pi \circ \rho^2) = \pi = \varphi(\pi \circ \rho^2).$$

Koska φ_1 on isomorfismi, myös φ_2 on. Lisäksi voidaan helposti varmistua myös siitä, että

$$\varphi_0(\sigma) = \varphi_{1+1+1}(\sigma) = \varphi(\varphi(\varphi(\sigma))) = \mathrm{id}(\sigma)$$

kaikilla $\sigma \in N$. Konjugoiva toiminta voidaan siis määritellä edellä kuvatulla tavalla, ja niinpä voidaan määritellä myös tätä toimintaa vastaava puolisuora tulo $N \rtimes \mathbb{Z}_3$.

Lasketaan lopuksi esimerkin vuoksi alkioiden kertaluvut ryhmässä $N \rtimes \mathbb{Z}_3$. Kaikilla $\sigma \in N$ pätee

$$(\sigma, 0)(\sigma, 0) = (\sigma \circ \varphi_0(\sigma), 0 + 0) = (\sigma \circ \sigma, 0) = (\mathrm{id}, 0),$$

sillä kaikkien N:n alkioiden kertaluku on 2. Muotoa $(\sigma, 0)$ olevien alkioiden kertaluku on siis kaksi (paitsi neutraalialkion $(\mathrm{id}, 0)$).

Olkoot sitten $\sigma \in N$ ja $k \neq 0$. Tällöin

$$(\sigma, k)(\sigma, k) = (\sigma \circ \varphi_k(\sigma), k + k) = (\sigma \circ \varphi_k(\sigma), 2k).$$

Saatu alkio ei ole neutraalialkio, koska $2k$ on nollasta poikkeava kaikilla $k \in \mathbb{Z}_3$. Toisaalta

$$\begin{aligned}(\sigma, k)^3 &= (\sigma \circ \varphi_k(\sigma), 2k)(\sigma, k) = (\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma), 2k + k) \\ &= (\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma), 0).\end{aligned}$$

Jos viimeisessä lausekkeessa $\sigma = \mathrm{id}$, niin tulo $\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma)$ on kolmen identtisen permutaation tulo. Jos taas $\sigma \neq \mathrm{id}$, niin kyseisessä tulossa on kolme eri identtisestä poikkeavaa permutaatiota. Molemmissa tapauksissa tulo on identtinen kuvaus, joten $(\sigma, k)^3$ on neutraalialkio. Siis jos $k \neq 0$, niin alkion (σ, k) kertaluku on kolme.

Tarkempi tutkimus osoittaisi, että puolisuora tulo $N \rtimes \mathbb{Z}_3$ on itse asiassa isomorfinen ryhmän A_{12} kanssa.

6 Kommutaattorit

Alkioiden kommutaattori on niiden vaihdannaisuuden mitta. Toisaalta kommutaattoreita voidaan käyttää hyväksi etsittäessä ryhmästä tietynlaisia alkioita.

6.1 Kommutaattorien perusominaisuudet

Jos alkiot g ja h eivät ole keskenään vaihdannaisia, eli ne eivät *kommutoi* keskenään, tulot gh ja hg eroavat toisistaan jollain tavoin. Tällöin löytyy jokin alkio r, jolle pätee $gh = r \cdot hg$. Tämä luku r ilmaisee ikään kuin eri päin laskettujen tulojen välisen suhteen.

Määritelmä 6.1. Olkoot g ja h ryhmän G alkioita. Yhdistelmää

$$[g,h] = (gh)(hg)^{-1} = ghg^{-1}h^{-1} \in G$$

kutsutaan alkioiden g ja h *kommutaattoriksi.*

Alkiot g ja h kommutoivat, jos ja vain jos niiden kommutaattori on neutraalialkio. Kommutaattorilla ja konjugaatilla on selvä yhteys, joka ilmenee esimerkiksi kaavoissa

$$[g,h] = {}^{g}h \cdot h^{-1} \quad \text{ja} \quad [g,h] = g \cdot {}^{h}\big(g^{-1}\big).$$

Lisäksi seuraavat kaavat ovat kommutaattoreita käsiteltäessä hyödyllisiä:

$$[g,h] \cdot g = g \cdot [h,g^{-1}] \quad \text{ja} \quad [g,h] \cdot h = h \cdot [h^{-1},g].$$

On myös muistettava, että alkioiden kommutaattori ei ole symmetrinen, vaan $[g,h] = [h,g]^{-1}$.

Esimerkki 6.2. Lasketaan permutaatioiden $\sigma = (123)(45)$ ja $\tau = (2345)$ kommutaattori ryhmässä S_5:

$$[\sigma,\tau] = {}^{\sigma}\tau \cdot \tau^{-1} = {}^{(123)(45)}(2345) \circ (2345)^{-1} = (3154) \circ (5432) = (15324).$$

Kommutaattorista tuli 5-sykli, johon osallistuvat kaikki perusjoukon luvut. Voidaan ajatella, että tämä 5-sykli on "verraten suuri" alkio ryhmässä S_5, mikä tarkoittaa sitä, että permutaatiot σ ja τ kommutoivat hyvin heikosti keskenään.

Paitsi, että kommutaattoreita voi käyttää mittaamaan alkioiden välistä kommutointia, niitä voi käyttää myös *tuottamaan* erityisen suuria tai pieniä alkioita. Jos nimittäin löydetään alkiot, jotka näyttävät olevan lähes vaihdannaisia keskenään, niiden kommutaattoriksi saadaan mitä luultavimmin hyvin pieni alkio. Alkion "suuruus" tai "pienuus" ei sinänsä ole yleensä ryhmässä selvästi määriteltyä, mutta jos ryhmä koostuu johonkin joukkoon vaikuttavista alkioista, kuten permutaatioista, pieni alkio on sellainen, joka vaikuttaa joukkoon mahdollisimman vähän.

Esimerkiksi kaksi permutaatiota kommutoivat keskenään varmasti, jos ne vaikuttavat kokonaan eri alkioihin. Mitä vähemmän on yhteisiä alkioita, joihin kummatkin vaikuttavat, sitä enemmän permutaatiot kommutoivat ja sitä pienempi on niiden kommutaattori. Kuitenkin jokainen kommutaattori on välttämättä parillinen permutaatio, ja pienin parillinen permutaatio on 3-sykli.

Lause 6.3. *Olkoot σ ja τ jonkin joukon X permutaatioita. Jos kantajien leikkaukselle pätee* $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \{x\}$ *jollain $x \in X$, niin*

$$[\sigma,\tau] = \big(x\ \sigma(x)\ \tau(x)\big).$$

Todistus. Näytetään ensin, että ehdosta $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \{x\}$ seuraa aina $[\sigma, \tau](x) = \sigma(x)$. Huomaa, että permutaation τ kantaja sisältää täsmälleen samat alkiot kuin käänteiskuvauksen τ^{-1} kantaja. Siispä $\tau(x)$ kuuluu aina σ:n kantajaan. Toisaalta esimerkiksi $\tau(x) \neq x$, joten $\tau(x) \notin \mathrm{supp}(\sigma)$. Nyt saadaan

$$[\sigma, \tau](x) = \sigma\tau\sigma^{-1} \underbrace{\tau^{-1}(x)}_{\notin \mathrm{supp}(\sigma)} = \sigma\tau\tau^{-1}(x) = \sigma(x).$$

Saadun tuloksen sekä aiemmin mainittujen kaavojen perusteella pätee myös

$$[\sigma, \tau](\sigma(x)) = \left(\sigma \circ [\tau, \sigma^{-1}]\right)(x) = \sigma(\tau(x)) = \tau(x)$$

ja

$$[\sigma, \tau](\tau(x)) = \left(\tau \circ [\tau^{-1}, \sigma]\right)(x) = \tau(\tau^{-1}(x)) = x.$$

Yllä nähtiin, että permutaatio $[\sigma, \tau]$ sisältää ainakin 3-syklin $(x\ \sigma(x)\ \tau(x))$. Jäljelle jää tarkistaa, mitä tapahtuu, jos $y \notin \{x, \sigma(x), \tau(x)\}$. Tällöin voidaan tarkastella kolmea vaihtoehtoa. Jos y ei ole σ:n eikä τ:n kantajassa, niin selvästikin $[\sigma, \tau](y) = y$. Jos taas $y \in \mathrm{supp}(\sigma)$, niin y ei voi olla samalla τ:n kantajassa (koska $y \neq x$), joten

$$[\sigma, \tau](y) = \sigma\tau\sigma^{-1}\tau^{-1}(y) = \sigma\tau \underbrace{\sigma^{-1}(y)}_{\neq x} = \sigma\sigma^{-1}(y) = y.$$

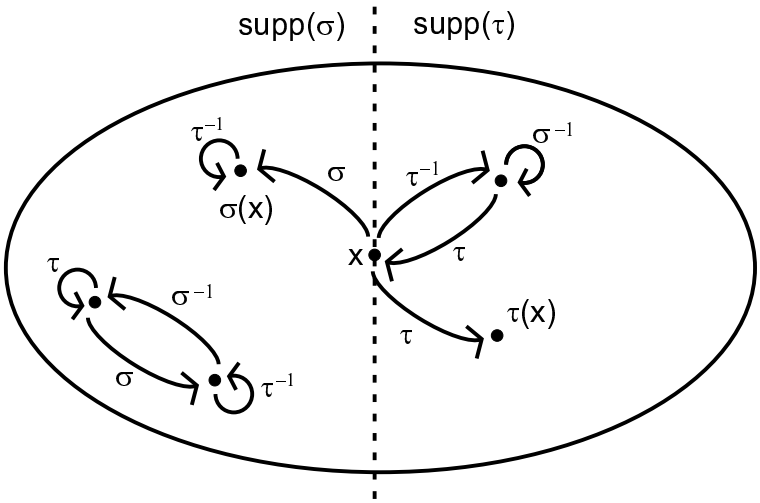
Edelleen, jos $y \in \mathrm{supp}(\tau)$, niin

$$[\sigma, \tau](y) = \sigma\tau\sigma^{-1} \underbrace{\tau^{-1}(y)}_{\neq x} = \sigma\tau\tau^{-1}(y) = \sigma(y) = y.$$

Nähtiin, että aiemmin löydetyn 3-syklin ulkopuoliset alkiot pysyvät paikallaan, joten kommutaattori on juuri tuo mainittu 3-sykli. □

6.2 Kommutaattorit Rubikin ryhmässä

Rubikin kuution ratkaisemisessa keskeinen ongelma on, että perussiirrot liikuttavat niin suurta osaa kuution ruuduista. Kun yksi perussiirto liikuttaa 20 ruutua 48:sta, on hyvin vaikea seurata, mihin kukin ruutu ajautuu. Kommutaattoreita voi tässä yhteydessä käyttää tehokkaasti hyödyksi, sillä niiden avulla saadaan tuotettua siirtoja, jotka liikuttavat paljon pienempää osaa kuutiosta kerrallaan.



Kuva 21: Miten kommutaattorista tulee 3-sykli

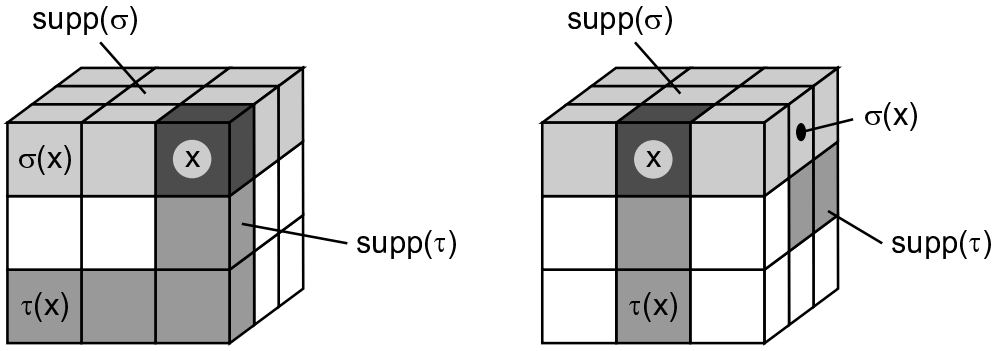
Tarkastellaan ensin tilannetta Rubikin paikkaryhmässä. Lauseen 6.3 mukaan voidaan tuottaa kolmen palan sykli, jos vain löydetään kaksi siirtoa, joiden yhteisen vaikutuksen piiriin kuuluu ainoastaan yksi pala. Yritetään saada tämä aikaan nurkkapaloilla niin, että tuloksena olisi luvussa 3.3 opittu nurkkapalojen 3-sykli.

Koska lauseen 6.3 mukaan siirtojen σ ja τ kommutaattorina on mahdollista saada 3-sykli $(x\ \sigma(x)\ \tau(x))$, on järjestettävä niin, että σ siirtää etutahkon oikeassa yläkulmassa olevan palan vasempaan yläkulmaan, ja τ siirtää saman palan vasempaan alakulmaan (ks. kuva 22). Siirroksi σ voidaan valita vaikkapa ylätahkon pyöritys U. Tämän jälkeen siirron τ on kuitenkin oltava sellainen, että se ei liikuta muita ylätahkon paloja kuin palaa x. Tämä saadaan aikaan *konjugoimalla* alatahkon pyöritys D^{-1}, joka ei liikuta ylätahkoa, sellaisella siirrolla, joka siirtää oikeassa alakulmassa olevan palan x:n paikalle. Näin saadaan siirroksi τ lopulta konjugaatti ${}^{R}D^{-1} = RD^{-1}R^{-1}$.

Särmäpalojen kohdalla tilanne on samanlainen. Opitussa siirtosarjassa siirtoa σ vastaa ylätahkon kierto U^{-1}. Siirron τ pitäisi nyt siirtää pala x alarivin keskipalan paikalle (ks. kuva 22) ilman että ylätahkon palan liikkuvat. Tämä onnistuu konjugoimalla etutahkon kierrolla pystysuoran keskirivin paikalle vaakasuora. Tällöin haluttu siirto muuttuu vaakasuoran keskitahkon siirroksi, joka puolestaan ei koske ylätahkoon.

Tilanne on nyt kuitenkin hieman mutkikkaampi kuin nurkkapalojen tapauksessa, sillä keskitahkon siirtämisen on alun perin tulkittu tarkoittavan rinnakkaisten sivutahkojen liikettä. Vaakasuoran keskitahkon kiertäminen siis liikuttaa oikeastaan myös ylätahkon paloja, mikä ei ollut tarkoitus. Tässä yhteydessä onkin parempi sallia hetkeksi keskitahkojen pyöritykset omiksi siirroikseen, jotka pitävät

sivutahkojen palat paikallaan, jotta päästään käyttämään lausetta 6.3. Sen nojalla tässäkin tapauksessa saadaan 3-sykli, vaikka tilannetta tulkittiinkin totutusta poikkeavalla tavalla. Lopuksi voidaan sitten nimetä käytetyt siirrot oikeaoppisesti, jolloin siirrosta τ tulee tavallisen konjugaatin sijaan yhdistelmä $\tau = F^{-1}U_S^{-1}L$.



Kuva 22: Paikkaryhmän 3-syklien muodostaminen

Asentoryhmässä 3-syklejä tuottavan lauseen käyttäminen ei kuitenkaan onnistu. Koska yhden ruudun liikkuessa liikkuvat samalla kaikki saman palan ruudut, ei kahden permutaation kantajien leikkaus voi olla yksiö. Merkitään tässä yhteydessä sitä palaa, johon ruutu x kuuluu, symbolilla P_x, ja tuon palan kaikkien ruutujen joukkoa symbolilla R_x. Jos siis kaksi siirtoa vaikuttavat molemmat ruutuun x, niiden yhteinen vaikutusalue voi olla pienimmillään joukko R_x. Niinpä tällaisten siirtojen kommutaattori on pienin löydettävissä oleva kommutaattori.

Tarkastellaan seuraavaksi, minkälaiset siirrot voitaisiin valita, jotta saataisiin kantajien leikkaukseksi joukko R_x ja siirtojen kommutaattorista tulisi asentoryhmän siirto. Jos kumpikaan siirto ei liikuta palaa P_x, ne ovat molemmat tuon palan ruutuihin rajoitettuina syklejä. Tällaiset siirrot kommutoivat keskenään palan P_x kohdalla, joten niiden kommutaattori ei liikuta lainkaan kyseisen palan ruutuja. Jos taas molemmat siirrot liikuttavat palaa P_x, tilanne palautuu takaisin paikkaryhmään. Tuloksena on tällöin palojen 3-sykli, joka ei kuulu asentoryhmään. Ainoa jäljellä oleva vaihtoehto on, että toinen siirroista liikuttaa palaa P_x ja toinen ainoastaan vaihtaa sen ruutujen järjestystä. Tällaisessa tilanteessa syntyvä kommutaattori kuuluu asentoryhmään, mikä voitaisiin haluttaessa myös helposti todistaa.

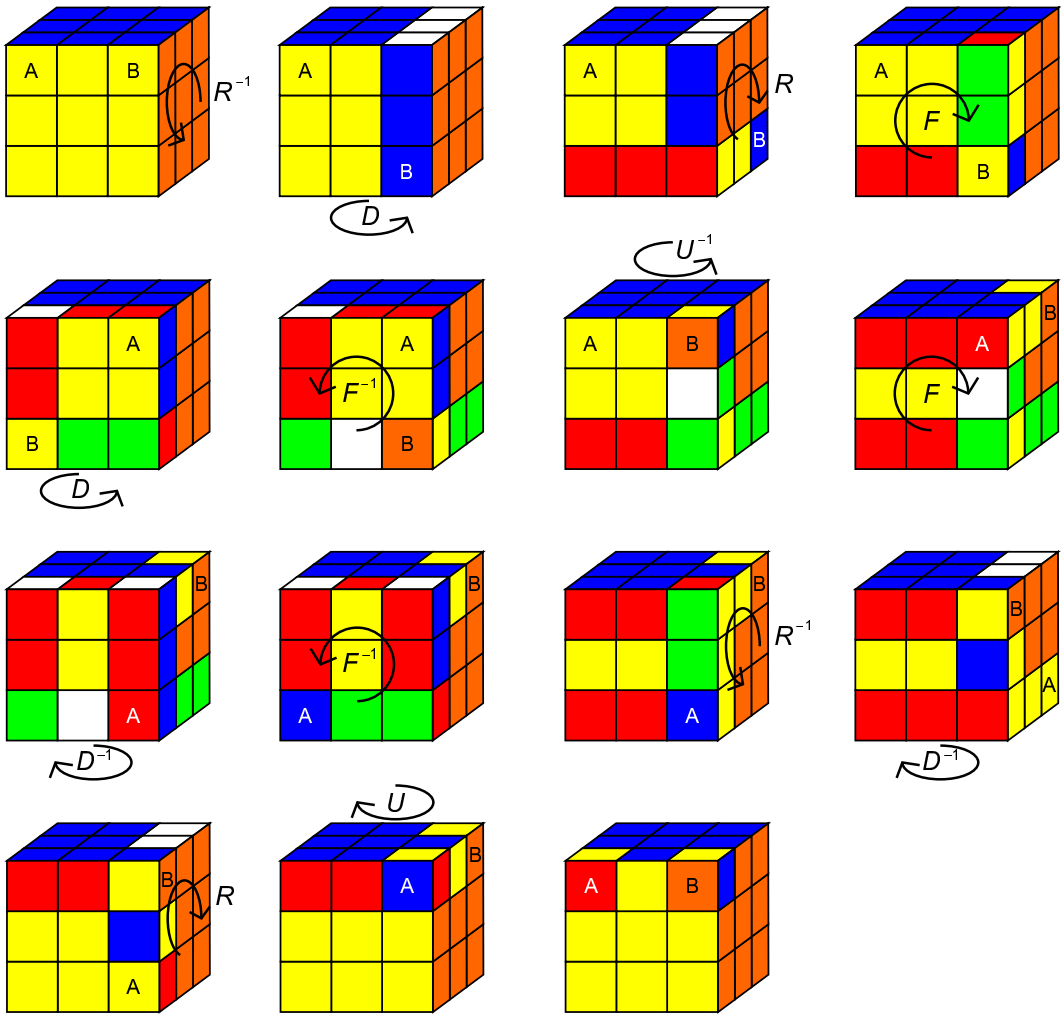
6.3 Algoritmi 3: nurkkapalojen kierto

Nurkkapalojen kierron tuottava siirtosarjan muodostaminen perustuu luvun 6.2 päätelmiin. Siirtosarja on kahden siirron kommutaattori, joista toinen kiertää nurk-

kapalaa ja toinen siirtää sitä paikaltaan. Siirtävä permutaatio σ on tässäkin algoritmissa ylätahkon kierto U. Kiertävä permutaatio puolestaan on yhdistelmä $\tau = RD^{-1}R^{-1}F^{-1}D^{-1}F$. Näistä muodostuu kommutaattori

$$[\sigma, \tau] = URD^{-1}R^{-1}F^{-1}D^{-1}FU^{-1}F^{-1}DFRDR^{-1}.$$

Tämä siirtosarja, joka on esitetty kuvassa 23, kiertää kahta vierekkäistä nurkkapalaa A ja B vastakkaisiin suuntiin. Pala A kiertyy vastapäivään ja pala B myötäpäivään.



Kuva 23: Nurkkapalojen kierto

Siirtosarjan voi hahmottaa esimerkiksi seuraavasti: Ensin kierretään palaa B myötäpäivään, jolloin kuution kaksi alinta tahkoa voivat sekoittua miten hyvänsä.

Sen jälkeen siirretään pala A palan B paikalle alempiin tahkoihin koskematta ja suoritetaan aiemmat siirrot uudestaan päinvastaisessa järjestyksessä. Nämä siirrot kiertävät nyt palaa A vastapäivään ja asettavat samalla kuution alaosan uudelleen järjestykseen. Lopuksi käännetään palat A ja B alkuperäisille paikoilleen.

Siirto τ, joka kiertää oikeassa ylänurkassa olevaa palaa, on puolestaan helpointa hahmottaa kahdessa osassa. Molemmat osat ovat samanlaisia konjugaattimuotoisia siirtoja; toinen koskee kuution etutahkoa, toinen oikeanpuoleista sivutahkoa.

6.4 Algoritmi 4: särmäpalojen kierto

Särmäpalojen kierto on samantapainen kommutaattori kuin nurkkapalojen kierto. Särmäpalaa siirtävä permutaatio σ on edelleen ylätahkon kierto U. Särmäpalan kääntävä permutaatio saadaan yhdistelmästä $\tau = RU_S B^{-2} U_S^{-2} F$. Koko siirtosarja on kommutaattori

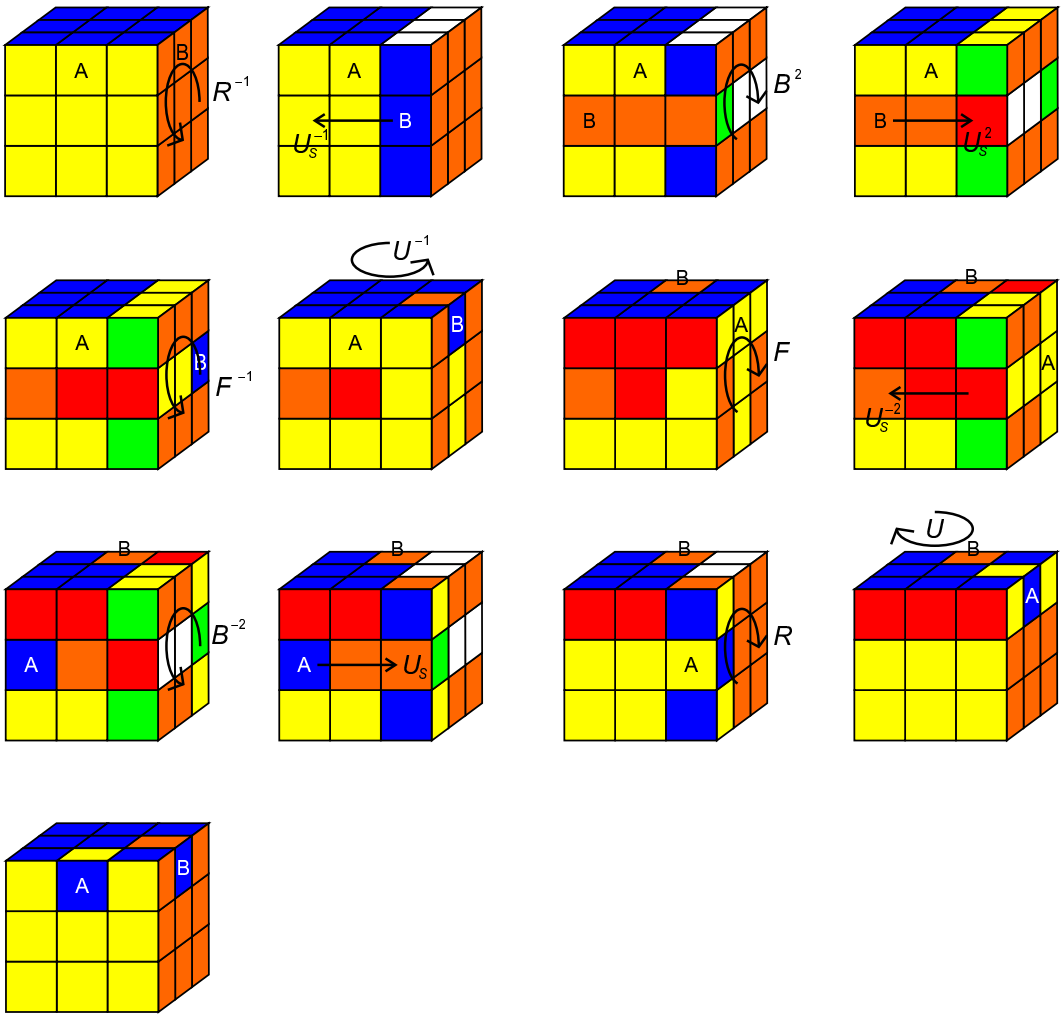
$$[\sigma, \tau] = URU_S B^{-2} U_S^{-2} F U^{-1} F^{-1} U_S^2 B^2 U_S^{-1} R^{-1}.$$

Tämä siirtosarja on esitetty kuvassa 24. Se kääntää ympäri kaksi vierekkäisillä reunoilla sijaitsevaa särmäpalaa (palat A ja B).

Siirtosarja perustuu siihen, että palan B ruudut ovat ainoat ruudut, joihin sekä σ että τ vaikuttavat. Näiden siirtojen kommutaattorista tulee siksi pieni ja helposti hallittava. Tarkalleen ottaen siirrot tosin vaikuttavat useampiinkin yhteisiin ruutuihin, koska keskitahkon kääntämisen ajatellaan liikuttavan myös ylätahkoa. Tässä kuitenkin luovutaan hetkeksi siitä ajattelutavasta, niin kuin tehtiin myös luvussa 6.2 särmäpalojen 3-sykliä tarkasteltaessa. Algoritmin siirrot on kuitenkin nimetty alkuperäisiä merkintöjä noudattaen. Esimerkiksi kolmanneksi suoritettava oikean sivutahkon 180 asteen kierto on nimeltään B^2, koska valkoisen keskipalan perusteella kyse on sillä hetkellä valkoisesta sivutahkosta.

6.5 Rubikin asentoryhmän ratkaiseminen

Edellisissä luvuissa on opittu siirtosarjoja, joiden avulla nurkka- tai reunapaloja on mahdollista kiertää paikallaan niin, että yhden palan kiertyessä yhteen suuntaan jokin toinen pala kiertyy samalla päinvastaiseen suuntaan. Tällöin palojen *kokonaiskiertymä* säilyy. Jotta saataisiin kaikki palat oikeaan asentoon, täytyy tutkia, mitä tuolle kokonaiskiertymälle tapahtuu erilaisissa siirroissa. Koska opitut algoritmit eivät muuta kokonaiskiertymää, olisi toivottavaa, että se säilyisi aina samana kaikissa asemissa, joissa palat ovat oikealla paikallaan.



Kuva 24: Särmäpalojen kierto

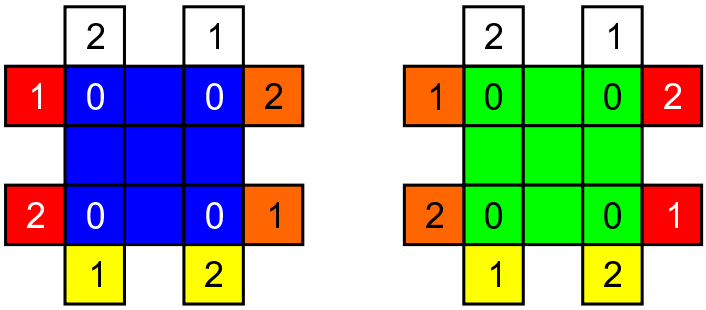
Sellaisisa ominaisuuksia, jotka säilyvät kaikissa tilanteissa, kutsutaan *invarianteiksi*. Invariantteja käytetään runsaasti esimerkiksi pelien ja algoritmien analysoinnissa. Tällä kurssilla on jo löydetty joitakin tällaisia invariantteja. Esimerkiksi jokainen paikkaryhmän siirto voidaan ilmoittaa muodossa $\nu \circ \sigma$, missä ν on nurkkiin ja σ paikkoihin kohdistuva permutaatio (jotka eivät itse välttämättä sisälly $\mathbb{R}_p$:hen). Lemmassa 5.17 osoitettiin, että $\text{sign}(\nu) \cdot \text{sign}(\sigma) = 1$ kaikissa mahdollisissa asemissa, joten tämä etumerkkien tulo on invariantti.

Vaikka jokin ominaisuus ei säilyisi aivan kaikissa tilanteissa, on yleensä hyötyä tarkastella, missä tilanteissa kyseinen ominaisuus kuitenkin säilyy. Paikkaryhmän siirroista tiedetään, että jos ne ilmoitetaan edellä kuvatussa muodossa, $\text{sign}(\nu)$ voi olla 1 tai -1. Perussiirrot kuitenkin vaihtavat tuon etumerkin, joten halut-

taessa siirtyä toisesta tilasta toiseen minkä tahansa perussiirron tekeminen riittää. Voidaankin sanoa, että sign(ν) on invariantti, jos siirroiksi sallitaan vain kahden perussiirron yhdistelmät.

Peleissä ja algoritmeissa jonkin ominaisuuden invarianssin osoittamiseksi on yleensä yksinkertaisinta näyttää, että kyseinen ominaisuus säilyy algoritmin perusaskelissa. Tämä lähestymistapa tuottaa kuitenkin ongelmia Rubikin asentojen ryhmässä, koska kuution perussiirrot eivät sisälly asentoryhmään. Jos palat ovat oikeilla paikoillaan mutta väärissä asennoissa, mistä tiedetään, miten sarja perussiirtoja vaikuttaa palojen kokonaiskiertymään? Perussiirto vie palat väärille paikoille, joissa niiden kiertymä menettää merkityksensä.

Asian ratkaisemiseksi määritellään jokaiselle palalle kiertymän käsite erikseen jokaisessa paikassa, missä pala voi olla. Tämä määrittely voidaan tehdä lähes miten tahansa, koska väärässä paikassa olevalla palalla ei ole mitään tiettyä oikeaa asentoa, vaan jokainen asento on sille samanarvoinen. Aloitetaan antamalla jokaisen nurkkapalan ruuduille numerointi kuvan 25 osoittamalla tavalla. Kuvassa on perusasemassa oleva kuutio kuvattu ylä- ja alapuolelta niin, että nurkkapalat on ikään kuin taiteltu auki.



Kuva 25: Nurkkapalojen numerointi

Kuvatussa numeroinnissa jokainen nurkkaruutu tulee numeroiduksi jollain luvuista 0, 1 ja 2. Laskujen yksinkertaistamiseksi ajatellaan, että nämä ovat syklisen ryhmän $\mathbb{Z}_3$ alkioita. Tällöin voidaan nimittäin sanoa, että jos ruudulla x on numero n, niin saman palan muiden ruutujen numerot ovat nurkan ympäri myötäpäivään kierrettäessä $n+1$ ja $n+2$.

Seuraavaksi merkitään ne ruutujen paikat, joissa on perusasemassa 0-ruutu. Tämä tarkoittaa sitä, että ajatellaan merkityiksi kaikki sinisen ja vihreän sivun nurkkaruutujen paikat riippumatta siitä, mikä ruutu niissä milloinkin sattuu olemaan. Jokaisesta palasta on aina täsmälleen yksi ruutu merkityllä paikalla. Näiden merkkien avulla voidaan määritellä nurkkapalojen kiertymät.

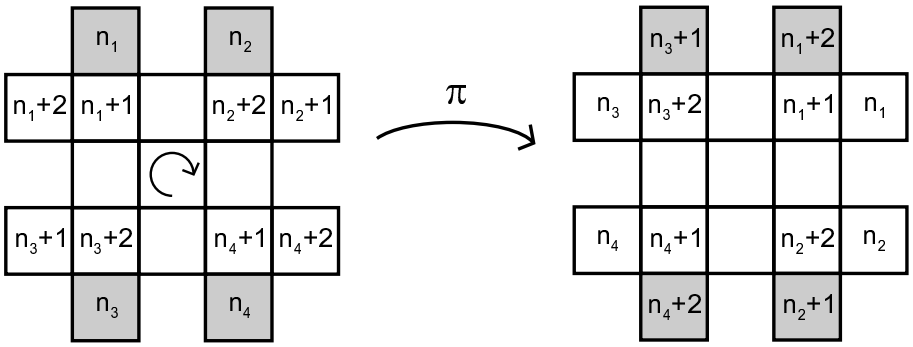
Määritelmä 6.4. Tarkastellaan palan x ruutuja asemassa σ. Palan kiertymä $k_x(\sigma) \in \mathbb{Z}_3$ on sen ruudun numero, joka sattuu olemaan kyseisessä asemassa jollakin merkityistä paikoista. Aseman σ kokonaiskiertymä on kaikkien palojen kiertymien summa, ja sitä merkitään $K_n(\sigma) = \sum_x k_x(\sigma)$.

Osoitetaan seuraavaksi, että kokonaiskiertymä ei muutu perussiirroissa. Kokonaiskiertymä on siis invariantti.

Lause 6.5. *Olkoon π jokin perussiirto. Tällöin $K_n(\pi \circ \sigma) = K_n(\sigma)$ kaikissa asemissa $\sigma \in \mathbb{R}$.*

Todistus. Tutkitaan, miten eri perussiirrot vaikuttavat kokonaiskiertymään. Kaikki merkityt paikat ovat kuution ylä- ja alatahkoilla, joten siirrot U ja D siirtävät kaikki merkityllä paikalla olevat ruudut jollekin toiselle merkitylle paikalle. Nämä siirrot eivät siis vaikuta kokonaiskiertymään lainkaan.

Siirrot F, B, L ja R ovat ruutujen numeroinnin ja paikkojen merkitsemisen suhteen symmetrisiä, joten riittää tarkastella yhtä niistä. Valittu siirto vaikuttaa vain niiden palojen kiertymään, jotka sijaitsevat kierrettävällä sivutahkolla. Nimetään nämä palat numeroilla 1, 2, 3 ja 4 ja merkitään jokaisen palan alkuperäistä kiertymää $k_i(\sigma) = n_i$. Kuvassa 26 näkyy, mitä sivutahkon paloille tapahtuu suoritettaessa perussiirto π. Merkityille paikoille osuvat ruudut on tummennettu.



Kuva 26: Perussiirron vaikutus nurkkapalojen kiertymään

Kuvan mukaan asemassa $\sigma \circ \pi$ saadaan neljän liikkuneen palan kokonaiskiertymäksi

$$\begin{aligned}\sum_{i=1}^{4} k_i(\pi \circ \sigma) &= (n_1 + 2) + (n_2 + 1) + (n_3 + 1) + (n_4 + 2) \\ &= n_1 + n_2 + n_3 + n_4 + 6 \qquad (\mathbb{Z}_3\text{:ssa } 6 = 0) \\ &= n_1 + n_2 + n_3 + n_4.\end{aligned}$$

Nurkkapalojen kokonaiskiertymä ei siis muutu myöskään perussiirroissa F, B, L tai R. □

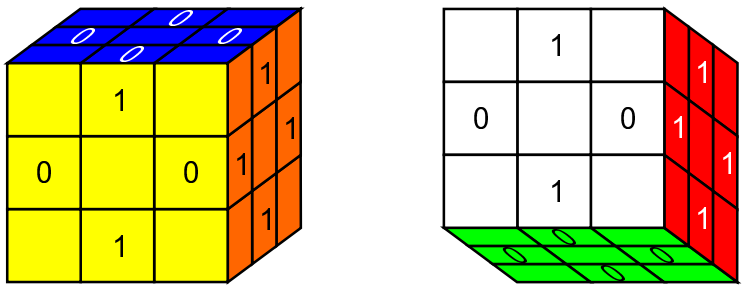
Koska alkuasemassa kokonaiskiertymä on nolla, saadaan edellisestä lauseesta heti seuraava korollaari.

Korollaari 6.6. *Kaikissa asemissa $\sigma \in \mathbb{R}$ pätee $K_n(\sigma) = 0$.*

Nyt saadaan kaikki nurkkapalat oikeisiin asentoihin. Eräs tapa tehdä tämä olisi valita aina kaksi väärässä asennossa olevaa nurkkapalaa, konjugoida ne vierekkäisiksi ja kiertää toinen niistä oikeaan asentoon. Tällä tavalla oikeassa asennossa olevien palojen määrä lisääntyy koko ajan, joten lopulta kaikki palat ovat oikeassa asennossa. Missään vaiheessa jäljellä ei voi olla vain yhtä väärässä asennossa olevaa nurkkapalaa, koska tällöin nurkkien kokonaiskiertymä olisi nollasta poikkeava.

Toinen tapa saada nurkat oikeisiin asentoihin ei vaadi konjugointia. Siinä järjestetään nurkkapalat aluksi jonoon $(x_1, x_2, \ldots, x_n)$, jossa sama pala voi esiintyä useammin kuin kerran, mutta kaksi peräkkäistä palaa sijaitsevat aina vierekkäin (eli samalla särmällä). Tämän jälkeen käydään läpi paloja jonon alusta lähtien. Aina kun löydetään väärin päin oleva pala x_k, missä $k < n$, käytetään opittua algoritmia paloihin x_k ja x_{k+1}, niin että pala x_k tulee oikeaan asentoon. Lopulta kaikki palat $x_1, \ldots, x_{n-1}$ ovat oikeassa asennossa, ja koska kokonaiskiertymän on oltava nolla, myös x_n on oikeassa asennossa.

Reunapalojen tapauksessa menetellään aivan samalla tavalla kuin nurkkapaloilla. Tarvittava ruutujen numero näkyy kuvasta 27, jossa kuutio on kuvattu perusasemassa edestä ja takaa. Ruutujen numeroiden ajatellaan nyt kuuluvan ryhmään $\mathbb{Z}_2$. Nollaruutuja ovat kaikki siniset ja virheät ruudut ja niissä paloissa, joissa kumpiakaan ei esiinny, keltaiset tai valkoiset ruudut.



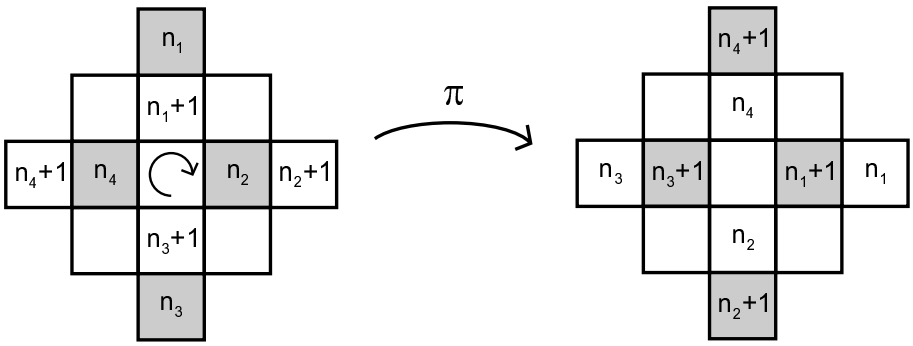
Kuva 27: Reunapalojen numerointi

Samoin kuin aikaisemmin, perusasemassa olevien nollaruutujen paikat merkitään, ja palan x kiertymä $k_x(\sigma)$ määräytyy siitä, mikä palan ruuduista sattuu olemaan merkityllä paikalla. Aseman σ kokonaiskiertymä $K_s(\sigma)$ on kaikkien palojen kiertymien summa.

Lause 6.7. *Särmäpalojen kokonaiskiertymä $K_s(\sigma)$ ei muutu perussiirroissa.*

Todistus. Käydään kaikki perussiirrot läpi. Siirrot U ja D siirtävät jokaisen merkityllä paikalla olevan ruudun jälleen merkitylle paikalle, joten ne eivät muuta kokonaiskiertymää. Toisaalta siirrot L ja R siirtävät jokaisen *merkitsemättömällä* paikalla olevan ruudun jälleen merkisemättömälle paikalle, joten kokonaiskiertymä ei niissäkään muutu.

Jäljelle jää tutkia, mitä tapahtuu siirroissa F ja B. Ne ovat palojen numeroinnin ja paikkojen merkitsemisen suhteen symmetrisiä, joten riittää tutkia toista niistä. Nimetään siirtoon osallistuvat särmäpalat numeroilla 1, 2, 3 ja 4 ja merkitään näiden kiertymiä alkuperäisessä asemassa $k_i(\sigma) = n_i$. Kuvassa 28 on näytetty, miten perussiirto vaikuttaa palojen kiertymiin. Särmäpalat on taiteltu auki ja merkityillä paikoilla sijaitsevat ruudut on tummennettu.



Kuva 28: Perussiirron vaikutus särmäpalojen kiertymään

Kuvasta nähdään, että tarkasteltavien neljän palan kiertymien summaksi tulee uudessa asemassa

$$\begin{aligned}\sum_{i=1}^{4} k_i(\pi \circ \sigma) &= (n_1 + 1) + (n_2 + 1) + (n_3 + 1) + (n_4 + 1) \\ &= n_1 + n_2 + n_3 + n_4 + 4 \qquad (\mathbb{Z}_2\text{:ssa } 4 = 0) \\ &= n_1 + n_2 + n_3 + n_4.\end{aligned}$$

Reunapalojen kokonaiskiertymä ei siis muutu myöskään perussiirroissa L tai R. □

Särmäpalat voidaan nyt saada oikeisiin asentoihin samalla periaatteella kuin reunapalatkin.

7 Rubikin kuution laajennoksia

Tavallista Rubikin kuutiota voidaan laajentaa monilla tavoilla. Ensi näkemältä nämä uudet versiot vaikuttavat paljon hankalammilta ratkaista, mutta tarkempi tarkastelu osoittaa, että samat perusideat ovat edelleen voimassa monimutkaisemmissakin muunnelmissa.

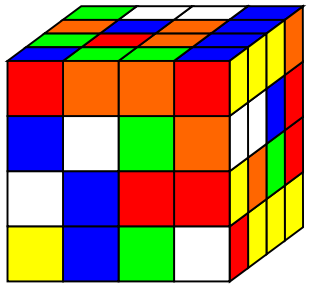
7.1 Suuremmat kuutiot

Ensimmäiseksi mieleen tuleva tapa laajentaa kuutiota on lisätä särmän pituutta. Tällä tavalla saadaan muun muassa suositut $4 \times 4 \times 4$- ja $5 \times 5 \times 5$-kuutiot. Vaikka ruutujen määrä — ja samalla myös mahdollisten asemien määrä — kasvaa näissä laajennoksissa huimasti, kuution perusrakenne säilyy kuitenkin samana. Siksi tällä kurssilla osoitettuja tuloksia voidaan yleensä soveltaa sellaisinaan. Esimerkiksi nurkkapaloja on edelleen kahdeksan kappaletta, ja jokainen perussiirto on nurkkapalojen paikkojen suhteen pariton permutaatio. Kommutaattoreilla voidaan tuottaa paikkojen 3-syklejä sekä erilaisia asentoryhmän siirtoja, ja palojen kokonaiskiertymistä saadaan invariantteja samaan tapaan kuin yksinkertaisemmassakin kuutiossa.

Suuremmissa kuutioissa keskipalatkin saavat merkityksen. Jos särmän pituus on pariton, kuutiossa on joka tahkolla yksi keskimmäinen pala, jonka voi ajatella pysyvän aina paikallaan. Tästä keskimmäisestä palasta voi päätellä kunkin sivun värin missä tahansa asemassa. Jos särmän pituus on enemmän kuin kolme, on kuutiossa kuitenkin useampiakin keskipaloja, jotka koostuvat vain yhdestä ruudusta, ja näiden paikalleen saaminen vaatii omanlaisensa siirtosarjat. Siirtosarjoihin tarvitaan nyt myös keskitahkojen siirtoja, joita ei enää voida jättää huomiotta. Kommutaattorit kuitenkin tehoavat edelleen, ja tilannetta helpottaa se, että kukin keskipala voi olla vain yhdessä asennossa.

Kuutiossa, jonka särmän pituus on parillinen, ei sen sijaan ole sellaisia keskimmäisiä paikallaan pysyviä paloja, joista voisi aina tarkistaa kuution sivujen oikean värin. Tällaisessa tapauksessa voidaan kuitenkin turvautua nurkkapaloihin. Nurkkapalojen rakenteesta johtuen kuutiossa vastakkaisten sivutahkojen värit on aina määrätty. Jos perusasemassa valkoinen sivu on keltaista vastassa, ei kuutiossa voi olla nurkkapalaa, jossa olisi sekä valkoinen että keltainen ruutu. Täten valkoinen ja keltainen sivu eivät voi ikinä olla vierekkäin. Kuution sivujen määräämiseksi riittää siis valita yksi nurkkapala, esimerkiksi sini-kelta-punainen. ja ajatella tuon nurkkapalan olevan aina oikealla paikallaan. Näin selviää, missä sininen, keltainen ja punainen sivu sijaitsevat kussakin asemassa, ja muut sivut ovat näille vastakkaisia. Kuvassa 29 on $4 \times 4 \times 4$-kuutio, jonka nurkkapalasta näkyy, että kuution punainen

sivu on katsojaan päin ja sininen sivu ylöspäin. Takasivu on tällöin oranssi, vasen sivu valkoinen ja alasivu virheä.



Kuva 29: $4 \times 4 \times 4$-kuutio, "Rubikin kosto"

Parillissärmäisillä kuutioilla on toinenkin erikoispiirre. Keskitahkojen siirrot voidaan nimittäin jakaa reuna- ja keskipaloja liikuttaviin osiin, joista edellinen on pariton permutaatio ja jälkimmäinen parillinen. Parillinen keskipalojen siirto voidaan tuottaa 3-syklien avulla, joten myös reunapalojen pariton permutaatio on mahdollinen siirto. Tällaisilla kuutioilla voidaankin tehdä esimerkiksi kahden reunapalan vaihto, joka ei onnistu paritonsärmäisillä kuutioilla.

Särmän pituuden lisääntyessä käytännön ongelmaksi tulee ratkaisualgoritmin pituus. Kuutiossa, jonka särmän pituus on kuusi, on jo 96 keskipalaa. Näiden kaikkien paikoilleen saaminen 3-syklien avulla on melkoisen työlästä.

7.2 Muita ruutujen määrään perustuvia laajennoksia

Kuution ruutujen määrää voi lisätä myös tekemällä kuutiosta neli- tai useampiulotteisen. Tällaisten kuutioiden käsitteleminen onnistuu yleensä vain tietokoneen avulla. Ulottuvuuksien lisääntyessä eri pala- ja siirtotyyppejä tulee huimasti lisää, mutta ratkaisun perusideat eivät kuitenkaan muutu.

Toinen peruskuution muunnelma ovat käyttää kuution sijasta erimuotoisia kappaleita. Rubikin kuution tapaisia pelejä voidaan tehdä sekä säännöllisistä että epäsäännöllisistä monitahokkaista, ja näiden avulla saadaan aikaan monenlaisia algebrallisia struktuureja. Kuitenkin niin kauan kuin on mahdollista tuottaa 3-syklejä, voidaan ratkaisua aina lähestyä niiden avulla. Siirtojen parillisuuskysymykset voivat erimuotoisissa kuutioissa sen sijaan olla hyvinkin erilaisia.

7.3 Superkuutio

Edellä mainituissa Rubikin kuution muunnelmissa on sama tavoite kuin perinteisessä kuutiossa: saada eriväriset ruudut samoille paikoille kuin perusasemassa. Ky-

se on siis ruutujen paikkojen permutaatioista. Jos ruutuja on n kappaletta, kuution siirtoja vastaavan permutaatioryhmän voi ajatella symmetrisen ryhmän S_n aliryhmäksi, olipa kyse sitten tavallisesta kolmiulotteisesta kuutiosta tai vaikkapa seitsenulotteisesta ikosaedrista.

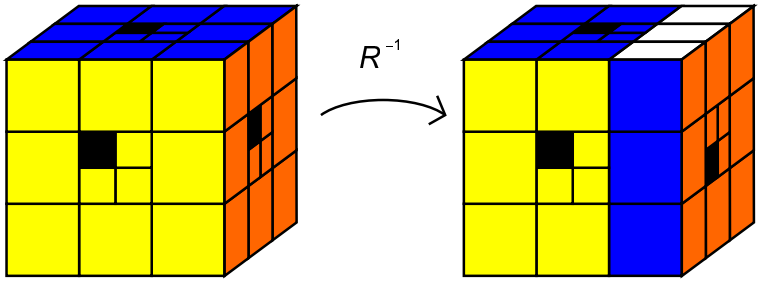
Yksi mahdollisuus perustavoitteen muunnelmaksi on tarkastella keskipalojen asentoja. Nurkka- ja reunapalojen asennot määräytyvät, kun niiden ruudut asettaa oikealle paikalleen. Keskipaloissa on kuitenkin vain yksi ruutu, ja keskipalaa voi siksi kiertää itsensä ympäri, ilman että mikään ruutu joutuu väärälle paikalle. Jos tavoitteeksi otetaan myös keskipalojen asentojen palauttaminen samaksi kuin alussa, saadaan ns. *superkuutio-ongelma.*

Tarkastellaan lähemmin $3 \times 3 \times 3$-kuution superkuutio-ongelmaa. Koska kyse ei enää ole pelkästään ruutujen paikoista, ei voida ajatella eri asemien muodostavan aliryhmää kaikkien ruutujen permutaatioiden ryhmässä S_{54}, kuten aiemmin tehtiin. Algebralliseen perusstruktuuriin tarvitaan siis jonkinlainen laajennos, toisin kuin ruutujen määrään perustuvissa Rubikin kuution muunnelmissa.

Yksi vaihtoehto perusstruktuurin laajentamiseksi on seuraava: Koska keskipalojen voidaan edelleen ajatella pysyvän kaikissa siirroissa paikoillaan ja keskipaloja koskevat siirrot ovat riippumattomia muita paloja koskevista siirroista, voidaan haluttu laajennos toteuttaa tuloryhmänä. Kukin keskipala voi olla neljässä eri asennossa, ja nämä asennot voidaan ajatella numeroiduiksi syklisen ryhmän $\mathbb{Z}_4$ alkioilla. Tällä tavalla saadaan laajennetuksi ryhmäksi suora tulo $S_{48} \times \mathbb{Z}_4^6$, jossa on ensimmäisenä tekijänä nurkka- ja reunaruutujen permutaatioryhmä ja seuraavina kaikkien kuuden keskipalan asentoryhmät.

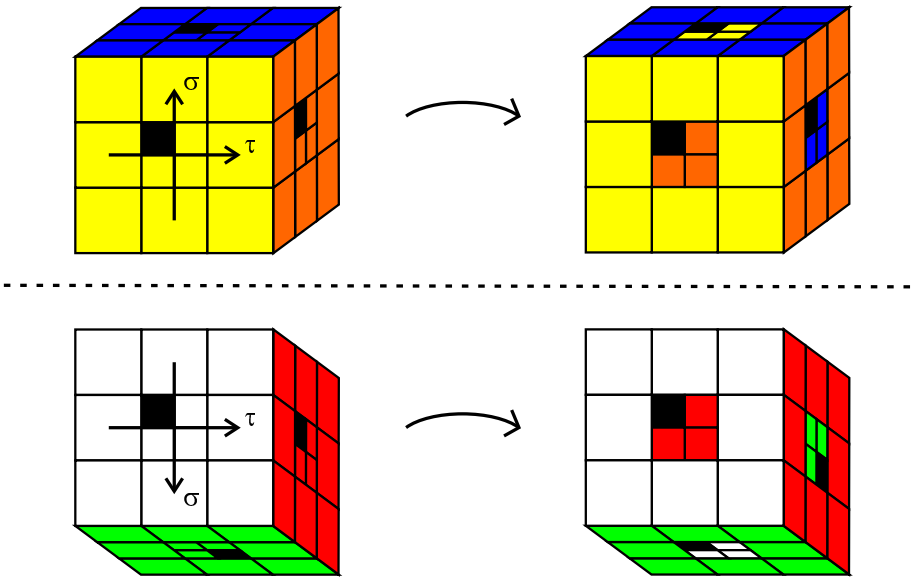
Toinen mahdollisuus on lisätä kuutioon keinotekoisia ruutuja. Jos ajatellaan myös jokainen keskipala jaetuksi neljään ruutuun, jotka sijaitsevat kaikki samalla sivulla, voidaan näiden valeruutujen paikoista päätellä keskipalan asento. Tällainen jako on esitetty kuvassa 30, josta näkyy samalla, miten perussiirto vaikuttaa keskipalan asentoon. Yksi keskipalan ruuduista on väritetty mustaksi selvyyden vuoksi. Jakamalla keskipala ruutuihin voidaan jälleen ajatella eri asemien muodostavan aliryhmän kaikkien ruutujen permutaatioiden ryhmässä, mutta nyt ruutuja on yhteensä 64, joten kyse on ryhmän S_{64} aliryhmästä. Tämä ryhmä on kooltaan paljon suurempi kuin ensimmäisen laajennosvaihtoehdon tuloryhmä, mutta koska kyse on nyt vain ruutujen lisäämisestä, voidaan aikaisempia ideoita jälleen käyttää hyväksi.

Tutkitaan nyt, minkälaisia kommutaattoreita keskipalan liikkeistä saadaan. Tätä varten luovutaan nyt niistä periaatteesta, että keskipalat pysyisivät aina paikallaan ja keskitahkon kierto tulkittaisiin rinnakkaisten sivutahkojen kierroksi. Perussiirrot (keskitahkojen siirrot mukaanlukien) nimetään kuitenkin edelleen totuttuun tapaan.



Kuva 30: Keskipalojen jako ruutuihin ja perussiirron vaikutus keskipalan asentoon

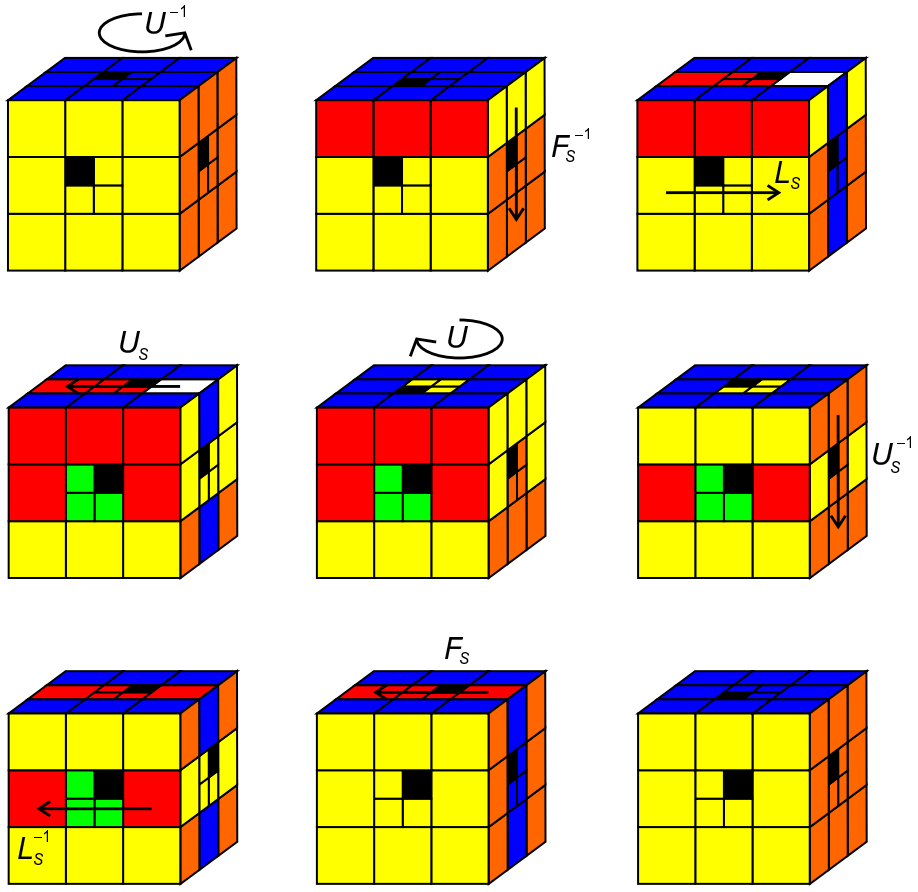
Ensinnäkin on huomattava, että jokainen siirto, joka siirtää jonkin keskipalan paikaltaan, siirtää samalla myös vastakkaista keskipalaa. Näin ollen keskipalojen paikkaryhmässä on mahdotonta löytää kahta permutaatiota, joiden yhteiseen kantajaan kuuluisi vain yksi keskipala. Kommutaattoriperiaatteella (lause 6.3) ei siis saada aikaan paikkojen 3-sykliä. Paikkaryhmässä pienin yhteinen kantaja, eli kahden vastakkaisen keskipalan pari, saadaan esimerkiksi valitsemalla siirroiksi kahden eri keskitahkon perussiirrot. Tämä on tähän mennessä esillä olleista kommutaattorisiirroista yksinkertaisin, ja se tuottaa vastakkaisten keskipalojen 3-syklit kuvan 31 mukaisesti. Kuvasta kuutio on kuvattuna edestä ja takaa. Tämä siirtosarja on helppo suorittaa, ja tulos on näyttävä, mutta siirtosarja ei itse asiassa auta keskipalojen oikean asennon löytämisessä.



Kuva 31: Vastakkaisten keskipalojen 3-syklit

Toinen mahdollisuus kommutaattorin tuottamiseen on valita sellaiset siirrot,

joista toinen kiertää keskipalaa paikallaan ja toinen siirtää sen johonkin muuhun paikkaan. Kiertäväksi permutaatioksi τ voidaan valita esimerkiksi perussiirto U. Siirtävä permutaatio σ saadaan puolestaan helposti kolmen keskitahkon siirron yhdistelmänä $F_S L_S^{-1} U_S^{-1}$ (oikeastaan konjugaattisiirto). Näistä muodostetun kommutaattorin $[\sigma, \tau]$ tuloksena sininen keskipala kiertyy vastapäivään ja keltainen keskipala myötäpäivään. Siirtosarja on esitetty kuvassa 32. Huomaa, että keskipalojen liikuttaminen vaikuttaa siirtojen merkitsemistapaan, ja siksi esimerkiksi siirto L_S kiertää kuvassa kuution yläpinnan suuntaista keskitahkoa.



Kuva 32: Keskipalojen kierto

Keskipalojen kiertymät $k_x(\sigma)$ voidaan määritellä samaan tapaan kuin luvussa 6.5. Tällöin kukin kiertymä on ajateltava $\mathbb{Z}_4$:n alkioksi. Koska yhden sivutahkon kierto muuttaa vain yhden keskipalan kiertymää yhdellä, keskipalojen kokonaiskiertymä $K_k(\sigma)$ voi olla mikä tahansa luvuista 0, 1, 2 tai 3. Edellä kuvattu siirtosarja ei vaikuta kokonaiskiertymään, joten tarvitaan muitakin siirtoja keskipalojen asentojen ratkaisemiseksi.

Nimitetään tässä yhteydessä *perusasemaksi* sitä asemaa, jossa kaikki palat ovat oikeilla paikoillaan ja oikeissa asennoissa, mukaanlukien keskipalat. Sellaisia asemia, joissa kaikki palat ovat oikeilla paikoillaan ja nurkka- ja reunapalat lisäksi oikeissa asennoissaan, kutsutaan *vanhaksi perusasemaksi.* Vanhasta perusasemasta toiseen siirtyminen vaatii parillisen määrän sivutahkojen perussiirtoja, sillä nämä perussiirrot ovat parittomia permutaatioita, jollei keskipaloja oteta lukuun. (Keskitahkon perussiirto lasketaan tässä jälleen kahdeksi sivutahkon perussiirroksi.) Koska perusasemassa keskipalojen kokonaiskiertymä on 0, täytyy jokaisessa vanhassa perusasemassa kokonaiskiertymän olla joko 0 tai 2.

Edellisen päättelyn nojalla keskipalat saadaan oikeaan asentoon seuraavasti: Ratkaistaan kuutio vanhan mallin mukaan, jolloin päädytään johonkin vanhaan perusasemaan. Keskipalat voivat olla nyt väärissä asennoissa, mutta niiden kokonaiskiertymä on 0 tai 2. Jos se on 0, keskipalat saadaan oikeisiin asentoihin yllä kuvattua siirtosarjaa soveltamalla. Jos kokonaiskiertymä on 2, tehdään ensin kaksi perussiirtoa esimerkiksi kiertämällä yhtä sivutahkoa puoli kierrosta. Tällöin kokonaiskiertymäksi tulee 0. Paikoiltaan siirtyneet nurkka- ja särmäpalat voidaan nyt palauttaa perusasemaan soveltamalla aiemmin opittuja algoritmeja, jotka *eivät vaikuta* keskipalojen kiertymiin. Tuloksena saadaan vanha perusasema, jossa keskipalojen kokonaiskiertymä on 0, ja tähän voidaan jälleen soveltaa keskipaloja kiertävää siirtosarjaa.

LOPPU