

Ryhäteoreettinen näkökulma Rubikin kuutioon

Jokke Häsä

Matematiikan ja tilastotieteen laitos, kevät 2008
Korjattu syksyllä 2012

Sain idean tämän kurssin pitämiseen luettuani Jyrki Lahtosen artikkelin *Rubikin kuutio ja permutaatioryhmät* (<http://users.utu.fi/lahtonen/rubik.html>). Olen käyttänyt suoraan tuossa artikkelissa esitettyjä algoritmeja kuution ratkaisemiseksi, vaikka yleisestä teoriasta voidaankin johtaa myös lukuisia muita ratkaisuun sopivia siirtosarjoja. Olen myös lainannut artikkelista idean Rubikin kuution symmetriaryhmän jakamisesta asento- ja paikkaryhmiin sekä menetelmän 3-syklisen tuottamiseksi kommutaattoreiden avulla. Muun materiaalin olen tuottanut itse tai ottanut alan peruskirjallisuudesta. Esitetyt todistukset ovat omaa käsialaani.

Jokke Häsä, 2.11.2012

Sisältö

1. Johdanto	5
1.1. Yleistä	5
1.2. Kuution rakenne	6
2. Permutaatioryhmät	8
2.1. Permutaation olemus	8
2.2. Permutaatioilla laskeminen	8
2.3. Rubikin ryhmä	9
2.4. Syklit	11
2.5. Permutaation etumerkki	13
3. Tekijäryhmät	18
3.1. Tekijäryhmän määritelmä	18
3.2. Rubikin ryhmän jako paikkojen ja asentojen mukaan	21
3.3. Algoritmi 1: nurkkapalojen 3-sykli	22
3.4. Alternoivat ryhmät	23
4. Konjugointi	26
4.1. Konjugoinnin määritelmä	26
4.2. Konjugointi permutaatioryhmissä	29
4.3. Konjugointi Rubikin ryhmässä	31
4.4. Ryhmän keskus	34
5. Tuloryhmät	38
5.1. Suorat tulot	38
5.2. Tuloryhmät Rubikin ryhmässä	44
5.3. Algoritmi 2: särmäpalojen 3-sykli	48
5.4. Rubikin paikkaryhmän ratkaiseminen	48
5.5. Puolisuorat tulot	52
6. Kommutaattorit	58
6.1. Kommutaattorien perusominaisuudet	58
6.2. Kommutaattorit Rubikin ryhmässä	60
6.3. Algoritmi 3: nurkkapalojen kierto	62
6.4. Algoritmi 4: särmäpalojen kääntö	62
6.5. Rubikin asentoryhmän ratkaiseminen	62
7. Rubikin kuution laajennoksia	67
7.1. Suuremmat kuutiot	67
7.2. Muita ruutujen määrään perustuvia laajennoksia	68
7.3. Superkuutio	68

A. Siirtosarjat	73
A.1. Nurkkapalojen 3-sykli	73
A.2. Särmäpalojen 3-sykli	74
A.3. Nurkkapalojen kierto	75
A.4. Särmäpalojen kääntö	75

1. Johdanto

1.1. Yleistä

Unkarilainen kuvanveistäjä ja arkkitehtuurin professori Ernő Rubik kehitti maineikkaan kuutionsa vuonna 1974. Kuutio oli alun perin eräänlainen harjoitelma tietyn kolmiulotteisen rakenteen kehittämiseksi, mutta siitä tuli sittemmin maailmankuulu ongelmanratkaisupeli. Rubik kutsui kuutiotaan 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 muun muassa sokkona, jaloilla ja yhdellä kädellä ratkaisemisessa. Tämänhetkinen (29.10.2012) virallinen nopeusennätys on australialaisella Feliks Zemdegsillä, joka vuonna 2011 ratkaisi kuution nopeimmillaan 5,66 sekunnissa. Myös suomalaiset ovat pärjänneet kuution mani- ja pedipuloinnissa: vielä vuonna 2010 jaloilla ratkaisemisen maailmanennätys kuului Anssi Vanhalalle ja Ville Seppäsellä oli hallussa maailmanennätykset $4 \times 4 \times 4$ - ja $5 \times 5 \times 5$ -kokoisten kuutioiden sokkoratkaisussa.¹

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.

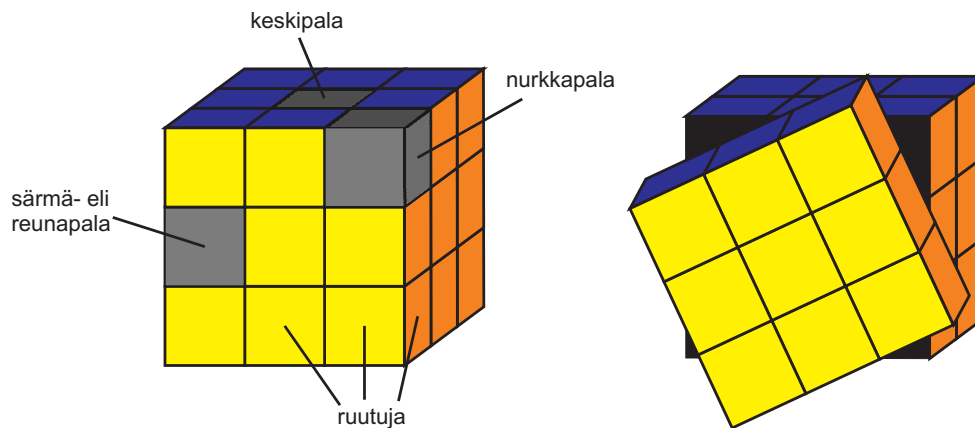
Ratkaisemiseen tarvittava pyöritysten määrä ei ole vielä täsmällisesti selvinnyt. Vuonna 1998 Michael Reid löysi kombinaation, jonka ratkaisemiseen vaaditaan vähintään 26 kappaletta sivutahkon pyöräytyksiä neljännesympyrän verran. (Tällaista pyöräytystä kutsutaan tässä materiaalissa *perussiirroksi* tai perussiirron käänteissiirroksi.) Toisaalta Tomas Rokicki osoitti vuonna 2009, että minkä tahansa aseman ratkaisemiseen tarvitaan korkeintaan 29 tällaista siirtoa. Näiden lukumäärien välissä on vielä tilaa tarkennukselle. Jos sen sijaan myös sivutahkon 180 asteen pyöräytys lasketaan perussiirroksi, tuorein ja samalla lopullinen tulos löytyy heinäkuulta 2010, jolloin Tomas Rokicki, Herbert Kociemba, Morley Davidson ja John Dethridge osoittivat Googlen laskentatietoa käyttäen, että kaikki kuution kombinaatiot voidaan ratkaista 20 siirrolla. Tämä on myös paras mahdollinen tulos, sillä eräiden asemien ratkaiseminen vaatii juuri 20 siirtoa (Michael Reidin tulos vuodelta 1995).²

¹ <http://www.worldcubeassociation.org/results/events.php>

² Lähteitä löytyy osoitteesta http://en.wikipedia.org/wiki/Optimal_solutions_for_Rubik's_Cube.

1.2. Kuution rakenne

Rubikin kuution jokainen *sivutahko* koostuu yhdeksästä 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.

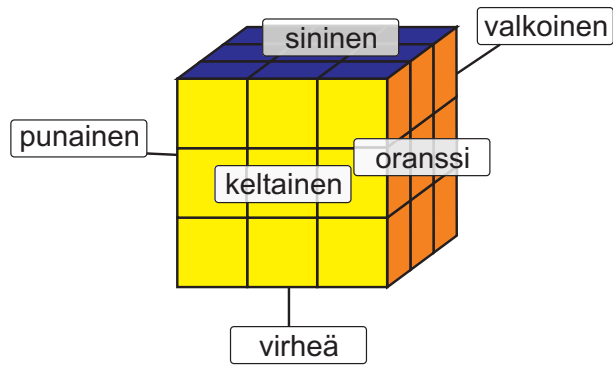
Mitä tahansa yhdistelmää kuution sivutahkojen kääntöjä kutsutaan *siirroksi*. Kaksi siirtoa samastetaan, mikäli niillä päästään tietystä alkutilanteesta samaan lopputilanteeseen.

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 yksiväriseksi.

Myynnissä olevien kuutioiden väriytykset 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 (ks. kuva 2).

On hyödyllistä huomioida heti aluksi, että kuution keskipalojen voidaan olettaa pysyvän paikallaan kuution sivuja pyöritettäessä. Kunkin sivutahkon keskipala nimittäin pysyy paikallaan, kun kyseistä sivua pyöritetään¹, eikä tämä pyöritys tietenkään vaikuta mitenkään muiden sivujen keskipalojen asemiin. Toisaalta keskitahkojen pyörittäminen

¹ 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.



Kuva 2: Kuution väritys.

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

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

2.1. Permutaation olemus

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

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

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

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

2.2. Permutaatioilla laskeminen

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

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

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

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

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

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

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

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

Kun tämä permutaatio kerrotaan vasemmalta eräällä toisella permutaatiolla, tuloksena on

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

Toisaalta permutaation σ käänteisalkio on

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

2.3. Rubikin ryhmä

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

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

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

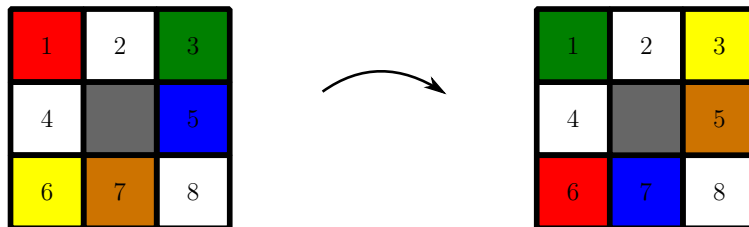
Määritelmä 2.3. Olkoon X joukko, johon kuuluvat kaikki Rubikin kuution ruudut keskiruutuja lukuunottamatta. *Rubikin ryhmä* \mathbb{R} on sellainen joukon X permutaatioiden joukko, jonka jokainen alkio vastaa jotakin Rubikin kuution laillista siirtoa. Rubikin ryhmä voidaan tulkita symmetrisen ryhmän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

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

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

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

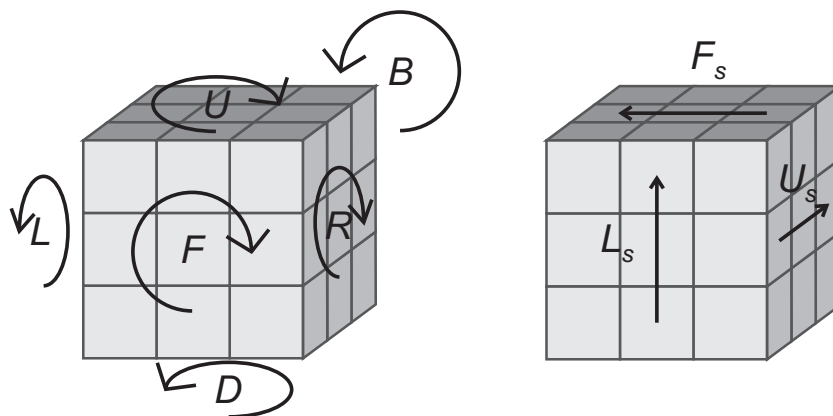
Tällä tavalla tulkittuna kuvan siirto on permutaatio $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 1 & 4 & 7 & 3 & 5 & 8 \end{pmatrix}$.



Kuva 3: Eräs Rubikin ryhmän siirto.

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

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



Kuva 4: Kuution perussiirrot ja keskitahkojen siirrot.

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

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

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

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

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

2.4. Syklit

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

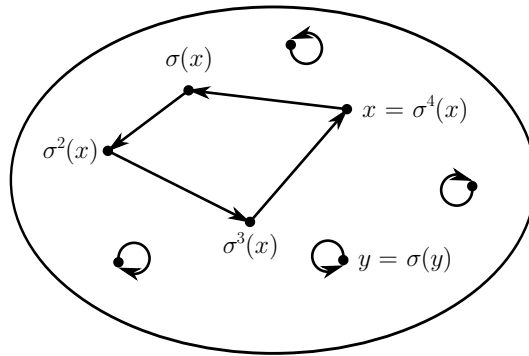
$$x_1 \mapsto x_2 \mapsto x_3 \mapsto \cdots \mapsto x_n \mapsto x_1.$$

Muut alkioit sykli pitää paikallaan.

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

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

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



Kuva 5: Eräs 4-sykli.

Sykliä, jonka pituus on n , voidaan merkitä seuraavasti:

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

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

Esimerkki 2.6. Permutaatio

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

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

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

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

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

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

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

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

2.5. Permutaation etumerkki

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

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

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

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

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

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

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

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

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

Olkoon $\sigma \in S_n$. Merkitään

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

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

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

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

Tällöin erityisesti

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Näin on väite todistettu. □

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

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

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

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

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

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

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

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

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

Jakamalla tämän yhtälön molemmat puolet luvulla Δ_n saadaan

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

kuten haluttiin. □

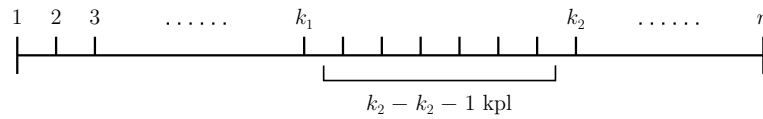
Permutaation etumerkin laskeminen määritelmän 2.11 perusteella on työlästä. Seuraavan lauseen avulla etumerkki voidaan laskea helposti sykliesityksestä lähtien.

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

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

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

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



Kuva 6: Vaihdon etumerkin laskeminen.

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

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

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

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

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

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

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

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

Esimerkki 2.15. Permutaatio

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

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

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

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

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

3. Tekijäryhmät

Tekijäryhmän käsitteen avulla voidaan monimutkainen ryhmä jakaa osiin. Ideana on, että voidaan erikseen tarkastella, miten laskutoimitus vaikuttaa näihin osiin kokonaisuuksina, ja jättää hetkeksi huomiotta se, mitä itse asiassa tapahtuu kunkin osan sisällä.

3.1. Tekijäryhmän määritelmä

Tekijäryhmiä 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 neutraali-alkio. 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

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

Etsitään sivuluokat havainnoimalla. Ensinnäkin yksi sivuluokista on

$$0 + 4\mathbb{Z} = 4\mathbb{Z} = \{\dots, -4, 0, 4, 8, 12, \dots\}.$$

(Huomaa, että kun ryhmän laskutoimituksena on yhteenlasku, sivuluokkamerkinnässäkin on kertomerkin sijaan +-merkki.)

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

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

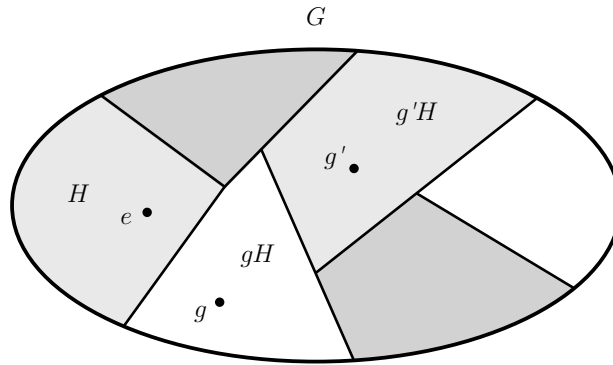
Huomataan, että $4 + 4\mathbb{Z}$ on sama joukko kuin $4\mathbb{Z}$ ja että sivuluokkia ei enää tule lisää, vaikka kokeiltaisiiin uusilla luvuilla: esimerkiksi $13 + \mathbb{Z}$ on sama joukko kuin $1 + \mathbb{Z}$. Jokainen kokonaisluku näyttää nyt kuuluvan johonkin neljästä sivuluokasta $4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$ 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 7). Tarkoituksena olisi nyt unohtaa sivuluokkien varsinaisen 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 alkioita $g_1h_1g_2h_2$, 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 alkioita kerrottuna vasemmalta alkioilla g_1 ja oikealta kaikilla aliryhmän H alkioilla.



Kuva 7: Aliryhmän H sivuluokat.

Ongelmana on nyt se, että joukko $g_1H \cdot g_2H$ ei välttämättä ole itse sivuluokka. Tällaisessa tapauksessa ei kokonaisuun sivuluokkiin rajoittumisesta olisi paljon iloa, kun sivuluokkien joukko ei olisi suljettu 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*, mikäli aliryhmän H vasemman- ja oikeanpuoleiset sivuluokat ovat samat eli kaikilla $g \in G$ pätee $gH = Hg$. Jos H on G :n normaali aliryhmä, merkitään $H \trianglelefteq G$.

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*

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

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

$$h = \underbrace{\hat{g}(\hat{g}^{-1}h\hat{g})\hat{g}^{-1}}_{\in H} \in \hat{g}H\hat{g}^{-1},$$

mistä seuraa, että $H \subset \hat{g}H\hat{g}^{-1}$. Koska \hat{g} oli mielivaltainen, pätee $H \subset gHg^{-1}$ kaikilla $g \in G$. Siispä $gHg^{-1} = H$ kaikilla $g \in G$, ja H on normaali. \square

Esimerkki 3.5. Ryhmä S_3 koostuu kuudesta alkioista: (12), (23), (13), (123), (132) ja id. Tarkistetaan, onko aliryhmä $H = \langle (123) \rangle = \{\text{id}, (123), (132)\}$ normaali. Lasketaan sitä varten muotoa ghg^{-1} olevat tulot, missä $h \in H$. Niissä tapauksissa, joissa $g \in H$ tai $h = \text{id}$, 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

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

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

Olkoon nyt $H' = \langle (12) \rangle = \{\text{id}, (12)\}$. 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 ryhmän jako paikkojen ja asentojen mukaan

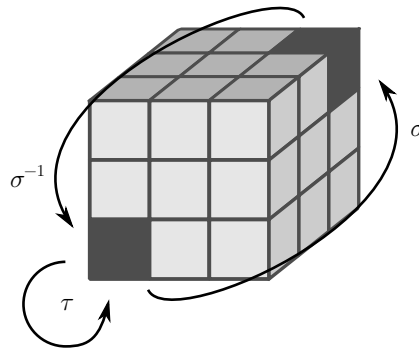
Tarkastellaan sellaista Rubikin ryhmän osajoukkoa \mathbb{R}_a , jonka permutaatiot pitävät kuution jokaisen palan paikallaan, vaikka voivatkin muuttaa niiden asentoa.

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 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. \square



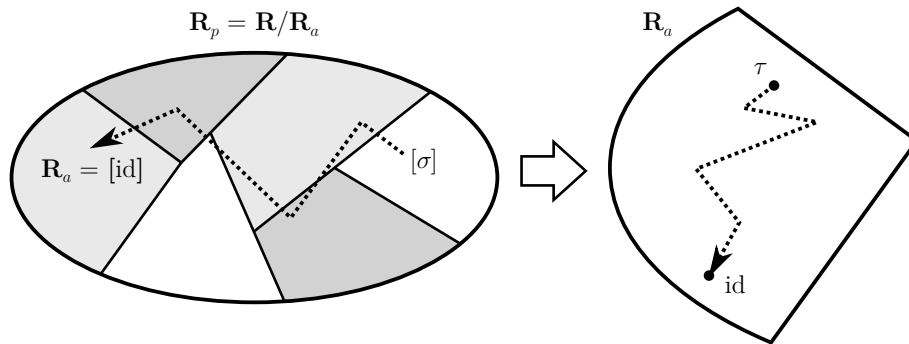
Kuva 8: Yhdistelmä $\sigma\tau\sigma^{-1}$ ei siirrä paloja.

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 $\sigma_1 \in [\sigma_2]$, eli $\sigma_1 = \sigma_2 \circ \tau$ 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 niiden siirtelyyn. Kuution ratkaisemiseksi olisi annetuista 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 $[\text{id}] = \mathbb{R}_a$, 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 9.

Huomaa, että toisinpäin eli asentoryhmästä paikkaryhmään eteneminen olisi mahdotonta, sillä paloilla ei voi ajatella olevan mitään ”oikeita asentoja”, elleivät ne ole oikeilla paikoillaan. Tämän seikan algebrallinen tulkinta on se, että aliryhmässä on aina neutraalialkio, mutta muissa sivuluokissa ei ole mitään tähän rinnastettavaa erityistä alkioita. Jos siis asema sijaitsee jossain väärässä sivuluokassa, ei sivuluokan sisällä ole mitään tiettyä suuntaa, johon ratkaisussa kannattaisi edetä.

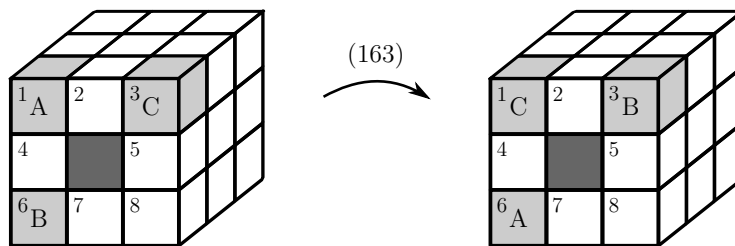


Kuva 9: Ratkaisun vaiheet.

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.

Liitteessä A.1 on esitetty siirtosarja, joka tuottaa eräiden nurkkapalojen 3-syklin paikkaryhmässä \mathbb{R}_p . Jos kuutio asetetaan siten, että keltainen sivu on katsojaan päin ja sininen sivu ylöspäin, ja keltaisen sivun palojen paikat numeroidaan vasemmalta oikealle ja ylhäältä alas keskipalaa lukuunottamatta numeroilla $\{1, \dots, 8\}$, saatava 3-sykli on (163). Se on esitetty kuvassa 10.



Kuva 10: Nurkkapalojen 3-sykli.

3.4. Alternoivat ryhmät

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

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

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 normaalisuus-kriteeriä. Olkoot $\tau \in A_n$ ja $\sigma \in S_n$ mielivaltaisia. Tarkastellaan yhdistelmän $\sigma\tau\sigma^{-1}$ etumerkkiä. Ensinnäkin havaitaan, että

$$\text{sign}(\sigma) \text{sign}(\sigma^{-1}) = \text{sign}(\sigma \circ \sigma^{-1}) = \text{sign}(\text{id}) = 1,$$

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

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

Nähdään, että $\sigma\tau\sigma^{-1} \in A_n$, mistä seuraa $\sigma A_n \sigma^{-1} \subset A_n$. Aliryhmä A_n on siis normaali. \square

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

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

Lagrange'n 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 $n \geq 2$.*

Todistus seuraisi suoraan nk. *homomorfialauseesta*, koska kuvaus $\text{sign} : S_n \rightarrow \{1, -1\}$ on homomorfismi, jonka ydin on A_n ja joka on surjektiivinen, kun $n \geq 2$. 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 homomorfialauseetta.

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 $\sigma \in (12)A_n$. Ensinnäkin

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

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

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

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

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

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

Todistus. Tarkastellaan mielivaltaista parillista 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-sykliden tulolla tai neutraalialkiolla.

Koska $(ab) = (ba)$ pätee kaikilla $a, b \in N_n$, mahdollisia tilanteita on kolme:

- 1) jos $\pi_k \rho_k$ on muotoa $(ab)(ab)$, niin $\pi_k \rho_k = \text{id}$
- 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 $\pi_k \rho_k = (abc)(bcd)$.

Nähdään, että jokainen kahden vaihdon yhdistelmä voidaan korvata 3-sykleillä tai neutraaliakiolla, joten permutaatio σ voidaan kirjoittaa 3-syklien tulona. \square

4. Konjugointi

4.1. Konjugoinnin määritelmä

Usein ryhmän alkiot kuvaavat operaatioita jossain joukossa. Ryhmäteoriassa tätä kutsutaan ryhmän *toiminnaksi*. Permutaatiot ovat hyvä esimerkki ryhmän toiminnasta. Kun ryhmän alkiot kuvaavat operaatioita, joukon tietyssä osassa toimiva operaatio voidaan siirtää toiseen osaan konjugoimalla.

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, joukko

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

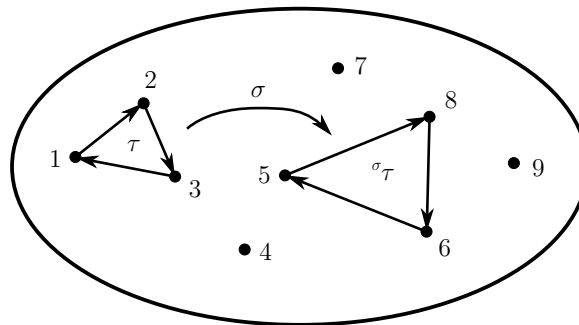
on joukon X *konjugaattijoukko*.

Konjugointi on kääntyvä operaatio: kun konjugoitu alkio ${}^g x$ konjugoidaan uudestaan alkion g^{-1} , saadaan alkuperäinen alkio x . Jos ryhmä on vaihdannainen, kullakin alkion x on ainoana konjugaattinaan vain alkio itse, sillä $gxg^{-1} = gg^{-1}x = x$ kaikilla $g \in G$. Toisaalta epävaihdannaisia ryhmiä käsiteltäessä konjugointi on hyvin yleinen työkalu. Esimerkiksi lauseen 3.4 normaalisuuskriteeri voidaan lausua muodossa: aliryhmä H on normaali, jos ja vain jos se sisältää kaikkien alkuidensa konjugaatit.

Esimerkki 4.2. Tarkastellaan ryhmän S_9 alkioita $\tau = (123)$ ja $\sigma = (167)(259)(38)$. Nyt $\sigma^{-1} = (761)(952)(83)$ ja

$$\sigma\tau = \underbrace{(167)(259)(38)}_{\sigma} \underbrace{(123)(761)(952)(83)}_{\sigma^{-1}} = (586).$$

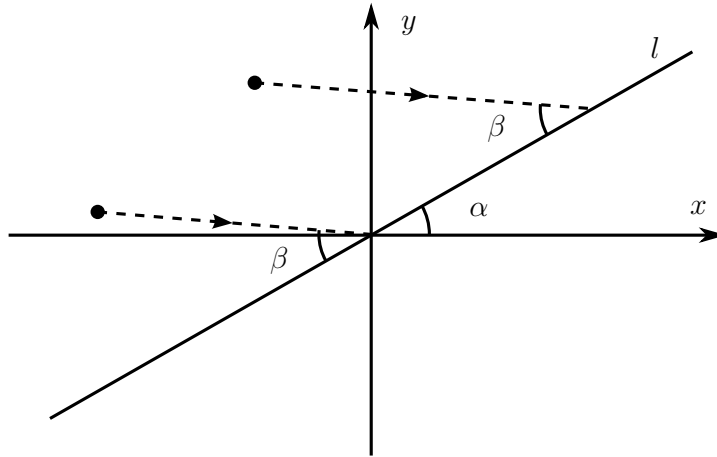
Konjugointi siirsi siis syklin τ toimimaan lukujen 1, 2 ja 3 sijasta luvuilla 5, 8 ja 6.



Kuva 11: Syklin siirto konjugoimalla.

Vaikka konjugointi onkin määritelty vain ryhmän sisäiseksi kuvaukseksi, kyse on oikeastaan yleisemmästä periaatteesta. Konjugoitavan alkion ei nimittäin tarvitse olla itse kääntyvä. Jos esimerkiksi L on vektoriavaruuden V sisäinen lineaarikuvaus ja P on kääntyvä lineaarikuvaus avaruudelta V avaruuteen W , voidaan konjugoimalla muodostaa avaruuden W sisäinen lineaarikuvaus PLP^{-1} . Samaten jos f on topologisten avaruuksien X ja Y välinen homeomorfismi ja g_X jokin jatkuva kuvaus avaruudelta X itselleen, saadaan avaruuteen Y jatkuva kuvaus $g_Y = f \circ g_X \circ f^{-1}$. Seuraava esimerkki on lineaarialgebrasta.

Esimerkki 4.3. Olkoon annettu tasossa origon kautta kulkeva nouseva suora l , joka muodostaa x -akselin kanssa kulman α (ks. kuva 12). Tarkastellaan lineaarikuvausta L , joka projisoi minkä tahansa tason pisteen kulmassa β suoralle l .



Kuva 12: Projektiokuvaus.

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

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

Myös kannanvaihtomatriisi P osataan muodostaa. Sillä kertominen kiertää kantavektoreita $(1, 0)$ ja $(0, 1)$ niin, että ne tulevat suoran ja projisoinnin suuntaisiksi, joten $P(1, 0) = (\cos \alpha, \sin \alpha)$ ja $P(0, 1) = (-\cos(\beta - \alpha), \sin(\beta - \alpha))$. Kannanvaihtomatriisiksi

tulee siis

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

Nyt siis alkuperäinen lineaarikuvaus on saadun diagonaalimatriisin konjugaatti:

$$L = PDP^{-1}.$$

Kuvauksen L matriisi voitaisiin helposti laskea tästä yhtälöstä.

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

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

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

Vaihdannaisuuden takia konjugointi ryhmässä T ei muuta alkioita lainkaan. Asia voidaan kuitenkin nähdä myös toisella tavalla.

Mikäli ryhmän alkioit 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 ovat tässä mielessä samankaltaisia.

Määritelmä 4.5. Olkoon G ryhmä ja olkoon $x \in G$. Alkion x *konjugaattiluokka* on joukko

$$G_x = \{gxg^{-1} \mid g \in G\}.$$

Kyseessä on siis niiden alkioiden joukko, jotka saadaan konjugoimalla alkioita x .

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 $e x = x$, kun e on ryhmän neutraalialkio. 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. Järjestämällä syklit tarvittaessa uudelleen voidaan olettaa, että $x = x_{1,1}$. Kun 1-syklit on jätetty pois, nähdään, että

$$\tau\sigma^{-1}(y) = \tau(x) = (x_{1,1} \dots x_{1,k_1})[x_{1,1}] = x_{1,2}.$$

Toisaalta $y = x'_{1,1}$, joten

$$\tau'(y) = (x'_{1,1} \dots x'_{1,k_1})[x'_{1,1}] = x'_{1,2} = \sigma(x_{1,2}).$$

Tässäkin tapauksessa siis pätee $\tau'(y) = \sigma(x_{1,2}) = \sigma\tau\sigma^{-1}(y)$, joten väite on todistettu. \square

Merkitään luvuin n_1, n_2, \dots, n_m permutaation σ sykliesityksessä esiintyvien syklien pituuksia (1-syklit mukaanluettuina) ja oletetaan lisäksi, että $n_1 \leq n_2 \leq \dots \leq n_m$. Tällöin jono (n_1, n_2, \dots, n_m) on permutaation σ *syklityyppi*. Lauseesta 4.6 saadaan suoraan seuraava seuraus.

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

Lause 4.6 nähtiin toiminnassa jo esimerkissä 4.2, jossa konjugoitiin 3-sykliä $\tau = (123)$ permutaatiolla $\sigma = (167)(259)(38)$. Koska σ :lle pätee $\sigma(1) = 6$, $\sigma(2) = 5$ ja $\sigma(3) = 8$, tuloksena on lauseen perusteella 3-sykli (658) , kuten myös esimerkissä nähtiin. Tarkastellaan seuraavaksi hieman monimutkaisempaa esimerkkiä.

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 $H = \{\text{id}, \tau, \tau^2, \dots, \tau^{n-1}\}$. Osoitetaan, että H ei voi olla normaali.

Jotta H olisi normaali, sen täytyy sisältää kaikkien alkuidensa konjugaatit. Kuitenkin, jos $\sigma = (x_1 x_2)$, niin lauseen 4.6 mukaan

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

On helppo tarkistaa, että $\tau^m(x_2) = x_1$ vain, jos $m = kn - 1$ jollain kokonaisluvulla k , mutta toisaalta $\tau^{kn-1}(x_1) = x_n \neq x_3$ kaikilla $k \in \mathbb{Z}$. Näin ollen $\sigma\tau$ on eri permutaatio kuin τ^m kaikilla m , joten $\sigma\tau$ ei kuulu aliryhmään H .

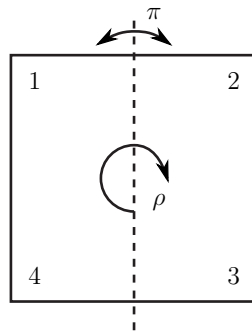
Tässä oletus $n > 3$ on välttämätön, sillä ryhmässä S_3 aliryhmä $\langle(123)\rangle = A_3$ on normaali.

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

Esimerkki 4.9. Tarkastellaan ryhmän S_4 aliryhmää

$$D_8 = \{\text{id}, (1234), (13)(24), (1432), (12)(34), (24), (14)(32), (13)\}.$$

Ryhmää D_8 nimitetään *neliön symmetriaryhmäksi*. Nimitys johtuu siitä, että jos neliön nurkkien alkuperäiset paikat numeroidaan kuvan 13 mukaisesti, jokainen ryhmän D_8 permutaatio vastaa sellaista nurkkien permutaatiota, joka säilyttää neliön rakenteen. Toisin sanoen, jos neliötä käännellään niin, että nurkat palaavat lopulta alkuperäisten nurkkien paikoille, saadaan paikkojen vaihtumisesta ryhmän D_8 permutaatio.



Kuva 13: Neliön kierto ja peilaus.

Neliötä voidaan käänellä pääasiassa kahdella tavalla. Ensimmäinen tapa, neljännesympyrän kierto myötäpäivään, vastaa permutaatiota $\rho = (1234)$. Tämä kierto voidaan

suorittaa neljä kertaa, minkä jälkeen neliö palaa alkuperäiseen asentoonsa, ja näin saadaan kierron virittämä aliryhmä

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

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. Neutraalialkion yksiö $\{\text{id}\}$ muodostaa aina oman konjugaattiluokkansa. Toisaalta syklytyyppi 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 myötöpäivään muuttuu-kin alkuperäisessä neliössä neljänneskierroksi vastapäivään. Sama toimii millä tahansa peilauksella, ja kaikki nämä myös tuottavat 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 $\rho(13) = (24)$.

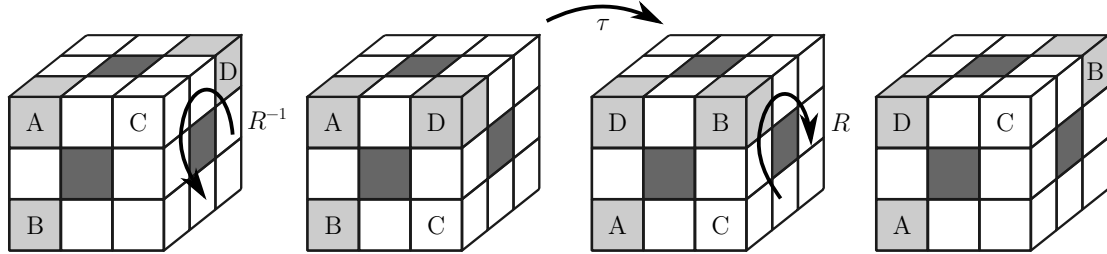
Jäljelle jää vielä kiertoalkio $\rho^2 = (13)(24)$, joka on samaa syklytyyppiä kuin vaaka- ja pystypeilaukset. Kierrolla konjugoiminen tuottaisi kuitenkin vain uuden kierron. Jos taas konjugoitaisiin jollain peilausalkiolla τ , tulisi neliö käännettyksi ensin nurin päin ja sitten kierron jälkeen jälleen 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: $\{\text{id}\}$, $\{(1234), (1432)\}$, $\{(13), (24)\}$, $\{(12)(34), (14)(23)\}$ ja $\{(13)(24)\}$.

4.3. Konjugointi Rubikin ryhmässä

Konjugointi auttaa Rubikin kuution ratkaisussa merkittävästi, sillä sen avulla voidaan opittu siirtosarja siirtää kuution toiseen osaan. Oletetaan esimerkiksi, että halutaan suorittaa paikkaryhmässä \mathbb{R}_p luvussa 3.3 esitetyn syklin asemesta kuvan 14 mukainen 3-sykli, joka liikuttaa paloja A, B ja D. Tällöin voidaan ensin suorittaa perussiirto R^{-1} ,

joka tuo palan D palan C paikalle (ja liikuttaa toki samalla muitakin paloja). Tämän jälkeen suoritetaan aiemmin opittu 3-sykli τ ja lopuksi palautetaan pala C paikalleen perussiirroilla R . On siis suoritettu konjugaattisiirto $R\tau$. Aiemman teoreettisen tarkastelun perusteella tiedetään, että kyseinen konjugaatti todella on 3-sykli eikä liikuta muita kuin haluttuja paloja.



Kuva 14: 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. Tämä johtuu siitä, että 3-syklit ja niiden tulot ovat parillisia. Toiseksi kaikkien konjugointiin tarvittavien permutaatioiden pitäisi olla laillisia siirtoja.

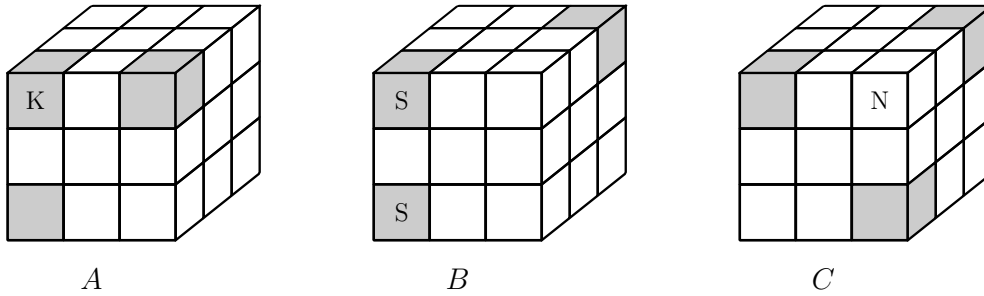
Ensimmäinen ehto ei kuitenkaan päde, koska mikä tahansa perussiirto on nurkkapalojen kannalta 4-sykli, joka ei ole parillinen. Toisaalta, jos nurkkapalat ovat asennossa, joka vastaa paritonta permutaatiota, niin tekemällä mikä tahansa perussiirto saadaan tilanne jälleen vastaamaan parillista permutaatiota. Tällöin se on periaatteessa mahdollista ratkaista 3-syklillä.

Käydään nyt läpi kaikki mahdolliset kolmen nurkkapalan kombinaatiot ja osoitetaan, että näistä jokaista kohti löytyy permutaatio σ , joka vie tunnettuun 3-sykliin τ osallistuvat palat niiden 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 15. Jokaisen joukon sisällä kombinaatiot saadaan johonkin kuvan kolmesta asennosta koko kuutiota kiertämällä.

Lasketaan nyt kussakin joukossa A , B ja C olevien kombinaatioiden lukumäärä, jotta varmistetaan 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 K merkitty pala voi olla neljässä eri kulmassa. 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 kääntämällä kuutio ylösalaisin.) Yhteensä saadaan siis 24 kombinaatiota.



Kuva 15: Kolmen nurkkapalan kombinaatiot.

C: Nämä kombinaatiot koostuvat kirjaimella N merkityn nurkkapalan viereisten nurkkien paloista. Nurkan N 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.

Seuraavaksi on tarkoitus osoittaa, että jokainen nurkkapalojen kombinaatio voidaan tietyllä konjugoinnilla palauttaa kuvan 15 vasemmanpuolimmaiseen asemaan, jossa lisäksi oletetaan keltaisen sivun olevan katsojaan päin ja sinisen ylöspäin. Tällöin opittua nurkkapalojen 3-sykliä soveltamalla saadaan palat oikeaan järjestykseen.

Kunkin joukon *A*, *B* ja *C* sisällä kombinaatiot saadaan johonkin kuvan muotoisista asemista koko kuutiota kiertämällä. Tässä on kuitenkin se ongelma, että kuution kierrossa sivujen merkinnät muuttuvat: katsojaa kohti oleva sivu ei ehkä enää olekaan keltainen vaan esimerkiksi punainen. Tällöin myös siirtojen merkinnät muuttuvat, ja jokaista tapausta varten pitäisi löytää oma konjugointi. Ongelmaan on kaksi ratkaisua.

Ensinnäkin koko kuution kiertämisen sijaan voidaan pitää keskitahtokosta kiinni ja kiertää vain rinnakkaisia sivutahkoja. Tällöin nurkkapalat pysyvät toistensa suhteen samassa asennossa, mutta sivujen värit eivät muutu (eli keltainen sivu on yhä katsojaan päin). Tämä siirto on sitten lisättävä konjugoivaan siirtoon. Käytännöllisempi tapa on kuitenkin yksinkertaisesti kääntää koko kuutiota ympäri ja nimetä sitten uudelleen perussiirrot niin, että edessä olevan uuden tahkon (ei ehkä enää keltainen) kierto on *F*, uuden ylätahkon kierto *U* jne. Tätä ratkaisua käytetään seuraavan lauseen todistuksessa.

Lause 4.10. *Mikä tahansa paikkaryhmän 3-sykli, joka liikuttaa vain nurkkapaloja, on mahdollinen siirto.*

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

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

1. Saatetaan koko kuutiota kiertämällä kuutio johonkin kuvan 15 kolmesta asemasta, minkä jälkeen nimetään siirrot uudestaan niin, että kuvan ylätahkon kiertäminen on U , etutahkon kiertäminen F jne.
- 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 nurkkapalat paikoilta a , b ja c paikoille 1, 2 ja 3. Tämän käänteissiirto on etsitty σ . \square

Käytännössä 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 alkioden 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 alkioden 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 alkioden joukko, jotka kommutoivat kaikkien alkioden 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. Tämä nähdään seuraavasta:

$$gxg^{-1} = x \iff gx = xg \iff g = xgx^{-1}.$$

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

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.

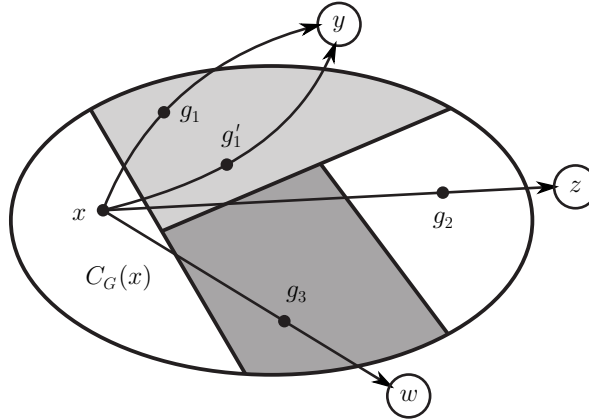
Lause 4.12. Olkoon G äärellinen ryhmä ja olkoon $x \in G$. Keskittäjän $C_G(x)$ sivuluokkien lukumäärä $[G : C_G(x)]$ on sama kuin alkion x konjugaattiluokan koko.

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

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

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. \square

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 $C_G(x)$, $g_1 C_G(x)$, $g_2 C_G(x)$ ja $g_3 C_G(x)$. 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 $y \in g_1 C_G(x)$.



Kuva 16: 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 $C_G(\tau) = \{\text{id}, (123), (132)\}$. 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-sykliden muodostama joukko $(12)C_G(\tau) = \{(12), (23), (13)\}$.

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 alkiolla saadaankin seuraavat tulokset:

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

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, \dots, 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

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

Tätä yhtälöä nimitetään luokkayhtälöksi.

Luokkayhtälö koskee keskittäjien indeksejä $[G : C_G(x_i)]$ eri konjugaattiluokkien edustajilla x_i . Keskukseen kuuluvilla alkiolla x_i on tähän liittyen erityisiä ominaisuuksia. Koska $\zeta G \leq C_G(x_i)$ kaikilla i , luku $|\zeta G|$ jakaa jokaisen luvun $|C_G(x_i)|$ Lagrangen lauseen mukaan. Löytyy siis luvut $k_i \in \mathbb{Z}$, joille pätee $|C_G(x_i)| = k_i \cdot |\zeta G|$ kaikilla i . Edelleen kaikilla i pätee siis

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

Siispä jokainen indeksi $[G : C_G(x_i)]$ jakaa keskuksen indeksin $[G : \zeta G]$. Lisäksi x_i kuuluu keskukseen ζG , 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.

Edellä tehtyjä huomioita käytetään seuraavassa, luvun lopuksi esitettävässä luokkayhtälön sovelluksessa.

Lause 4.14. *Jos ryhmän G koko on p^r , missä p on alkuluku ja r nollaa suurempi kokonaisluku, ryhmällä G on epätriviaali keskus.*

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

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

Lagrangen lauseen perusteella jokainen indeksi n_i jakaa koko ryhmän koon p^r . 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, löytyisi vain yksi indeksi i , jolla $p^{k_i} = 1$. Voidaan olettaa, että kyseinen indeksi on m , jolloin saadaan yhtälö

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

Kyseisen yhtälön vasen puoli on jaollinen luvulla p mutta oikea puoli ei. Tämä on ristiriita, joten keskus ei voi olla triviaali. \square

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, Lagrangen lauseen mukaan $|\zeta G| \in \{1, p, p^2\}$. Edellisen lemmän 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. \square

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

$$H = \langle (1234) \rangle = \{\text{id}, (1234), (13)(24), (1432)\}$$

ja

$$K = \langle (123) \rangle = \{\text{id}, (123), (132)\}.$$

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

$$HK = \{ \text{id}, (1234), (13)(24), (1432), \\ (123), (1324), (142), (34), \\ (132), (14), (234), (1243) \}.$$

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 . Eräs tapa korjata tilanne on vaatia, että aliryhmien H ja K alkio olisivat vaihdannaisia keskenään. Jos tämä ehto toteutuu, edellä mainitussa tulossa pätee

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

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

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 $H \times K$ 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. Myöhemmin nähdään myös toinen tilanne, jossa kahden aliryhmän tulosta HK tulee aliryhmä.

Esimerkki 5.3. Tarkastellaan symmetrisen ryhmän S_5 aliryhmiä

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

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

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

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

Esimerkki 5.4. Tarkastellaan yhteenlaskuryhmää $\mathbb{Z}_{15} = \{[0], [1], [2], \dots, [14]\}$, missä $[n] = [m]$ aina, kun $m - n$ on jaollinen luvulla 15. Tällä ryhmällä on aliryhmät

$$H = \langle [5] \rangle = \{[0], [5], [10]\} \quad \text{ja} \quad K = \langle [3] \rangle = \{[0], [3], [6], [9], [12]\}.$$

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 selvyuden 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 tulona.

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

- 1) Ryhmät H ja K ovat G :n normaaleja aliryhmiä.
- 2) Jokaisella alkioilla $g \in G$ on yksikäsitteinen esitys $g = hk$, missä $h \in H$ ja $k \in K$.

Todistus. Osoitetaan ensin, että ehto 1) pätee. Olkoot sitä varten $x \in H$, $y \in K$ ja $g \in G$. Osoitetaan, että konjugaatit ${}^g x$ ja ${}^g y$ 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 $kx = xk$, joten

$$g x g^{-1} = h(kx)k^{-1}h^{-1} = h(xk)k^{-1}h^{-1} = hxh^{-1} \in H.$$

Toisaalta myös $h(kyk^{-1}) = (kyk^{-1})h$, joten

$$g y g^{-1} = h(kyk^{-1})h^{-1} = (kyk^{-1})hh^{-1} = kyk^{-1} \in K.$$

Siispä ${}^g x \in H$ ja ${}^g y \in K$, joten aliryhmät H ja K ovat normaaleja.

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

$$h_2^{-1} h_1 = k_2 k_1^{-1}.$$

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

Lisätieto. Aliryhmien sisäinen suora tulo voidaan määrittellä myös useammalle kuin kahdelle aliryhmälle. Määritelmä on aivan samanlainen kuin kahden aliryhmän tapauksessa. Jos aliryhmät ovat H_1, \dots, H_r , ehdoiksi tulee

- 1) $h_i h_j = h_j h_i$, kun $i \neq j$, $h_i \in H_i$ ja $h_j \in H_j$
- 2) $H_i \cap (H_{j_1} H_{j_2} \cdots H_{j_{r-1}}) = \{e\}$, kun $i \notin \{j_1, \dots, j_{r-1}\}$.

Suoraa tuloa voidaan tällöin merkitä $H_1 \times H_2 \times \cdots \times H_n$ tai tulomerkinällä $\prod_{i=1}^n H_i$. Määritelmä toimii myös äärettömän monen aliryhmän tapauksessa. Tällöin kuitenkin jokaisella suoran tulon $\prod_{i \in I} H_i$ alkiolla on *äärellinen* esitys $h_{i_1} h_{i_2} \cdots h_{i_n}$, missä $h_{i_k} \in H_{i_k}$ kaikilla k . Ääretöntä alkioiden tuloa ei nimittäin voida ryhmässä yleensä määrittellä.

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

Määritelmä 5.6. 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 $G_1 \times G_2$ tai toisinaan $(G_1 \times G_2)_u$. Jos molemmissa ryhmissä käytetään laskutoimituksena yhteenlaskua, voidaan ulkoista suoraa tuloa kutsua myös *ulkoiseksi suoraksi summaksi* ja merkitä $G_1 \oplus G_2$.

Se, että ulkoinen suora tulo todellakin on ryhmä, on varsin helppo tarkistaa. Erityisesti neutraalialkiona toimii pari (e_1, e_2) , missä e_1 ja e_2 ovat ryhmien G_1 ja G_2 neutraalialkiot, ja alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on (g_1^{-1}, g_2^{-1}) .

Esimerkki 5.7. 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 oikein taulukon muotoon. (Jätetään jälleen taulukosta pois hakasulut alkoiden 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 esimerkin 5.4 vastaavaan, 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 alkioita vastaa pari $([2]_3, [2]_5)$, ja jos lasketaan kyseisen parin monikerrat summaryhmässä $\mathbb{Z}_3 \oplus \mathbb{Z}_5$, saadaan

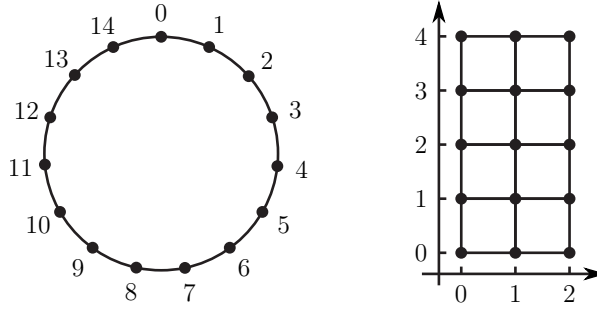
$$\begin{aligned} 2 \cdot (2_3, 2_5) &= (4_3, 4_5) = (1_3, 4_5), \\ 3 \cdot (2_3, 2_5) &= (6_3, 6_5) = (0_3, 1_5), \\ 4 \cdot (2_3, 2_5) &= (8_3, 8_5) = (2_3, 3_5), \\ 5 \cdot (2_3, 2_5) &= (10_3, 10_5) = (1_3, 0_5) \\ &\text{jne.} \end{aligned}$$

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 sykliisiä.

Kuvassa 17 on piirretty syklinen ryhmä \mathbb{Z}_{15} kahdella tavalla: yhtenä pitkänä syklinä ja kahden ryhmän tulona.

Esimerkki 5.8. 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. Pätee myös tuloryhmässä

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



Kuva 17: Kaksi tapaa hahmottaa 15 alkion syklinen ryhmä.

eli kahden ”negatiivisen” permutaation tulo on positiivinen. 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 voidaan osoittaa, että ryhmät $A_n \times (\{1, -1\}, \cdot)$ ja S_n eivät ole isomorfisia muuten kuin tapauksessa $n = 2$.

Jos H_1 ja H_2 ovat ryhmien G_1 ja G_2 aliryhmiä, 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 5.9. *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

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

Lisäksi, koska H_1 ja H_2 ovat normaaleja, konjugaateille täytyy päteä $g_1 h_1 g_1^{-1} \in H_1$ 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. \square

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

Lause 5.10. *Olkoot G_1 ja G_2 ryhmiä.*

- On olemassa aliryhmät $\tilde{G}_1, \tilde{G}_2 \leq (G_1 \times G_2)_u$, joille pätee $\tilde{G}_1 \cong G_1$, $\tilde{G}_2 \cong G_2$ ja $(\tilde{G}_1 \times \tilde{G}_2)_s = (G_1 \times G_2)_u$.*
- Jos H ja K ovat ryhmän G aliryhmiä, jotka muodostavat sisäisen suoran tulon, niin $(H \times K)_s \cong (H \times K)_u$.*

Jos ryhmä G on joidenkin aliryhmiensä H ja K sisäinen suora tulo, sitä voidaan lauseen nojalla ajatella myös ulkoisena tuloryhmänä $H \times K$, jonka alkiot ovat pareja (h, k) . Tällainen pari samastetaan siinä tapauksessa ryhmän G alkioon hk . Toisaalta, jos G_1 ja G_2 ovat eri ryhmiä, voidaan niiden ulkoisen suoran tulon alkioita (g_1, g_2) toisinaan merkitä yksinkertaisemmin $g_1 g_2$.

Lauseen 5.10 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 $\tilde{G}_1 = (G_1 \times \{e_2\})_u$ ja $\tilde{G}_2 = (\{e_1\} \times G_2)_u$. Selvästikin $\tilde{G}_1 \cong G_1$ ja $\tilde{G}_2 \cong G_2$. (Isomorfismit kuvaavat $(g_1, e_2) \mapsto g_1$ ja $(e_1, g_2) \mapsto g_2$.) Lisäksi $\tilde{G}_1 \cap \tilde{G}_2 = \{(e_1, e_2)\}$ ja kaikilla $g_1 \in G_1$ ja $g_2 \in G_2$ pätee

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

Aliryhmien \tilde{G}_1 ja \tilde{G}_2 tulo on siis suora, ja sitä voidaan merkitä $(\tilde{G}_1 \times \tilde{G}_2)_s$. Edelleen 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 $(g_1, e_2) \in \tilde{G}_1$ ja $(e_1, g_2) \in \tilde{G}_2$. Täten $(\tilde{G}_1 \times \tilde{G}_2)_s = (G_1 \times G_2)_u$.

Todistetaan sitten toinen väite. Olkoot H ja K ryhmän G aliryhmiä. Määritellään kuvaus $\varphi: (H \times K)_u \rightarrow (H \times K)_s$ kaavalla $\varphi(h, k) = hk$ ja osoitetaan, että se on isomorfismi. Ensinnäkin jokainen sisäisen suoran tulon alkio on muotoa hk joillakin $h \in H$ ja $k \in K$. Nyt pätee $\varphi(h, k) = hk$, 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 $h_1 k_1 = h_2 k_2$ ryhmässä $(H \times K)_s$, ja koska lemmän 5.5 mukaan jokaisen sisäisen suoran tulon alkion esitys tällaisena tulona on yksikäsitteinen, täytyy olla $h_1 = h_2$ ja $k_1 = k_2$ ja edelleen $(h_1, k_1) = (h_2, k_2)$. Kuvaus φ on siis myös injektio. Homomorfisuus seuraa siitä, että yhtälöketju

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

pätee kaikilla $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Tässä käytettiin sisäisen suoran tulon tekijöiden vaihdannaisuutta. \square

Suoran summan käsite esiintyy usein modulien ja vektoriavaruuksien yhteydessä, jotka ovat yhteenlaskun suhteen vaihdannaisia ryhmiä. Esimerkiksi taso \mathbf{R}^2 on ulkoinen suora summa kahdesta ryhmästä $(\mathbf{R}, +)$, sillä sen alkiot ovat pareja (x, y) , ja yhteenlasku toimii komponenteittain: $(x, y) + (z, w) = (x + z, y + w)$. Toisaalta taso on myös x - ja y -akselin *sisäinen* suora summa, sillä jokainen tason vektori voidaan kirjoittaa eräiden muotoa $\tilde{x} = (x, 0)$ ja $\tilde{y} = (0, y)$ olevien vektorien summana. Molemmat esitystavat kuvaavat samaa rakennetta, ja niiden yhteys ilmenee kaavasta $(x, y) = \tilde{x} + \tilde{y}$.

Esimerkki 5.11. 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 lemmän 5.5 perusteella, ja toinen niistä sisältää neutraalialkion lisäksi vain yhden alkion: olkoon esimerkiksi $C = \{\text{id}, \sigma\}$. Näytetään, että C ei voi olla normaali.

Koska $\sigma^2 = \text{id}$, 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 nurkkapalaa kiinnitettyä ruutua särmäpalaan tai päinvastoin. Siispä sellaiset siirrot, jotka koskevat vain nurkkaruutuja, ovat täysin riippumattomia särmäruutuja liikuttavista siirroista, jolloin on samantekevää, tekeekö pelkkiin nurkkaruutuihin vaikuttavan siirron ennen pelkkiin särmäruutuihin vaikuttavaa siirtoa vai toisinpäin. Tällaisten pelkästään yhdentyypisiin ruutuihin vaikuttavat siirtojen joukot muodostavat Rubikin ryhmässä sisäisen suoran tulon.

Tässä luvussa määritellään edellä mainittu Rubikin ryhmän sisäinen suora tulo sekä osoitetaan muutama tämän tuloryhmän ja Rubikin ryhmän väliseen suhteeseen 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 nurkkaruutujen permutaatioiden ryhmä, ja S_S vastaavasti särmäruutujen permutaatioiden ryhmä. Jos kaikki ruudut numeroidaan luvuilla $1, \dots, 48$, näiden permutaatioryhmien voidaan ajatella olevan ryhmän S_{48} aliryhmiä.

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

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

Permutaation kantaja on siis niiden alkioiden joukko, joihin permutaatio vaikuttaa epätriviaalisti. Esimerkiksi permutaation (156)(28) kantaja ryhmässä S_9 on $\{1, 2, 5, 6, 8\}$. Permutaation kantajalle pätee muun muassa seuraavat ominaisuudet:

- 1) $\sigma(x) \in \text{supp}(\sigma)$, jos ja vain jos $x \in \text{supp}(\sigma)$
- 2) $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$
- 3) $\text{supp}(\sigma \circ \tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$.

Näiden ominaisuuksien todistaminen on helppo harjoitustehtävä.

Nyt voidaan määritellä ryhmät S_N ja S_S kantajan käsitteen avulla seuraavasti:

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

Koska mikään ruutu ei ole kiinni sekä nurkka- että särmäpalassa, joukot N ja S ovat erillisiä. Tästä seuraa, että nurkka- ja särmäpaloja permutoivat aliryhmät S_N ja S_S muodostavat suoran tulon ryhmässä S_{48} . Tämä todistetaan seuraavassa lauseessa hieman yleisemmässä muodossa.

Lause 5.12. *Olkoot G ja H joukon X symmetrisen ryhmän S_X aliryhmiä. Oletetaan, että joillain joukoilla $A, B \subset X$ pätee $A \cap B = \emptyset$, $\text{supp}(\sigma) \subset A$ kaikilla $\sigma \in G$ ja $\text{supp}(\sigma) \subset B$ kaikilla $\sigma \in H$. Tällöin G ja H muodostavat suoran tulon ryhmässä S_X .*

Todistus. Ensinnäkin huomataan, että jos σ kuuluu molempiin ryhmiin G ja H , täytyy päteä $\text{supp}(\sigma) \subset A \cap B = \emptyset$, eli $\sigma(x) = x$ kaikilla alkioilla $x \in X$. Täten $\sigma = \text{id}$.

Olkoot sitten $\sigma \in G$ ja $\tau \in H$. Jos $x \in \text{supp}(\sigma)$, permutaation kantajan ominaisuuksien perusteella pätee $\sigma(x) \in \text{supp}(\sigma)$. Koska $\text{supp}(\tau) \cap \text{supp}(\sigma) = \emptyset$, nähdään että $\tau(x) = x$ ja myöskin $\tau\sigma(x) = \sigma(x)$. Täten

$$\tau\sigma(x) = \sigma(x) = \sigma\tau(x).$$

Jos taas $x \in \text{supp}(\tau)$, niin $\tau(x) \in \text{supp}(\tau)$, ja samoin kuin edellä saadaan

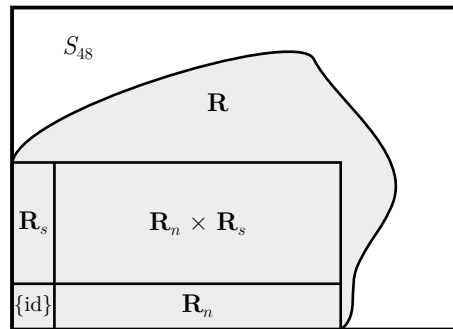
$$\sigma\tau(x) = \tau(x) = \tau\sigma(x).$$

Lopulta jos $x \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$, niin $\sigma(x) = \tau(x) = x$, joten $\sigma\tau(x) = \tau\sigma(x)$. Näin on osoitettu, että $\sigma\tau = \tau\sigma$, eli aliryhmät G ja H ovat keskenään vaihdannaisia. Ne muodostavat siis suoran tulon. \square

Ryhmät S_N ja S_S muodostavat suoran tulon kaikkien ruutujen permutaatioryhmässä S_{48} . Kaikki näiden ryhmien alkiot eivät kuitenkaan ole laillisia siirtoja. Määritellään siksi vielä erikseen edellä käsiteltyjen ryhmien Rubikin ryhmään sisältyvät osat.

Määritelmä 5.13. Leikkausjoukkoa $\mathbb{R}_n = \mathbb{R} \cap S_N$ kutsutaan Rubikin *nurkkaryhmäksi* ja leikkausjoukkoa $\mathbb{R}_s = \mathbb{R} \cap S_S$ puolestaan Rubikin *särmäryhmäksi*.

Rubikin nurkkaryhmä sisältää sellaiset lailliset siirrot, jotka liikuttavat vain nurkka-ruutuja, ja särmäryhmä puolestaan on niiden laillisten siirtojen joukko, jotka liikuttavat vain särmäruutuja. Koska nämä joukot on määritelty kahden ryhmän leikkauksina, ne ovat itsekin ryhmiä ja siten Rubikin ryhmän aliryhmiä. Edelleen ryhmät \mathbb{R}_n ja \mathbb{R}_s muodostavat Rubikin ryhmän sisäisen suoran tulon, sillä niiden kantajat ovat erilliset (kantajat sisältyvät edelleen joukkoihin N ja S). Tuloryhmään $\mathbb{R}_n \times \mathbb{R}_s$ kuuluvat siirrot koostuvat nurkkiin ja särmiin vaikuttavista osista, joita voidaan käsitellä toisistaan riippumatta. Rubikin ryhmässä on kuitenkin myös sellaisia siirtoja, jotka eivät kuulu kyseiseen tuloryhmään. Kuvassa 18 on esitetty Venn-diagrammina Rubikin ryhmän ja tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ suhde.



Kuva 18: Tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ asema Rubikin ryhmässä.

Jako nurkka- ja särmäryhmiin heijastuu myös asento- ja paikkaryhmiin. Asentoryhmää koskeva tulos voidaan jälleen antaa yleisessä muodossa.

Lause 5.14. Jos $H \leq G$ ja $N \trianglelefteq G$, niin $H \cap N \trianglelefteq H$.

Todistus. Kahden aliryhmän leikkaus on aliryhmä, joka sisältyy kumpaankin leikkaavaan aliryhmään. Se on siis erityisesti niiden molempien aliryhmä. Lisäksi, jos $n \in H \cap N$ ja $h \in H$, niin $h_n \in N$, koska N on normaali G :ssä, ja $h_n \in H$, koska $n \in H$. Täten $H \cap N$ on normaali aliryhmä H :ssa. \square

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

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

edellisen lauseen nojalla normaaleja vastaavissa ryhmissä \mathbb{R}_n ja \mathbb{R}_s . Näin ollen 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} :n alkiot vain *särmäpalojen paikkoja*, niiden asennoista välittämättä.

Näytetään vielä lopuksi, että tekijäryhmät \mathbb{R}_{np} ja \mathbb{R}_{sp} voidaan upottaa luonnollisella tavalla Rubikin paikkaryhmään, jossa ne muodostavat suoran tulon. Merkitään tässä yhteydessä eri aliryhmiin liittyviä sivuluokkia seuraavasti:

$$[\sigma]_n = \sigma \mathbb{R}_{na}, \quad [\tau]_s = \tau \mathbb{R}_{sa} \quad \text{ja} \quad [\rho] = \rho \mathbb{R}_a.$$

Tässä tietysti $\sigma \in \mathbb{R}_n$, $\tau \in \mathbb{R}_s$ ja $\rho \in \mathbb{R}$.

Lause 5.15. a) *Tekijäryhmät \mathbb{R}_{np} ja \mathbb{R}_{sp} ovat isomorfisia joidenkin Rubikin paikkaryhmän \mathbb{R}_p aliryhmien kanssa. Isomorfismeiksi voidaan lisäksi valita kuvaukset φ_1 ja φ_2 , joille pätee $\varphi_1: [\sigma]_n \mapsto [\sigma]$ kaikilla $\sigma \in \mathbb{R}_n$ ja $\varphi_2: [\tau]_s \mapsto [\tau]$ kaikilla $\tau \in \mathbb{R}_s$.*

b) *Ryhmien \mathbb{R}_{np} ja \mathbb{R}_{sp} kuvat a)-kohdan isomorfismeissa muodostavat suoran tulon ryhmässä \mathbb{R}_p .*

Lauseen a)-kohdan merkitys on seuraava. Ajatellaan esimerkiksi nurkkaryhmään kuuluvia permutaatioita välittämättä palojen asennoista. Tämä on tietysti sama asia kuin jos ajateltaisiin sellaisia paikkaryhmän siirtoja, jotka vaikuttavat vain nurkkapaloihin. Kyseessä on kuitenkin eri tekijäryhmät, sillä ne on muodostettu eri normaalien aliryhmien avulla. Teknisesti ottaen aliryhmän \mathbb{R}_{na} sivuluokat ovat suppeampia kuin aliryhmän \mathbb{R}_a . Nyt todistettava lause antaa tekijäryhmien välille luonnollisen isomorfismin.

Lauseen 5.15 todistus. a) Tarkastellaan ryhmää \mathbb{R}_{np} . Toisen ryhmän tapauksessa todistus on aivan samanlainen. Koska ollaan määrittelemässä kuvausta tekijäryhmältä johonkin toiseen ryhmään, on aluksi tarkistettava, että kuvauksen arvot eivät riipu sivuluokan edustajan valinnasta.

Olkoon $\sigma \in \mathbb{R}_n$. Jos nyt $[\sigma]_n = [\sigma']_n$ jollain $\sigma' \in \mathbb{R}_n$, niin $\sigma^{-1}\sigma' \in \mathbb{R}_{na}$. Erityisesti tällöin pätee $\sigma^{-1}\sigma' \in \mathbb{R}_a$ eli $[\sigma] = [\sigma']$. Siispä jokaista sivuluokkaa $[\sigma]_n \in \mathbb{R}_{np}$ vastaa yksikäsitteinen sivuluokka $[\sigma] \in \mathbb{R}_p$, joten voidaan määritellä kuvaus $\varphi: \mathbb{R}_{np} \rightarrow \mathbb{R}_p$, jolle

pätee $\varphi([\sigma]_n) = [\sigma]$. Tällainen kuvaus on lisäksi homomorfismi, sillä kaikilla $\sigma_1, \sigma_2 \in \mathbb{R}_n$ pätee

$$\varphi([\sigma_1]_n) \cdot \varphi([\sigma_2]_n) = [\sigma_1] \cdot [\sigma_2] = [\sigma_1\sigma_2] = \varphi([\sigma_1\sigma_2]_n) = \varphi([\sigma_1]_n \cdot [\sigma_2]_n).$$

Osoitetaan, että kuvaus φ on injektio. Oletetaan sitä varten, että $[\sigma_1] = [\sigma_2]$ joillain $\sigma_1, \sigma_2 \in \mathbb{R}_n$. Tällöin pätee $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_a$. Toisaalta pätee myös $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_n$, koska \mathbb{R}_n on ryhmä. Siispä $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_{na}$ eli $[\sigma_1]_n = [\sigma_2]_n$. Kuvaus φ on siis injektiivinen homomorfismi ryhmälle \mathbb{R}_p , joten lähtöryhmä \mathbb{R}_{np} on isomorfinen kuvaryhmän $\text{Im}(\varphi) \leq \mathbb{R}_p$ kanssa.

b) Osoitetaan, että kuvaryhmät

$$H = \{[\sigma] \in \mathbb{R}_p \mid \sigma \in \mathbb{R}_n\} \quad \text{ja} \quad K = \{[\tau] \in \mathbb{R}_p \mid \tau \in \mathbb{R}_s\}$$

muodostavat suoran tulon paikkaryhmässä \mathbb{R}_p . Olkoot $\sigma \in \mathbb{R}_n$ ja $\tau \in \mathbb{R}_s$. Koska \mathbb{R}_n ja \mathbb{R}_s muodostavat suoran tulon, pätee $\sigma\tau = \tau\sigma$. Niinpä

$$[\sigma] \cdot [\tau] = [\sigma\tau] = [\tau\sigma] = [\tau] \cdot [\sigma].$$

Kuvaryhmät H ja K ovat siis keskenään vaihdannaisia.

Oletetaan sitten, että $[\pi] \in H \cap K$ jollain \mathbb{R} . Tällöin $[\pi] = [\sigma]$ joillain $\sigma \in \mathbb{R}_n$ ja $[\pi] = [\tau]$ jollain $\tau \in \mathbb{R}_s$. Pyritään osoittamaan, että $[\pi] = [\text{id}]$. Tällöin kuvaryhmien leikkaus on triviaali.

(Huomaa, että tässä ei voida olettaa alkion π kuuluvan molempiin ryhmiin \mathbb{R}_n ja \mathbb{R}_s . Voisi nimittäin olla, että joukoilla $\mathbb{R}_n \cap [\pi]$ ja $\mathbb{R}_s \cap [\pi]$ ei olisi yhtään yhteisiä alkioita.)

Koska $[\sigma] = [\tau]$, nähdään että

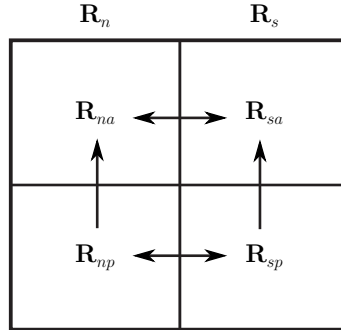
$$\sigma = \tau\rho \quad \text{jollain } \rho \in \mathbb{R}_a.$$

Tämän yhtälön vasemmalla puolella oleva permutaatio kuuluu ryhmään \mathbb{R}_n , joten se ei liikuta särmäpaloja paikoiltaan. Toisaalta oikealla puolella oleva permutaatio on tulo särmäryhmän ja asentoryhmän siirroista, joten se ei liikuta nurkkapaloja paikoiltaan. Koska vasen ja oikea puoli ovat samat, kumpikaan permutaatio ei liikuta mitään paloja paikoiltaan. Täten $\sigma \in \mathbb{R}_a$ eli $[\sigma] = [\pi] = [\text{id}]$. \square

Lauseen a)-kohta pätee ryhmissä yleisesti, kun ryhmät on määritelty lausetta 5.14 vastaavalla tavalla: tällöin ryhmää \mathbb{R}_{np} vastaa ryhmä $H/(H \cap N)$ jne. Tällaiset aliryhmän tekijäryhmät voidaan siis aina upottaa laajempaan tekijäryhmään G/N . Sen sijaan b)-kohdan tulos ei päde yleisesti edes permutaatioryhmillä, vaikka aliryhmien kantajat olisivatkin erilliset. Upotetut tekijäryhmät saattavat nimittäin yleisessä tapauksessa leikata toisiaan epätriviaalisti. Rubikin kuution rakenne kuitenkin estää tämän.

Kuvassa 19 on kaavamaisesti esitetty tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ rakenne. Kullakin vaakarivillä vierekkäiset ryhmät muodostavat suoran tulon. Niin kuin aiemmin on mainittu, jos annettu Rubikin kuution asema sisältyy tuloryhmään $\mathbb{R}_n \times \mathbb{R}_s$, nurkkaruudut voidaan ratkaista särmäruuduista riippumatta. Asema on nimittäin tällöin tulo kahdesta permutaatiosta, joista toinen vaikuttaa pelkkiin nurkkaruutuihin ja toinen pelkkiin särmäruutuihin. Voidaan esimerkiksi ratkaista ensin nurkkaruudut (vasen sarake), sitten

särmäruudut (oikea sarake). Edelleen sekä nurkka- että särmäpalojen kohdalla voidaan noudattaa aikaisempaa jakoa, jossa ratkaistaan ensin palojen paikat, sitten niiden asennot. Ensin siis käytettäisiin jompaa kumpaa kuvion alarivin ryhmää (paikkaryhmä), sitten sen yläpuolella oleva ryhmää.



Kuva 19: Tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ rakenne.

Toisaalta mikä tahansa asema voidaan ratkaista myös ratkaisemalla ensin kaikkien palojen paikat, sitten niiden asennot. Lauseen 5.15 a)-kohdan perusteella paikkoja muuttavat nurkkaryhmän permutaatiot ovat sama asia kuin nurkkiin kohdistuvat paikkaryhmän permutaatiot, ja sama pätee särmäryhmälle. Lisäksi saman lauseen b)-kohdan mukaan nurkka- ja särmäpalojen paikkaryhmät muodostavat suoran tulon koko paikkaryhmässä, joten ne voidaan myös ratkaista toisistaan täysin riippumatta. Jokainen tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ asema voidaan siis ratkaista esimerkiksi siirtämällä ensin nurkkapalat paikoilleen, ratkaisemalla sitten särmien paikat ja asennot, ja asettamalla lopuksi nurkat oikeisiin asentoihin. Muutkin yhdistelmät ovat mahdollisia; ainoa rajoitus on, että ennen kutakin ylärivin ryhmää on ratkaistava sen alapuolella oleva ryhmä.

Edellä esitetyt ratkaisuvaihtoehdot toimivat kuitenkin vain tuloryhmässä $\mathbb{R}_n \times \mathbb{R}_s$, joka ei sisällä kaikkia mahdollisia asemia. Luvussa 5.4 selvitetään, miten yleisestä tapauksesta voidaan aina siirtyä tuloryhmään.

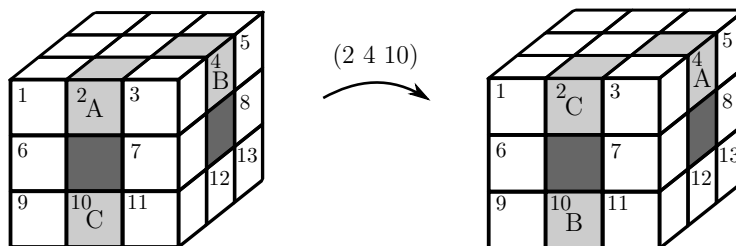
5.3. Algoritmi 2: särmäpalojen 3-sykli

Särmäpalojen siirtelyä varten on tunnettava jokin särmäpalojen 3-sykli. Jäljempänä tullaan näkemään, että tämä 3-sykli voidaan konjugoida mille tahansa toiselle särmäpalojen 3-syklille, ja tämä johtaa lopulta koko paikkaryhmän ratkaisuun.

Valittu 3-sykli on esitetty kuvassa 20. Kun palojen paikat numeroidaan kuvan mukaisesti, sykli on muotoa $(2\ 4\ 10)$. Itse siirtosarja löytyy perussiirtojen avulla esitettynä liitteestä A.2.

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.

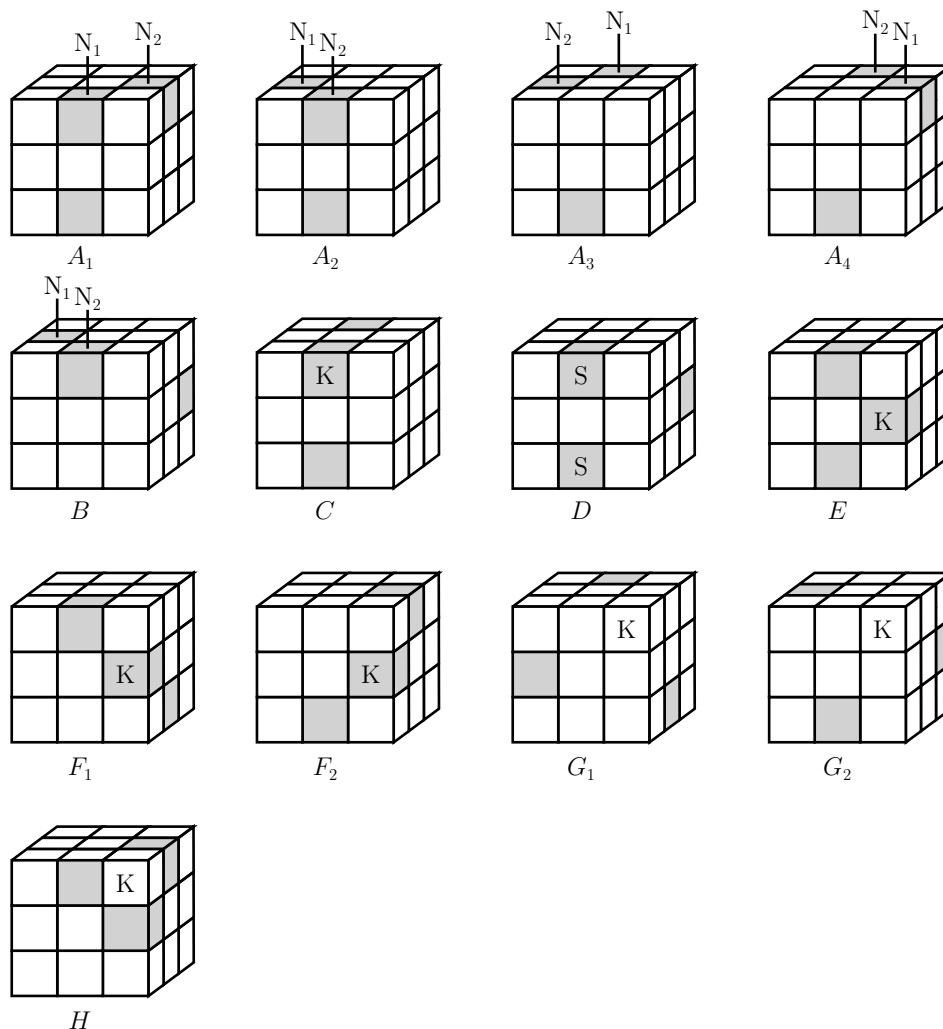


Kuva 20: Särmäpalojen 3-sykli.

Käydään ensin läpi kaikki kolmen särmäpalan kombinaatiot samalla tavoin kuin luvussa 4.3 tehtiin nurkkapaloille. Tällä kertaa kombinaatioita tulee yhteensä $\binom{12}{3} = 220$ kappaletta, ja ne voidaan jakaa 13 joukkoon kuvan 21 mukaisesti. Kunkin joukon sisällä kombinaatiot saadaan kuvan mukaiseen asentoon 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.
- A_2, A_3, A_4 Nämä kombinaatiot saadaan joukon A_1 kombinaatioista yksikäsitteisellä tavalla, nimittäin kiertämällä ylätahkoa kussakin tapauksessa tietyn verran. Kussakin 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 kullakin tahkolla 4 palan 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.



Kuva 21: Kolmen särmäpalan kombinaatiot.

G_1, G_2 Kirjaimella K merkitty pala voidaan valita vapaasti kaikkien nurkkapalojen joukosta, ja muut 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 21 lueteltua kombinaatioiden joukkoa kohti löytyy siirto, jolla palat saadaan kirjaimella A_1 merkittyyn perusasemaan. Edelleen kunkin kombinaatiojoukon sisällä kombinaatio saadaan kuvan mukaiseen asemaan kuutiota kiertämällä, jonka jälkeen siirrot voidaan nimetä uudelleen niin, että katsojaan päin olevan tahkon kierroksi tulee F , ylätahkon kierroksi U jne.

Konjugoivan siirron käänteissiirto löytyy seuraavasti. Ensin saatetaan kuutiota kiertämällä kuutio johonkin kuvan 21 kolmestatoista asemasta, joista jokaisessa oletetaan sinisen sivun osoittavan ylöspäin ja keltaisen sivun katsojaan päin. Jos päädyttiin asemaan A_1 , siirto on valmis. Muuten suoritetaan (uudelleen nimettyjä) perussiirtoja oikeisen 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	RU
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. \square

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) aliryhminä. Ne 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, sille löytyy yksikäsitteinen esitys parina $\tau = (\nu, \sigma)$, missä $\nu \in S_N^p$ ja $\sigma \in S_S^p$. Lisäksi pätee $\text{sign}(\nu) = \text{sign}(\sigma)$.*

Todistus. Koska τ on paikkaryhmän siirto, se voidaan esittää paikkaryhmän perussiirtojen τ_1, \dots, τ_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

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

Jokainen Rubikin paikkaryhmän \mathbb{R}_p siirto voidaan kirjoittaa parina $(\nu, \sigma) \in S_N^p \times S_S^p$. Jos myös ν ja σ kuuluvat ryhmään \mathbb{R}_p , niin (ν, σ) on tuloryhmässä $\tilde{\mathbb{R}}_{np} \times \tilde{\mathbb{R}}_{sp}$, missä $\tilde{\mathbb{R}}_{np}$ ja $\tilde{\mathbb{R}}_{sp}$ ovat lauseen 5.15 antamat ryhmien \mathbb{R}_{np} ja \mathbb{R}_{sp} isomorfiset kuvat ryhmässä \mathbb{R}_p . Edellisen lemmän avulla saadaan nyt lause, joka mahdollistaa paikkaryhmän ratkaisemisen. Merkinnöissä samastetaan tästedes ryhmät \mathbb{R}_{np} ja \mathbb{R}_{ns} isomorfisten kuviensa kanssa.

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 lemmän perusteella pätee tällöin $\text{sign}(\nu) = \text{sign}(\sigma) = 1$. Lauseissa 4.10 ja 5.16 on osoitettu, että kaikki nurkka- ja särmäpalojen 3-syklit ovat mahdollisia siirtoja, ja lauseen 3.12 mukaan jokainen parillinen permutaatio saadaan 3-sykliden 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 paikkaryhmän perussiirto. Oletetaan, että $\tau = (\nu, \sigma) \in \mathbb{R}_p$ 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 lemmän mukaan olla $\text{sign}(\nu) = \text{sign}(\sigma) = -1$, ja koska perussiirrolle toisaalta 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 $\tau \in \pi(\mathbb{R}_{np} \times \mathbb{R}_{sp})$. Koska mikä tahansa tuloryhmään kuuluvan permutaatio kuuluu yhteen tiettyyn tuloryhmän sivuluokkaan, sivuluokkia voi olla korkeintaan kaksi. \square

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

1. Selvitetään, onko ratkaistavassa asemassa nurkkapalojen (tai särmäpalojen) permutaatio parillinen. Jos ei ole, tehdään jokin perussiirto. Tämän jälkeen *sekä* nurkka- *että* särmäpalojen permutaatio on parillinen.
2. Ratkaistaan nurkat ja särmät erikseen aiemmin opittujen 3-sykliden 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 $n_1h_1n_2h_2$. Jotta tämä alkio kuuluisi

edelleen joukkoon NH , riittää että toinen aliryhmistä, vaikkapa 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 $HN = H \rtimes N$.

Esimerkki 5.20. Alternoivalla ryhmällä A_4 on normaali aliryhmä

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

Tarkastellaan tämän lisäksi 3-syklin virittämää aliryhmää $H = \{\text{id}, (123), (132)\}$, 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. Voidaan siis todeta, että $N \rtimes H = A_4$ 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 yhtälöstä, joka pätee kaikissa ryhmissä:

$$n_1h_1 \cdot n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1{}^{h_1}n_2 \cdot h_1h_2. \quad (5.1)$$

Puolisuoran tulon tapauksessa aliryhmä N on normaali, joten konjugaatti ${}^{h_1}n_2$ kuuluu edelleen aliryhmään N .

Yllä oleva kaava kertoo, että ei-normaalien ryhmien H alkioita voidaan kertoa keskenään N :n alkioista riippumatta aivan kuten suorassa tulossa, mutta normaalien aliryhmien alkioita kerrottaessa on toista konjugoitava ensin H :n alkiolla. Kyseessä on siis eräänlainen puolittainen riippumattomuus.

Jos normaali aliryhmä on tulossa oikeanpuoleisena, kaava (5.1) tulee muotoon

$$h_1 n_1 \cdot h_2 n_2 = h_1 h_2 \cdot h_2^{-1} n_1 n_2.$$

Kaavan (5.1) 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 $x \mapsto {}^g x$. 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 alkioden tuloa vastaa yhdistetty kuvaus, nimittäin ${}^{gh} x = {}^g ({}^h x)$. Nämä ominaisuudet huomioiden voidaan määritellä ryhmän konjugointi toisessa ryhmässä.

Määritelmä 5.21. Olkoot G ja H ryhmiä. Kuvausta $g \mapsto \varphi_g$, joka liittyy 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) $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ kaikilla $g_1, g_2 \in G$.

Konjugoivan toiminnan käsitteen sekä kaavan (5.1) avulla voidaan määritellä kahden mielivaltaisen ryhmän puolisuora tulo.

Määritelmä 5.22. Olkoot (N, \diamond) ja $(G, *)$ ryhmiä. Oletetaan, että on määritelty jokin ryhmän G konjugoiva toiminta $g \mapsto \varphi_g$ ryhmässä N . Ryhmien N ja G *ulkoinen puolisuora tulo* $N \rtimes G$ muodostuu pareista (n, g) , missä $n \in N$ ja $g \in G$. Laskutoimitus määritellään kaavalla

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

Toisin päin merkityssä puolisuorassa tulossa $G \rtimes N$ laskutoimitus on vastaavasti

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

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

Ulkoisen suoran tulon rakenne riippuu valitusta konjugoivasta toiminnasta ja eri valinnat tuottavat erilaisen tulon. Toiminnaksi voidaan myös valita $\varphi_g = \text{id}$ kaikilla g , jolloin puolisuorasta tulosta tulee suora tulo.

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

Lause 5.23. *Ryhmien (N, \diamond) ja $(H, *)$ puolisuora tulo on ryhmä.*

Todistus. Puolisuora tulo on suljettu määritellyn 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

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

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 ja e_G ovat ryhmien N ja G neutraalialkiot. 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 $\varphi_{e_N} = \text{id}$ ja $\varphi_g(e_N) = e_N$ (homomorfismin ominaisuus).

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

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

ja

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

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

Esimerkki 5.24. Tarkastellaan neliön symmetriaryhmän aliryhmää

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

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

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

Muodostetaan nyt ryhmän N puolisuora tulo ryhmän $\mathbb{Z}_3 = \{[0], [1], [2]\}$ kanssa. Sitä varten on ensin määriteltävä ryhmän \mathbb{Z}_3 konjugoiva toiminta ryhmässä N .

Konjugoivan toiminnan määritelmän mukaan täytyy päteä $\varphi_0 = \text{id}$ ja toisaalta myös $\varphi_2 = \varphi_{1+1} = \varphi_1 \circ \varphi_1$. Toiminta riippuu siis vain alkioita $[1] \in \mathbb{Z}_3$ vastaavasta isomorfisista φ_1 . Määritellään se seuraavan taulukon mukaisesti:

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

$$\varphi_1(\pi)\varphi_1(\rho^2) = \rho^2 \cdot \pi\rho^2 = \pi = \varphi_1(\pi\rho^2).$$

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

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

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

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

sillä kaikkien ryhmän N alkioiden kertaluku on 2. Muotoa $(\sigma, 0)$ olevien alkioiden kertaluku on siis kaksi, lukuunottamatta neutraalialkiota $(\text{id}, 0)$.

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 nolasta 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 $\sigma = \text{id}$, niin tulo $\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma)$ on kolmen identtisen permutaation tulo. Jos taas $\sigma \neq \text{id}$, 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_4 kanssa.

6. Kommutaattorit

Ryhmässä kahden alkion kommutaattori on kolmas alkio, joka mittaa alkuperäisten alkoiden vaihdannaisuutta. Jos alkiot kommutoivat keskenään, niiden kommutaattori on neutraali-alkio. Kommutaattorit ovat hyödyllinen apuväline epävaihdannaisia ryhmiä tarkasteltaessa.

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 alkoiden g ja h *kommutaattoriksi*.

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

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

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 kommutaattorin laskeminen ei ole symmetrinen operaatio, sillä $[g, h] = [h, g]^{-1}$.

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 alkoiden välistä kommutointia, niitä voi käyttää myös *tuottamaan* erityisen suuria tai pieniä alkioita. Jos nimittäin löydetään alkioita, jotka näyttävät olevan lähes vaihdannaisia keskenään, niiden kommutaattoriksi saadaan 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 $\text{supp}(\sigma) \cap \text{supp}(\tau) = \{x\}$ jollain $x \in X$, niin*

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

Todistus. Todistuksen seuraamisessa saattaa olla hyötyä kuvasta 22. Näytetään ensin, että ehdosta $\text{supp}(\alpha) \cap \text{supp}(\beta) = \{x\}$ seuraa aina $[\alpha, \beta](x) = \alpha(x)$. Huomataan aluksi, että $\beta(x) \in \text{supp}(\beta)$, koska alkion kuva permutaatioissa kuuluu aina permutaation kantajaan. Samaten $\beta^{-1}(x) \in \text{supp}(\beta)$, koska permutaation ja käänteispermutaation kantajat ovat samat. Edelleen $x \in \text{supp}(\beta^{-1})$, joten $\beta^{-1}(x) \neq x$, mistä seuraa, että $\beta^{-1}(x) \notin \text{supp}(\alpha)$. Nyt saadaan

$$[\alpha, \beta](x) = \alpha\beta\alpha^{-1} \underbrace{\beta^{-1}(x)}_{\notin \text{supp}(\alpha)} = \alpha\beta\beta^{-1}(x) = \alpha(x).$$

Koska $\text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$, $\text{supp}(\tau^{-1}) = \text{supp}(\tau)$ ja $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$, yllä saadusta tuloksesta sekä luvun alkupuolella mainituista kaavoista seuraa, että

$$\begin{aligned} [\sigma, \tau](x) &= \sigma(x), \\ [\sigma, \tau](\sigma(x)) &= (\sigma \circ [\tau, \sigma^{-1}])(x) = \sigma(\tau(x)) = \tau(x) \quad \text{ja} \\ [\sigma, \tau](\tau(x)) &= (\tau \circ [\tau^{-1}, \sigma])(x) = \tau(\tau^{-1}(x)) = x. \end{aligned}$$

Nyt on näytetty, 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 $[\sigma, \tau](y) = y$. Toisaalta ehdosta $y \notin \{x, \sigma(x), \tau(x)\}$ seuraa, että $y \neq x$ ja $x \neq \sigma^{-1}(y)$.

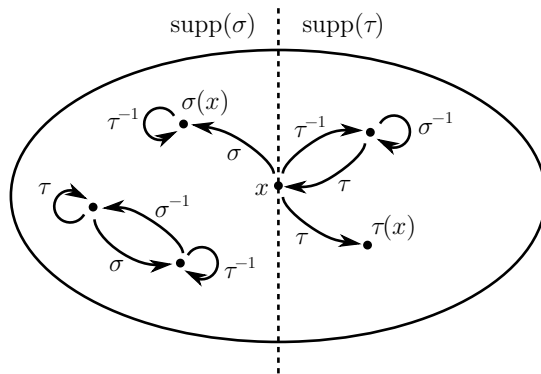
Jos nyt $y \in \text{supp}(\sigma)$, niin y ja $\sigma^{-1}(y)$ eivät kumpikaan voi olla τ :n kantajassa, koska $y \neq x$ ja $\sigma^{-1}(y) \neq x$. Täten

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

Vastaavasti, jos $y \in \text{supp}(\tau)$, niin y ja $\tau^{-1}(y)$ eivät kumpikaan voi olla σ :n kantajassa, joten

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

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



Kuva 22: Kuinka kommutaattorista tulee 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 aikaan siirtoja, jotka liikuttavat paljon pienempää osaa kuutiosta kerrallaan. Itse asiassa aiemmin opitut siirtosarjat on muodostettu juuri tällä periaatteella, ja seuraavaksi tutkitaan tarkemmin, miten tämä tapahtuu käytännössä.

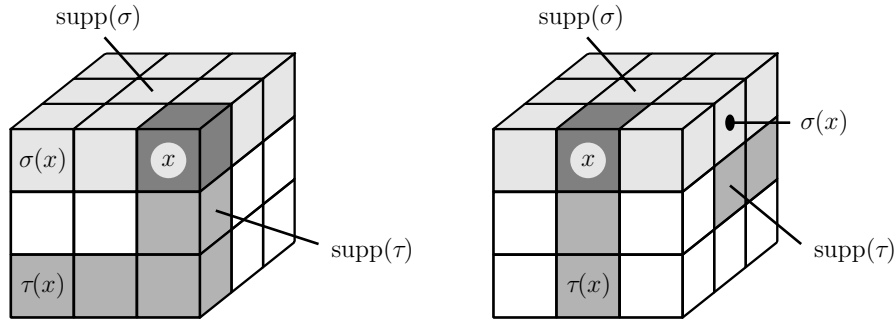
Tarkastellaan ensin tilannetta Rubikin paikkaryhmässä. Lauseen 6.3 mukaan voidaan tuottaa kolmen palan sykli, jos vain löydetään kaksi siirtoa, joiden yhteisen vaikutuksen piiriin kuuluu ainoastaan yksi pala. Yritetään saada tämä aikaan nurkkapaloilla niin, että tuloksena olisi luvussa 3.3 opittu nurkkapalojen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

Koska lauseen 6.3 mukaan kahden siirron 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 23). 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 ${}^R D^{-1} = R D^{-1} R^{-1}$.

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 23), ilman että ylätahkon palan liikkuvat. Tämä onnistuu konjugoimalla etutahkon kierrolla pystysuoran keskivirran 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 keskitah-

kojen pyöriytykset omiksi siirroikseen, jotka pitävät sivutahkojen palat paikallaan, jotta päästään käyttämään lausetta 6.3. Lauseen 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 23: Paikkaryhmän 3-sykliden muodostaminen.

Asentoryhmässä 3-syklejä tuottavan lauseen käyttäminen ei kuitenkaan onnistu. Koska yhden ruudun liikkuaessa liikkuvat samalla kaikki saman palan ruudut, ei kahden permutaation kantajien leikkaus voi olla vain yksi ruutu. Pienin mahdollinen kantajien leikkaus sisältää sen sijaan kokonaisen palan kaikki ruudut.

Olkoon A se pala, johon ruutu x kuuluu. Jos siis kaksi siirtoa vaikuttavat molemmat ruutuun x , niiden yhteinen vaikutusalue voi olla pienimmillään palan A ruutujen joukko. Aiemman esimerkin perusteella voitaisiin odottaa, että tällaisten siirtojen kommutaattori olisi mahdollisesti pienin löydettävissä oleva kommutaattori.

Oletetaan seuraavaksi, että Ruikin ryhmän siirtojen σ ja τ kantajien leikkaus sisältää täsmälleen palan A ruudut. Tarkastellaan seuraavaksi, mitkä ehdot siirtojen σ ja τ on toteutettava, jotta niiden kommutaattorista tulisi asentoryhmän siirto, joka vaikuttaisi epätriviaalisti palaan A .

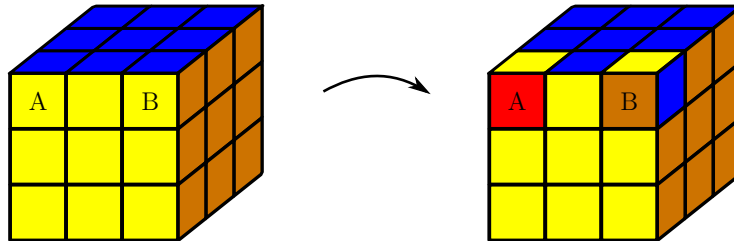
Jos kumpikaan siirroista σ ja τ ei liikuta palaa A paikaltaan, ne ovat molemmat tuon palan ruutuihin rajoitettuina syklejä. Tällaiset siirrot kommutoivat keskenään palan A kohdalla, joten niiden kommutaattori ei liikuta lainkaan kyseisen palan ruutuja. Jos taas molemmat siirrot liikuttavat palaa A , voidaan tarkastella vastaavia paikkaryhmän siirtoja $\sigma\mathbb{R}_a$ ja $\tau\mathbb{R}_a$. Näiden paikkaryhmän siirtojen kantajien leikkaus on pala A , siis yksiö, joten lauseen 6.3 nojalla kommutaattorista $[\sigma\mathbb{R}_a, \tau\mathbb{R}_a]$ tulee 3-sykli, joka liikuttaa palan A paikaltaan. Täten kommutaattori $[\sigma, \tau]$ ei kuulu asentoryhmään.

Ainoa jäljellä oleva vaihtoehto on, että toinen siirroista liikuttaa palaa A ja toinen ainoastaan vaihtaa sen ruutujen järjestystä. Tällaisessa tilanteessa syntyvä kommutaattori kuuluu asentoryhmään, mikä voidaan nähdä esimerkiksi siitä, että asentoryhmä on normaali aliryhmä. Kommutaattori $[\sigma, \tau]$ voidaan nimittäin kirjoittaa muodossa $\sigma\tau\cdot\tau^{-1}$, joten jos τ on asentoryhmän siirto, koko kommutaattori kuuluu asentoryhmään.

6.3. Algoritmi 3: nurkkapalojen kierto

Nurkkapalojen kierron tuottavan siirtosarjan muodostaminen perustuu edellisen luvun päätelmiin. Siirtosarja on kahden siirron kommutaattori, joista toinen kiertää nurkkapalaa ja toinen siirtää sitä paikaltaan. Toinen siirroista siis kuuluu asentoryhmään ja toinen ei.

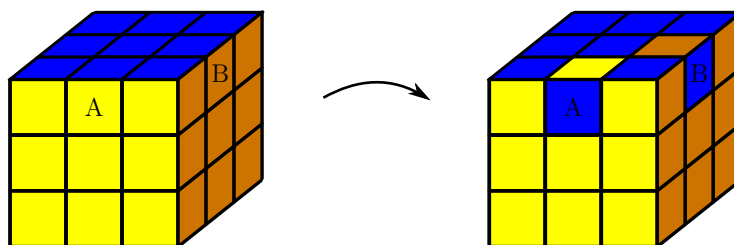
Siirto kiertää kiertää kahta vierekkäistä nurkkapalaa vastakkaisiin suuntiin. Tulos on esitetty kuvassa 24. Pala A kiertyy vastapäivään ja pala B myötäpäivään. Siirtosarjan vaiheet löytyvät liitteestä A.3.



Kuva 24: Nurkkapalojen kierto.

6.4. Algoritmi 4: särmäpalojen kääntö

Särmäpalojen kääntö on samantapainen kahden siirron kommutaattori kuin nurkkapalojen kierto: toinen siirroista kääntää yhden särmäpalan ja toinen siirtää sen paikaltaan. Syntyvä siirtosarja kääntää kaksi samaa nurkkapalaa reunustavaa särmäpalaa ympäri, ja tulos on esitetty kuvassa 25. Tarkemmat yksityiskohdat löytyvät liitteestä A.4.



Kuva 25: Särmäpalojen kääntö.

6.5. Rubikin asentoryhmän ratkaiseminen

Edellisissä luvuissa on esitetty siirrot, joiden avulla nurkka- ja reunapaloja on mahdollista kääntää paikallaan niin, että yhden palan kiertyessä yhteen suuntaan jokin toinen pala kiertyy samalla päinvastaiseen suuntaan. Tällöin palojen yhteenlaskettu kiertymä eli *kokonaiskiertymä* säilyy. Jotta saataisiin kaikki palat oikeaan asentoon, täytyy tutkia, mitä tuolle kokonaiskiertymälle tapahtuu erilaisissa siirroissa. Koska opitut palojen

asentoa muuttavat algoritmit eivät muuta kokonaiskiertymää, olisi toivottavaa, että se säilyisi aina samana kaikissa asemissa, joissa palat ovat oikealla paikallaan. Muuten opitut algoritmit eivät riittäisi asentojen ratkaisemiseen.

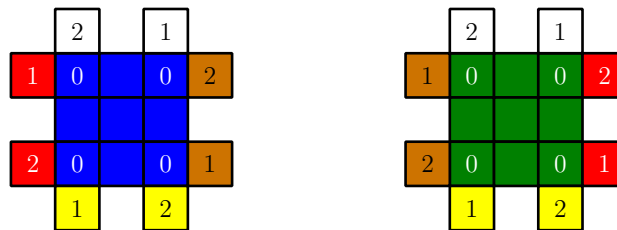
Sellaisia ominaisuuksia, jotka säilyvät kaikissa tilanteissa, kutsutaan *invariantteiksi*. Invariantteja käytetään runsaasti esimerkiksi pelien ja algoritmien analysoinnissa. Tällä kurssilla on jo löydetty joitakin tällaisia invariantteja. Esimerkiksi jokainen paikkaryhmän siirto voidaan ilmoittaa muodossa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

Vaikka jokin ominaisuus ei säilyisi aivan kaikissa tilanteissa, on yleensä hyödyksi tarkastella, missä tilanteissa kyseinen ominaisuus kuitenkin säilyy ja millä tavoin ominaisuutta voidaan muuttaa. Paikkaryhmän siirroista tiedetään, että jos ne ilmoitetaan edellä kuvatussa muodossa, $\text{sign}(\nu)$ voi olla 1 tai -1 . Perussiirrot kuitenkin vaihtavat tuon etumerkin, joten haluttaessa siirtyä yhdestä tilasta toiseen minkä tahansa perussiirron tekeminen riittää. Voidaan myös sanoa, että $\text{sign}(\nu)$ 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.

Aloitetaan antamalla jokaisen nurkkapalan ruuduille numerointi kuvan 26 osoittamalla tavalla. Kuvassa on perusasemassa oleva kuutio kuvattu ylä- ja alapuolelta niin, että nurkkapalat on ikään kuin taiteltu auki.



Kuva 26: Nurkkapalojen numerointi.

Kuvatulla tavalla jokainen nurkkaruutu tulee numeroiduksi jollain luvuista 0, 1 ja 2. Laskujen yksinkertaistamiseksi ajatellaan näitä lukuja jäännösluokkaryhmän \mathbb{Z}_3 alkioina. 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 nurkkapalasta on aina täsmälleen yksi ruutu merkityllä paikalla. Näiden merkkien avulla voidaan määritellä nurkkapalojen kiertymät.

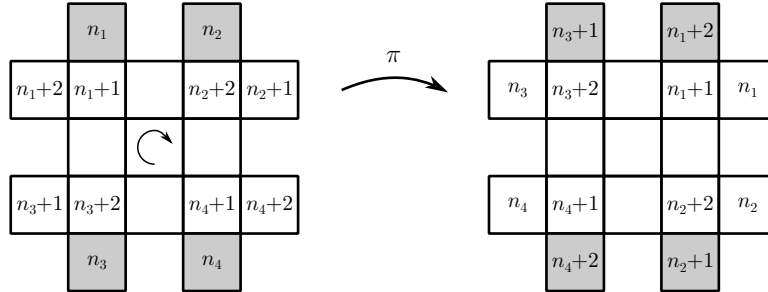
Määritelmä 6.4. Tarkastellaan nurkkapalan x ruutuja asemassa σ . Palan x *kiertymä* $k_x(\sigma) \in \mathbb{Z}_3$ on sen palaan x kuuluvan ruudun numero, joka sattuu asemassa σ olemaan jollakin merkityistä paikoista. Aseman σ *nurkkapalojen kokonaiskiertymä* on kaikkien nurkkapalojen kiertymien summa,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

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

Lause 6.5. *Olkoon π 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 perussiirto vaikuttaa vain niiden palojen kiertymään, jotka sijaitsevat kierrettävällä sivutahkolla. Numeroidaan nämä palat luvuin 1–4 ja oletetaan, että kunkin palan alkuperäinen kiertymä on $n_i = k_i(\sigma)$. Kuvassa 27 näkyy, mitä sivutahkon paloille tapahtuu suoritettaessa perussiirto π . Merkityille paikoille osuvat ruudut on tummennettu.



Kuva 27: Perussiirron vaikutus nurkkapalojen kiertymään.

Kuvan 27 mukaan asemassa $\sigma \circ \pi$ saadaan neljän liikkuneen palan kokonaiskiertymäksi

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

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

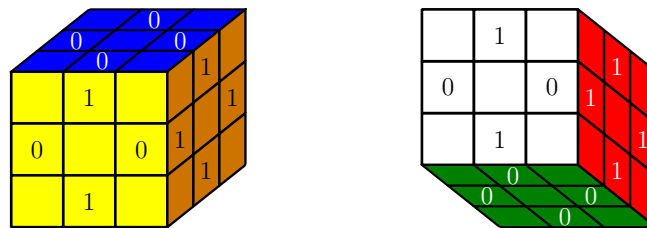
Koska alkuasemassa kokonaiskiertymä on nolla, saadaan edellisestä lauseesta heti seuraava korollaari.

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

Oletetaan, että nurkkapalat ovat jo oikeilla paikoillaan. Nyt ne saadaan myös oikeisiin asentoihin edellistä korollaaria soveltamalla. 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 nollostaan poikkeava.

Toinen tapa saada nurkat oikeisiin asentoihin ei vaadi konjugointia. Siinä järjestetään nurkkapalat aluksi jonoon (x_1, x_2, \dots, 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, \dots, 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 numerointi näkyy kuvasta 28, jossa kuutio on kuvattu perusasemassa edestä ja takaa. Ruutujen numeroiden ajatellaan nyt kuuluvan ryhmään \mathbb{Z}_2 . Nollaruutuja ovat kaikki siniset ja vihreät ruudut, ja niissä paloissa, joissa kumpiakaan ei esiinny, keltaiset tai valkoiset ruudut.



Kuva 28: Särmäpalojen numerointi.

Kuten aikaisemmin, perusasemassa olevien nollaruutujen paikat merkitään, ja palan kiertymä määräytyy siitä, mikä palan ruuduista sattuu olemaan merkityllä paikalla.

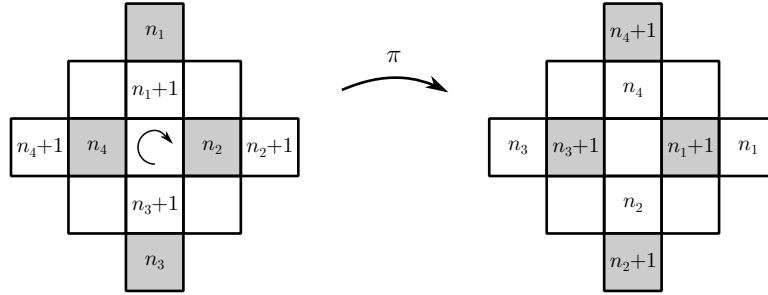
Määritelmä 6.7. Särmäpalan x kiertymä $k_x(\sigma) \in \mathbb{Z}_2$ asemassa σ on sen palaan x kuuluvan ruudun numero, joka sattuu olemaan asemassa σ jollakin merkityistä paikoista. Aseman σ särmäpalojen kokonaiskiertymä on kaikkien särmäpalojen kiertymien summa, ja sitä merkitään $K_S(\sigma) = \sum_x k_x(\sigma)$.

Lause 6.8. *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.

tymää. Toisaalta siirrot L ja R siirtävät jokaisen merkitsemättömällä paikalla olevan ruudun merkitsemättömälle 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. Nimitetään siirtoon osallistuvat särmäpalat numeroilla 1, 2, 3 ja 4 ja oletetaan, että kunkin kiertymä alkuperäisessä asemassa $\sigma \in \mathbb{R}$ on $n_i = k_i(\sigma)$. Kuvassa 29 on näytetty, miten perussiirto vaikuttaa palojen kiertymiin. Särmäpalat on taiteltu auki ja merkityillä paikoilla sijaitsevat ruudut tummennettu.



Kuva 29: Perussiirron vaikutus särmäpalojen kiertymään.

Kuvasta 29 nähdään, että tarkasteltavien neljän palan kiertymien summaksi tulee uudessa asemassa

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

Reunapalojen kokonaiskiertymä ei siis muutu myöskään perussiirroissa F tai B . \square

Särmäpalat voidaan nyt saada oikeisiin asentoihin samalla periaatteella kuin nurkka-palatkin.

7. Rubikin kuution laajennoksia

Tavallista Rubikin kuutiota voidaan laajentaa monilla tavoilla. Ensi näkemältä nämä uudet versiot saattavat vaikuttaa hankalammilta ratkaista, mutta lähemmin tarkasteltaessa yleensä nähdään, että samat perusideat ovat edelleen voimassa monimutkaisissakin muunnelmissa.

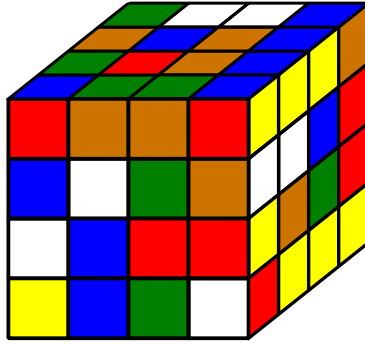
7.1. Suuremmat kuutiot

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 huomasti, 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 keskimmainen pala, jonka voi ajatella pysyvän aina paikallaan. Tästä keskimmaisesta palasta voi päätellä kunkin sivun värin missä tahansa asemassa. Jos särmän pituus on enemmän kuin kolme, on kuutiossa kuitenkin useampia 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.

Sen sijaan kuutiossa, jonka särmän pituus on parillinen, ei ole sellaisia keskimmisiä 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 30 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.

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-syklarilla avulla, joten myös reunapalojen pariton permutaatio on mahdollinen siirto. Tällaisilla kuutioilla voidaankin tehdä esimerkiksi kahden reunapalan vaihto, joka ei onnistu pariton särmäisillä kuutioilla.



Kuva 30: $4 \times 4 \times 4$ -kuutio, "Rubikin kosto".

Särmän pituuden lisääntyessä käytännön ongelmaksi tulee ratkaisualgoritmin pituus. Kuutiosta, jonka särmän pituus on kuusi, on jo 96 keskipalaa. Näiden kaikkien paikoilleen saaminen 3-syklillä on melko 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 siirtotyyppäjä tulee huomattavasti lisää, mutta ratkaisun perusideat eivät kuitenkaan muutu.

Toinen peruskuution muunnos on käyttää kuution sijasta erimuotoisia kappaleita. Rubikin kuution tapaisia pelejä voidaan tehdä sekä säännöllisistä että epäsäännöllisistä monitahokkaista, ja näiden avulla saadaan aikaan monenlaisia algebrallisia rakenteita. Kuitenkin niin kauan kuin on mahdollista tuottaa 3-syklejä, voidaan ratkaisua aina lähestyä niiden avulla. Siirtojen parillisuuskytokset voivat erimuotoisissa kuutioissa sen sijaan olla hyvinkin erilaisia. Esimerkiksi dodekaedrin muotoisessa Megaminx-pelissä jokainen perussiirto on parillinen permutaatio sekä nurkka- että särmäpalojen paikkaryhmissä ja koko paikkaryhmä on suora tulo nurkkien ja särmien paikkaryhmistä. Tässä mielessä Megaminx on jopa yksinkertaisempi kuin tavallinen kuutio.

7.3. Superkuutio

Edellä mainituissa Rubikin kuution muunnelmissa on sama tavoite kuin perinteisessä kuutiosta: saada eriväriset ruudut samoille paikoille kuin perusasemassa. Kyse on siis ruutujen paikkojen permutaatioista. Jos ruutujen määrä on n , kuution siirtoja vastaavan permutaatioryhmän voi ajatella symmetrisen ryhmän S_n aliryhmäksi, olipa kyse sitten tavallisesta kolmiulotteisesta kuutiosta tai vaikkapa seitsenulotteisesta ikosaedristä.

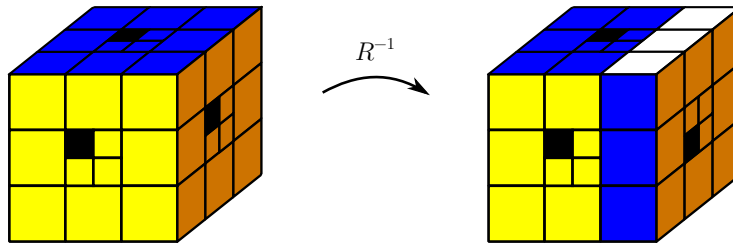
Yksi mahdollisuus perustavoitteen muunnelmaksi on tarkastella keskipalojen asentoja. Nurkka- ja reunapalojen asennot määräytyvät, kun niiden ruudut asetetaan oikealle paikalleen. Keskipaloissa on kuitenkin vain yksi ruutu, ja keskipalaa onkin mahdollista kiertää itsensä ympäri ilman, että mikään ruutu joutuu väärälle paikalle. Jos tavoitteek-

si 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} . 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 syklisten ryhmän \mathbb{Z}_4 alkioilla. Tällä tavalla saadaan laajennetuksi ryhmäksi seitsemän ryhmän 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 31, josta näkyy samalla, miten perussiirto vaikuttaa keskipalan asentoon. Yksi keskipalan ruuduista on väritetty mustaksi selvyys 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 ryhmäteoreettisia ideoita jälleen käyttää hyväksi.

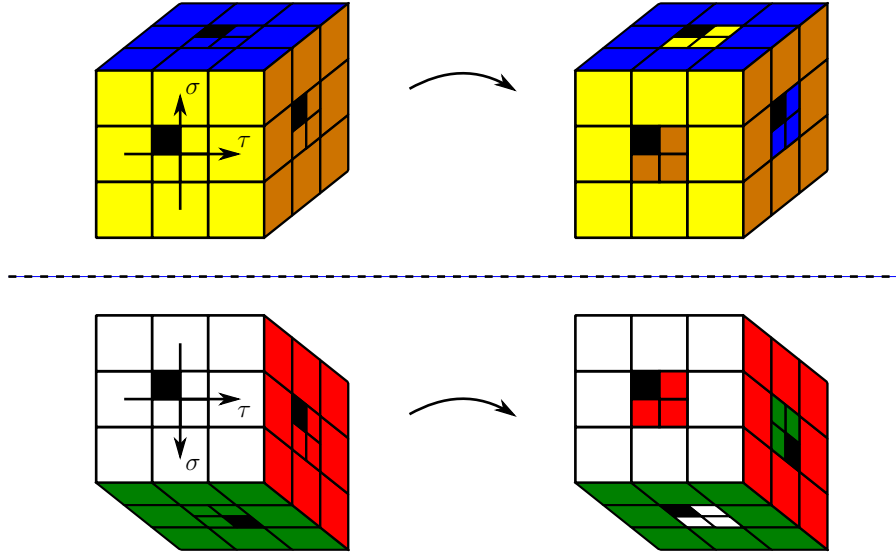


Kuva 31: Keskipalojen jako ruutuihin ja perussiirron vaikutus keskipalan asentoon.

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

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 paikko-

jen 3-sykliä. Paikkaryhmässä pienin yhteinen kantaja, eli kahden vastakkaisen keskipalan pari, saadaan esimerkiksi valitsemalla siirroiksi kahden eri keskitahkon perussiirrot. Näiden siirtojen kommutaattori on tähän mennessä esillä olleista kommutaattorisiirroista yksinkertaisin, ja se tuottaa vastakkaisten keskipalojen 3-syklit kuvan 32 mukaisesti. Kuvassa kuutio on kuvattuna sekä edestä että takaa. Siirrot on helppo suorittaa, ja tulos on näyttävä, mutta siirtosarja ei itse asiassa auta keskipalojen oikean asennon löytämisessä.

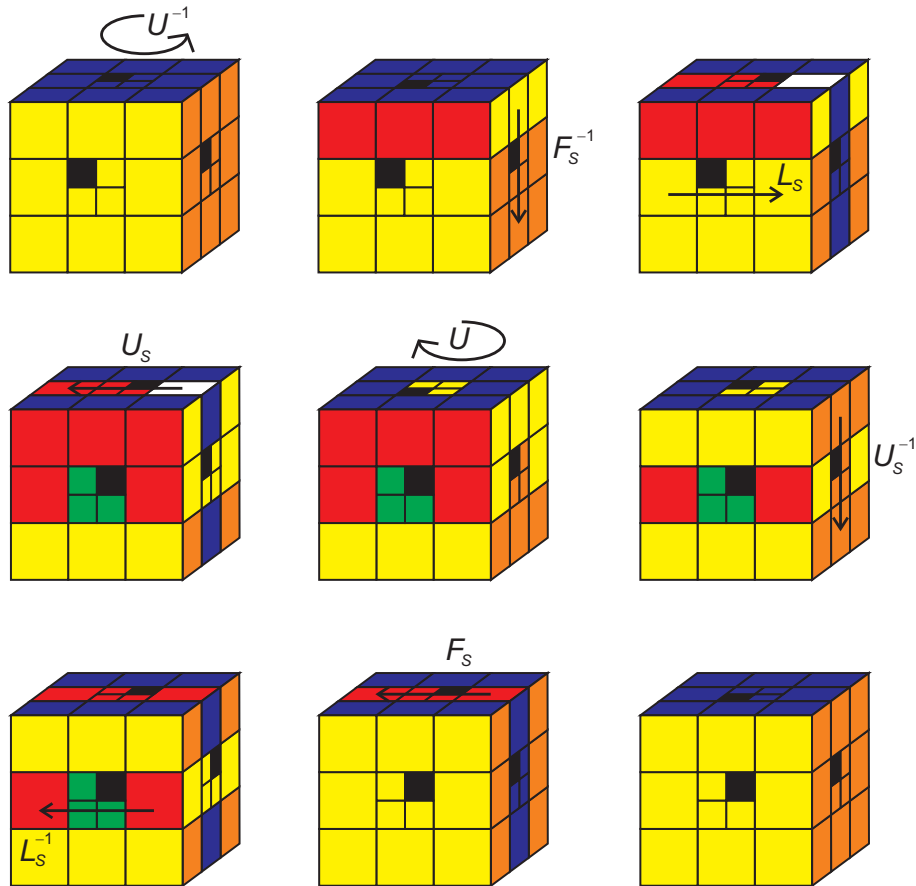


Kuva 32: Vastakkaisten keskipalojen 3-syklit.

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 33. Huomaa, että keskipalojen liikuttaminen vaikuttaa siirtojen merkitsemistapaan, ja siksi esimerkiksi siirto L_S kiertää kuvassa kuution yläpinnan suuntaista keskitahkoa.

Keskipalojen kiertymät $k_x(\sigma)$ voidaan määritellä samaan tapaan kuin luvussa 6.5. Tällöin kukin kiertymä on ajateltava syklisen ryhmän \mathbb{Z}_4 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 keskipaloja kiertävä 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*. Yhdestä vanhasta perusasemasta toiseen



Kuva 33: Keskipalojen kierto.

siirtyminen vaatii parillisen määrän perussiirtoja, sillä perussiirrot ovat ruutujen parittomia permutaatioita, jollei keskipalojen asentoa oteta lukuun. (Keskitahkon perussiirto voidaan laskea omaksi perussiirroksi tai 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 siirtosarjoja. Kyseisten siirtosarjojen kantajat eivät sisällä keskipaloja, joten näiden kiertymät eivät tässä vaiheessa muutu. (Tämä on helpointa nähdä ajatteleamalla keskitahkojen perussiirtoja sivutahkojen pyöriytyksinä, jolloin keskipalat eivät liiku paikoiltaan. Keskipalojen asentoryhmä puolestaan on vaihdannainen, joten jokai-

nen kommutaattori on tuohon asentoryhmään rajoitettuna triviaali.) Tuloksena saadaan vanha perusasema, jossa keskipalojen kokonaiskiertymä on 0, ja tähän voidaan jälleen soveltaa keskipaloja kiertävää siirtosarjaa.

LOPPU

A. Siirtosarjat

Tässä liitteessä esitetään siirtosarjat, joihin muualla materiaalissa viitataan. Ensin käsitellään paikkaryhmän siirrot, sitten asentoryhmän siirrot.

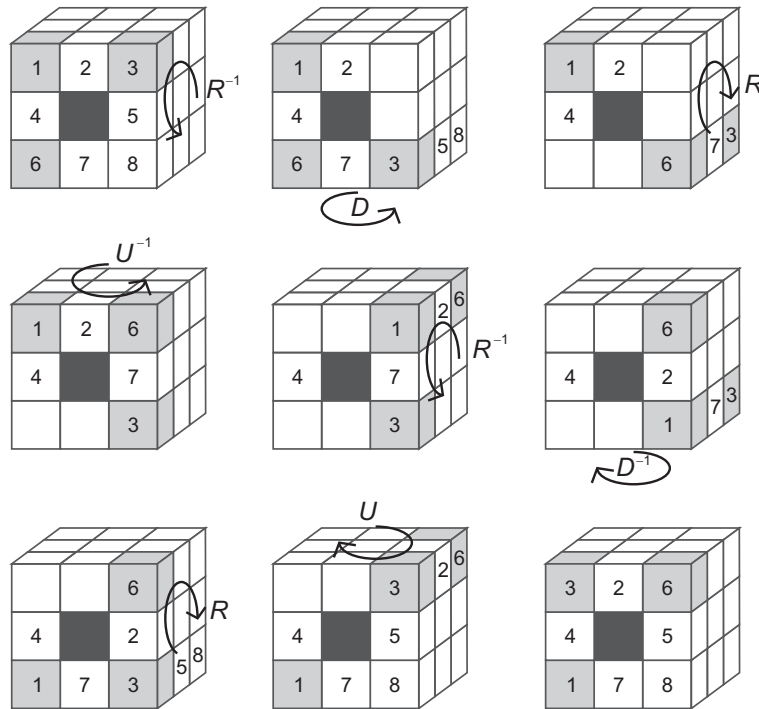
A.1. Nurkkapalojen 3-sykli

Ensimmäinen algoritmi tuottaa 3-syklin paikkaryhmässä \mathbb{R}_p . Tämä sykli on esitelty luvussa 3.3. Se koostuu kahdenlaisista siirroista: ensimmäinen on perussiirto $\sigma = U$ ja toinen kolmen perussiirron yhdistelmä $\tau = RD^{-1}R^{-1}$. Näistä kootaan yhdistelmä $\sigma\tau\sigma^{-1}\tau^{-1}$. Kokonaisuudessaan siirtosarja on siis seuraavanlainen:

$$\sigma\tau\sigma^{-1}\tau^{-1} = URD^{-1}R^{-1}U^{-1}RDR^{-1}.$$

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

Kuvassa 34 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 permutaatioissa $\sigma^{-1}\tau^{-1}$ jonnekin, mistä ne sitten palaavat takaisin permutaatioissa $\sigma\tau$. Näiden palojen kannalta kyseiset permutaatiot toimivat siis kuin toistensa käänteis-siirrot. Tosiasiassa kuitenkin $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. Permutaatioiden $\tau\sigma$ ja $\sigma\tau$ (tai niiden käänteisalkioiden) ero tulee näkyviin vain 3-sykliin osallistuvissa paloissa.



Kuva 34: Nurkkapalojen 3-sykli vaiheittain.

Algoritmin opettelu helpottuu, kun huomaa, että permutaatio τ eroaa permutaatiosta τ^{-1} vain siten, että jälkimmäisessä on keskimmäisenä siirtona perussiirto D , edellisessä D^{-1} . Koko sykli voidaan helposti myös kiertää vastakkaiseen suuntaan. Tarvittava käänteisalkio on

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

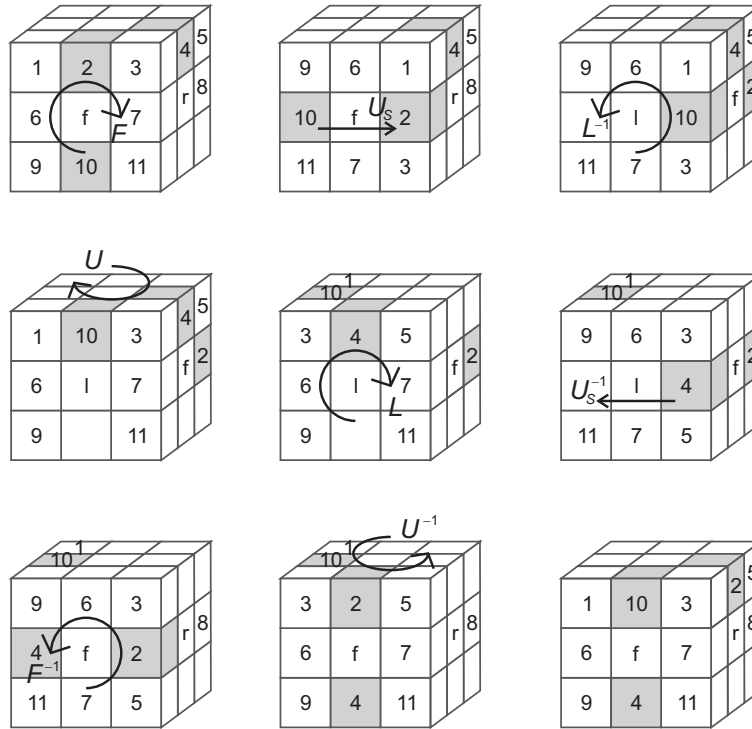
Käänteisalkiossa tehdään siis edelleen ensin käänteissiirrot; ero alkuperäiseen 3-sykliin on vain se, että σ -siirrot tehdään ennen τ -siirtoja.

A.2. Särmäpalojen 3-sykli

Särmäpaloja kiertävä 3-sykli on esitelty luvussa 5.3. Siirroiltaan se on samankaltainen kuin nurkkapalojen 3-sykli. Se on nimittäin 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 kuvassa 35 esitetty kahdeksan siirron sarja

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

Siirtosarja suoritetaan tietysti oikealta vasemmalle, aloittaen siirrosta F .



Kuva 35: Särmäpalojen 3-sykli vaiheittain.

Algoritmi on tässä kirjoitettu siirron U_S avulla, joka on kuution keskitalikon siirto. Tämä on tehty sen vuoksi, että siirtosarja 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 ruvetaan käyttämään siirtoa L^{-1} , ja tilalle on tullut aiemmin vasemmalla sivulla ollut tahko. Kuvassa tahkoja merkitään keskipalojen kirjaimilla f (etutahko), l (vasemmanpuoleinen tahko) ja r (oikeanpuoleinen tahko).

A.3. Nurkkapalojen kierto

Nurkkapalojen kiertämiseen soveltuva siirto on esitelty luvussa 6.3. Se on kahden siirron kommutaattori $[\sigma, \tau]$ kuten edellisekin siirrot. Tällä kertaa siirroista toinen kuuluu asentoryhmään ja toinen ei. Paloja siirtävä permutaatio σ on ylätahkon kierto U . Asentoryhmän siirto puolestaan kiertää yhtä nurkkapaloista, ja se on perussiirtojen yhdistelmänä $\tau = RD^{-1}R^{-1}F^{-1}D^{-1}F$. Näistä muodostuu kommutaattori

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

Tämä siirtosarja, joka on esitetty vaihe vaiheelta kuvassa 36, kiertää kahta vierekkäistä nurkkapalaa A ja B vastakkaisiin suuntiin. Pala A kiertyy vastapäivään ja pala B myötäpäivään.

Siirtosarjan voi hahmottaa esimerkiksi seuraavasti. Aluksi tehdään joukko siirtoja, joissa pala B kiertyy myötäpäivään, ja samalla kuution kaksi alinta tahkoa saavat sekoitua miten hyvänsä. Sen jälkeen siirretään pala A palan B paikalle koskematta alempiin tahkoihin 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 myös itsessään helpointa hahmottaa kahdessa osassa. Molemmat osat ovat samanlaisia konjugaattimuotoisia siirtoja: toinen koskee kuution oikeanpuoleista sivutahkoa, toinen etutahkoa.

A.4. Särmäpalojen kääntö

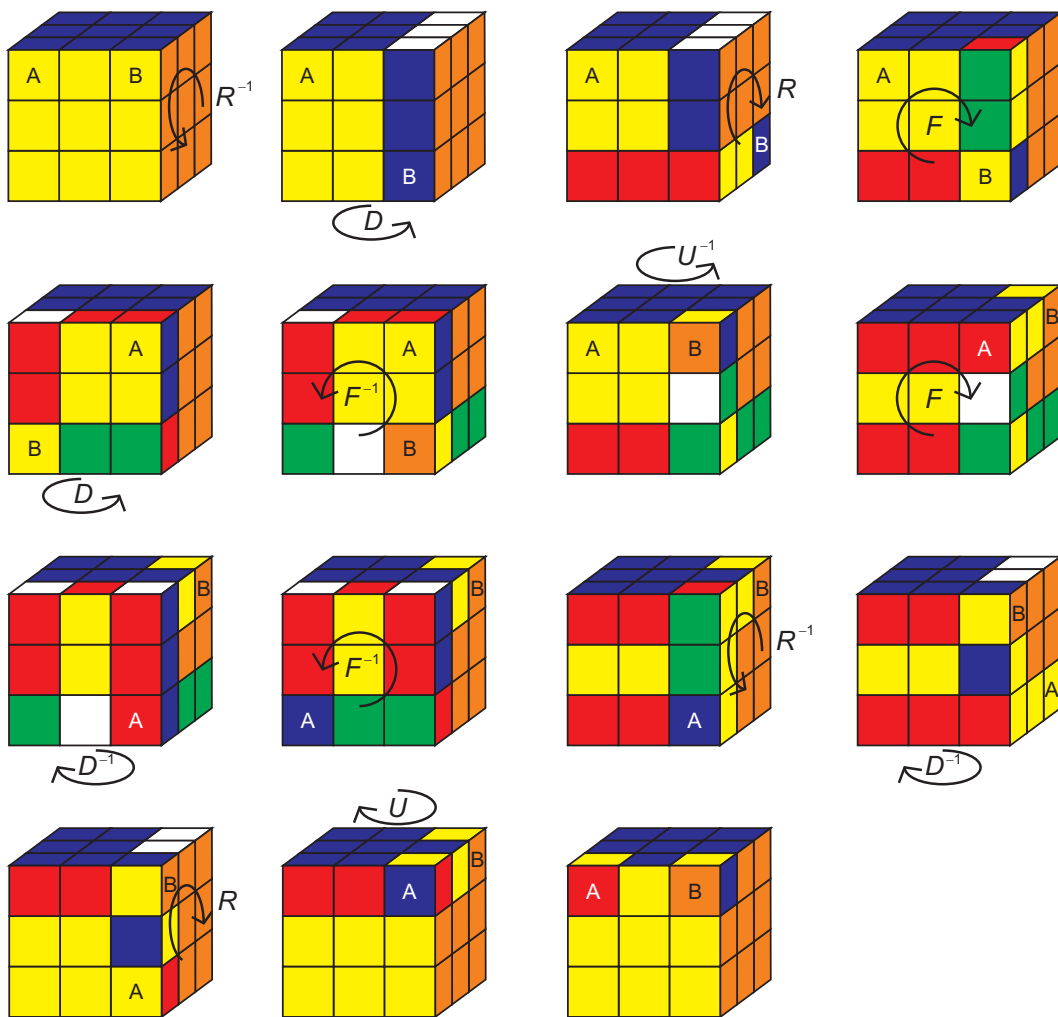
Särmäpalojen kääntäminen onnistuu luvussa 6.4 esitetyllä siirrolla. Tämä on jälleen kahden siirron kommutaattori, joista toinen siirtää särmäpalan paikaltaan ja toinen kääntää sen. Särmäpalaa siirtävä permutaatio σ on edelleen ylätahkon kierto U . Särmäpalan kääntävä permutaatio saadaan yhdistelmästä $\tau = RU_S B^{-2} U_S^{-2} F$. Koko siirtosarja on kommutaattori

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

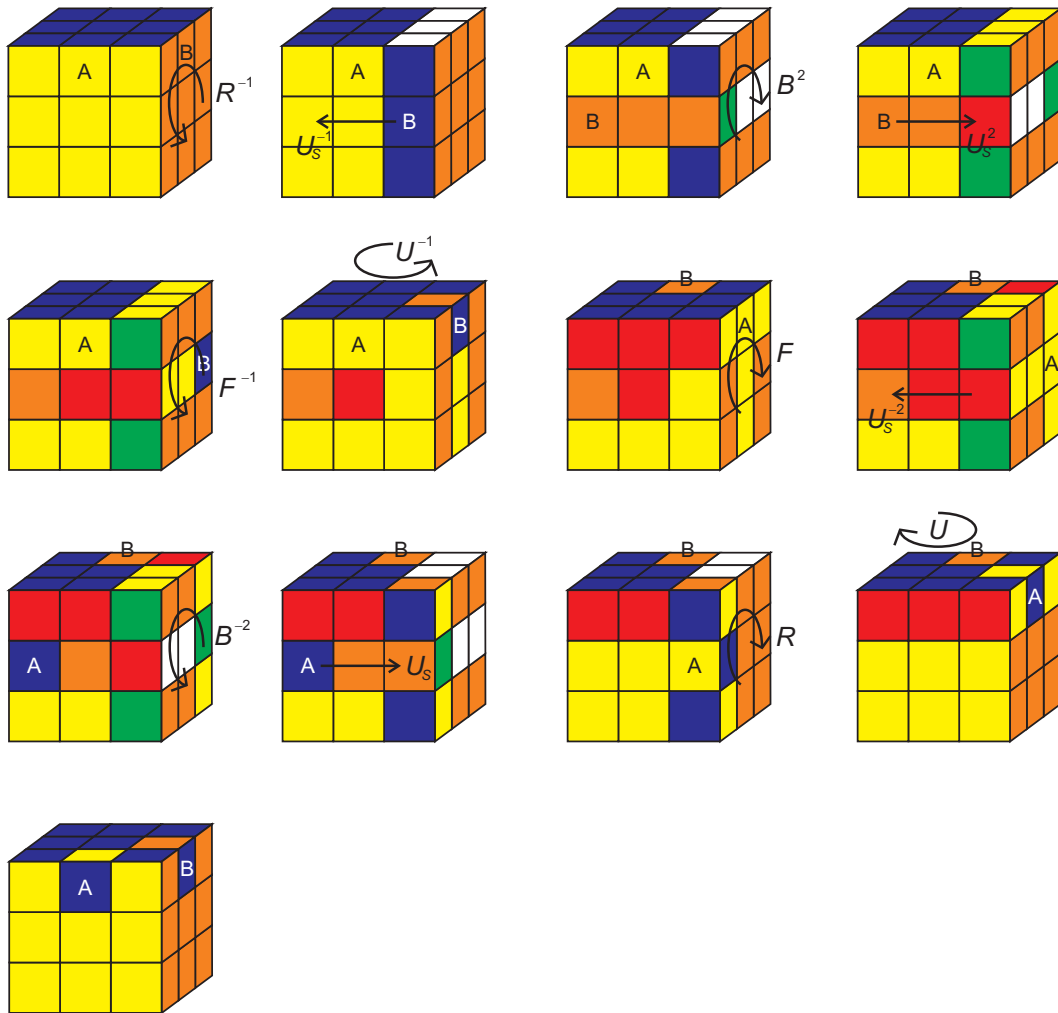
Tämä siirtosarja on esitetty kuvassa 37. Se kääntää ympäri kaksi vierekkäisillä reunoilla sijaitsevaa särmäpalaa (palat A ja B).

Siirtosarja perustuu siihen, että palan B ruudut ovat ainoat ruudut, joihin sekä σ että τ vaikuttavat. 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.



Kuva 36: Nurkkapalojen kierto vaiheittain.



Kuva 37: Särmäpalojen kierto.