Rubikin kuutio ja ryhmäteoria

Pro Gradu -tutkielma
Jani Luokkanen
2372781
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2018

Sisältö

Johdanto

Tässä tutkielmassa selvitetään Rubikin kuution matemaattinen tausta. Tutkielma koostuu neljästä luvusta. Ensimmäisessä luvussa määritellään Rubikin kuution ryhmärakenteen määrittämisen kannalta tarpeelliset ryhmäteoreettiset peruskäsitteet ja osoitetaan tarvittavia lauseita.

Toisessa luvussa määritellään Rubikin kuution matemaattisen tarkastelun kannalta oleelliset algebralliset rakenteet; suora tulo, ryhmän toiminta joukossa ja kranssitulo, jonka avulla Rubikin kuution ryhmärakenne esitetään, sekä todistetaan niihin liittyviä tuloksia.

Kolmas luku on tutkielman pääaihe, eli Rubikin kuution matemaattinen tarkastelu. Tässä luvussa määritellään kuutioon liittyvät peruskäsitteet, johdetaan Rubikin kuution ryhmän rakenne ja määritellään sen ryhmäoperaatio, sekä todistetaan Rubikin kuution kannalta oleelliset lauseet.

Neljäs luku on lyhyt katsaus 2x2x2-kuutioon, ja sen yhtäläisyyksiin ja eroavuuksiin Rubikin kuutioon verrattuna.

Luettuaan ja sisäistettyään tutkielman lukija ymmärtää Rubikin kuution toimintaperiaatteen matemaattisen taustan ja osaa esimerkiksi päätellä sekoitettua kuutiota katsomalla, onko se ratkaistavissa. Lisäksi tutkielma tarjoaa erään lauseen todistuksen yhteydessä täysin toimivan, vaikkakin vaivalloisen, Rubikin kuution ratkaisumenetelmän.

1 Ryhmäteoria

Tässä luvussa määritellään tarvittavia ryhmäteorian käsitteitä, tapoja konstruoida eräitä ryhmiä sekä todistetaan tarvittavia lauseita.

1.1 Perusteet

Määritelmä 1.1.1. Olkoon $G \neq \emptyset$ joukko, johon on liitetty operaatio $(*)$, jolle

$$* : G \times G \longrightarrow G,\ (g_1,\ g_2) \mapsto g_1 * g_2.$$

Tällöin $(G, *)$ on ***ryhmä***, jos seuraavat ehdot toteutuvat:

1) $(a * b) * c = a * (b * c)$ kaikilla $a, b, c \in G$ eli $(*)$ on assosiatiivinen.

2) Joukossa G on olemassa sellainen alkio e, että $a * e = e * a = a$ kaikilla $a \in G$. Tällöin alkiota e kutsutaan ***neutraalialkioksi***.

3) Kaikilla $a \in G$ on olemassa sellainen alkio $a^{-1} \in G$, että $a * a^{-1} = a^{-1} * a = e$. Tällöin alkiota a^{-1} kutsutaan alkion a ***käänteisalkioksi***.

Ryhmää $(G, *)$ voidaan merkitä G, mikäli operaatiosta $(*)$ ei ole epäselvyyttä. Tällöin merkitään myös $a * b = ab$. Ryhmää G kutsutaan ***Abelin ryhmäksi***, jos $ab = ba$ kaikilla $a, b \in G$.

Lause 1.1.2. *Olkoon G ryhmä. Tällöin*

1) neutraalialkio e on yksikäsitteinen,

2) käänteisalkio on yksikäsitteinen kaikille $a \in G$.

Todistus. 1) Olkoot e ja e' neutraalialkioita. Tällöin $e' = ee' = e$ eli $e = e'$.

2) Olkoot a_1^{-1} ja a_2^{-1} alkion $a \in G$ käänteisalkioita. Tällöin

$$a_1^{-1} = a_1^{-1}e = a_1^{-1}(aa_2^{-1}) = (a_1^{-1}a)a_2^{-1} = ea_2^{-1} = a_2^{-1}.$$

Siis $a_1^{-1} = a_2^{-1}$.

□

Jos $a \in G$ ja $n \in \mathbb{Z}_+$, asetetaan $a^n = a * a * ... * a$ ja $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1}$, missä operandeja on n kappaletta. Lisäksi $a^0 = e$.

Määritelmä 1.1.3. Ryhmän G alkioiden lukumäärää eli ryhmän G ***mahtavuutta*** eli ***kertalukua*** merkitään $|G|$. Ryhmä G on ***äärellinen ryhmä***, jos $|G| < \infty$. Ryhmän ***alkion*** a ***kertaluku*** $|a| = n$, jos n on pienin positiivinen kokonaisluku, jolla $a^n = e$.

Määritelmä 1.1.4. Olkoot $A_1, A_2, \ldots, A_m$ epätyhjiä joukkoja. Tällöin joukkojen $A_1, A_2, \ldots, A_m$ ***karteesinen tulo*** on joukko

$$A_1 \times A_2 \times \cdots \times A_m = \{(a_1, a_2, \ldots, a_m) \mid a_i \in A_i \text{ kaikilla } 1 \leq i \leq m\}.$$

Lemma 1.1.5. *Jos $A_1,\ A_2, \ldots, A_m$ ovat äärellisiä joukkoja, niin*

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|.$$

Todistus. Nyt $A_1 \times A_2 \times \cdots \times A_m = \{(a_1, a_2, \ldots, a_m) \mid a_i \in A_i\}$. Nyt paikalle a_1 voidaan valita $|A_1|$ eri alkiota, paikalle a_2 vastaavasti $|A_2|$ eri alkiota jne. Tällöin edellisen päättelyn, eli kombinatoriikan tuloperiaatteen nojalla

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|.$$

□

Määritelmä 1.1.6. Jos $(G, *)$ on ryhmä, $\emptyset \neq H \subseteq G$ ja $(H, *)$ on myös ryhmä, niin tällöin sanotaan, että $(H, *)$ on ryhmän $(G, *)$ ***aliryhmä*** ja merkitään $(H, *) \leqslant (G, *)$ tai $H \leqslant G$. Tällöin myös $e_H = e_G$, sillä neutraalialkio on yksikäsitteinen. Huomaa, että $G \leqslant G$ ja $\{e_G\} \leqslant G$. Nämä ovat ryhmän G ***triviaalit aliryhmät***.

Lause 1.1.7. *(Kaksiosainen aliryhmäkriteeri.) Olkoon G ryhmä ja $\emptyset \neq H \subseteq G$. Tällöin $H \leqslant G$ jos ja vain jos seuraavat ehdot toteutuvat:*

1) $a, b \in H \Rightarrow ab \in H$,

2) $a \in H \Rightarrow a^{-1} \in H$.

Todistus. Oletetaan, että $H \leqslant G$. Tällöin ehdot 1) ja 2) ovat voimassa.

Oletetaan, että ehdot 1) ja 2) ovat voimassa. Tällöin

i) ehdosta 1) seuraa, että H on suljettu operaation $(*)$ suhteen;

ii) koska $(*)$ on assosiatiivinen joukossa G, se on assosiatiivinen joukossa H;

iii) ehdoista 1) ja 2) seuraa, että $aa^{-1} = e \in H$.

Näin ollen ryhmän ehdot ovat voimassa joukolle H. Tällöin $(H, *)$ on ryhmä ja $H \leqslant G$. □

Lause 1.1.8. [6]. *(Yksiosainen aliryhmäkriteeri.) Olkoon G ryhmä ja $\emptyset \neq H \subseteq G$. Tällöin $H \leqslant G$ jos ja vain jos kaikilla $a, b \in H$ pätee $ab^{-1} \in H$.*

Todistus. Oletetaan, että $H \leqslant G$. Tällöin H on ryhmä ja $ab^{-1} \in H$.

Oletetaan, että $ab^{-1} \in H$. Tällöin, jos $a \in H$, niin $aa^{-1} = e \in H$. Tästä seuraa, että $ea^{-1} = a^{-1} \in H$. Nyt Lauseen 1.1.7 ehto 2) on voimassa.

Jos $a, b \in H$, niin tällöin $b^{-1} \in H$ ja $ab = a(b^{-1})^{-1} \in H$. Nyt myös ehto 1) on voimassa. Tällöin Lauseen 1.1.7 nojalla $H \leqslant G$. □

Osoitetaan vielä yksi aliryhmäkriteeri äärellisille osajoukoille. Tämä osoittautuu erittäin hyödylliseksi tarkasteltaessa Rubikin kuution ryhmää ja sen aliryhmiä.

Lause 1.1.9. *Olkoon G ryhmä ja $H \neq \emptyset$ ryhmän G äärellinen osajoukko. Tällöin $H \leqslant G$ jos ja vain jos kaikilla $a, b \in H$ pätee $ab \in H$.*

Todistus. Oletetaan, että $H \leqslant G$. Tällöin yllä oleva ehto on voimassa, sillä H on ryhmä.

Oletetaan nyt, että $ab \in H$ kaikilla $a, b \in H$. Tällöin Lauseen 1.1.7 ehto 1) on voimassa.

Selvästi $a^n \in H$ kaikilla $n \in \mathbb{Z}_+$. Koska H on äärellinen, niin tällöin myös alkion a kertaluku on äärellinen, sillä on mahdotonta, että alkio a^i olisi eri kaikilla $i \in \mathbb{Z}$, sillä $|\mathbb{Z}| = \infty$. Tällöin on olemassa sellaiset $i_1, i_2 \in \mathbb{Z}$, että $a^{i_1} = a^{i_2}$. Tästä seuraa, että $a^{i_2 - i_1} = e$. Olkoon $|a| = m$. Tällöin

$$a^m = e \Leftrightarrow a^m a^{-1} = ea^{-1} \Leftrightarrow a^{m-1} = a^{-1} \in H.$$

Näin ollen Lauseen 1.1.7 ehto 2) on voimassa. Täten Lauseen 1.1.7 nojalla $H \leqslant G$. □

Määritelmä 1.1.10. Olkoon $H \leqslant G$ ja $a \in G$. Tällöin joukko $aH = \{ah \mid h \in H\}$ on ***alkion*** a ***määräämä aliryhmän*** H ***vasen sivuluokka***. Vastaavasti määritellään ***oikea sivuluokka*** Ha.

Lause 1.1.11. *Olkoon G ryhmä ja $H \leqslant G$. Tällöin joukossa G määritelty relaatio*

$$aRb \Leftrightarrow b^{-1}a \in H$$

on ekvivalenssirelaatio ja jos $a \in G$, niin ekvivalenssiluokka $[a] = aH$.

Todistus. 1) Selvästi $e = a^{-1}a \in H$ eli aRa.

2) Olkoon aRb eli $b^{-1}a \in H$. Tällöin, koska H on ryhmä, myös $(b^{-1}a)^{-1} = a^{-1}b \in H$ eli bRa.

3) Olkoon aRb ja bRc eli $b^{-1}a, c^{-1}b \in H$. Tällöin myös $c^{-1}bb^{-1}a = c^{-1}a \in H$, sillä H on ryhmä. Näin ollen aRc.

Kohdista 1)-3) seuraa, että R on ekvivalenssirelaatio ja G jakaantuu pistevieraisiin ekvivalenssiluokkiin. Nyt alkion a määräämä ekvivalenssiluokka $[a] = \{b \in G \mid bRa\}$.

Oletetaan, että $y \in [a]$ eli yRa eli $a^{-1}y \in H$. Tällöin $y = a(a^{-1}y) \in aH$, joten $[a] \subseteq aH$.

Oletetaan, että $y \in aH$. Tällöin $y = ah$ jollakin $h \in H$ ja siten $a^{-1}y = h \in H$ eli yRa eli $y \in [a]$. Siis $aH \subseteq [a]$. Näin ollen $[a] = aH$. □

Ekvivalenssiluokan ominaisuuksista seuraa, että

$$G = \bigcup_i a_i H,\ a_i H \cap a_j H = \emptyset \text{ kaikilla } i \neq j$$

ja $b \in aH \Leftrightarrow aH = bH$. Nyt tiedetään, että kaikki sivuluokat ovat erillisiä.

Lemma 1.1.12. *Olkoon G ryhmä, $H \leqslant G$ ja $a \in G$. Tällöin $|H| = |aH|$.*

Todistus. Olkoon $f : H \longrightarrow aH,\ f(h) = ah$. Tällöin $f(H) = \{ah \mid h \in H\} = aH$ ja joukon aH alkukuva on funktion f määrittelyjoukko H. Selvästi, jos $f(h_1) = f(h_2)$, niin $h_1 = h_2$. Tällöin f on sekä surjektio että injektio, eli bijektio ja siten $|H| = |aH|$. □

Lause 1.1.13. *(Lagrangen lause.) Olkoot G äärellinen ryhmä ja $H \leqslant G$. Tällöin $|G| = n|H|$, missä n on aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G.*

Todistus. Lauseen 1.1.11 nojalla

$$G = \bigcup_i a_i H,\ a_i H \cap a_j H = \emptyset \text{ kaikilla } i \neq j.$$

Lemman 1.1.12 nojalla $|a_i H| = |H|$ kaikilla $1 \leq i \leq n$. Näin ollen

$$|G| = \sum_{i=1}^{n} |a_i H| = \sum_{i=1}^{n} |H| = n|H|.$$

□

Lauseesta 1.1.13 seuraa, että aliryhmän mahtavuus jakaa ryhmän mahtavuuden.

Määritelmä 1.1.14. Olkoon G ryhmä ja $H \leqslant G$. Tällöin aliryhmän H ***indeksi*** ryhmässä G on

$$[G : H] = \frac{|G|}{|H|}.$$

Lauseen 1.1.13 nojalla indeksi on yhtä suuri kuin vasempien sivuluokkien lukumäärä.

Määritelmä 1.1.15. Olkoon G ryhmä ja $H \leqslant G$. Jos $aH = Ha$ kaikilla $a \in G$, niin H on ***normaali aliryhmä*** ja merkitään $H \trianglelefteq G$.

Lause 1.1.16. *$H \trianglelefteq G$ jos ja vain jos $aHa^{-1} \subseteq H$ kaikilla $a \in G$.*

Todistus. Oletetaan, että $H \trianglelefteq G$. Tällöin $aH = Ha$ kaikilla $a \in G$. Olkoon nyt $y \in aHa^{-1}$. Tällöin $y = aha^{-1}$ jollakin $h \in H$. Nyt $ah \in aH = Ha$. Siten $ah = h'a$ ja $y = aha^{-1} = h'aa^{-1} = h' \in H$. Siis $aHa^{-1} \subseteq H$.

Oletetaan seuraavaksi, että $aHa^{-1} \subseteq H$ kaikilla $a \in G$. Olkoon $y \in aH$. Tällöin $y = ah$ jollakin $h \in H$. Nyt $y = aha^{-1}a \in Ha$, sillä $aha^{-1} \in H$. Siis $aH \subseteq Ha$.

Olkoon $y \in Ha$. Tällöin $y = ha$ jollakin $h \in H$. Nyt $y = ha = aa^{-1}ha = a(a^{-1}h(a^{-1})^{-1}) \in aH$. Siis $Ha \subseteq aH$. Näin ollen $aH = Ha$ kaikilla $a \in G$. □

Lause 1.1.17. *Olkoon* $(H, *) \trianglelefteq (G, *)$. *Tällöin sivuluokkien joukossa* $\{aH \mid a \in G\}$ *voidaan määritellä operaatio* $(*)$ *siten, että*

$$aH * bH = (a * b)H.$$

Tällöin $(*)$ *on hyvin määritelty ja* $(\{aH \mid a \in G\}, *)$ *on ryhmä.*

Todistus. Olkoon $aH = a'H$ ja $bH = b'H$. Nyt $a' \in aH$, joten $a' = ax$ jollakin $x \in H$ ja $b' \in bH$, joten $b' = by$ jollakin $y \in H$. Tällöin $a'b' = axby$.

Koska $H \trianglelefteq G$, niin $bH = Hb$, jolloin $xb \in bH$ ja edelleen $xb = bz$ jollakin $z \in H$. Tästä seuraa, että $a'b' = axby = abzy \in abH$. Siis $a'b'H = abH$.

Näin ollen $(*)$ on hyvin määritelty. Osoitetaan ryhmärakenne. Nyt

1) Selvästi $(*)$ on suljettu operaatio.

2) $(aH * bH) * cH = abH * cH = abcH = aH * bcH = aH * (bH * cH)$.

3) $e_G H \in \{aH \mid a \in G\}$ ja $e_G H * aH = aH = aH * e_G H$ kaikilla $a \in G$.

4) $a \in G \Rightarrow \exists a^{-1} \in G$ ja $aH * a^{-1}H = e_G H = a^{-1}H * aH$.

Kohdista 1)-4) seuraa, että $(\{aH \mid a \in G\}, *)$ on ryhmä. Tätä ryhmää kutsutaan ***ryhmän*** G ***tekijäryhmäksi normaalin aliryhmän*** H ***suhteen*** ja merkitään ryhmää G/H. Lagrangen lauseen nojalla

$$|G/H| = \frac{|G|}{|H|},$$

jos G on äärellinen.

□

Lause 1.1.18. *Indeksin* 2 *aliryhmä on normaali.*

Todistus. Olkoon $H \leqslant G$ siten, että $[G : H] = 2$. Tällöin ryhmässä G on kaksi vasenta (ja oikeaa) sivuluokkaa. Jos $g \in H$, niin $gH = H = Hg$, sillä H on ryhmä. Jos $g \notin H$, niin on oltava $gH = G \setminus H = Hg$ Lauseen 1.1.11 nojalla. Siis $gH = Hg$. Näin ollen $H \trianglelefteq G$. □

1.2 Erilaisia ryhmiä

Olkoon G ryhmä ja $a \in G$. Tällöin $H = \{a^k \mid k \in \mathbb{Z}\} \subseteq G$. Jos $x, y \in H$, niin $x = a^m$ ja $y = a^n$ joillakin $m, n \in \mathbb{Z}$. Lisäksi $xy^{-1} = a^m a^{-n} = a^{m-n} \in H$ ja Lauseen 1.1.8 nojalla H on ryhmä.

Määritelmä 1.2.1. Ryhmää $H = \{a^k \mid k \in \mathbb{Z}\}$ kutsutaan ***alkion*** a ***generoimaksi sykliseksi ryhmäksi***, ja merkitään $H = \langle a \rangle$. Alkiota a kutsutaan ***generoijaksi***.

Syklistä ryhmää, jonka kertaluku on n, merkitään C_n.

Määritelmä 1.2.2. Olkoon $X \neq \emptyset$ joukko ja kuvaus $\alpha : X \longrightarrow X$ bijektio. Tällöin α on joukon X ***permutaatio***.

Määritelmä 1.2.3. Olkoon X epätyhjä joukko, jolle $|X| = n$. Tällöin kaikkien joukon X permutaatioiden joukkoa merkitään S_n.

Määritelmä 1.2.4. Olkoot $\alpha, \beta \in S_n$ ja $i \in X$. Tällöin ***permutaatioiden tulo vasemmalta oikealle*** määritellään

$$(i)(\alpha \circ \beta) = ((i)\alpha)\beta.$$

Toisin sanoen, kuvataan jokainen $i \in X$ permutaatiolla α, jonka jälkeen jokainen uusi alkio $(i)\alpha$ kuvataan permutaatiolla β. Tässä tutkielmassa permutaatioiden tulo määritellään näin päin. Tavallisesti käytetään tuloa oikealta vasemmalle, mutta erään luvussa 3 esiintyvän ryhmärakenteen operaation määrittelyn selkeyden vuoksi tulo määritellään nyt vasemmalta oikealle.

Lause 1.2.5. *Olkoon S_n kuten Määritelmässä 1.2.3 ja $(\circ)$ kuvausten yhdistämisoperaatio. Tällöin $(S_n, \circ)$ on ryhmä.*

Todistus. Nyt

1) $\alpha, \beta \in S_n \Rightarrow \alpha \circ \beta \in S_n$, sillä bijektioiden yhdiste on bijektio.

2) $\alpha, \beta, \gamma \in S_n \Rightarrow (\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.

3) Identiteettipermutaatio $id \in S_n$ määritellään siten, että $(x)id = x$ kaikilla $x \in X$, jolloin $\alpha \circ id = id \circ \alpha = \alpha$ kaikilla $\alpha \in S_n$. Alkiota $id \in S_n$ merkitään (1). Siis (1) on joukon S_n neutraalialkio.

4) Olkoon $\alpha \in S_n$. Koska α on bijektio $X \longrightarrow X$, niin on olemassa käänteiskuvaus α^{-1}. Käänteiskuvaus on myös bijektio $X \longrightarrow X$ eli $\alpha^{-1} \in S_n$. Lisäksi $\alpha \circ \alpha^{-1} = id = \alpha^{-1} \circ \alpha$.

Kohdista 1)-4) seuraa, että $(S_n, \circ)$ on ryhmä ja sitä kutsutaan ***symmetriseksi ryhmäksi astetta*** n. □

Huomaa, että $|S_n| = n!$ tuloperiaatteen nojalla, sillä koska permutaatio on bijektio, niin tätä bijektiota rakentaessa alkio 1 voidaan kuvata n eri alkioksi, alkio 2 voidaan kuvata $n-1$ eri alkioksi, ... ja alkio n voidaan kuvata vain yhdeksi alkioksi. Tällöin ryhmässä S_n on kombinatoriikan tuloperiaatteen nojalla $n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!$ eri permutaatiota.

Määritelmä 1.2.6. Olkoon $X = \{1, 2, \ldots, n\}$. Joukon X permutaatio on ***sykli***, jos sille pätee $x_1 \mapsto x_2 \mapsto ... \mapsto x_k \mapsto x_1$, missä $x_i \in X$ kaikilla i sekä $x_i \neq x_j$ kaikilla $i \neq j$, ja muut alkiot pysyvät paikoillaan. Tällaista sykliä merkitään $(x_1\ x_2\ x_3\ \ldots\ x_k)$ ja sen ***pituus*** on k. Sykliä, jonka pituus on k, kutsutaan ***k-sykliksi***.

Huomaa, että $(x_1\ x_2\ x_3\ \ldots\ x_k) = (x_2\ x_3\ \ldots\ x_k\ x_1) = (x_3\ x_4\ \ldots\ x_k\ x_1\ x_2) = \ldots = (x_k\ x_1\ \ldots\ x_{k-3}\ x_{k-2}\ x_{k-1})$.

Määritelmä 1.2.7. Jos $\alpha \in S_n$ ja $i \in X$, niin

1) α ***säilyttää*** alkion i, jos $(i)\alpha = i$ ja

2) α ***siirtää*** alkion i, jos $(i)\alpha \neq i$.

Syklit ovat ***erillisiä***, jos ne eivät siirrä yhtään samaa alkiota.

Esimerkki permutaatioiden tulosta. Olkoon $\alpha = (1\ 5\ 7\ 2), \beta = (2\ 3\ 1\ 4) \in S_7$. Tällöin tarkastellaan jokainen alkio joukosta $X = \{1, \ldots, 7\}$ erikseen seuraavasti:

Aloitetaan alkiosta 1. Nyt

$$\begin{aligned}
&(1)\alpha = 5 \text{ ja } (5)\beta = 5 \Rightarrow (1)(\alpha\beta) = 5,\\
&(5)\alpha = 7 \text{ ja } (7)\beta = 7 \Rightarrow (5)(\alpha\beta) = 7,\\
&(7)\alpha = 2 \text{ ja } (2)\beta = 3 \Rightarrow (7)(\alpha\beta) = 3,\\
&(3)\alpha = 3 \text{ ja } (3)\beta = 1 \Rightarrow (3)(\alpha\beta) = 1.
\end{aligned}$$

Koska päädyttiin alkioon 1, sykli suljetaan ja jatketaan tarkastelua pienimmästä sykliin kuulumattomasta alkiosta, eli luvusta 2. Nyt

$$\begin{aligned}
&(2)\alpha = 1 \text{ ja } (1)\beta = 4 \Rightarrow (2)(\alpha\beta) = 4,\\
&(4)\alpha = 4 \text{ ja } (4)\beta = 2 \Rightarrow (4)(\alpha\beta) = 2.
\end{aligned}$$

Päädyttiin alkioon 2, jolloin sykli suljetaan. Kuvaamatta on alkio 6, mutta koska $(6)\alpha = (6)\beta = 6$, niin $\alpha\beta$ säilyttää alkion 6. Tällöin

$$\alpha\beta = (1\ 5\ 7\ 2)(2\ 3\ 1\ 4) = (1\ 5\ 7\ 3)(2\ 4)(6) = (1\ 5\ 7\ 3)(2\ 4).$$

1-syklit jätetään merkitsemättä, sillä $(i) = e_{S_n}$ kaikilla $i \in X$.

Määritelmä 1.2.8. Olkoon $G \leqslant S_n$, $\alpha \in G$ ja $i \in X$. Tällöin ***alkion*** i ***rata ryhmässä*** G

$$\mathrm{Orb}_G(i) = \{(i)\alpha \mid \alpha \in G\} \subseteq X.$$

Toisin sanoen, alkion i rata permutaatioryhmässä G sisältää kaikki ne joukon X alkiot, joihin i voidaan siirtää ryhmän G permutaatioilla.

Lause 1.2.9. *Jos $\alpha \in S_n$, niin α voidaan esittää erillisten syklien tulona.*

Todistus. Olkoon $\alpha \in S_n$. Tällöin permutaation α generoima syklinen ryhmä $\langle\alpha\rangle$ permutoi joukon $X = \{1, 2, \ldots, n\}$ alkioita. Olkoon relaatio O joukossa X siten, että xOx' jos, ja vain jos $x' \in \mathrm{Orb}_{\langle\alpha\rangle}(x)$. Selvästi O on ekvivalenssirelaatio radan määritelmän nojalla. Tällöin joukko X jakaantuu pistevieraisiin ekvivalenssiluokkiin, ja kukin rata vastaa sykliä permutaatiossa α. Näin ollen väite pätee.

□

Lemma 1.2.10. *Olkoon $\alpha \in S_n$. Tällöin α voidaan kirjoittaa 2-syklien tulona.*

Todistus. Olkoon $\alpha = (\alpha_1\ \alpha_2\ \alpha_3\ \ldots\ \alpha_k) \in S_n$ k-sykli. Tällöin permutaatioiden tulon määritelmästä seuraa, että

$$(\alpha_1\ \alpha_2\ \alpha_3\ \ldots\ \alpha_k) = (\alpha_{k-1}\ \alpha_k)(\alpha_{k-2}\ \alpha_{k-1})\cdots(\alpha_2\ \alpha_3)(\alpha_1\ \alpha_2).$$

Lauseen 1.2.9 nojalla jokainen permutaatio voidaan esittää erillisten syklien tulona. Edellisen nojalla nämä syklit voidaan purkaa 2-syklien tuloksi. Näin ollen kaikilla permutaatioilla on esitys 2-syklien tulona.

□

Määritelmä 1.2.11. Olkoon $\alpha \in S_n$ ja k sen Lemman 1.2.10 mukaisen tuloesityksen 2-syklien lukumäärä. Permutaation α ***merkki***

$$\mathrm{sgn}(\alpha) = \begin{cases} 1, & k \text{ parillinen} \\ -1, & k \text{ pariton.} \end{cases}$$

Permutaation α ***pariteetti*** on parillinen, jos $\mathrm{sgn}(\alpha) = 1$ ja pariton, jos $\mathrm{sgn}(\alpha) = -1$.

Määritelmä 1.2.12. Olkoon $\alpha \in S_n$. Permutaation α ***merkki*** voidaan määritellä myös

$$\mathrm{sgn}(\alpha) = (-1)^k,$$

missä k on Lemman 1.2.10 mukaisen tuloesityksen 2-syklien lukumäärä.

Lause 1.2.13. *Määritelmät 1.2.11 ja 1.2.12 ovat yhtäpitävät.*

Todistus. Olkoon permutaatiolla $\alpha \in S_n$ esitys k 2-syklin tulona Lauseen 1.2.10 mukaisesti. Tällöin

1) jos k on parillinen, niin $\mathrm{sgn}(\alpha) = 1$, jolloin myös $(-1)^k = 1$,

2) jos k on pariton, niin $\mathrm{sgn}(\alpha) = -1$, jolloin myös $(-1)^k = -1$.

Siis määritelmät ovat yhtenevät.

□

Määritelmä 1.2.14. Olkoot S_n ja X kuten Määritelmässä 1.2.3. Tällöin ***joukon*** X ***alternoiva ryhmä*** A_n on kaikkien joukon X parillisten permutaatioiden joukko. Toisin sanoen

$$A_n = \{\alpha \in S_n \mid \operatorname{sgn}(\alpha) = 1\}.$$

Loput joukon A_n keskeisistä ominaisuuksista todistetaan seuraavan kappaleen lopussa.

1.3 Isomorfismit

Isomorfismin käsite on erittäin tärkeä, sillä sen avulla ryhmiä voidaan käsitellä samoina objekteina. Jos kaksi ryhmää ovat keskenään isomorfiset, niillä on täysin sama rakenne. Tätä ominaisuutta käyttäen saadaan selville Rubikin kuution ryhmän rakenne.

Määritelmä 1.3.1. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvaus $f : G \longrightarrow H$ on ***ryhmähomomorfismi***, jos $f(a \cdot b) = f(a) * f(b)$ kaikilla $a, b \in G$.

Lause 1.3.2. *Olkoon $f : (G, \cdot) \longrightarrow (H, *)$ ryhmähomomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin $f(e_G) = e_H$ ja $f(a^{-1}) = f(a)^{-1}$ kaikilla $a \in G$.*

Todistus. $e_G \in G \Rightarrow f(e_G) \in H$. Tällöin $f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G)$.
Siten $f(e_G) * f(e_G) * f(e_G)^{-1} = f(e_G) * f(e_G)^{-1} \Leftrightarrow f(e_G) = e_H$.
Näin ollen $f(a) * f(a^{-1}) = f(e_G) = e_H = f(e_G) = f(a^{-1}) * f(a)$ kaikilla $a \in G$.

□

Lause 1.3.3. *Olkoon* $\operatorname{sgn} : S_n \longrightarrow (\{1, -1\}, \cdot)$ *määritelty kuten edellä. Tällöin* sgn *on ryhmähomomorfismi.*

Todistus. Olkoon $\alpha, \beta \in S_n$. Nyt Lemman 1.2.10 nojalla α ja β voidaan esittää 2-syklien tuloina. Olkoon permutaation α 2-sykliesityksessä k 2-sykliä, ja permutaation β esityksessä l 2-sykliä. Tällöin

$$\operatorname{sgn}(\alpha\beta) = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

□

Lause 1.3.4. *Olkoon $\alpha \in S_n$ k-sykli. Tällöin* $\operatorname{sgn}(\alpha) = (-1)^{k-1}$.

Todistus. Nyt Lemman 1.2.10 nojalla

$$\alpha = (i_1\ i_2\ i_3\ \ldots\ i_k) = (i_{k-1}\ i_k)(i_{k-2}\ i_{k-1}) \cdots (i_2\ i_3)(i_1\ i_2).$$

Esityksessä on $k-1$ kappaletta 2-syklejä. Lauseen 1.3.3 nojalla

$$\begin{aligned}\operatorname{sgn}(\alpha) &= \operatorname{sgn}(i_{k-1}\ i_k)\operatorname{sgn}(i_{k-2}\ i_{k-1}) \cdots \operatorname{sgn}(i_2\ i_3)\operatorname{sgn}(i_1\ i_2) \\ &= \underbrace{(-1)(-1)\cdots(-1)(-1)}_{k-1 \text{ kpl}} = (-1)^{k-1}.\end{aligned}$$

□

Määritelmä 1.3.5. Olkoon $f : G \longrightarrow H$ ryhmähomomorfismi. Tällöin homomorfismin f ***kuva*** on joukko

$$Im(f) = f(G) = \{f(x) \mid x \in G\}$$

ja homomorfismin f ***ydin*** on joukko

$$Ker(f) = \{x \in G \mid f(x) = e_H\}.$$

Lause 1.3.6. *Olkoon $f : (G, \cdot) \longrightarrow (H, *)$ ryhmähomomorfismi. Tällöin $Im(f) \leqslant H$.*

Todistus. Lauseen 1.3.2 nojalla $f(e_G) = e_H \in Im(f)$. Olkoot $a, b \in Im(f)$. Tällöin on olemassa sellaiset $a', b' \in G$, että $f(a') = a$ ja $f(b') = b$. Koska G on ryhmä, niin $a' \cdot b'^{-1} \in G$, jolloin Lauseen 1.3.2 nojalla $f(a' \cdot b'^{-1}) = f(a') * f(b'^{-1}) = f(a') * f(b')^{-1} = a * b^{-1} \in Im(f)$. Lauseen 1.1.8 nojalla $Im(f) \leqslant H$.

□

Määritelmä 1.3.7. Olkoon $f : G \longrightarrow H$ ryhmähomomorfismi. Jos f on bijektio, niin f on ***ryhmäisomorfismi***. Tällöin merkitään $G \cong H$. Jos G on äärellinen ryhmä, niin $|G| = |H|$.

Määritelmä 1.3.8. Olkoon G ryhmä ja $f : G \longrightarrow G$ ryhmäisomorfismi. Tällöin f on ***automorfismi***. Merkitään $\operatorname{Aut}(G) = \{f \mid f \text{ automorfismi ryhmällä } G\}$.

Lause 1.3.9. *Olkoon $f : G \longrightarrow H$ ryhmähomomorfismi. Tällöin $Ker(f) \trianglelefteq G$ ja $G/Ker(f)$ on ryhmä.*

Todistus. Selvästi $Ker(f) \neq \emptyset$. Olkoon $a, b \in Ker(f)$. Tällöin $f(a) = f(b) = e_H$. Siten

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H e_H^{-1} = e_H.$$

Näin ollen $ab^{-1} \in Ker(f)$ ja Lauseen 1.1.8. nojalla $Ker(f) \leqslant G$.

Olkoon nyt $g \in G$ ja $k \in Ker(f)$. Tällöin

$$f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)e_H f(g)^{-1} = e_H.$$

Siten $gkg^{-1} \in Ker(f)$ ja näin ollen $Ker(f) \trianglelefteq G$. Tällöin tekijäryhmän määritelmän nojalla $G/Ker(f)$ on ryhmä.

□

Lause 1.3.10. [6]. *(Homomorfismien peruslause.) Olkoon $f : (G, \cdot) \longrightarrow (H, *)$ ryhmähomomorfismi. Tällöin*

$$G/Ker(f) \cong Im(f).$$

Todistus. Lauseen 1.3.6 nojalla $Im(f)$ on ryhmä. Olkoon nyt $Ker(f) = K$ ja $F : G/K \longrightarrow Im(f)$, $F(aK) = f(a)$. On tarkistettava, että F on hyvin määritelty. Olkoon siis $a'K = aK$. Tällöin $a' = a \cdot k$ jollakin $k \in K$. Siten

$$F(a'K) = f(a') = f(a \cdot k) = f(a) * f(k) = f(a) * e_H = f(a) = F(aK).$$

Siis F on hyvin määritelty.

Nyt

$$\begin{aligned} & F(aK) = F(bK) \\ \Rightarrow\ & f(a) = f(b) \\ \Rightarrow\ & e_H = f(b)^{-1} * f(a) = f(b^{-1}) * f(a) = f(b^{-1} \cdot a) \\ \Rightarrow\ & b^{-1} \cdot a \in K \\ \Rightarrow\ & K = b^{-1}K \cdot aK \\ \Rightarrow\ & bK = aK. \end{aligned}$$

Siten F on injektio.

Olkoon $f(b) \in Im(f)$. Tällöin $bK \in G/K$ ja $F(bK) = f(b)$, joten F on surjektio.

Olkoon $aK, bK \in G/K$. Tällöin

$$F(aK \cdot bK) = F((a \cdot b)K) = f(a \cdot b) = f(a) * f(b) = F(aK) * F(bK).$$

Näin ollen F on isomorfismi ja $G/Ker(f) \cong Im(f)$.

□

Lause 1.3.11. *Olkoon A_n kuten Määritelmässä 1.2.14. Tällöin $A_n \trianglelefteq S_n$.*

Todistus. Tapaus $n = 1$ on triviaali. Olkoon siis $n > 1$. Lauseen 1.3.3 nojalla kuvaus sgn : $S_n \longrightarrow (\{1, -1\}, \cdot)$ on ryhmähomomorfismi. Selvästi kuvaus sgn on surjektiivinen, eli $Im(\text{sgn}) = \{1, -1\}$. Tällöin, koska

$$A_n = \{\alpha \in S_n \mid \text{sgn}(\alpha) = 1 = e_{Im(\text{sgn})}\},$$

niin $A_n = Ker(\text{sgn})$. Siten Lauseen 1.3.9 nojalla $A_n \trianglelefteq S_n$.

□

Homomorfismien peruslauseen nojalla $S_n/A_n \cong \{1, -1\}$, jolloin Lagrangen lauseen nojalla $|S_n/A_n| = \dfrac{|S_n|}{|A_n|} = |\{1, -1\}| = 2$ eli $|A_n| = \dfrac{|S_n|}{2}$.

Lause 1.3.12. *Kaikkien ryhmän S_n 3-syklien joukko generoi ryhmän A_n.*

Todistus. Lemman 1.2.10 nojalla kaikille $\alpha \in S_n$ on olemassa esitys 2-syklien tulona. Lisäksi 2-sykli on pariton. Tällöin jokainen parillinen permutaatio voidaan esittää tulona parillisesta määrästä 2-syklejä. Toisin sanoen, jos $\alpha \in A_n$, niin $\alpha = \alpha_1 \cdots \alpha_{2k}$, missä $k \in \mathbb{Z}_+$ ja α_i on 2-sykli kaikilla $1 \leq i \leq 2k$. Tarkastellaan kahden peräkkäisen 2-syklin tuloa $\alpha_i\alpha_{i+1}$, missä i on pariton luku. Huomaa, että $(a\ b) = (b\ a)$.

Jos $\alpha_i = \alpha_{i+1}$, niin ne ovat muotoa $(a\ b)$. Tällöin

$$\alpha_i\alpha_{i+1} = (a\ b)(a\ b) = (1) = (a\ b\ c)^3.$$

Jos $\alpha_i = (a\ b)$ ja $\alpha_{i+1} = (a\ c)$, niin

$$\alpha_i\alpha_{i+1} = (a\ b)(a\ c) = (a\ b\ c).$$

Jos $\alpha_i = (a\ b)$ ja $\alpha_{i+1} = (c\ d)$, niin

$$\alpha_i\alpha_{i+1} = (a\ b)(c\ d) = (a\ b\ d)(d\ a\ c).$$

Siis kaikissa tapauksissa kahden 2-syklin tulo voidaan esittää 3-syklien tulona. Näin ollen kaikille ryhmän A_n permutaatioille α löytyy esitys 3-syklien tulona.

Lisäksi, koska $(a\ b\ c) = (a\ b)(a\ c)$, niin

$$\text{sgn}(a\ b\ c) = \text{sgn}((a\ b)(a\ c)) = \text{sgn}(a\ b)\,\text{sgn}(a\ c) = (-1) \cdot (-1) = 1$$

Lauseen 1.3.3 nojalla. Tällöin $(a\ b\ c) \in A_n$ eli kaikki 3-syklit ryhmästä S_n ovat ryhmässä A_n.

Näin ollen 3-syklien joukko generoi ryhmän A_n.

□

Lause 1.3.13. *A_n on ainoa ryhmän S_n indeksin 2 aliryhmä, kun $n \leq 2$.*

Todistus. Jos $n = 2$, niin selvästi A_2 on ainoa indeksin 2 aliryhmä ryhmässä S_2. Olkoon nyt $n > 2$. Tällöin on olemassa 3-sykli $\sigma \in S_n$. Olkoon H ryhmän S_n indeksin 2 aliryhmä, eli ryhmällä S_n on täsmälleen kaksi sivuluokkaa normaalin aliryhmän H suhteen. Oletetaan, että $\sigma \notin H$. Tällöin $\sigma^{-1} \notin H$. Koska σ on 3-sykli, niin $\sigma^{-1} = \sigma^2$. Koska sivuluokkia on vain kaksi, niin

$$H \neq \sigma H = \sigma^{-1}H = \sigma^2 H = \sigma H * \sigma H = \sigma H * \sigma^{-1}H = (\sigma\sigma^{-1})H = (1)H = H,$$

mikä on ristiriita. Tällöin on oltava $\sigma \in H$. Näin ollen H sisältää kaikki 3-syklit ryhmästä S_n, jolloin Lauseen 1.3.12 nojalla $H = A_n$, sillä $|H| = |A_n|$.

□

2 Ryhmien välisiä operaatioita

Ryhmistä on mahdollista konstruoida uusia ryhmiä erinäisillä ryhmien välisillä tuloilla. Tässä luvussa tarkastellaan suoraa tuloa, ryhmän toimintaa joukossa ja kranssituloa.

2.1 Suora tulo ja ryhmän toiminta

Määritelmä 2.1.1. Olkoot G_1 ja G_2 ryhmiä. Tällöin ryhmien G_1 ja G_2 ***suora tulo*** on karteesinen tulo $G_1 \times G_2$ varustettuna operaatiolla $(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$, missä $g_1, g_1' \in G_1$ ja $g_2, g_2' \in G_2$.

Lause 2.1.2. *Olkoot G_1, G_2 ryhmiä. Tällöin $(G_1 \times G_2, \cdot)$, missä $(\cdot)$ on kuten Määritelmässä 2.1.1, on ryhmä.*

Todistus. 1) Operaation $(\cdot)$ määritelmän nojalla joukko $G_1 \times G_2$ on suljettu operaation $(\cdot)$ suhteen.

2) Jos $(g_1, g_1'), (g_2, g_2'), (g_3, g_3') \in G_1 \times G_2$, niin

$$\begin{aligned} &\big((g_1, g_1') \cdot (g_2, g_2')\big) \cdot (g_3, g_3') \\ &= (g_1 g_2, g_1' g_2') \cdot (g_3, g_3') \\ &= (g_1 g_2 g_3, g_1' g_2' g_3') \\ &= (g_1, g_1') \cdot (g_2 g_3, g_2' g_3') \\ &= (g_1, g_1') \cdot \big((g_2, g_2') \cdot (g_3, g_3')\big). \end{aligned}$$

Täten $(\cdot)$ on assosiatiivinen joukossa $G_1 \times G_2$.

3) Jos $(g_1, g_2) \in G_1 \times G_2$, niin

$$(g_1, g_2) \cdot (e_{G_1}, e_{G_2}) = (g_1, g_2) = (e_{G_1}, e_{G_2}) \cdot (g_1, g_2).$$

Siten (e_{G_1}, e_{G_2}) on joukon $G_1 \times G_2$ neutraalialkio.

4) Jos $(g_1, g_2) \in G_1 \times G_2$, niin $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$. Tällöin

$$(g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) = (e_{G_1}, e_{G_2}) = (g_1^{-1}, g_2^{-1}) \cdot (g_1, g_2).$$

Siten alkion (g_1, g_2) käänteisalkio joukossa $G_1 \times G_2$ on alkio (g_1^{-1}, g_2^{-1}).

Kohdista 1)-4) seuraa, että $(G_1 \times G_2, \cdot)$ on ryhmä. □

Määritelmä 2.1.3. Olkoon G ryhmä ja X joukko. Olkoon lisäksi kuvaus

$$\phi : X \times G \longrightarrow X,\ (x, g) \mapsto \phi(x, g).$$

Merkitään $\phi(x, g) = x.g$. Tällöin kuvaus ϕ on ***ryhmän G oikea toiminta joukossa*** X, jos

1) $x.e = x$ kaikilla $x \in X$,

2) $x.(gh) = (x.g).h$ kaikilla $g, h \in G, x \in X$.

Lause 2.1.4. *Olkoon $g \in G$ kiinnitetty. Tällöin kuvaus $\phi(x, g) = x.g$ on bijektio joukossa X.*

Todistus. Olkoon $x, y \in X$. Tällöin

$$\begin{aligned} & \phi(x, g) = \phi(y, g) \\ \Leftrightarrow\ & x.g = y.g \\ \Leftrightarrow\ & (x.g).g^{-1} = (y.g).g^{-1} \\ \Leftrightarrow\ & x.(gg^{-1}) = y.(gg^{-1}) \\ \Leftrightarrow\ & x.e = y.e \\ \Leftrightarrow\ & x = y, \end{aligned}$$

missä $g \in G$. Lisäksi

$$x = x.e = x.(g^{-1}g) = (x.g^{-1}).g = z.g = \phi(z, g),$$

missä $z = x.g^{-1} \in X$ ja $g \in G$. Näin ollen väite pätee. □

Lauseen 2.1.4 nojalla ryhmän toiminta määrittää bijektion joukossa X. Toisin sanoen, jokainen $g \in G$ määrää permutaation joukossa X. Tästä permutaatiosta käytetään jatkossa merkintää $(x)\phi_g = \phi(x, g)$.

Määritelmä 2.1.5. Olkoon G ryhmä, X joukko ja $\mathrm{Sym}(X)$ joukon X permutaatioiden ryhmä. ***Ryhmän G permutaatioesitys*** on ryhmähomomorfismi ryhmältä G ryhmälle $\mathrm{Sym}(X)$.

Määritelmä 2.1.6. Olkoon G ryhmä, X joukko, $\mathrm{Sym}(X)$ joukon X permutaatioiden ryhmä ja $\psi : G \longrightarrow \mathrm{Sym}(X)$ ryhmän G permutaatioesitys.
Ryhmän G oikea toiminta ryhmän permutaatioesityksestä ψ on sellainen ryhmän G oikea toiminta $\overline{\psi} : X \times G \longrightarrow X$, jolle $\overline{\psi}(x, g) = (x)\psi(g)$.

Huomaa, että koska ϕ_g on permutaatio, käytetään Määritelmän 1.2.4 mukaista merkintätapaa, eli permutoitava alkio on permutaation vasemmalla puolella. Osoitetaan, että Määritelmien 2.1.3 ja 2.1.6 mukaiset ryhmän toiminnot ovat samat.

Lause 2.1.7. *Ryhmän toimintojen ja permutaatioesitysten välillä on yksikäsitteinen vastaavuus.*

Todistus. ($\Rightarrow$) Olkoon ryhmän toiminta ϕ määritelty kuten Määritelmässä 2.1.3 ja $\overline{\phi} : G \longrightarrow \mathrm{Sym}(X)$ sellainen kuvaus, että $\overline{\phi}(g) = \phi_g$. Tällöin Lauseen 2.1.4 nojalla ϕ määrää bijektion ϕ_g joukossa X. Tällöin ϕ_g on permutaatio joukossa X eli $\phi_g \in \mathrm{Sym}(X), g \in G$. Olkoon nyt $g, h \in G$. Määritelmän 2.1.3 ehdon 1) nojalla

$$(x)\phi_g = \phi(x, g) = x.g \in X \text{ kaikilla } (x, g) \in X \times G.$$

Lisäksi

$$\begin{aligned}(x)(\phi_g \circ \phi_h) &= ((x)\phi_g)\phi_h \\ &= (x.g).h \\ &= x.(gh) \\ &= (x)\phi_{gh}.\end{aligned}$$

Tällöin $\overline{\phi}(g) \circ \overline{\phi}(h) = \overline{\phi}(gh)$, eli $\overline{\phi}$ on ryhmähomomorfismi. Tällöin voidaan asettaa $\overline{\phi} = \psi$, missä ψ on kuten Määritelmässä 2.1.6. Siis ryhmän toimintaa ϕ vastaa ryhmähomomorfismi eli permutaatioesitys $\psi : G \longrightarrow \mathrm{Sym}(X), \psi(g) = \phi_g$.

($\Leftarrow$) Olkoon G ryhmä, X joukko, $\mathrm{Sym}(X)$ joukon X permutaatioiden ryhmä ja $\psi : G \longrightarrow \mathrm{Sym}(X)$ ryhmän G permutaatioesitys kuten Määritelmässä 2.1.6. Olkoon myös $g, h \in G$ ja $x \in X$. Tällöin Määritelmän 2.1.6 nojalla permutaatioesitys ψ määrää kuvauksen $\overline{\psi}$, jolle $\overline{\psi}(x, g) = (x)\psi(g)$. Siis

$$x.g = \overline{\psi}(x, g) = (x)\psi(g) \in X \text{ kaikilla } (x, g) \in X \times G.$$

Jos e on ryhmän G neutraalialkio, niin

$$\begin{aligned}x.e &= (x)\psi(e) \\ &= (x)id && \text{(Lause 1.3.2, } id \text{ on identiteettipermutaatio)} \\ &= x.\end{aligned}$$

Lisäksi

$$\begin{aligned}(x.g).h &= ((x)\psi(g))\psi(h) \\ &= (x)(\psi(g) \circ \psi(h)) \\ &= (x)\psi(gh) && (\psi \text{ on homomorfismi}) \\ &= x.(gh).\end{aligned}$$

Näin ollen Määritelmän 2.1.6 määräämä ryhmän toiminto $\overline{\psi}$ toteuttaa Määritelmän 2.1.3 ehdot.

Tästä seuraa, että määritelmät ovat yhtäpitäviä. □

Lauseen 2.1.7 nojalla ryhmän G toiminnossa joukossa X ryhmän G alkio g kuvataan Määritelmän 2.1.6 homomorfismilla ψ joukon X permutaatioksi $\psi(g) = \phi_g$, jolla joukon X alkio x kuvataan joksikin toiseksi joukon X alkioksi $(x)\phi_g = x'$.

Esimerkki. Olkoon $G = S_3$ ja $X = \{1, 2, 3\}$. Tällöin ryhmän S_3 toimintoja joukolla X ovat esimerkiksi

2.$(1\ 3\ 2) = 1$, missä permutaatio $(1\ 3\ 2)$ kuvataan bijektioksi

$$\psi(1\ 3\ 2) = \begin{cases} 1 \mapsto 3 \\ 3 \mapsto 2 \\ 2 \mapsto 1 \end{cases},$$

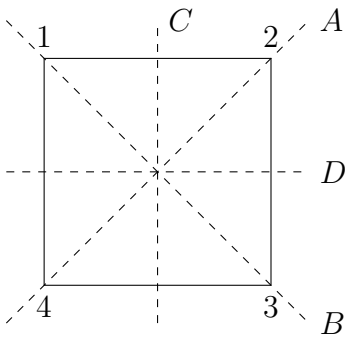
jolloin $(2)\psi(1\ 3\ 2) = 1$.

Vastaavasti 3.$(2\ 1)(1\ 3)(2\ 3) = 1$ ja 2.$(2\ 3) = 3$.

Käytännössä kuvaus ϕ_g kuvaa joukon X alkion permutaatiolla $g \in S_3$ joukon X alkioksi permutaation määritelmän mukaisesti, sillä tässä $G = S_3 = \mathrm{Sym}(X)$.

Esimerkki. Olkoon $G = D_4$, missä D_4 on neliön diedriryhmä, eli neliön symmetrioiden ryhmä. Siis kukin ryhmän D_4 alkio on sellainen tason kierto, peilaus tai niiden yhdistelmä, joka kuvaa neliön takaisin itselleen.

Merkitään neliön kulmia kuten oheisessa kuvassa. Tällöin muodostuu kulmien joukko $X = \{1, 2, 3, 4\}$. Neliön diedriryhmään kuuluu nyt neljä kiertoa ja neljä peilausta. Kierrot tapahtuvat neliön keskipisteen ympäri myötäpäivään ja peilaukset merkittyjen akselien suhteen. Nyt D_4 voidaan esittää joukon X permutaatioiden avulla.



Merkitään

$R_0 = 0$ asteen kierto,
$R_1 = 90$ asteen kierto,
$R_2 = 180$ asteen kierto,
$R_3 = 270$ asteen kierto,

$P_A =$ peilaus suoran A suhteen,
$P_B =$ peilaus suoran B suhteen,
$P_C =$ peilaus suoran C suhteen,
$P_D =$ peilaus suoran D suhteen.

Tällöin

$R_0 = (1)$,
$R_1 = (1\ 2\ 3\ 4)$,
$R_2 = (1\ 3)(2\ 4)$,
$R_3 = (1\ 4\ 3\ 2)$,

$P_A = (1\ 3)$,
$P_B = (2\ 4)$,
$P_C = (1\ 2)(3\ 4)$,
$P_D = (1\ 4)(2\ 3)$.

Huomataan, että $D_4 \subset S_4 = \mathrm{Sym}(X)$. Tällöin voidaan määritellä sellainen kuvaus ψ, että $\psi : D_4 \longrightarrow S_4,\ \psi(\alpha) = \alpha$ kaikilla $\alpha \in D_4$.

Olkoon $\alpha, \beta \in D_4$. Tällöin

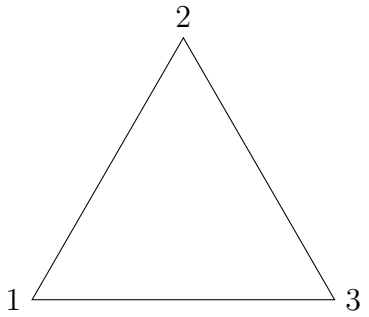
$$\psi(\alpha\beta) = \alpha\beta = \psi(\alpha)\psi(\beta).$$

Siis ψ on ryhmähomomorfismi. Lauseen 2.1.7 nojalla ψ määrää ryhmän D_4 oikean toiminnan joukossa X. Kyseinen toiminta on permutaatio $\psi(\alpha) = \alpha$.

Käytännössä tämä toimii täysin samoin kuin edellinen esimerkki. Havainnollistetaan ryhmän toimintaa vielä sellaisella esimerkillä, jossa toimiva ryhmä ja käsiteltävän joukon permutaatioryhmä ovat erilliset.

Esimerkki. Tarkastellaan tasasivuisen kolmion rotaatioiden muodostamaa ryhmää. Kyseessä on siis diedriryhmän D_3 aliryhmä, joka koostuu vain ryhmän D_3 rotaatioalkioista.

Merkitään kolmion kulmia kuten oheisessa kuvassa. Tällöin muodostuu joukko $X = \{1, 2, 3\}$.



Kolmion rotaatioita myötäpäivään kuvaavat permutaatiot ovat $(1), (1\ 2\ 3)$ sekä $(1\ 3\ 2)$. Selvästi nähdään, että nämä muodostavat ryhmän. Merkitään siis

$$R_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Selvästi $R_3 \leqslant S_3$. Olkoon $G = (\mathbb{Z}_3, +)$. Määritellään kuvaus

$$\psi : \mathbb{Z}_3 \longrightarrow R_3,\ \psi([n]) = (1\ 2\ 3)^n.$$

Jos $[n], [m] \in \mathbb{Z}_3$, niin

$$\begin{aligned}\psi([n])\psi([m]) &= (1\ 2\ 3)^n(1\ 2\ 3)^m \\ &= (1\ 2\ 3)^{n+m} \\ &= \psi([n+m]) \\ &= \psi([n] + [m]).\end{aligned}$$

Siis ψ on ryhmähomomorfismi. Näin ollen Lauseen 2.1.7 nojalla kuvaus ψ määrää ryhmän $\mathbb{Z}_3$ oikean toiminnan joukossa X. Kyseessä on kuvaus $\phi : X \times \mathbb{Z}_3 \longrightarrow X$, joka kuvaa kunkin kolmion kulman siirtymistä n rotaatiossa.

2.2 Kranssitulo

Olkoot G ja H ryhmiä, joista H toimii joukolla $X = \{1, 2, \ldots, n\}$, missä $|X| = n$. Siis on olemassa kuvaus $\phi : H \longrightarrow \mathrm{Sym}(X) = S_n$, joka kuvaa jokaisen ryhmän H alkion h joukon X permutaatioksi ϕ_h. Olkoon nyt G^n ryhmän G suora tulo itsensä kanssa n kertaa. Tällöin joukko X indeksoi tämän suoran tulon siten, että

$$G^n = G \times G \times \cdots \times G = \{(g_1^1, g_2^2, \ldots, g_n^n) \mid g_i \in G \text{ kaikilla } 1 \leq i \leq n\}.$$

Merkinnässä alaindeksit erottavat alkiot toisistaan, ja yläindeksi merkitsee alkion paikkaa monikossa. Tällöin alkioiden aito järjestys määräytyy pelkästään yläindeksien perusteella, eikä alkioiden kirjoitusjärjestyksellä monikossa sinänsä ole merkitystä. Koska ryhmä H toimii ryhmän G^n indeksoivalla joukolla X, niin ryhmän H toiminta voidaan laajentaa luonnollisesti ryhmään G^n siten, että joukon H alkio h kuvataan ensin kuvauksella ϕ joukon X permutaatioksi ϕ_h, jonka jälkeen ryhmän G^n alkion, eli n-monikon alkioiden yläindeksejä, eli järjestystä kuvataan permutaatiolla ϕ_h. Kuvauksessa paikalla j oleva alkio siirtyy paikalle $(j)\phi_h$.

Siis ryhmä H toimii ryhmässä G^n permutoimalla monikkojen alkioiden paikkoja eli alkioiden yläindeksejä. Nyt, kun kuvaus ϕ on tunnettu, voidaan määritellä kuvaus

$$\psi : G^n \times H \longrightarrow G^n,\ \psi(g, h) = g.h = (g_1^{(1)\phi_h}, g_2^{(2)\phi_h}, ..., g_n^{(n)\phi_h}),$$

missä $g \in G^n, h \in H$. Kuvauksen jälkeen alkiot järjestetään monikon sisällä uudelleen niin, että uusien yläindeksien järjestys on $1, 2, \ldots, n$. Jos yläindeksejä ei ole merkitty alkioihin, oletetaan niiden olevan luonnollisessa järjestyksessä $1, 2, \ldots, n$. Esimerkiksi $(g_1, g_2, g_3, g_4) = (g_1^1, g_2^2, g_3^3, g_4^4)$.

Osoitetaan, että näin määritelty kuvaus ψ on ryhmän toiminto.

Lause 2.2.1. *Edellä määritelty kuvaus ψ on ryhmän H toiminto ryhmässä G^n.*

Todistus. Tarkastetaan ryhmän toiminnon määritelmän ehdot.

1) Olkoon $g \in G^n$ ja $e \in H$ neutraalialkio. Tällöin $\phi_e = (1) \in S_n$ ja siten

$$g.e = (g_1^{(1)\phi_e}, g_2^{(2)\phi_e}, ..., g_n^{(n)\phi_e}) = (g_1^1, g_2^2, ..., g_n^n) = g.$$

2) Olkoon $h, h' \in H$. On osoitettava, että $g.(hh') = (g.h).h'$. Koska ryhmän H toiminta joukolla X, eli ϕ, on ryhmähomomorfismi, niin

$$(i)\phi(hh') = ((i)\phi(h))\phi(h'),$$

missä $i \in X$. Tällöin

$$\begin{aligned} g.(hh') &= (g_1^{(1)\phi_{hh'}}, g_2^{(2)\phi_{hh'}}, ..., g_n^{(n)\phi_{hh'}}) \\ &= (g_1^{((1)\phi_h)\phi_{h'}}, g_2^{((2)\phi_h)\phi_{h'}}, ..., g_n^{((n)\phi_h)\phi_{h'}}) \\ &= (g_1^{(1)\phi_h}, g_2^{(2)\phi_h}, ..., g_n^{(n)\phi_h}).h' \\ &= (g.h).h'. \end{aligned}$$

Kohdista 1) ja 2) seuraa, että ψ on ryhmän H toiminto ryhmässä G^n. □

Määritelmä 2.2.2. Ryhmien G^n ja H ***kranssitulo*** on rakenne, jossa H toimii ryhmällä G^n sen alkioiden yläindeksien suhteen samalla toiminnolla kuin joukolla $X = \{1, 2 \ldots, n\}$. Toisin sanoen, ryhmien G^n ja H kranssitulo on karteesinen tulo $G^n \times H$, jossa H toimii ryhmällä G^n edellä määritellyn toiminnon $\psi : G^n \times H \longrightarrow G^n$ mukaisesti. Tätä kranssituloa merkitään $G^n \wr H$.

Kranssitulo toimii siis permutoimalla ryhmän G^n monikkojen alkioiden paikkoja jonkin alkion $h \in H$ määräämän permutaation ϕ_h mukaisesti, eli käytännössä vain vaihtaa monikon alkioiden paikkoja monikossa, mutta ei vaihda itse monikon alkioita toisiin.

Kranssitulon $G^n \wr H$ taustajoukkona on karteesinen tulo $G^n \times H$, sillä kranssitulon rakenteen muodostaa ryhmän toiminta ψ, eli alkion $g.h$ määräämiseen tarvitaan alkiot $g \in G^n$ ja $h \in H$. Tämä tarkoittaa, että alkion $g.h$ määrää alkio (g, h) karteesisesta tulosta $G^n \times H$. Lisäksi kaikki joukon $G^n \times H$ alkiot määräävät jonkin alkion $g.h$.

Jos $(g, h), (g', h') \in G^n \wr H$, niin alkioiden välille voidaan määritellä ryhmän oikeaa toimintoa mukaileva operaatio

$$(g, h) \blacktriangleleft (g', h') = ((g.h')g', hh'),$$

missä $(g.h')g' \in G^n$, $hh' \in H$ ja alkioiden väliset operaatiot tehdään ryhmien omilla operaatioilla.

Tämä rakenne voidaan osoittaa ryhmäksi, ja Rubikin kuution suhteen osoitus tehdään tätä operaatiota muistuttavan Rubikin kuutiolle luonnollisen ryhmäoperaation avulla luvussa 3.

Esimerkki. Olkoon $G = \mathbb{Z}_2$, $H = S_3$ ja $X = \{1, 2, 3\}$. Tällöin ryhmien G^3 ja H kranssitulo on

$$\begin{aligned}
\mathbb{Z}_2^3 \wr S_3 =& \{((0,0,0),\alpha), ((0,0,1),\alpha), ((0,1,0),\alpha), ((0,1,1),\alpha), ((1,0,0),\alpha), \\
& ((1,0,1),\alpha), ((1,1,0),\alpha), ((1,1,1),\alpha) \mid \alpha \in S_3\} \\
=& \{(g, \alpha) \mid g \in \mathbb{Z}_2^3,\ \alpha \in S_3, \\
& \text{missä } \alpha \text{ toimii kolmikkoon } g \text{ kuvauksen } \psi \text{ mukaisesti}\}.
\end{aligned}$$

Lopputuloksena on tällöin jokin ryhmän $\mathbb{Z}_2^3$ alkio, kuten seuraavassa esimerkissä.

Tarkastellaan alkiota $((0,1,0),\alpha)$. Jos $\alpha = (1) = e_{S_3}$, niin $(0,1,0).\alpha = (0,1,0)$.
Jos $\alpha = (2\ 3)$, niin $(0,1,0).\alpha = (0,0,1)$. Jos $\alpha = (2\ 3)(3\ 1)$, niin $(0,1,0).\alpha = (1,0,0)$.

Tarkastellaan seuraavaksi kahta alkiota, $((1,0,1),(1\ 2))$ ja $((0,0,1),(2\ 3))$. Tällöin kranssitulorakenteen operaation mukaisesti

$$\begin{aligned}
((1,0,1),(1\ 2)) \blacktriangleleft ((0,0,1),(2\ 3)) &= ((1,0,1).(2\ 3) + (0,0,1), (1\ 2)(2\ 3)) \\
&= ((1,1,0) + (0,0,1), (1\ 2)(2\ 3)) \\
&= ((1,1,1), (1\ 3\ 2)) \in \mathbb{Z}_2^3 \wr S_3.
\end{aligned}$$

Lemma 2.2.3. *Olkoot* $(G^n, *)$, H *ja* ψ *kuten edellä sekä* $x, y \in G^n$, $h \in H$. *Tällöin*

$$(x * y).h = (x.h) * (y.h).$$

Todistus. Koska $\psi : G^n \times H \longrightarrow G^n$ ja $x.h, y.h \in G^n$, niin

$$\begin{aligned}
(x * y).h &= \psi(x * y, h) \\
&= \psi((x_1^1, x_2^2, \ldots, x_n^n) * (y_1^1, y_2^2, \ldots, y_n^n), h) \\
&= \psi(((x_1 * y_1)^1, (x_2 * y_2)^2, \ldots, (x_n * y_n)^n), h) \\
&= ((x_1 * y_1)^{(1)\phi_h}, (x_2 * y_2)^{(2)\phi_h}, \ldots, (x_n * y_n)^{(n)\phi_h}) \\
&= (x_1^{(1)\phi_h} * y_1^{(1)\phi_h}, x_2^{(2)\phi_h} * y_2^{(2)\phi_h}, \ldots, x_n^{(n)\phi_h} * y_n^{(n)\phi_h}) \\
&= (x_1^{(1)\phi_h}, x_2^{(2)\phi_h}, \ldots, x_n^{(n)\phi_h}) * (y_1^{(1)\phi_h}, y_2^{(2)\phi_h}, \ldots, y_n^{(n)\phi_h}) \\
&= \psi(x, h) * \psi(y, h) \\
&= (x.h) * (y.h).
\end{aligned}$$

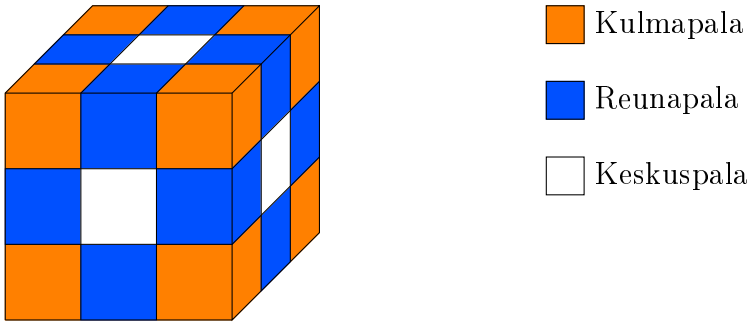
□

3 Rubikin kuutio

Tässä luvussa tarkastellaan Rubikin kuutiota ryhmäteoreettisesta näkökulmasta edellisten lukujen tietojen perusteella. Ensin on määriteltävä kuution rakenteelle käsitteet, joita käyttämällä Rubikin kuution ryhmän konstruointi etenee.

3.1 Kuution rakenne

Määritelmä 3.1.1. Rubikin kuutio koostuu kolmesta eri palatyypistä. Nämä ovat ***keskuspala, reunapala*** ja ***kulmapala.*** Kukin palatyyppi on esitetty alla olevassa kuvassa.



Kuva 1: Kuution palatyypit

Nähdään, että kuutiossa on kuusi keskuspalaa, 12 reunapalaa ja kahdeksan kulmapalaa. Kuution sisällä ei ajatella olevan palaa, jolloin kaikkia paloja on yhteensä 26. Lisäksi huomataan, että keskuspalat eivät siirry minkään sivun käännöllä. Tällöin niiden keskinäisiä sijainteja ei voi muuttaa. Tästä seuraa, että liikkuvia paloja on 20 kappaletta.

Pala voi esiintyä ainoastaan sen tyypin kanssa samantyyppisen palan paikoilla. Esimerkiksi kulmapala ei voi koskaan olla reunapalan kohdalla.

Määrätään lisäksi, että koko kuutiota ei voi pyörittää.

Määritelmä 3.1.2. ***Tarra*** on kunkin palan kunkin näkyvän sivun väri, ja värejä on Rubikin kuutiossa yhteensä kuusi. Tarrat ovat pysyvästi kiinnitettyjä paloihinsa. Tarroja on 54 kappaletta.

Määritelmä 3.1.3. Kuutio on ***ratkaistu***, mikäli kunkin kuuden sivun tarrat ovat keskenään samanvärisiä. Rubikin kuutiossa on kuusi eri väriä, jolloin kukin sivu on omanvärisensä.

Määritelmä 3.1.4. Kuution keskuspalat ovat pysyvästi kiinnitettyjä suhteessa toisiinsa. Tämä tarkoittaa sitä, että keskuspaloja ei voi irrottaa kuutiosta. Kun tämä yhdistetään Määritelmään 3.1.1, vain kuution reuna- ja kulmapalat voidaan irrottaa kuutiosta, ja asettaa vain kyseisen palatyypin mukaisille paikoille. Tämä on kuution ***kokoonpanorajoitus.***

Määritelmä 3.1.5. ***Kääntö*** on minkä tahansa kuution sivun kääntö 90 asteen monikerroissa myötä- tai vastapäivään. Käännöt määritellään tarkemmin myöhemmin.

Määritelmä 3.1.6. ***Kääntöjono*** on jokin äärellinen jono kääntöjä. Jos $K_1, \ldots, K_n$ ovat kääntöjä, niin K_1 K_2 ... K_n on kääntöjono, joka suoritetaan vasemmalta oikealle, ts. ensin kääntö K_1, seuraavaksi K_2 jne., ja lopuksi kääntö K_n. Tästä syystä permutaatio ja ryhmän toiminta on määriteltävä kuten Määritelmissä 1.2.4 ja 2.1.3. Lisäksi sanotaan, että edellisen kääntöjonon ***pituus*** on n.

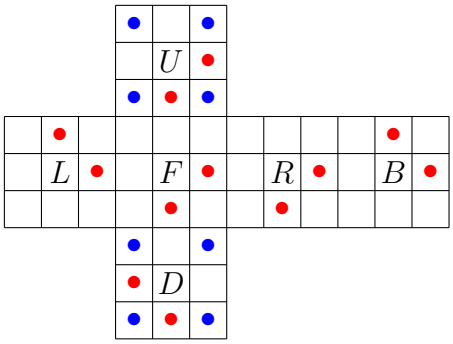
Kääntöjonoja suoritettaessa kuutio pysyy aina samassa asennossa. Tämä tarkoittaa, että keskuspalat osoittavat koko kääntöjonon ajan samoihin suuntiin.

Määritelmä 3.1.7. ***Kombinaatio*** eli ***järjestys*** on jokin tapa irrottaa ratkaistusta kuutiosta kaikki kulma- ja reunapalat ja asettaa ne kokoonpanorajoituksen mukaisesti takaisin kuutioon. Merkitään kaikkien kombinaatioiden joukkoa $\mathcal{K}$.

Määritelmä 3.1.8. Kombinaatio on ***ratkeava*** jos ja vain jos se voidaan saavuttaa ratkaistusta kuutiosta jollakin kääntöjonolla. Lisäksi kaikkien ***ratkeavien kombinaatioiden joukkoa*** merkitään $\mathcal{R}$.

Määritelmä 3.1.9. ***Kuution permutaatiotila*** sisältää tiedon kaikkien kuution palojen sijainnista kuutiossa. Edelleen, kuution permutaatiotila koostuu ***reunapalojen permutaatiotilojen*** ja ***kulmapalojen permutaatiotilojen*** yhdisteestä. Reunapalojen permutaatiotila sisältää tiedon reunapalojen sijainnista kuutiossa, ja vastaavasti kulmapaloille. Permutaatiotilat eivät ota kantaa palojen asentoon.

Määritelmä 3.1.10. ***Kuution orientaatiotila*** sisältää tiedon kaikkien kuution palojen asennosta kuutiossa verrattuna ratkaistuun kuutioon. Tehdään ratkaistuun kuutioon seuraavan kuvan mukaiset merkinnät.



Kuva 2: Orientaatiomerkit [3]

Kuution orientaatiotila saadaan selville vertaamalla kullakin paikalla olevan palan merkin sijaintia ratkaistussa kuutiossa samalla paikalla olevan palan merkin sijaintiin. Reunapalalla on kullakin reunapaikalla kaksi eri asentoa ja kulmapalalla on kullakin kulmapaikalla kolme eri asentoa. Asennot ovat kuten seuraavissa kuvissa, joissa värillinen tahko kuvaa merkkiä.

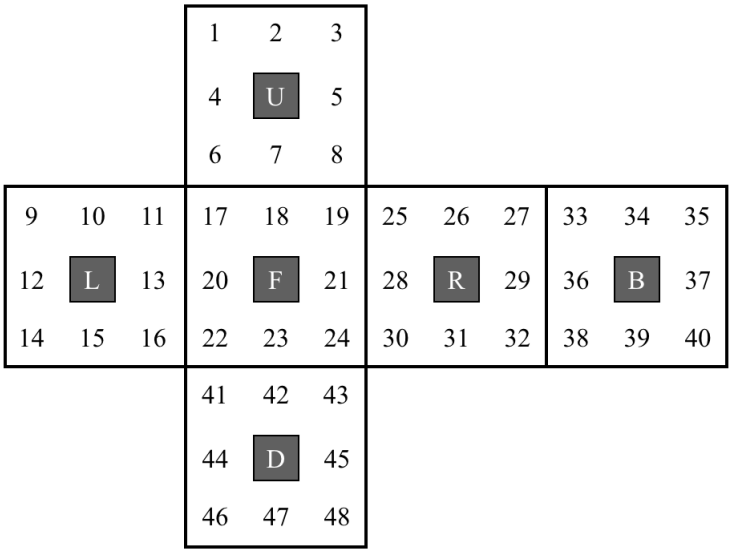
Reunapalat; 0, 1 Kulmapala, tila 0 Kulmapala, tila 1 Kulmapala, tila 2

Vastaavasti kuin kuution permutaatiotiloilla, kuution orientaatiotila koostuu ***reunapalojen orientaatiotilojen*** ja ***kulmapalojen orientaatiotilojen*** yhdisteestä. Orientaatiotilat eivät ota kantaa palojen sijaintiin.

Määritelmä 3.1.11. ***Järjestely*** on sellainen kuution kombinaation vaihto, joka noudattaa kokoonpanorajoitusta.

3.2 Kääntöjen ryhmä

Koska Rubikin kuutiossa on 54 tarraa ja kombinaatiot ovat tässä joukossa, on Rubikin kuution ratkeava joukko symmetrisen ryhmän S_{54} osajoukko. Mutta kokoonpanorajoituksen nojalla keskuspaloja ei voi siirtää. Tällöin kuutiossa on 48 liikkuvaa tarraa, ja siten ratkeavan joukon on oltava myös symmetrisen ryhmän S_{48} osajoukko. Nyt kuutio voidaan esittää seuraavasti:



Kuva 3: Tarrojen indeksointi ratkaistussa kuutiossa (Lähteestä [5].)

Kuvassa U, L, F, R, B ja D ovat yläsivun, vasemman sivun, etusivun, oikean sivun, takasivun ja alasivun tunnukset suuntia vastaavien englannin kielen sanojen mukaisesti. Nähdään, että käännöt operoivat joukkoa $\{1, 2, ..., 48\}$. Otetaan käännöille käyttöön Singmasterin merkintätapa.

Määritelmä 3.2.1. ***Singmasterin merkintätavassa*** sivujen tunnukset ovat kuten edellä, ja kääntöjä merkitään seuraavan taulukon mukaisesti:

	90 astetta myötäpäivään	90 astetta vastapäivään	180 astetta
Etusivu	F	F^{-1}	F^2
Takasivu	B	B^{-1}	B^2
Vasen sivu	L	L^{-1}	L^2
Oikea sivu	R	R^{-1}	R^2
Yläsivu	U	U^{-1}	U^2
Alasivu	D	D^{-1}	D^2

Käännön suunta on kyseisen sivun suunnalta katsottaessa. Huomaa, että jos K on jokin näistä käännöistä, niin $KKK = K^{-1}$.

Tällöin saadaan käännöille $F,\ B,\ L,\ R,\ U$ ja D seuraavat esitykset erillisten syklien tulona:

$$F = (17\ 19\ 24\ 22)(18\ 21\ 23\ 20)(6\ 25\ 43\ 16)(7\ 28\ 42\ 13)(8\ 30\ 41\ 11),$$
$$B = (33\ 35\ 40\ 38)(34\ 37\ 39\ 36)(3\ 9\ 46\ 32)(2\ 12\ 47\ 29)(1\ 14\ 48\ 27),$$
$$L = (9\ 11\ 16\ 14)(10\ 13\ 15\ 12)(1\ 17\ 41\ 40)(4\ 20\ 44\ 37)(6\ 22\ 46\ 35),$$
$$R = (25\ 27\ 32\ 30)(26\ 29\ 31\ 28)(3\ 38\ 43\ 19)(5\ 36\ 45\ 21)(8\ 33\ 48\ 24),$$
$$U = (1\ 3\ 8\ 6)(2\ 5\ 7\ 4)(9\ 33\ 25\ 17)(10\ 34\ 26\ 18)(11\ 35\ 27\ 19),$$
$$D = (41\ 43\ 48\ 46)(42\ 45\ 47\ 44)(14\ 22\ 30\ 38)(15\ 23\ 31\ 39)(16\ 24\ 32\ 40).$$

Määritelmä 3.2.2. Olkoon $S = \{F, B, L, R, U, D\}$. Tällöin kaikki ratkeavat kombinaatiot voidaan Määritelmän 3.1.8 mukaan saavuttaa joukon S alkioiden jonoilla. Näin muodostuva joukko on kaikkien ***kääntöjonojen joukko***, jota merkitään $\langle S \rangle$.

Erilaisia äärellisiä kääntöjonoja on ääretön määrä, mutta Rubikin kuution kombinaatioita on selvästi äärellinen määrä. Ennen kuin edetään pidemmälle, on mielekästä osoittaa, että $\mathcal{R}$ on ryhmärakenne. Tämä tapahtuu seuraavasti: osoitetaan, että joukko $\langle S \rangle$ voidaan jakaa ekvivalenssiluokkiin, joista kukin vastaa täsmälleen yhtä kombinaatiota joukosta $\mathcal{R}$. Tämän jälkeen osoitetaan joukko $\langle S \rangle$ ryhmäksi. Käyttäen tätä ominaisuutta joukko $\mathcal{R}$ osoitetaan ryhmäksi.

On tärkeää huomata, että **kääntöjono toimii ratkeavaan kombinaatioon täsmälleen samalla tavalla kuin ratkeamattomaan kombinaatioon**. Lisäksi ryhmän $\mathcal{R}$ rakenne on vaikea selvittää kääntöjen permutaatioesityksistä. Tarvitaan toisenlainen esitys.

Lemma 3.2.3. *Ratkeavat kombinaatiot ovat ekvivalenssiluokkia, joiden alkiot ovat kääntöjonoja, jotka suoritetaan ratkaistuun kombinaatioon.*

Todistus. Olkoon e ratkaistu kuutio, $S = \{F, B, L, R, U, D\}$ ja $f, g, h \in \langle S \rangle$. Kääntöjono f, suoritettuna ratkaistuun kuutioon e, tuottaa kombinaation r_f. Olkoon nyt $\sim$ sellainen relaatio joukossa $\langle S \rangle$, että

$$f \sim g \Leftrightarrow r_f = r_g.$$

Tällöin

1) $r_f = r_f \Leftrightarrow f \sim f$.

2) $f \sim g \Leftrightarrow r_f = r_g \Leftrightarrow r_g = r_f \Leftrightarrow g \sim f$.

3) $(f \sim g \wedge g \sim h) \Leftrightarrow (r_f = r_g \wedge r_g = r_h) \Rightarrow r_f = r_h \Leftrightarrow f \sim h$.

Kohdista 1)-3) seuraa, että $\langle S \rangle$ jakaantuu erillisiin ekvivalenssiluokkiin

$$[f] = \{x \in \langle S \rangle \mid r_x = r_f\} = \{x \in \langle S \rangle \mid e.x = r_f\},$$

missä $e.x$ on kääntöjonon x toiminta ratkaistuun kuutioon. Näin ollen väite pätee. □

Ekvivalenssiluokkien ominaisuuksien nojalla kaikki kääntöjonot kuuluvat täsmälleen yhteen ekvivalenssiluokkaan, ja saman luokan kääntöjonot tuottavat saman kombinaation. Siis kukin ekvivalenssiluokka vastaa täsmälleen yhtä ratkeavaa kombinaatiota. Lisäksi, jos r on ratkeava kombinaatio, niin on olemassa jokin kääntöjono M, joka tuottaa ratkaistusta kuutiosta kombinaation r. Tällöin kombinaatiota r vastaa vain ekvivalenssiluokka $[M]$. Tällöin kaikkia ratkeavia kombinaatioita vastaa täsmälleen yksi ekvivalenssiluokka. Näin ollen ekvivalenssiluokkien joukko ja ratkeavien kombinaatioiden joukko voidaan samaistaa, ja kukin ratkeava kombinaatio voidaan esittää jollakin kääntöjonolla sitä vastaavasta ekvivalenssiluokasta. Ratkeavien kombinaatioiden joukkoa voidaan siis merkitä

$$\mathcal{R} = \{[f] \mid f \in \langle S \rangle\}.$$

Osoitetaan seuraavaksi joukon $\langle S \rangle$ olevan ryhmä.

Lause 3.2.4. *Olkoon $S = \{F, B, L, R, U, D\}$ ja $\circ : \langle S \rangle \times \langle S \rangle \longrightarrow \langle S \rangle$ sellainen operaatio, että jos $f \in \langle S \rangle$ ja $g \in \langle S \rangle$, niin $f \circ g$ on kääntöjono, joka saadaan suorittamalla ratkaistuun kuutioon kääntöjono fg. Tällöin $(\langle S \rangle, \circ)$ on ryhmä ja alkiota $f \circ g = fg$ sanotaan kääntöjonojen f ja g ketjuksi ryhmässä $\langle S \rangle$.*

Todistus. Tarkastetaan ryhmän ehdot.

1) $f \circ g \in \langle S \rangle$ operaation $(\circ)$ määritelmän nojalla.

2) $f \circ E = f = E \circ f$, missä E on tyhjä kääntö.

3) Jos $f, g, h \in \langle S \rangle$ ja P on jokin kuution pala, niin

$$\begin{aligned}(f \circ (g \circ h))(P) &= (g \circ h)(f(P)) = h(g(f(P)))\\ ((f \circ g) \circ h))(P) &= h((f \circ g)(P)) = h(g(f(P)))\\ &\Rightarrow f \circ (g \circ h) = (f \circ g) \circ h.\end{aligned}$$

Edellä kääntöjonot vaikuttavat järjestyksessä vasemmalta oikealle.

4) Olkoon $T = S \cup \{K^{-1} \mid K \in S\}$ ja $f = K_1 K_2 ... K_n$, missä $K_i \in T$ kaikilla $1 \leq i \leq n$. Määritelmän 3.2.1 nojalla $\langle T \rangle = \langle S \rangle$.
Jos $g = K_n^{-1} K_{n-1}^{-1} ... K_1^{-1} \in \langle S \rangle$, niin

$$\begin{aligned}f \circ g &= (K_1 K_2 ... K_n) \circ (K_n^{-1} K_{n-1}^{-1} ... K_1^{-1}) \qquad (\circ \text{ assosiatiivinen})\\ &= K_1 K_2 ... K_{n-1} E K_{n-1}^{-1} ... K_1^{-1}\\ &= E^n = E.\end{aligned}$$

Vastaavasti saadaan $g \circ f = E$. Näin ollen $g = f^{-1} \in \langle S \rangle$.

Kohdista 1)-4) seuraa, että $(\langle S \rangle, \circ)$ todella on ryhmä. □

Lause 3.2.5. *Olkoon $\mathcal{R} = \{[f] \mid f \in \langle S \rangle\}$ ratkeavien kombinaatioiden joukko ja tässä joukossa määritelty operaatio $[f] * [g] = [f \circ g]$ kaikilla $[f], [g] \in \mathcal{R}$, missä $(\circ)$ on kuten edellä. Osoitetaan, että operaatio on hyvin määritelty ja että $\mathcal{R}$ on ryhmä.*

Todistus. Olkoot f ja f' sellaiset kääntöjonot, että ne tuottavat saman kombinaation r_f sekä g ja g' sellaiset kääntöjonot, että ne tuottavat saman kombinaation r_g. Tästä seuraa, että $f \circ g = f' \circ g'$, sillä tarkastellessa kombinaatiossa tapahtunutta muutosta prosessilla ei ole väliä, vain ainoastaan alku- ja lopputilojoen erolla. Lisäksi ekvivalenssiluokkien ominaisuuksien nojalla $[f] = [f']$ ja $[g] = [g']$. Näin ollen

$$[f] * [g] = [f \circ g] = [f' \circ g'] = [f'] * [g'].$$

Siis ketjutusoperaatio joukossa $\mathcal{R}$ on hyvin määritelty. Osoitetaan nyt ryhmärakenne. Olkoon $f, g, h, E \in \langle S \rangle$, missä E on tyhjä kääntö.

1) Lauseen 3.2.4 nojalla $f \circ g \in \langle S \rangle$, joten $[f] * [g] = [f \circ g] \in \mathcal{R}$.

2) $[f] * [E] = [f \circ E] = [f] = [E \circ f] = [E] * [f]$.

3) $[f] * \Big([g] * [h]\Big) = [f] * [g \circ h] = [f \circ g \circ h] = [f \circ g] * [h] = \Big([f] * [g]\Big) * [h]$.

4) Lauseen 3.2.4 nojalla kaikilla $f \in \langle S \rangle$ on olemassa käänteisalkio $f^{-1} \in \langle S \rangle$. Tällöin
$$[f] * [f^{-1}] = [f \circ f^{-1}] = [E] = [f^{-1} \circ f] = [f^{-1}] * [f].$$

□

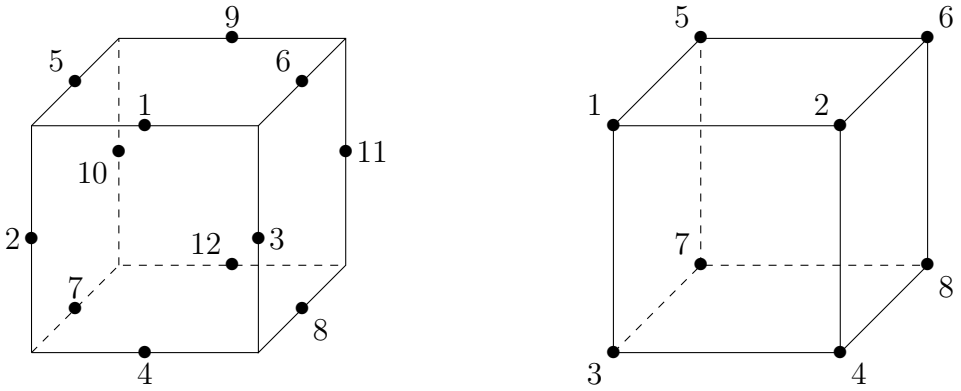
Nyt on todistettu, että kaikki ratkeavat kombinaatiot varustettuna ketjutusoperaatiolla on ryhmä, jolloin on mahdollista löytää kyseisen ryhmän rakenne.

Lemma 3.2.6. *Olkoot* $[f], [g] \subseteq \mathcal{R}$ *joillekin kääntöjonoille* f *ja* g*. Tällöin on olemassa sellainen kääntöjono* h*, että* $[fh] = [g]$*.*

Todistus. Lauseen 3.2.4 nojalla on olemassa sellainen kääntöjono f^{-1}, että $ff^{-1} = E$, jolloin $[ff^{-1}] = [E]$. Siis $Eg = ff^{-1}g \in [ff^{-1}g]$. Toisaalta $Eg = g \in [g]$. Näin ollen $[ff^{-1}g] = [g]$, joten $fh = ff^{-1}g = g$ ja etsitty kääntöjono on siten $h = f^{-1}g$. □

3.3 Rubikin kuution yleinen ryhmä

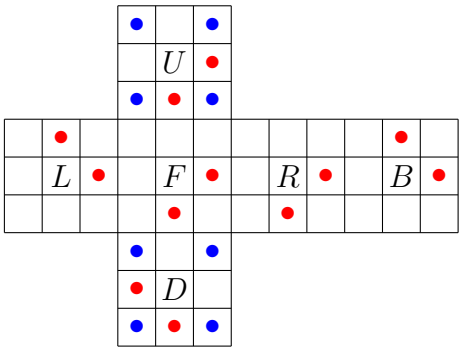
Rubikin kuution yleinen ryhmä on joukko $\mathcal{K}$ varustettuna kombinaatioiden yhdistämisoperaatiolla. Ennen operaation määrittelyä täytyy konstruoida joukon $\mathcal{K}$ rakenne. Määritelmien 3.1.7, 3.1.9 ja 3.1.10 nojalla mielivaltaisen kombinaation konstruoimiseen tarvitaan tiedot palojen paikoista ja asennoista, eli permutaatiotiloista ja orientaatiotiloista. Tarkastellaan kumpaakin palatyyppiä erikseen. Merkitään ensin reuna- ja kulmapaloja luvuilla seuraavien kuvien mukaisesti:



Kuva 4: Reuna- ja kulmapalojen indeksointi

Näin jokaiseen reuna- ja kulmapalan paikkaan voidaan viitata luvulla. Eri palatyyppejä ei käsitellä yhtä aikaa näillä luvuilla, jolloin sekaannusta ei synny. Ennen palojen tarkastelua on todistettava lause, joka antaa keinon edellämainitun mielivaltaisen kombinaation konstruoimiseen.

Lause 3.3.1. [3]. *(Kuutioteorian ensimmäinen peruslause.) Olkoon* $k \in \mathcal{K}$ *jokin kombinaatio. Olkoon lisäksi ratkaistuun kuutioon tehty kuvan* 2 *mukaiset merkinnät. Tällöin kombinaatio* k *on määrätty yksikäsitteisesti, jos tiedetään:*



1) Mikä on keskuspalojen permutaatiotila?
2) Mikä on reunapalojen permutaatiotila?
3) Mikä on kulmapalojen permutaatiotila?
4) Mitkä reunapalojen merkeistä kohdalla i ovat kääntyneet verrattuna ratkaistun kuution kohdan i merkkeihin?
5) Mitkä kulmapalojen merkeistä kohdalla j ovat kääntyneet verrattuna ratkaistun kuution kohdan j merkkeihin, ja jos ne ovat kääntyneet, ovatko ne kääntyneet 120 astetta myötä- vai vastapäivään?

Todistus. Nähdään, että kaikissa paloissa, paitsi keskuspaloissa, on yksi merkki. Kysymyksen 1) vastaus kertoo, miten päin kuutio on. Kysymysten 2) ja 3) vastaukset antavat Määritelmän 3.1.9 nojalla tietoon kuution permutaatiotilan. Kysymysten 4) ja 5) vastaukset antavat Määritelmän 3.1.10 nojalla tietoon kuution orientaatiotilan.

Näin ollen Määritelmän 3.1.7 nojalla nyt on tiedossa kaikki tiedot, jotka vaaditaan kombinaation konstruoimiseen. Lisäksi, jos jonkin palan permutaatio- tai orientaatiotila muuttuu, koko kombinaatio muuttuu. Tällöin kombinaatio on yksikäsitteinen. Jos palan merkki jollakin kohdalla on samalla paikalla kuin ratkaistun kuution merkki samalla kohdalla, niin sanotaan, että pala on oikein päin. Jos palan merkki on eri paikalla kuin ratkaistussa kuutiossa, niin sanotaan, että pala on kääntynyt.

□

Kullakin reuna- ja kulmapalan asennolla on sitä vastaava lukuarvo. Jos reunapala tai kulmapala on oikein päin, sen lukuarvo on 0. Jos reunapala on kääntynyt tai kulmapala on kääntynyt myötäpäivään, sen lukuarvo on 1. Jos kulmapala on kääntynyt vastapäivään, sen lukuarvo on 2.

Reunapalat; 0, 1 Kulmapala, tila 0 Kulmapala, tila 1 Kulmapala, tila 2

Kaikissa tapauksissa kuutio on samoin päin. Jos vasemmanpuoleinen reunapala on tilassa 0, niin oikeanpuoleinen on sama pala tilassa 1.

Reunapalat

Olkoon $\mathcal{K}^r$ yleinen reunapalojen orientaatio- ja permutaatiotilojen joukko. Joukko $\mathcal{K}^r$ kuvaa siis täydellisesti reunapaloja ja vain reunapaloja. Joukon alkiosta selviää reunapalojen sijainnit sekä niiden asennot. Koska reunapaloja on 12 kappaletta, permutaatio $\sigma_f \in S_{12}$ kuvaa järjestyksen f aiheuttamaa reunapalojen siirtymistä. Esimerkiksi käännölle F saadaan kuvasta 3 permutaatioesitys $\sigma_F = (1\ 3\ 4\ 2)$.

Koska kukin reunapala voi olla kahdessa eri asennossa, 0 tai 1, on reunapalan i orientaatiotilaa kuvaava alkio $\omega_i \in \mathbb{Z}_2$. Koska reunapaloja on 12, reunapalojen orientaatiotilaa kuvaa joukko $\mathbb{Z}_2^{12}$. Tällöin

$$\mathcal{K}^r = \{(\omega, \sigma) \mid \omega \in \mathbb{Z}_2^{12},\ \sigma \in S_{12}\}.$$

Kulmapalat

Olkoon $\mathcal{K}^k$ yleinen kulmapalojen orientaatio- ja permutaatiotilojen joukko. Joukko $\mathcal{K}^k$ kuvaa täydellisesti kulmapaloja ja vain kulmapaloja. Joukon alkiosta selviää kulmapalojen sijainnit sekä niiden asennot. Koska kulmapaloja on kahdeksan kappaletta, permutaatio $\rho_f \in S_8$ kuvaa järjestyksen f aiheuttamaa kulmapalojen siirtymistä. Esimerkiksi kääntöä F vastaa permutaatio $\rho_F = (1\ 2\ 4\ 3)$.

Koska kukin kulmapala voi olla kolmessa eri asennossa, 0, 1 tai 2, on kulmapalan i orientaatiotilaa kuvaava alkio $\nu_i \in \mathbb{Z}_3$. Koska kulmapaloja on kahdeksan, kulmapalojen orientaatiotilaa kuvaa joukko $\mathbb{Z}_3^8$. Tällöin

$$\mathcal{K}^k = \{(\nu, \rho) \mid \nu \in \mathbb{Z}_3^8,\ \rho \in S_8\}.$$

Yleisen ryhmän rakenne

Kuution permutaatio- ja orientaatiotilojen määritelmien nojalla jokainen kombinaatio joukossa $\mathcal{K}$ koostuu reunapalojen ja kulmapalojen permutaatio- ja orientaatiotilojen yhdistelmästä. Näin ollen muodostuu kahden karteesisen tulon karteesinen tulo

$$\mathcal{K} = \mathcal{K}^r \times \mathcal{K}^k = (\mathbb{Z}_2^{12} \times S_{12}) \times (\mathbb{Z}_3^8 \times S_8).$$

Huomaa, että tämä on vielä vain joukko. Tällöin, jos $x \in \mathcal{K}$, niin

$$x = (\omega_x, \sigma_x, \nu_x, \rho_x),$$

missä kukin nelikön alkio vastaa järjestelyn x ratkaistuun kuutioon tekemää muutosta. Siten näiden alkioiden muodostama nelikkö muodostaa järjestelyn x kokonaisvaikutuksen. Järjestelyn permutaatiovaikutus, eli permutaatiot σ_x ja ρ_x, ovat yksiselitteisiä. Ne siirtävät paloja itsensä mukaisesti, kun käytetään kuvan 4 indeksointia.

Orientaatiotiloja tulkitaan seuraavasti. Olkoon x jokin kombinaatio. Tällöin monikot $\omega_x \in \mathbb{Z}_2^{12}$ ja $\nu_x \in \mathbb{Z}_3^8$ kuvaavat orientaatiotiloja, johon palat kääntyvät, kun ratkaistuun kuutioon suoritetaan järjestely x. Tällöin

$$\omega_x = (\omega_{x,1},\ \omega_{x,2},\ \omega_{x,3},\ \omega_{x,4},\ \omega_{x,5},\ \omega_{x,6},\ \omega_{x,7},\ \omega_{x,8},\ \omega_{x,9},\ \omega_{x,10},\ \omega_{x,11},\ \omega_{x,12}),$$

missä $\omega_{x,i} = 0, 1$ kaikilla $1 \leq i \leq 12$ ja

$$\nu_x = (\nu_{x,1},\ \nu_{x,2},\ \nu_{x,3},\ \nu_{x,4},\ \nu_{x,5},\ \nu_{x,6},\ \nu_{x,7},\ \nu_{x,8}),$$

missä $\nu_{x,i} = 0, 1, 2$ kaikilla $1 \leq i \leq 8$. Tällaisten alkioiden käsittely on vaivalloista. Käytetään siis merkintätapaa, joka poistaa monikosta ne alkiot, joiden arvo on nolla. Esimerkiksi, jos $\omega_x = (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$, niin merkitään

$$\omega_x = (1^1, 1^5, 1^6, 1^9, 1^{12}).$$

Merkinnässä kantaluku kertoo palan orientaatiotilan arvon, ja yläindeksi kertoo palan paikan.

Jos $\nu_x = (0, 0, 1, 0, 2, 2, 1, 1)$, niin merkitään

$$\nu_x = (1^3, 2^5, 2^6, 1^7, 1^8).$$

Jos monikko sisältää vain nollia, sitä merkitään $\overline{0}$. Edelleen, tällaista monikkoa voidaan käsitellä järjestämättömänä, koska yläindeksi kertoo paikan, jonka orientaatiotila on kantaluku. Tällaista merkintää on helpompi lukea, sillä siitä nähdään heti kaikkien palojen orientaatiotila selvemmin kuin alkuperäisessä monikossa. Lisäksi kun määritellään ryhmäoperaatio joukossa $\mathcal{K}$, operaation manuaalinen käyttö helpottuu huomattavasti tällä merkintätavalla.

Yleisen ryhmän ketjutusoperaatio

Yleisessä ryhmässä on mahdollista määritellä Lauseen 3.2.5 operaatiota vastaava ketjutus. Itse asiassa se operaatio on nyt määriteltävän operaation kanssa täsmälleen sama operaatio, mutta vain ratkeavien kombinaatioiden joukossa $\mathcal{R}$. Mutta koska operaatio on määritelty kääntöjonojen ketjutusoperaation ($\circ$) kautta, sitä ei voi sellaisenaan laajentaa joukkoon $\mathcal{K}$.

Operaation määrittelyä varten on tarkasteltava kahden peräkkäin suoritettavan järjestelyn keskinäistä vaikutusta. Lähde [1] sisältää vastaavan tarkastelun.

Olkoot x ja y järjestelyjä. Toisin sanoen $x, y \in \mathcal{K}$. Tällöin järjestelyt voidaan kirjoittaa nelikköinä. Edellisen nojalla saadaan

$$x = (\omega_x, \sigma_x, \nu_x, \rho_x),\ y = (\omega_y, \sigma_y, \nu_y, \rho_y),\ xy = (\omega_{xy}, \sigma_{xy}, \nu_{xy}, \rho_{xy}).$$

Nämä ovat kutakin järjestelyä vastaavat kombinaatiot eli niiden vaikutukset ratkaistuun kuutioon. Koska reuna- ja kulmapalat eivät voi vaikuttaa toisiinsa, niitä on tarkasteltava erikseen. Tarkastellaan ensin reunapaloja.

Olkoon $i \in \{1, \ldots, 12\}$ ratkaistun kuution jonkin reunapalan paikka. Tällöin kuution permutaatiotila on $(1) \in S_{12}$ ja palan orientaatiotila on 0^i. Kun ratkaistuun kuutioon tehdään järjestely x, pala siirtyy järjestelyn x permutaatiovaikutusta kuvaavan permutaation σ_x mukaisesti paikalta i paikalle $(i)\sigma_x$. Tällöin kyseisen palan orientaatiotila on $\omega_{x,(i)\sigma_x} \in \{0, 1\}$.

Seuraavaksi suoritetaan järjestely y, jolloin pala siirtyy paikalta $(i)\sigma_x$ paikalle $((i)\sigma_x)\sigma_y) = (i)(\sigma_x\sigma_y)$. Toisaalta pala on nyt lopullisella paikallaan $(i)\sigma_{xy}$. Tällöin on oltava $\sigma_{xy} = \sigma_x\sigma_y$. Lisäksi palan orientaatiotila on nyt $\omega_{xy,(i)\sigma_{xy}}$.

Jos $\omega_{x,(i)\sigma_x} = 0$, niin lopullinen orientaatiotila on sama kuin järjestelyn y vaikutus kyseiseen palaan, eli $\omega_{xy,(i)\sigma_{xy}} = \omega_{y,(i)\sigma_{xy}} = 0 +_2 \omega_{y,(i)\sigma_{xy}} = \omega_{x,(i)\sigma_x} +_2 \omega_{y,(i)\sigma_{xy}}$, missä $+_2$ on yhteenlasku modulo 2.

Vastaavasti, jos $\omega_{x,(i)\sigma_x} = 1$, niin tilanne on päinvastainen edelliseen tapaukseen verrattuna, eli $\omega_{xy,(i)\sigma_{xy}} = \omega_{y,(i)\sigma_{xy}} +_2 1 = 1 +_2 \omega_{y,(i)\sigma_{xy}} = \omega_{x,(i)\sigma_x} +_2 \omega_{y,(i)\sigma_{xy}}$.

Molemmissa tapauksissa on siis voimassa $\omega_{xy,(i)\sigma_{xy}} = \omega_{x,(i)\sigma_x} +_2 \omega_{y,(i)\sigma_{xy}}$. Merkitään $(i)\sigma_{xy} = j$, jolloin $(i)\sigma_x = (j)\sigma_y^{-1}$, josta edelleen saadaan

$$\omega_{xy,j} = \omega_{x,(j)\sigma_y^{-1}} + \omega_{y,j},\ j \in \{1, \ldots, 12\}.$$

$\omega_{x,(i)\sigma_x}$	$\omega_{y,(i)\sigma_{xy}}$	$\omega_{xy,(i)\sigma_{xy}}$
0	0	$0 = 0 +_2 0$
0	1	$1 = 0 +_2 1$
1	0	$1 = 1 +_2 0$
1	1	$0 = 1 +_2 1$

Oheinen taulukko ilmaisee orientaatiotilojen yhteisvaikutuksen kussakin tapauksessa: 0 tarkoittaa oikein päin olevaa palaa ja orientaation säilymistä, 1 tarkoittaa väärin päin olevaa palaa ja orientaatiotilan kääntymistä. Esimerkiksi tapauksessa 1 ja 1 järjestely x kääntää palan tilaan 1, ja y kääntää palan uudestaan, jolloin se palaa tilaan 0.

Koska ryhmä $\mathbb{Z}_2^{12}$ on suora tulo, yhteen voidaan laskea ainoastaan saman indeksin alkioita. Siksi alkion $\omega_{x,(j)\sigma_y^{-1}}$ indeksi täytyy ensin kuvata permutaatiolla σ_y. Määritellään siis reunapalojen permutaatiotiloja kuvaavan ryhmän S_{12} toiminto orientaatiotiloja kuvaavalle ryhmälle $\mathbb{Z}_2^{12}$ seuraavasti:

$$\omega_{x,(j)\sigma_y^{-1}}.\sigma_y = \omega_{x,((j)\sigma_y^{-1})\sigma_y} = \omega_{x,j}.$$

Toistamalla edellinen päättely kaikille reunapaloille, eli kaikilla $i \in \{1, \ldots, 12\}$, saadaan yleinen kaava

$$\omega_{xy} = \omega_x.\sigma_y +_2 \omega_y,$$

missä $\omega_x.\sigma_y = (\omega_{x,1}^{(1)\sigma_y}, \omega_{x,2}^{(2)\sigma_y}, \ldots, \omega_{x,12}^{(12)\sigma_y})$, mikä vastaa kranssitulon määritelmää. Siis reunapalojen permutaatio- ja orientaatiotilojen joukko $\mathcal{K}^r$ on reunapalojen keskinäisen vaikutuksen suhteen kranssitulo $\mathbb{Z}_2^{12} \wr S_{12}$.

Tarkastellaan seuraavaksi kulmapaloja. Olkoon nyt $i \in \{1, \ldots, 8\}$ ratkaistun kuution jonkin kulmapalan paikka. Kulmapalojen käsittely on täysin analoginen reunapalojen käsittelyn kanssa, poislukien yksi ylimääräinen orientaatiotila sekä operaation $(+_2)$ korvaamista yhteenlaskulla modulo 3 eli operaatiolla $(+_3)$. Vastaavasti kuin reunapalojen tapauksessa, voidaan muodostaa seuraava taulukko:

$\nu_{x,(i)\rho_x}$	0	0	0	1	1	1	2	2	2
$\nu_{y,(i)\rho_{xy}}$	0	1	2	0	1	2	0	1	2
$\nu_{xy,(i)\rho_{xy}}$	0	1	2	1	2	0	2	0	1

Alin rivi saadaan laskemalla kunkin sarakkeen kaksi ylintä alkiota yhteen modulo 3. Kuten reunapalojen taulukossa, 0 vastaa oikein päin olevaa palaa ja orientaatiotilan säilymistä. Nyt 1 vastaa kiertymistä yhden kerran 120 astetta myötäpäivään tai tällaista palaa ja 2 vastaa kiertymistä kaksi kertaa 120 astetta myötäpäivään tai tällaista palaa.

Analogisesti reunapalojen tapauksen kanssa saadaan lopputulos

$$\nu_{xy} = \nu_x.\rho_y +_3 \nu_y,$$

missä $\nu_x.\rho_y = (\nu_{x,1}^{(1)\rho_y}, \nu_{x,2}^{(2)\rho_y}, \ldots, \nu_{x,8}^{(8)\rho_y})$, mikä vastaa kranssitulon määritelmää. Siis kulmapalojen permutaatio- ja orientaatiotilojen joukko $\mathcal{K}^k$ on kulmapalojen keskinäisen vaikutuksen suhteen kranssitulo $\mathbb{Z}_3^8 \wr S_8$.

Näin ollen voidaan kirjoittaa

$$\mathcal{K} = (\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8),$$

missä $\times$ on *suora tulo*. Otetaan seuraavaksi esimerkki kranssitulon toiminnosta. Olkoon esimerkiksi

$$\omega = (1^2, 1^4, 1^5, 1^7, 1^9, 1^{11}),\ \sigma = (2\ 3\ 6\ 1\ 9)(10\ 4\ 5).$$

Tällöin

$$\begin{aligned}\omega.\sigma &= (1^2, 1^4, 1^5, 1^7, 1^9, 1^{11}).(2\ 3\ 6\ 1\ 9)(10\ 4\ 5)\\ &= (1^{(2)\sigma}, 1^{(4)\sigma}, 1^{(5)\sigma}, 1^{(7)\sigma}, 1^{(9)\sigma}, 1^{(11)\sigma})\\ &= (1^3, 1^5, 1^{10}, 1^7, 1^2, 1^{11})\\ &= (1^2, 1^3, 1^5, 1^7, 1^{10}, 1^{11}).\end{aligned}$$

Määritelmä 3.3.2. Olkoon $\bullet : \mathcal{K} \times \mathcal{K} \longrightarrow \mathcal{K}$ sellainen operaatio, että jos

$$f, g \in \mathcal{K},\ f = (\omega_f, \sigma_f, \nu_f, \rho_f),\ g = (\omega_g, \sigma_g, \nu_g, \rho_g),$$

niin järjestysten f ja g ***ketju***

$$f \bullet g = (\omega_f.\sigma_g +_2 \omega_g,\ \sigma_f\sigma_g,\ \nu_f.\rho_g +_3 \nu_g,\ \rho_f\rho_g),$$

missä $(.)$ on edellä konstruoitu toiminta, $+_2$ on yhteenlasku modulo 2 ja $+_3$ on yhteenlasku modulo 3. Järjestysten f ja g ketjussa toimii ensin f ja sitten g.

Lause 3.3.3. *Olkoon* $\mathcal{K} = (\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8)$ *ja* $\bullet : \mathcal{K} \times \mathcal{K} \longrightarrow \mathcal{K}$ *sellainen operaatio, että jos*

$$f, g \in \mathcal{K},\ f = (\omega_f, \sigma_f, \nu_f, \rho_f),\ g = (\omega_g, \sigma_g, \nu_g, \rho_g),$$

niin

$$f \bullet g = (\omega_f.\sigma_g +_2 \omega_g,\ \sigma_f\sigma_g,\ \nu_f.\rho_g +_3 \nu_g,\ \rho_f\rho_g).$$

Tällöin $(\mathcal{K}, \bullet)$ *on ryhmä.*

Todistus. Tarkastetaan ryhmän ehdot. Aluksi huomataan, että operaatio $(\bullet)$ käyttää permutaatioiden tulo-operaatiota. Tällöin tulot $\sigma_f\sigma_g$ ja $\rho_f\rho_g$ ovat ryhmäoperaatioita Lauseen 1.2.5 nojalla. Tällöin riittää osoittaa orientaatiotiloja koskevien termien operaatioiden toteuttavan ryhmän ehdot.

1) Määritelmän 2.1.3 nojalla $\omega_f.\sigma_g \in \mathbb{Z}_2^{12}$ ja $\nu_f.\rho_g \in \mathbb{Z}_3^8$. Tällöin $\omega_f.\sigma_g +_2 \omega_g \in \mathbb{Z}_2^{12}$ ja $\nu_f.\rho_g +_3 \nu_g \in \mathbb{Z}_3^8$, jolloin joukko $\mathcal{K}$ on suljettu operaation $(\bullet)$ suhteen.

2) Olkoon lisäksi $h \in \mathcal{K}$. Tällöin

$$\begin{aligned}
\omega_{(fg)h} &= \omega_{fg}.\sigma_h +_2 \omega_h \\
&= (\omega_f.\sigma_g +_2 \omega_g).\sigma_h +_2 \omega_h && \text{(Määritelmä 3.3.2)} \\
&= (\omega_f.\sigma_g).\sigma_h +_2 \omega_g.\sigma_h +_2 \omega_h && \text{(Lemma 2.2.3)}
\end{aligned}$$

ja

$$\begin{aligned}
\omega_{f(gh)} &= \omega_f.\sigma_{gh} +_2 \omega_{gh} \\
&= \omega_f.(\sigma_g\sigma_h) +_2 \omega_g.\sigma_h +_2 \omega_h && \text{(Määritelmät 1.2.4 ja 3.3.2)} \\
&= (\omega_f.\sigma_g).\sigma_h +_2 \omega_g.\sigma_h +_2 \omega_h && \text{(Määritelmä 2.1.3).}
\end{aligned}$$

Kulmapalojen orientaatiotilojen operaation assosiatiivisuus todistetaan täysin analogisesti. Näin ollen operaatio $(\bullet)$ on assosiatiivinen joukossa $\mathcal{K}$.

3) Olkoon $e \in \mathcal{K}$ ratkaistu kombinaatio. Tällöin $\omega_e = \overline{0}, \nu_e = \overline{0}$, $\sigma_e = (1)$ ja $\rho_e = (1)$. Tästä seuraa, että

$$\omega_{fe} = \omega_f.\sigma_e +_2 \omega_e = \omega_f +_2 \overline{0} = \omega_f$$

ja

$$\omega_{ef} = \omega_e.\sigma_f +_2 \omega_f = \overline{0} +_2 \omega_f = \omega_f.$$

Kulmapaloille voidaan tehdä täysin analoginen prosessi. Näin ollen $e \in \mathcal{K}$ on operaation $(\bullet)$ neutraalialkio joukossa $\mathcal{K}$.

4) Jos $f \in \mathcal{K}$ ja $g \in \mathcal{K}$ on järjestys, joka kumoaa järjestyksen f vaikutuksen, niin g on järjestyksen f käänteisalkio. Jos $g = (\omega_f.\sigma_f^{-1},\ \sigma_f^{-1},\ (\nu_f +_3 \nu_f).\rho_f^{-1},\ \rho_f^{-1})$, niin

$$\begin{aligned}
&\sigma_{fg} = \sigma_f\sigma_g = \sigma_f\sigma_f^{-1} = (1) = \sigma_f^{-1}\sigma_f = \sigma_g\sigma_f = \sigma_{gf}, \\
&\rho_{fg} = \rho_f\rho_g = \rho_f\rho_f^{-1} = (1) = \rho_f^{-1}\rho_f = \rho_g\rho_f = \rho_{gf}, \\
&\omega_{fg} = \omega_f.\sigma_g +_2 \omega_g \\
&\quad = \omega_f.\sigma_f^{-1} +_2 \omega_f.\sigma_f^{-1} \\
&\quad = (\omega_f +_2 \omega_f).\sigma_f^{-1} && \text{(Lemma 2.2.3)} \\
&\quad = (\omega_{f,1} +_2 \omega_{f,1}, ..., \omega_{f,12} +_2 \omega_{f,12}).\sigma_f^{-1},\ \omega_f^i = 0,1 \text{ kaikilla } 1 \leq i \leq 12 \\
&\quad = \overline{0}.\sigma_f^{-1} \\
&\quad = \overline{0},
\end{aligned}$$

$$\begin{aligned}
\omega_{gf} &= \omega_g.\sigma_f +_2 \omega_f \\
&= (\omega_f.\sigma_f^{-1}).\sigma_f +_2 \omega_f \\
&= \omega_f.(\sigma_f^{-1}\sigma_f) +_2 \omega_f && \text{(Määritelmä 2.1.3)} \\
&= \omega_f.(1) +_2 \omega_f \\
&= \omega_f +_2 \omega_f \\
&= (\omega_{f,1} +_2 \omega_{f,1}, ..., \omega_{f,12} +_2 \omega_{f,12}),\ \omega_f^i = 0,1 \text{ kaikilla } 1 \leq i \leq 12 \\
&= \overline{0},
\end{aligned}$$

$$\begin{aligned}
\nu_{fg} &= \nu_f.\rho_g +_3 \nu_g \\
&= \nu_f.\rho_f^{-1} +_3 (\nu_f +_3 \nu_f).\rho_f^{-1} \\
&= (\nu_f +_3 \nu_f +_3 \nu_f).\rho_f^{-1} && \text{(Lemma 2.2.3)} \\
&= (\nu_{f,1} +_3 \nu_{f,1} +_3 \nu_{f,1}, ..., \nu_{f,8} +_3 \nu_{f,8} +_3 \nu_{f,8}).\rho_f^{-1} \\
&= \overline{0}.\rho_f^{-1} \\
&= \overline{0}
\end{aligned}$$

ja

$$\begin{aligned}
\nu_{gf} &= \nu_g.\rho_f +_3 \nu_f \\
&= ((\nu_f +_3 \nu_f).\rho_f^{-1}).\rho_f +_3 \nu_f \\
&= (\nu_f +_3 \nu_f).(\rho_f^{-1}\rho_f) +_3 \nu_f && \text{(Määritelmä 2.1.3)} \\
&= (\nu_f +_3 \nu_f).(1) +_3 \nu_f \\
&= \nu_f +_3 \nu_f +_3 \nu_f \\
&= (\nu_{f,1} +_3 \nu_{f,1} +_3 \nu_{f,1}, ..., \nu_{f,8} +_3 \nu_{f,8} +_3 \nu_{f,8}) \\
&= \overline{0}.
\end{aligned}$$

Näin ollen $g = f^{-1}$. Tällöin kohdista 1)-4) seuraa, että $(\mathcal{K}, \bullet)$ on ryhmä.

□

Seuraava tarkastelu on luonteeltaan tarkentava. Siinä osoitetaan, että orientaatiotilojen käänteisalkiot on mahdollista johtaa pelkästään tarkasteltavan kombinaation avulla.

Olkoon f järjestely ja g sen käänteisjärjestely. Tällöin

$$\begin{aligned}
&\omega_g.\sigma_f +_2 \omega_f = \overline{0} \\
\Leftrightarrow\ &\omega_g.\sigma_f = \overline{0} -_2 \omega_f = (0 -_2 \omega_{f,i})_{i=1}^{12}.
\end{aligned}$$

Koska $\omega_{f,i} = 0,1$ kaikilla i, niin

$$\begin{cases}
\omega_{f,i} = 0 \Rightarrow 0 -_2 \omega_{f,i} = 0 -_2 0 = 0 = \omega_{f,i} \\
\omega_{f,i} = 1 \Rightarrow 0 -_2 \omega_{f,i} = 0 -_2 1 = -1 \equiv 1 = \omega_{f,i}.
\end{cases}$$

Näin ollen

$$\begin{aligned}
&\omega_g.\sigma_f = \overline{0} -_2 \omega_f = \omega_f \\
\Leftrightarrow\ &(\omega_g.\sigma_f).\sigma_f^{-1} = \omega_f.\sigma_f^{-1} \\
\Leftrightarrow\ &\omega_g.(\sigma_f\sigma_f^{-1}) = \omega_f.\sigma_f^{-1} \\
\Leftrightarrow\ &\omega_g.(1) = \omega_f.\sigma_f^{-1} \\
\Leftrightarrow\ &\omega_g = \omega_f.\sigma_f^{-1} \\
\Rightarrow\ &\omega_{f^{-1}} = \omega_f.\sigma_f^{-1}.
\end{aligned}$$

Edelleen,

$$\begin{aligned}
&\nu_g.\rho_f +_3 \nu_f = \overline{0} \\
\Leftrightarrow\ &\nu_g.\rho_f = \overline{0} -_3 \nu_f = (0 - \nu_{f,i})_{i=1}^{8}.
\end{aligned}$$

Koska $\nu_{f,i} = 0, 1, 2$ kaikilla i, niin

$$\begin{cases}
\nu_{f,i} = 0 \Rightarrow 0 -_3 \nu_{f,i} = 0 -_3 0 = 0 = 0 +_3 0 = \nu_{f,i} +_3 \nu_{f,i} \\
\nu_{f,i} = 1 \Rightarrow 0 -_3 \nu_{f,i} = 0 -_3 1 = -1 \equiv 2 = 1 +_3 1 = \nu_{f,i} +_3 \nu_{f,i} \\
\nu_{f,i} = 2 \Rightarrow 0 -_3 \nu_{f,i} = 0 -_3 2 = -2 \equiv 1 \equiv 4 = 2 +_3 2 = \nu_{f,i} +_3 \nu_{f,i}.
\end{cases}$$

Näin ollen

$$\begin{aligned}
&\nu_g.\rho_f = \overline{0} -_3 \nu_f = \nu_f +_3 \nu_f \\
\Leftrightarrow\ &(\nu_g.\rho_f).\rho_f^{-1} = (\nu_f +_3 \nu_f).\rho_f^{-1} \\
\Leftrightarrow\ &\nu_g.(\rho_f\rho_f^{-1}) = (\nu_f +_3 \nu_f).\rho_f^{-1} \\
\Leftrightarrow\ &\nu_g.(1) = (\nu_f +_3 \nu_f).\rho_f^{-1} \\
\Leftrightarrow\ &\nu_g = (\nu_f +_3 \nu_f).\rho_f^{-1} \\
\Rightarrow\ &\nu_{f^{-1}} = (\nu_f +_3 \nu_f).\rho_f^{-1}.
\end{aligned}$$

Toisaalta, jos $g = f^{-1}$, niin $g^{-1} = (f^{-1})^{-1} = f$. Tällöin

$$\begin{aligned}
&\omega_f.\sigma_g +_2 \omega_g = \overline{0} \\
\Leftrightarrow\ &\omega_f.\sigma_g = \overline{0} -_2 \omega_g = (0 -_2 \omega_{g,i})_{i=1}^{12}, \\
&\nu_f.\rho_g +_3 \nu_g = \overline{0} \\
\Leftrightarrow\ &\nu_f.\rho_g = \overline{0} -_3 \nu_g = (0 - \nu_{g,i})_{i=1}^{8}.
\end{aligned}$$

Edellisen nojalla tästä seuraa, että

$$\begin{aligned}
&\omega_f.\sigma_g = \overline{0} -_2 \omega_g = \omega_g \\
\Leftrightarrow\ &(\omega_f.\sigma_g).\sigma_g^{-1} = \omega_g.\sigma_g^{-1} \\
\Leftrightarrow\ &\omega_f.(\sigma_g\sigma_g^{-1}) = \omega_g.\sigma_g^{-1} \\
\Leftrightarrow\ &\omega_f.(1) = \omega_g.\sigma_g^{-1} \\
\Leftrightarrow\ &\omega_f = \omega_g.\sigma_g^{-1} \\
\Rightarrow\ &\omega_{g^{-1}} = \omega_g.\sigma_g^{-1}
\end{aligned}$$

ja

$$\begin{aligned}
&\nu_f.\rho_g = \overline{0} -_3 \nu_g = \nu_g +_3 \nu_g \\
\Leftrightarrow\ &(\nu_f.\rho_g).\rho_g^{-1} = (\nu_g +_3 \nu_g).\rho_g^{-1} \\
\Leftrightarrow\ &\nu_f.(\rho_g\rho_g^{-1}) = (\nu_g +_3 \nu_g).\rho_g^{-1} \\
\Leftrightarrow\ &\nu_f.(1) = (\nu_g +_3 \nu_g).\rho_g^{-1} \\
\Leftrightarrow\ &\nu_f = (\nu_g +_3 \nu_g).\rho_g^{-1} \\
\Rightarrow\ &\nu_{g^{-1}} = (\nu_g +_3 \nu_g).\rho_g^{-1}.
\end{aligned}$$

Nämä kaksi esitystä ovat täysin analogiset edellisiin verrattuna.

Lemma 3.3.4. $|\mathcal{K}| = |(\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8)| = 519\ 024\ 039\ 293\ 878\ 272\ 000.$

Todistus. Joukon $\mathcal{K}$ alkioon voidaan valita yksi mikä tahansa alkio kustakin joukosta $\mathbb{Z}_2^{12}$, S_{12}, $\mathbb{Z}_3^8$ ja S_8, joten tuloperiaatteen nojalla on olemassa $|\mathbb{Z}_2^{12}| \cdot |S_{12}| \cdot |\mathbb{Z}_3^8| \cdot |S_8|$ erilaista nelikköä. Koska kranssitulon $A \wr B$ taustajoukko on $A \times B$, niin Lemman 1.1.5 nojalla

$$|\mathcal{K}| = |\mathbb{Z}_2^{12}| \cdot |S_{12}| \cdot |\mathbb{Z}_3^8| \cdot |S_8| = 2^{12} \cdot 12! \cdot 3^8 \cdot 8! = 519\ 024\ 039\ 293\ 878\ 272\ 000.$$

□

3.4 Rubikin kuution ratkeava ryhmä

Rubikin kuution ratkeava ryhmä koostuu niistä ryhmän $\mathcal{K}$ alkioista, jotka voidaan generoida joukon $S = \{F, B, L, R, U, D\}$ alkioilla ratkaistusta kuutiosta $e = (\overline{0}, (1), \overline{0}, (1))$. Tässä kappaleessa etsitään ne ehdot, joiden voimassaolon kanssa kombinaation ratkeavuus on yhtäpitävää. Tällöin ratkeavan ryhmän rakenne saadaan selville ilman työlästä generointia joukon S alkioista.

Lause 3.4.1. [3]. *Olkoon* $(\omega, \sigma, \nu, \rho) \in (\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8)$. *Tällöin nelikkö* $(\omega, \sigma, \nu, \rho)$ *vastaa ratkeavaa kombinaatiota, jos ja vain jos*

1) $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\rho)$,

2) $\nu_1 + \nu_2 + ... + \nu_8 \equiv 0\ (mod\ 3)$,

3) $\omega_1 + \omega_2 + ... + \omega_{12} \equiv 0\ (mod\ 2)$.

Todistus. ($\Rightarrow$) Olkoon f kääntöjono, joka saattaa kuution ratkeavaan kombinaatioon $(\omega, \sigma, \nu, \rho)$. Tällöin $f = f_1 f_2 ... f_n$, missä $f_i \in S$. Jokainen kääntö f_i permutoi neljää reunapalaa ja neljää kulmapalaa kuvan 3 indeksoinnin mukaisesti, joten saadaan suoraan $\operatorname{sgn}(\sigma_i) = \operatorname{sgn}(\rho_i)$ kaikilla i, ja siten

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{n} \operatorname{sgn}(\sigma_i) = \prod_{i=1}^{n} \operatorname{sgn}(\rho_i) = \operatorname{sgn}(\rho),$$

jolloin ehto 1) on voimassa. Kun tarkastellaan joukon S alkioiden orientaatiovaikutusta, saadaan seuraavat taulukot:

K	ω_K	$\sum \omega_{K,i}\ (mod\ 2)$
F	$(1^2, 1^3)$	0
B	$(1^9, 1^{12})$	0
L	$(1^5, 1^7)$	0
R	$(1^3, 1^{11})$	0
U	$(1^5, 1^6)$	0
D	$(1^4, 1^{12})$	0

K	ν_K	$\sum \nu_{K,i}\ (mod\ 3)$
F	$(2^1, 1^2, 1^3, 2^4)$	0
B	$(1^5, 2^6, 2^7, 1^8)$	0
L	$(1^1, 2^3, 2^5, 1^7)$	0
R	$(2^2, 1^4, 1^6, 2^8)$	0
U	$\overline{0}$	0
D	$\overline{0}$	0

Näin ollen ehdot 2) ja 3) ovat voimassa, sillä joukko S generoi joukon $\mathcal{R}$, ja kaikki joukon S alkiot säilyttävät orientaatiosumman. Lisäksi ratkeavan kombinaation permutaatiotilaa kuvaavat permutaatiot σ ja ρ koostuvat molemmat joko parillisesta tai parittomasta määrästä 2-syklejä. Seuraavaksi osoitetaan lauseen toinen suunta. Tässä todistuksen osassa on tarkoitus ratkaista kuutio lähtien ehdoista 1)-3). Todistuksessa ratkaistaan ensin permutaatiotilat, ja sitten orientaatiotilat.

($\Leftarrow$) **Ehto 1).** Oletetaan seuraavaksi, että ehdot 1)-3) ovat voimassa. Tällöin $\text{sgn}(\sigma) = \text{sgn}(\rho)$. Jos permutaatiot ovat parittomia, suoritetaan jokin joukon S kääntö K, jolloin permutaatiotilat ovat parillisia, sillä $\text{sgn}(\sigma_K) = \text{sgn}(\rho_K) = -1$. Lauseen 1.3.3 nojalla $\text{sgn}(\sigma\sigma_K) = (-1) \cdot (-1) = 1$ ja $\text{sgn}(\rho\rho_K) = (-1) \cdot (-1) = 1$. Tällöin riittää tarkastella tapausta, jossa $\text{sgn}(\sigma) = \text{sgn}(\rho) = 1$. Lisäksi nyt orientaatiotiloja ei tarvitse huomioida, sillä nyt tarkastellaan vain permutaatiotiloja. Olkoon siis $\text{sgn}(\sigma) = \text{sgn}(\rho) = 1$. Olkoon kääntöjono

$$f = U\ R\ U^{-1}\ L^{-1}\ U\ R^{-1}\ U^{-1}\ L.$$

Tällöin $\rho_f = (1\ 6\ 5)$ ja $\sigma_f = (1)$. Siten kääntöjono f vaikuttaa ainoastaan kulmapalojen 1, 5 ja 6 permutaatiotiloihin ja $\text{sgn}(\rho_f) = \text{sgn}(\sigma_f) = 1$. Olkoot kulmapalat $k_1, k_2, ..., k_8 \in \{1, 2, ..., 8\}$. Osoitetaan, että mielivaltaisten kulmapalojen k_i, k_j ja k_l 3-sykli $(k_i\ k_j\ k_l)$ voidaan muodostaa kääntöjonon f avulla.

Selvästi mielivaltainen kulmapala k_i voidaan siirtää jollakin kääntöjonolla x_1 paikalle 1, ellei se ole jo. Toisin sanoen, on olemassa sellainen kääntöjono x_1, että permutaatio ρ_{x_1} sisältää siirron $k_i \mapsto 1$.

Seuraavaksi, siirretään kulmapala k_l paikalle 5 säilyttäen paikka 1. Käännöt R, D ja B säilyttävät kulmapalan 1, mutta niiden generoimalla kääntöjonojen joukolla mikä tahansa muu kulmapala saadaan mihin tahansa muulle paikalle. Tällöin kulmapala k_l voidaan jollakin tällaisella kääntöjonolla $x_2 \in \langle\{R, D, B\}\rangle$ siirtää paikalle 5. Toisin sanoen, ρ_{x_2} sisältää siirron $k_l \mapsto 5$.

Siirretään vielä kulmapala k_j paikalle 6 säilyttäen paikat 1 ja 5. Nyt käännöt R ja D säilyttävät paikat 1 ja 5, mutta niiden generoimalla joukolla mikä tahansa muu

kulmapala saadaan mihin tahansa muulle paikalle. Tällöin on olemassa sellainen kääntöjono $x_3 \in \langle\{R, D\}\rangle$, että ρ_{x_3} sisältää siirron $k_j \mapsto 6$.

Alla on taulukko, josta ilmenee esimerkki kuhunkin eri tilanteeseen tarvittavasta kääntöjonosta ilmoitetuin rajoituksin.

Siirrettävän palan paikka	$x_1 \in \langle S\rangle$	$x_2 \in \langle\{R, D, B\}\rangle$	$x_3 \in \langle\{R, D\}\rangle$
1	E	-	-
2	F^{-1}	$R\ B$	R
3	F	$D^2\ B^2$	$D\ R^2$
4	F^2	$R^2\ B$	R^2
5	L	E	-
6	U^2	B	E
7	L^2	B^{-1}	$D^{-1}\ R^{-1}$
8	$R^2\ U$	B^2	R^{-1}

Koska edellisten vaiheiden merkitykselliset siirrot ovat keskenään erillisiä, kääntöjonon $x = x_1x_2x_3$ kulmapalojen permutaatio $\rho_x = \rho_{x_1x_2x_3}$ sisältää siirrot $k_i \mapsto 1,\ k_j \mapsto 6$ ja $k_l \mapsto 5$. Siis on löydetty sellainen kääntöjono x, joka siirtää kolme mielivaltaista kulmapalaa haluttuun järjestykseen paikoille 1, 5 ja 6. Lisäksi kääntöjono $x^{-1} = x_3^{-1}x_2^{-1}x_1^{-1}$ kumoaa tämän järjestelyn vaikutuksen täydellisesti. Tällöin kääntöjonossa xfx^{-1} tapahtuu järjestyksessä seuraava:

1) Kääntöjono x tekee siirrot $k_i \mapsto 1,\ k_j \mapsto 6$ ja $k_l \mapsto 5$.

2) Kääntöjonolle f pätee $\rho_f = (1\ 6\ 5)$, mutta koska kääntöjono x on siirtänyt palan k_i paikalle 1, palan k_j paikalle 6 ja palan k_l paikalle 5 ennen kääntöjonoa f, niin tapahtuu $(k_i\ k_j\ k_l)$.

3) Kääntöjonon x^{-1} vaikutuksesta kaikki palat palautuvat alkuperäisiin tiloihinsa, paitsi pala k_i siirtyy palan k_j alkuperäiselle paikalle, pala k_j palan k_l alkuperäiselle paikalle ja pala k_l palan k_i alkuperäiselle paikalle. Tämä johtuu siitä, että kääntöjono f on vaikuttanut vain näihin kolmeen kulmapalaan. Kaikille muille paloille on tapahtunut käytännössä sama kääntöjono kuin xx^{-1}, sillä f ei vaikuta niihin.

Näin ollen kuutioon tapahtunut kokonaismuutos on pelkästään permutaatio

$$\rho_{xfx^{-1}} = (k_i\ k_j\ k_l).$$

Lisäksi, koska käsittely koostuu vain käännöistä, se säilyttää ehdon 1) kaikissa vaiheissa, sillä $\operatorname{sgn}(\rho_K) = \operatorname{sgn}(\sigma_K) = -1$ kaikilla $K \in S$. Lauseen 1.3.12 nojalla kaikki parilliset permutaatiot voidaan esittää 3-syklien tulona. Koska ennen kulmapalojen käsittelyä menetelmällä on voimassa $\operatorname{sgn}(\rho) = 1$, niin ρ voidaan esittää 3-syklien tulona. Tämä takaa sen, että kulmapalat saadaan siirrettyä ratkaistuille paikoilleen käytetyllä menetelmällä.

Mutta kulmapalat saadaan ratkaistuille paikoilleen riippumatta ehdosta 1). Ehdon vaikutus näkyy, kun vastaava käsittely tehdään reunapaloille.

Tehdään siis vastaava käsittely reunapaloille. Oletetaan, että kulmapalat on siirretty ratkaistuille paikoilleen ja olkoon kääntöjono

$$g = U^2\ R\ U^{-1}\ (R\ U)^2\ R\ U^{-1}\ R^{-1}\ U^{-1}\ R^2\ U^2.$$

Tällöin $\sigma_g = (5\ 6\ 9)$ ja $\rho_g = (1)$. Siis kääntöjono g säilyttää nyt kulmapalojen ratkaistun permutaatiotilan. Merkitään reunapaloja $r_1, r_2, ..., r_{12} \in \{1, 2, ..., 12\}$. Osoitetaan, että mielivaltaisten reunapalojen $r_i,\ r_j$ ja r_l 3-sykli voidaan muodostaa kääntöjonon g avulla.

Selvästi mielivaltainen reunapala r_i voidaan siirtää jollakin kääntöjonolla y_1 paikalle 5, ellei se ole jo. Toisin sanoen, on olemassa sellainen kääntöjono y_1, että permutaatio σ_{y_1} sisältää siirron $r_i \mapsto 5$.

Seuraavaksi siirretään reunapala r_j paikalle 6 säilyttäen paikka 5. Käännöt F, B, R ja D säilyttävät reunapalan 5, mutta niiden generoimalla kääntöjonojen joukolla mikä tahansa muu reunapala saadaan mihin tahansa muulle paikalle. Tällöin reunapala r_j voidaan jollakin tällaisella kääntöjonolla $y_2 \in \langle\{F, B, R, D\}\rangle$ siirtää paikalle 6. Toisin sanoen, σ_{y_2} sisältää siirron $r_j \mapsto 6$.

Siirretään vielä reunapala r_l paikalle 9 säilyttäen paikat 5 ja 6. Nyt käännöt F, B ja D säilyttävät paikat 5 ja 6, mutta niiden generoimalla kääntöjonojen joukolla mikä tahansa muu reunapala saadaan mihin tahansa muulle paikalle. Tällöin on olemassa sellainen kääntöjono $y_3 \in \langle\{F, B, D\}\rangle$, että σ_{y_3} sisältää siirron $r_l \mapsto 9$.

Alla on taulukko, josta ilmenee esimerkki kuhunkin eri tilanteeseen tarvittavasta kääntöjonosta ilmoitetuin rajoituksin.

Siirrettävän palan paikka	$y_1 \in \langle S\rangle$	$y_2 \in \langle\{F, B, R, D\}\rangle$	$y_3 \in \langle\{F, B, D\}\rangle$
1	U	$F\ R$	$F^2\ D^2\ B^2$
2	L^{-1}	$F^2\ R$	$F^{-1}\ D^2\ B^2$
3	$R\ U^2$	R	$F\ D^2\ B^2$
4	$F^2\ U$	$D\ R^2$	$D^2\ B^2$
5	E	-	-
6	U^2	E	-
7	L^2	$D^2\ R^2$	$D^{-1}\ B^2$
8	$R^2\ U^2$	R^2	$D\ B^2$
9	U^{-1}	$B^{-1}\ R^{-1}$	E
10	L	$B^2\ R^{-1}$	B^{-1}
11	$R^{-1}\ U^2$	R^{-1}	B
12	$B^2\ U^{-1}$	$D^{-1}\ R^2$	B^2

Koska edellisten vaiheiden merkitykselliset siirrot ovat keskenään erillisiä, kääntöjonon $y = y_1y_2y_3$ reunapalojen permutaatio $\sigma_y = \sigma_{y_1y_2y_3}$ sisältää siirrot $r_i \mapsto 5$, $r_j \mapsto 6$ ja $r_l \mapsto 9$. Siis on löydetty sellainen kääntöjono y, joka siirtää kolme mielivaltaista reunapalaa haluttuun järjestykseen paikoille 5, 6 ja 9. Lisäksi kääntöjono $y^{-1} = y_3^{-1}y_2^{-1}y_1^{-1}$ kumoaa tämän järjestelyn vaikutuksen täydellisesti. Tällöin kääntöjonossa ygy^{-1} tapahtuu järjestyksessä seuraava:

1) Kääntöjono y sisältää siirrot $r_i \mapsto 5$, $r_j \mapsto 6$ ja $r_l \mapsto 9$.

2) Kääntöjonolle g pätee $\sigma_g = (5\ 6\ 9)$, mutta koska kääntöjono y on siirtänyt palan r_i paikalle 5, palan r_j paikalle 6 ja palan r_l paikalle 9, niin tapahtuu $(r_i\ r_j\ r_l)$.

3) Kääntöjonon y^{-1} vaikutuksesta kaikki palat palautuvat alkuperäisiin tiloihinsa, paitsi pala r_i siirtyy palan r_j alkuperäiselle paikalle, pala r_j palan r_l alkuperäiselle paikalle ja pala r_l palan r_i alkuperäiselle paikalle. Tämä johtuu siitä, että kääntöjono g on vaikuttanut vain näihin kolmeen reunapalaan. Kaikille muille paloille on tapahtunut käytännössä sama kääntöjono kuin yy^{-1}, sillä g ei vaikuta niihin.

Näin ollen kuutioon tapahtunut kokonaismuutos on pelkästään permutaatio

$$\sigma_{ygy^{-1}} = (r_i\ r_j\ r_l).$$

Lisäksi, koska käsittely koostuu vain käännöistä, se säilyttää ehdon 1) kaikissa vaiheissa, sillä $\operatorname{sgn}(\rho_K)\operatorname{sgn}(\sigma_K) = 1$ kaikilla $K \in S$. Tällöin, koska kääntöjonon ygy^{-1} vaikutus reunapaloihin $\sigma_{ygy^{-1}}$ on parillinen 3-sykli, pätee $\operatorname{sgn}(\sigma_{ygy^{-1}}) = 1$ ja käsittelyn jälkeen ehto 1) on edelleen voimassa. Lauseen 1.3.12 nojalla kaikki parilliset permutaatiot voidaan esittää 3-syklien tulona. Tällöin, koska ennen reunapalojen käsittelyä $\operatorname{sgn}(\sigma) = 1$ ehdon 1) todistuksen alussa tehdyn tarkastelun mukaisesti, niin σ on nyt jokin 3-syklien tulo. Tämä takaa sen, että käytetty menetelmä, joka koostuu vain 3-sykleistä, voi palauttaa myös reunapalat ratkaistuille paikoilleen, eli permutaatiotilaan, jota vastaa permutaatio $(1) \in S_{12}$. Täten ehdosta 1) seuraa kuution permutaatiotilan ratkeavuus.

Ehto 2). Olkoon nyt

$$f = (R^{-1}\ D^{-1}\ R\ D)^2\ U\ (R^{-1}\ D^{-1}\ R\ D)^4\ U^{-1}.$$

Tällöin kääntöjonon f vaikutus kuutioon on ainoastaan muutos kulmapalojen orientaatiotilaan siten, että $\nu_f = (1^2, 2^6)$. Edellä käytettyä menetelmää soveltamalla kahdelle kulmapalalle löydetään sellainen kääntöjono z, että z siirtää kulmapalan k_i paikalle 2 ja palan k_j paikalle 6 kahdelle mielivaltaiselle kulmapalalle k_i ja k_j. Tämä tapahtuu seuraavasti.

Selvästi mielivaltainen kulmapala k_i voidaan siirtää jollakin kääntöjonolla z_1 paikalle 2, ellei se ole jo. Seuraavaksi siirretään pala k_j paikalle 6 kääntöjonolla z_2 säilyttäen paikka 2. Seuraavalla sivulla olevassa taulukossa on listattuna esimerkit tällaisista kääntöjonoista.

Siirrettävän palan paikka	z_1	z_2
1	F	$L^{-1}\ B^{-1}$
2	E	-
3	F^2	L^2B^{-1}
4	F^{-1}	$D\ B$
5	U^2	B^{-1}
6	U	E
7	$D\ F^2$	B^2
8	R^2	B

Tällöin merkityksellisten permutaatiovaikutusten erillisyyden nojalla kääntöjono $z = z_1z_2$ sisältää siirrot $k_i \mapsto 2,\ k_j \mapsto 6$. Lisäksi kääntöjono z^{-1} kumoaa vaikutuksen täydellisesti.

Kulmapalojen orientaatiotiloille on kolme tapausta:

1) orientaatiotiloja 1 ja 2 on yhtä monta (myös 0 kappaletta),

2) orientaatiotiloja 1 on enemmän kuin tiloja 2,

3) orientaatiotiloja 2 on enemmän kuin tiloja 1.

Jos tapauksessa 1) on nollasta eroavia orientaatiotiloja, niin ehdon 2) nojalla voidaan muodostaa kulmapalapareja (k_i, k_j), missä $\nu_i = 2, \nu_j = 1$. Tutkitaan nyt kääntöjonon zfz^{-1} vaikutusta kuutioon.

Tutkitaan ensin, mitä tapahtuu muille kulmapaloille, kuin paloille k_i ja k_j. Olkoon k_x tällainen kulmapala. Kääntöjonon z seurauksena $k_x \mapsto k_y$, missä $y \neq 2, 6$. Tällöin kääntöjono f ei vaikuta kulmapalaan k_y. Tämän jälkeen kääntöjonon z^{-1} seurauksena $k_y \mapsto k_x$. Siis kääntöjonon zfz^{-1} seurauksena $k_x \mapsto k_x$. Lisäksi palan k_x orientaatiotila ei muutu Lauseen 3.3.3 nojalla. Toisin sanoen, kääntöjono zfz^{-1} ei vaikuta muihin kulmapaloihin kuin paloihin k_i ja k_j.

Tarkastellaan kääntöjonon vaikutusta näihin kulmapaloihin. Kulmapala k_i siirtyy paikalle 2. Tämän jälkeen kääntöjono f tekee paikalla 2 olevaan palaan, eli palaan k_i, orientaatiotilaan muutoksen +1. Lopuksi pala k_i palaa alkuperäiselle paikalleen. Kulmapala k_j siirtyy paikalle 6. Tämän jälkeen kääntöjono f tekee paikalla 6 olevaan palaan, eli palaan k_j, orientaatiotilaan muutoksen +2. Lopuksi pala k_j palaa alkuperäiselle paikalleen.

Näin ollen kääntöjonon zfz^{-1} kokonaisvaikutus on $\nu_{zfz^{-1}} = (1^{k_i}, 2^{k_j})$. Tällöin, kun kääntöjono zfz^{-1} suoritetaan edellämainittuun kulmapalapariin (k_i, k_j), molemmat palat kääntyvät oikein päin. Tällöin jäljellä on yksi vähemmän kumpaakin nollasta poikkeavaa orientaatiotilaa. Toistetaan käsittely kaikille tällaisille pareille. Lopputuloksena kaikki kulmapalat ovat oikein päin, eli $\nu = \overline{0}$.

Tapauksessa 2) pätee ehdon 2) nojalla seuraava taulukko:

Erikoistapaus	Tilojen 1 lkm.	Tilojen 2 lkm.
1	3 kpl	0 kpl
2	6 kpl	0 kpl
3	4 kpl	1 kpl
4	5 kpl	2 kpl
5	7 kpl	1 kpl

Erikoistapauksissa 3, 4 ja 5 on ainakin yksi tapauksen 1) mukainen kulmapalapari, jolloin sovelletaan ensin tapauksen 1) menetelmää, jonka seurauksena tämä pari/nämä parit eliminoituvat, ja saadaan joko erikoistapaus 1 tai erikoistapaus 2. Erikoistapauksissa 1 ja 2 voidaan muodostaa kolmikko (k_i, k_j, k_l), missä kaikkien palojen orientaatiotila on 1.

Sovelletaan tapauksen 1) menetelmää ensin pariin (k_i, k_j), missä $(1^i, 1^j) \mapsto (2^i, 0^j)$, ja sitten pariin (k_i, k_l), missä $(2^i, 1^l) \mapsto (0^i, 0^l)$. Erikoistapauksessa 2) tämä käsittely toistetaan jäljellä oleville kolmelle kulmapalalle. Näin ollen kaikki kulmapalat saadaan käännettyä oikein päin.

Tapauksessa 3) pätee ehdon 2) nojalla seuraava taulukko:

Erikoistapaus	Tilojen 1 lkm.	Tilojen 2 lkm.
1	0 kpl	3 kpl
2	0 kpl	6 kpl
3	2 kpl	5 kpl
4	1 kpl	4 kpl
5	1 kpl	7 kpl

Erikoistapauksissa 3, 4 ja 5 voidaan muodostaa tapauksen 1) mukaisia pareja, jotka eliminoidaan kuten tapauksessa 1). Tällöin saadaan joko erikoistapaus 1 tai 2. Tällöin voidaan muodostaa orientaatiotilan 2 omaavien kulmapalojen kolmikko (k_i, k_j, k_l), johon sovelletaan tapauksen 1) menetelmää ensin pariin (k_i, k_j), missä $(2^i, 2^j) \mapsto (0^i, 1^j)$ ja sitten pariin (k_l, k_j), missä $(2^l, 1^j) \mapsto (0^l, 0^j)$. Erikoistapauksessa 2 tämä käsittely tehdään kahdesti, sillä kuudesta palasta muodostetaan kaksi kolmikkoa. Näin ollen kaikki kulmapalat saadaan käännettyä oikein päin kaikissa tapauksissa, ja ehdosta 2) seuraa kulmapalojen orientaatiotilan ratkeavuus.

Ehto 3). Olkoon nyt

$$g = L\ F\ R^{-1}\ F^{-1}\ L^{-1}\ U^2\ R\ U\ R\ U^{-1}\ R^2\ U^2\ R.$$

Tällöin kääntöjonon g vaikutus kuutioon on ainoastaan muutos reunapalojen orientaatiotilaan siten, että $\omega_g = (1^1, 1^6)$. Edelleen, edellä käytettyä menetelmää soveltamalla löydetään sellainen kääntöjono c, että c siirtää reunapalan r_i paikalle 1 ja palan r_j paikalle 6 kahdelle mielivaltaiselle reunapalalle r_i ja r_j. Tämä tapahtuu seuraavasti.

Selvästi mielivaltainen reunapala r_i voidaan siirtää jollakin kääntöjonolla c_1 paikalle 1, ellei se ole jo. Seuraavaksi siirretään pala r_j paikalle 6 kääntöjonolla c_2 säilyttäen paikka 1. Alla olevassa taulukossa on listattuna esimerkit tällaisista kääntöjonoista.

Siirrettävän palan paikka	c_1	c_2
1	E	-
2	F	$L\ D^2\ R^2$
3	F^{-1}	R
4	F^2	$D\ R^2$
5	U^{-1}	$L^2\ D^2\ R^2$
6	U	E
7	$D\ F^2$	$D^2\ R^2$
8	$D^{-1}\ F^2$	R^2
9	U^2	$B^{-1}\ R^{-1}$
10	$L\ U^{-1}$	$B^2\ R^{-1}$
11	$R^{-1}\ U$	R^{-1}
12	$D^2\ F^2$	$B\ R^{-1}$

Tällöin merkityksellisten permutaatiovaikutusten erillisyyden nojalla kääntöjono $c = c_1c_2$ sisältää siirrot $r_i \mapsto 1,\ r_j \mapsto 6$. Lisäksi kääntöjono c^{-1} kumoaa vaikutuksen täydellisesti.

Ehdon 3) nojalla kääntyneitä reunapaloja on oltava parillinen määrä, joten mikäli kuutiossa on nollasta poikkeavia orientaatiotiloja, voidaan muodostaa reunapalapareja (r_i, r_j), missä $\omega_i = \omega_j = 1$. Tutkitaan kääntöjonon cgc^{-1} vaikutusta kuutioon.

Tutkitaan ensin, mitä tapahtuu muille reunapaloille, kuin paloille r_i ja r_j. Olkoon r_x tällainen reunapala. Kääntöjonon c seurauksena $r_x \mapsto r_y$, missä $y \neq 1, 6$. Tällöin kääntöjono g ei vaikuta reunapalaan r_y. Tämän jälkeen kääntöjonon c^{-1} seurauksena $r_y \mapsto r_x$. Siis kääntöjonon cgc^{-1} seurauksena $r_x \mapsto r_x$. Lisäksi palan r_x orientaatiotila ei muutu Lauseen 3.3.3 nojalla. Toisin sanoen, kääntöjono cgc^{-1} ei vaikuta muihin reunapaloihin kuin paloihin r_i ja r_j.

Tarkastellaan kääntöjonon vaikutusta näihin reunapaloihin. Reunapala r_i siirtyy paikalle 1. Tämän jälkeen kääntöjono g tekee paikalla 1 olevaan palaan, eli palaan r_i, orientaatiotilaan muutoksen $+1$. Lopuksi pala r_i palaa alkuperäiselle paikalleen. Reunapala r_j siirtyy paikalle 6. Tämän jälkeen kääntöjono g tekee paikalla 6 olevaan palaan, eli palaan r_j, orientaatiotilaan muutoksen $+1$. Lopuksi pala r_j palaa alkuperäiselle paikalleen.

Siis kääntöjono cgc^{-1} tekee reunapalojen r_i ja r_j orientaatiotiloihin muutoksen $+1$. Tällöin, kun kääntöjono cgc^{-1} suoritetaan edellämainittuun reunapalapariin, molemmat palat kääntyvät oikein päin. Toistetaan käsittely kaikille pareille, jolloin

lopputuloksena kaikki reunapalat ovat oikein päin, eli $\omega = \overline{0}$. Näin ollen ehdosta 3) seuraa reunapalojen orientaatiotilan ratkeavuus.

Nyt ehdoista 1)-3) seuraa kuution permutaatiotilan sekä kulma- ja reunapalojen orientaatiotilojen ratkeavuudet, jolloin kombinaation määritelmän nojalla ehdoista seuraa myös kombinaation ratkeavuus, ja lauseen todistus on valmis. □

Eräs edellisen todistuksen mielenkiintoinen sivuvaikutus on se, että suunnan ($\Leftarrow$) todistuksen avulla voidaan ratkaista Rubikin kuutio, mikäli alkuperäinen kombinaatio on ratkeava.

Kuten kappaleessa 3.2 mainittiin, kukin kääntöjono operoi kuutiota aina samalla tavalla riippumatta kombinaatiosta. Tämä antaa aihetta kysyä, jakaako kääntöjonojen joukko $\langle S \rangle$ kombinaatioiden joukon $\mathcal{K}$ pistevieraisiin ratoihin?

Lause 3.4.2. [2]. *(Kääntöjonolause) Olkoon* $f \in (\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8)$. *Tällöin järjestelyä* f *vastaa jokin kääntöjono, jos ja vain jos:*

1) Permutaatiot σ_f *ja* ρ_f *voidaan esittää* 2*-syklien tuloina siten, että esityksissä on yhteensä parillinen määrä* 2*-syklejä.*

2) Järjestely f *kääntää yhtä monta kulmapalaa 120 astetta myötäpäivään ja vastapäivään (modulo 3).*

3) Järjestely f *kääntää parillisen määrän reunapaloja.*

Todistus. ($\Rightarrow$) Olkoon f sellainen kääntöjono, että f saattaa ratkaistun kuution tilaan $(\omega_f, \sigma_f, \nu_f, \rho_f)$.

1) Koska järjestelyä f vastaa jokin kääntöjono, niin Lauseen 3.4.1 nojalla $\text{sgn}(\sigma_f) = \text{sgn}(\rho_f)$. Tällöin σ_f ja ρ_f voidaan esittää 2-syklien tulona siten, että molemmissa esityksissä on joko parillinen tai pariton määrä 2-syklejä. Tällöin 2-syklejä on yhteensä parillinen määrä. Näin ollen ehto 1) on voimassa.

2) Koska järjestelyä f vastaa jokin kääntöjono, niin sen tuottama kombinaatio on ratkeava. Tällöin Lauseen 3.4.1 nojalla kulmapalojen orientaatiotilojen summa on 0 (*mod* 3). Siis ehto 2) on voimassa kaikilla joukon $\langle S \rangle$ alkioilla, eli kaikilla kääntöjonoilla.

3) Koska järjestelyä f vastaa jokin kääntöjono, niin sen tuottama kombinaatio on ratkeava. Tällöin Lauseen 3.4.1 nojalla f säilyttää reunapalojen orientaatiosumman. Tällöin f tekee muutoksen (+1) parilliseen määrään paloja. Siis ehto 3) on voimassa.

($\Leftarrow$) Oletetaan, että ehdot 1)-3) ovat voimassa, ja että kuutio oli alussa ratkaistu. Siis kuutioon tehdään sellainen järjestely f, joka toteuttaa ehdot 1)-3). Tällöin järjestelylle f on voimassa

$$\text{sgn}(\sigma_f) = \text{sgn}(\rho_f),\ \sum \nu_{f,i} \equiv 0\ (mod\ 3) \text{ ja } \sum \omega_{f,i} \equiv 0\ (mod\ 2).$$

Lauseen 3.4.1 nojalla kombinaatio r_f on ratkeava, jolloin Lemman 3.2.3 nojalla on olemassa sellainen kääntöjono $M \in [f]$, että M saattaa kuution ratkaistusta tilasta kombinaatioon r_f. Siten järjestelyä f vastaa kääntöjono M.

□

Kääntöjonolauseen nojalla suoritettaessa mikä tahansa kääntöjono f kombinaatioon $(\omega, \sigma, \nu, \rho)$, kääntöjono f säilyttää permutaatiotilojen pariteettien tulon $\operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)$ ja sekä reuna- että kulmapalojen orientaatiosummat. Näin ollen kääntöjonojen joukko $\langle S \rangle$ muodostaa pistevieraita ratoja joukkoon $\mathcal{K}$ siten, että kussakin radassa edellämainitut kolme ominaisuutta ovat kaikilla radan alkioilla samat. Näin radan määritelmän nojalla voidaan jokaisesta radasta valita edustaja, joiden avulla ratoja voidaan vertailla keskenään. Valitaan ratkeavan radan edustajaksi ratkaistu kuutio e.

Lauseen 3.4.1 nojalla kahdeksasta kulmapalasta seitsemän voidaan asettaa mihin orientaatiotilaan tahansa. Tällöin kahdeksas orientaatiotila määräytyy seitsemän edellisen perusteella, sillä orientaatiosumman on oltava nolla modulo 3. Siten vain yksi kolmesta vaihtoehdosta käy.

Vastaavasti 12 reunapalasta 11 voidaan asettaa kumpaan orientaatiotilaan tahansa, jolloin 12. reunapala määräytyy 11 edellisen perusteella, sillä orientaatiosumman on oltava nolla modulo 2. Siten vain toinen kahdesta vaihtoehdosta käy.

Tämä tarkoittaa sitä, että ryhmä $\mathcal{K} = (\mathbb{Z}_2^{12} \wr S_{12}) \times (\mathbb{Z}_3^8 \wr S_8)$ menettää yhden vapausasteen molemmista orientaatiotilojen joukoista $\mathbb{Z}_2^{12}$ ja $\mathbb{Z}_3^8$. Tällöin Lauseen 3.4.1 mukaiset orientaatiotiloja kuvaavat joukot ovat

$$\{(\omega_1, \omega_2, \ldots, \omega_{11}, 2{-_2}\sum_{i=1}^{11} \omega_i) \in \mathbb{Z}_2^{12}\} \subset \mathbb{Z}_2^{12} \text{ ja } \{(\nu_1, \nu_2, \ldots, \nu_7, 3{-_3}\sum_{j=1}^{7} \nu_j) \in \mathbb{Z}_3^8\} \subset \mathbb{Z}_3^8.$$

Merkitään

$$\{(\omega_1, \omega_2, \ldots, \omega_{11}, 2{-_2}\sum_{i=1}^{11} \omega_i) \in \mathbb{Z}_2^{12}\} = Z_2^{11} \text{ ja } \{(\nu_1, \nu_2, \ldots, \nu_7, 3{-_3}\sum_{j=1}^{7} \nu_j) \in \mathbb{Z}_3^8\} = Z_3^7.$$

Lemma 3.4.3. *$Z_2^{11} \leqslant \mathbb{Z}_2^{12}$ ja $Z_3^7 \leqslant \mathbb{Z}_3^8$.*

Todistus. Olkoon $\omega, \pi \in Z_2^{11}$ ja $\nu, \mu \in Z_3^7$. Tällöin

$$\begin{aligned} \omega +_2 \pi &= (\omega_1, \ldots, \omega_{11}, \omega_{12}) +_2 (\pi_1, \ldots, \pi_{11}, \pi_{12}) \\ &= (\omega_1 +_2 \pi_1, \ldots, \omega_{11} +_2 \pi_{11}, \omega_{12} +_2 \pi_{12}) \end{aligned}$$

ja

$$\begin{aligned} \nu +_3 \mu &= (\nu_1, \ldots, \nu_7, \nu_8) +_3 (\mu_1, \ldots, \mu_7, \mu_8) \\ &= (\nu_1 +_3 \mu_1, \ldots, \nu_7 +_3 \mu_7, \nu_8 +_3 \mu_8), \end{aligned}$$

missä

$$\begin{aligned}\omega_{12} +_2 \pi_{12} &= (2 -_2 \sum_{i=1}^{11} \omega_i) +_2 (2 -_2 \sum_{i=1}^{11} \pi_i) \\ &= 4 -_2 (\sum_{i=1}^{11} \omega_i +_2 \sum_{i=1}^{11} \pi_i) \\ &\equiv 2 -_2 \sum_{i=1}^{11} (\omega_i +_2 \pi_i)\end{aligned}$$

ja

$$\begin{aligned}\nu_8 +_3 \mu_8 &= (3 -_3 \sum_{i=1}^{7} \nu_i) +_3 (3 -_3 \sum_{i=1}^{7} \mu_i) \\ &= 6 -_3 (\sum_{i=1}^{7} \nu_i +_3 \sum_{i=1}^{7} \mu_i) \\ &\equiv 3 -_3 \sum_{i=1}^{7} (\nu_i +_3 \mu_i).\end{aligned}$$

Lisäksi, koska summattavien alkioiden orientaatiosummat ovat nolla, niin myös summa-alkioiden orientaatiosummat ovat nollia. Siten $\omega +_2 \pi \in Z_2^{11}$ ja $\nu +_3 \mu \in Z_3^7$. Näin ollen Lauseen 1.1.9 nojalla $Z_2^{11} \leqslant \mathbb{Z}_2^{12}$ ja $Z_3^7 \leqslant \mathbb{Z}_3^8$.

□

Lemma 3.4.4. *$Z_2^{11} \cong \mathbb{Z}_2^{11}$ ja $Z_3^7 \cong \mathbb{Z}_3^7$.*

Todistus. Merkitään $2 -_2 \sum_{i=1}^{11} \omega_i = \omega_{12}$ ja $3 -_3 \sum_{j=1}^{7} \nu_j = \nu_8$. Olkoon

$$F : Z_2^{11} \longrightarrow \mathbb{Z}_2^{11},\ F(\omega_1, \ldots, \omega_{11}, \omega_{12}) = (\omega_1, \ldots, \omega_{11}).$$

Tällöin, jos $\omega, \pi \in Z_2^{11}$, niin

$$\begin{aligned}F(\omega +_2 \pi) &= F((\omega_1, \ldots, \omega_{11}, \omega_{12}) +_2 (\pi_1, \ldots, \pi_{11}, \pi_{12})) \\ &= F(\omega_1 +_2 \pi_1, \ldots, \omega_{11} +_2 \pi_{11}, \omega_{12} +_2 \pi_{12}) \\ &= (\omega_1 +_2 \pi_1, \ldots, \omega_{11} +_2 \pi_{11}) \\ &= (\omega_1, \ldots, \omega_{11}) +_2 (\pi_1, \ldots, \pi_{11}) \\ &= F(\omega_1, \ldots, \omega_{11}, \omega_{12}) +_2 F(\pi_1, \ldots, \pi_{11}, \pi_{12}).\end{aligned}$$

Siis F on ryhmähomomorfismi. Lisäksi

$$\begin{aligned}&F(\omega) = F(\pi) \\ &\Rightarrow \omega_i = \pi_i \text{ kaikilla } 1 \leq i \leq 11 \\ &\Rightarrow 2 -_2 \sum_{i=1}^{11} \omega_i = 2 -_2 \sum_{i=1}^{11} \pi_i \\ &\Rightarrow \omega_{12} = \pi_{12} \\ &\Rightarrow \omega = \pi.\end{aligned}$$

Siis F on injektio. Jos $\omega = (\omega_1, \ldots, \omega_{11}) \in \mathbb{Z}_2^{11}$, niin $\omega = F(\omega_1, \ldots, \omega_{11}, 2 -_2 \sum_{i=1}^{11} \omega_i)$, missä $(\omega_1, \ldots, \omega_{11}, 2 -_2 \sum_{i=1}^{11} \omega_i) \in Z_2^{11}$. Siis F on surjektio. Näin ollen F on isomorfismi ja $Z_2^{11} \cong \mathbb{Z}_2^{11}$.

Käyttäen kuvausta

$$G : Z_3^7 \longrightarrow \mathbb{Z}_3^7,\ G(\nu_1, \ldots, \nu_7, \nu_8) = (\nu_1, \ldots, \nu_7)$$

voidaan osoittaa edellisen kanssa täysin analogisesti, että $Z_3^7 \cong \mathbb{Z}_3^7$. □

Nyt tiedetään, että $|Z_2^{11}| = |\mathbb{Z}_2^{11}| = 2^{11}$ ja $|Z_3^7| = |\mathbb{Z}_3^7| = 3^7$. Lemman 3.4.3 mukaan ryhmät Z_2^{11} ja Z_3^7 ovat suljettuja suoran tulon yhteenlaskun suhteen. Osoitetaan, että ryhmät ovat suljettuja yhteenlaskun suhteen myös silloin, kun monikkoja on permutoitu niiden alkioiden indeksien suhteen. Toisin sanoen, on osoitettava, että

$$\omega.\sigma \in Z_2^{11} \text{ kaikilla } \omega \in Z_2^{11}, \sigma \in S_{12} \text{ ja että } \nu.\rho \in Z_3^7 \text{ kaikilla } \nu \in Z_3^7, \rho \in S_8,$$

missä (.) merkitsee Määritelmän 2.2.2 kuvauksen ψ mukaista indeksipermutaatiota.

Lemma 3.4.5. *Ryhmät Z_2^{11} ja Z_3^7 ovat suljettuja indeksipermutaation suhteen.*

Todistus. Olkoon $\omega = (\omega_1, \ldots, \omega_{12}) \in Z_2^{11}$ ja $\nu = (\nu_1, \nu_2, \ldots, \nu_8) \in Z_3^7$. Tällöin

$$\sum_{i=1}^{12} \omega_i \equiv 0\ (2) \text{ ja } \sum_{i=1}^{8} \nu_i \equiv 0\ (3).$$

Jos alkioita ω ja ν permutoidaan, eli monikon alkioiden järjestystä vaihdetaan, niin kokonaislukujen yhteenlaskun kommutatiivisuuden nojalla kummankin monikon alkioiden summa säilyy samana, jolloin myös permutoinnin jälkeen pätee

$$\sum_{i=1}^{12} \omega_i' \equiv 0\ (2) \text{ ja } \sum_{i=1}^{8} \nu_i' \equiv 0\ (3),$$

missä ω' ja ν' ovat permutoituja monikkoja. Tästä seuraa, että kummankin monikon viimeinen alkio on edelleen oltava sellainen luku, joka saattaa orientaatiosumman nollaan, kun kaikki muut alkiot on valittu. Tällöin

$$\omega' = (\omega_1', \ldots, \omega_{11}', 2 -_2 \sum_{i=1}^{11} \omega_i') \in Z_2^{11}$$

ja

$$\nu' = (\nu_1', \ldots, \nu_7', 3 -_3 \sum_{i=1}^{7} \nu_i') \in Z_3^8.$$

Siis väite pätee. □

Seuraava tarkastelu on tapauskohtainen perustelu edellisen lemman tulokselle.

Olkoon $\omega = (\omega_1, \ldots, \omega_{11}, 2 -_2 \sum_{i=1}^{11} \omega_i) \in Z_2^{11}$ ja merkitään $S = \sum_{i=1}^{11} \omega_i \ (mod\ 2)$ sekä paikalle i kuvautuvaa alkiota merkitään ω_i'. Reunapaloilla on indeksipermutaatiossa monikon viimeisen alkion suhteen neljä tapausta:

1) $S = 0 \Leftrightarrow \omega_{12} = 0$ ja $0 \mapsto \omega_{12}'$, 2) $S = 0 \Leftrightarrow \omega_{12} = 0$ ja $1 \mapsto \omega_{12}'$,
3) $S = 1 \Leftrightarrow \omega_{12} = 1$ ja $0 \mapsto \omega_{12}'$, 4) $S = 1 \Leftrightarrow \omega_{12} = 1$ ja $1 \mapsto \omega_{12}'$.

Luonnollisesti, kun jokin 11 ensimmäisestä alkiosta kuvautuu paikalle 12, niin paikalla 12 oleva alkio kuvautuu jollekin 11 ensimmäisestä alkiosta. Kootaan tapausten tiedot taulukkoon, jossa $S' = \sum_{i=1}^{11} \omega_i' \ (mod\ 2)$.

Tapaus	S	ω_{12}	S'	ω_{12}'
1)	0	0	0	0
2)	0	0	1	1
3)	1	1	0	0
4)	1	1	1	1

Viimeisessä sarakkeessa on uusi paikan 12 alkio, ja nähdään, että kaikissa tapauksissa $\omega_{12}' = S'$ eli $\omega_{12}' = 2 -_2 S'$, siis indeksipermutaatiolla kuvattu alkio on edelleen muotoa $(\omega_1, \ldots, \omega_{11}, 2 -_2 \sum_{i=1}^{11} \omega_i) \in Z_2^{11}$.

Kulmapaloille voidaan tehdä vastaava päättely. Merkitään $T = \sum_{i=1}^{7} \nu_i \ (mod\ 3)$ ja paikalle i kuvautuvaa alkiota merkitään ν_i'. Kulmapaloilla tapauksia on yhdeksän kappaletta:

1) $T = 0 \Leftrightarrow \nu_8 = 0$ ja $0 \mapsto \nu_8'$, 2) $T = 0 \Leftrightarrow \nu_8 = 0$ ja $1 \mapsto \nu_8'$,
3) $T = 0 \Leftrightarrow \nu_8 = 0$ ja $2 \mapsto \nu_8'$, 4) $T = 1 \Leftrightarrow \nu_8 = 2$ ja $0 \mapsto \nu_8'$.
5) $T = 1 \Leftrightarrow \nu_8 = 2$ ja $1 \mapsto \nu_8'$, 6) $T = 1 \Leftrightarrow \nu_8 = 2$ ja $2 \mapsto \nu_8'$,
7) $T = 2 \Leftrightarrow \nu_8 = 1$ ja $0 \mapsto \nu_8'$, 8) $T = 2 \Leftrightarrow \nu_8 = 1$ ja $1 \mapsto \nu_8'$,
9) $T = 2 \Leftrightarrow \nu_8 = 1$ ja $2 \mapsto \nu_8'$.

Kootaan tapausten tiedot taulukkoon, jossa käytetään edellistä vastaavia merkintöjä.

Tapaus	T	ν_8	T'	ν'_8
1)	0	0	0	0
2)	0	0	2	1
3)	0	0	1	2
4)	1	2	0	0
5)	1	2	2	1
6)	1	2	1	2
7)	2	1	0	0
8)	2	1	2	1
9)	2	1	1	2

Vastaavasti kuin reunapalojen tapauksessa, myös ν' on aina muotoa $(\nu_1, \nu_2, \ldots, \nu_7, 3 -_3 \sum_{i=1}^{7} \nu_i) \in Z_3^7$. Näin ollen väite pätee.

Lemmojen 3.4.3 ja 3.4.5 nojalla $\omega_a.\sigma_b +_2 \omega_b \in Z_2^{11}$ ja $\nu_a.\rho_b +_3 \nu_b \in Z_3^7$ kaikilla $\omega \in Z_2^{11}, \sigma \in S_{12}, \nu \in Z_3^7, \rho \in S_8$, mutta nämä ryhmät eivät voi muodostaa Määritelmän 2.2.2 mukaista kranssituloa, sillä orientaatiotiloja kuvaavat ryhmät eivät ole sopivan muotoisia. Edelliset lemmat mahdollistavat kuitenkin uuden kranssituloa vastaavan rakenteen määrittelyn näille ryhmille. Tämä määritelmä on kehitetty tätä työtä varten, eikä perustu lähteisiin.

Määritelmä 3.4.6. Ryhmien Z_2^{11} ja S_{12} sekä ryhmien Z_3^7 ja S_8 ***suppea kranssitulo*** on rakenne, jossa ryhmä S_{12} toimii ryhmässä Z_2^{11} ja ryhmä S_8 toimii ryhmässä Z_3^7 täsmälleen samalla tavalla kuin Määritelmän 2.2.2 kuvaus ψ. Näin saatu kuvaus on Lemmojen 3.4.3 ja 3.4.5 nojalla hyvin määritelty. Suppeaa kranssituloa merkitään $(Z_2^{11} \wr S_{12})$ ja $(Z_3^7 \wr S_8)$.

Nämä rakenteet ovat suljettuja operaation $(\bullet)$ suhteen, ja perivät osajoukkoina muut ryhmän ominaisuudet ryhmästä $\mathcal{K}$. Näin ollen ryhmää, jossa Lauseen 3.4.1 ehdot 2) ja 3) ovat voimassa, merkitään $\mathcal{R}'$. Siis

$$\begin{aligned}\mathcal{R}' &= \{(\omega, \sigma, \nu, \rho) \in \mathcal{K} \mid \sum \omega_i \equiv 0 \ (mod\ 2), \sum \nu_i \equiv 0 \ (mod\ 3)\} \\ &= (Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8).\end{aligned}$$

Koska suppean kranssitulon $A \wr B$ taustajoukko on karteesinen tulo $A \times B$, niin Lemmojen 1.1.5 ja 3.4.4 nojalla

$$|\mathcal{R}'| = |Z_2^{11} \times S_{12} \times Z_3^7 \times S_8| = |\mathbb{Z}_2^{11}| \cdot |S_{12}| \cdot |\mathbb{Z}_3^7| \cdot |S_8| = 2^{11} \cdot 12! \cdot 3^7 \cdot 8!.$$

Joukko $\mathcal{R}'$ sisältää kaikki sellaiset kombinaatiot, joiden orientaatiosummat ovat nolla, mutta joiden permutaatiotiloja vastaavien permutaatioiden pariteeteilla ei ole rajoituksia. Lauseen 3.4.1 ehdon 1) mukainen rajoite on asetettava, jotta saataisiin ratkeavien kombinaatioiden ryhmä $\mathcal{R}$.

Tarkastellaan kuvausta

$$\Theta : (Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8) \longrightarrow (\{1, -1\}, \cdot), \ \Theta((\omega, \sigma, \nu, \rho)) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\rho).$$

Osoitetaan, että kuvaus Θ on ryhmähomomorfismi.

Lause 3.4.7. *Olkoon*

$$\Theta : (Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8) \longrightarrow (\{1,-1\},\cdot),\ \Theta((\omega,\sigma,\nu,\rho)) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho).$$

Tällöin Θ on ryhmähomomorfismi.

Todistus. Olkoon $(\omega_1,\sigma_1,\nu_1,\rho_1),(\omega_2,\sigma_2,\nu_2,\rho_2) \in \mathcal{R}'$. Tällöin

$$\begin{aligned}\Theta((\omega_1,\sigma_1,\nu_1,\rho_1)) \cdot \Theta((\omega_2,\sigma_2,\nu_2,\rho_2)) &= \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\rho_1)\operatorname{sgn}(\sigma_2)\operatorname{sgn}(\rho_2)\\ &= \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)\operatorname{sgn}(\rho_1)\operatorname{sgn}(\rho_2)\\ &= \operatorname{sgn}(\sigma_1\sigma_2)\operatorname{sgn}(\rho_1\rho_2)\\ &= \Theta(\omega_1.\sigma_2 +_2 \omega_2,\ \sigma_1\sigma_2,\ \nu_1.\rho_2 +_3 \nu_2,\ \rho_1\rho_2)\\ &= \Theta((\omega_1,\sigma_1,\nu_1,\rho_1) \bullet (\omega_2,\sigma_2,\nu_2,\rho_2)).\end{aligned}$$

Siis Θ on ryhmähomomorfismi. □

Koska Lauseen 3.4.1 nojalla ryhmälle $\mathcal{R}$ on oltava $\operatorname{sgn}(\sigma)\operatorname{sgn}(\rho) = 1$, niin pätee $\mathcal{R} \subseteq Ker(\Theta)$. Toisaalta kaikille joukon $Ker(\Theta)$ alkioille pätee $\operatorname{sgn}(\sigma)\operatorname{sgn}(\rho) = 1$, joten $Ker(\Theta) \subseteq \mathcal{R}$. Tällöin $\mathcal{R} = Ker(\Theta)$. Näin ollen homomorfismien peruslauseen ja Lagrangen lauseen nojalla $(Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8)/\mathcal{R} \cong \{1,-1\} \cong \mathbb{Z}_2$ ja

$$|\mathcal{R}| = \frac{|(Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8)|}{|\mathbb{Z}_2|} = \frac{|Z_2^{11}| \cdot |S_{12}| \cdot |Z_3^7| \cdot |S_8|}{2}$$

$$= 2^{10} \cdot 12! \cdot 3^7 \cdot 8! = 43\ 252\ 003\ 274\ 489\ 856\ 000.$$

Ottaen huomioon kaikki Lauseen 3.4.1 ehdot, voidaan Rubikin kuution ryhmä kirjoittaa muodossa

$$\begin{aligned}R &= \{(\omega,\sigma,\nu,\rho) \in \mathcal{K} \mid \operatorname{sgn}(\sigma) = \operatorname{sgn}(\rho),\ \sum \nu_i \equiv 0\ (mod\ 3),\ \sum \omega_i \equiv 0\ (mod\ 2)\}\\ &= \{(\omega,\sigma,\nu,\rho) \in (Z_2^{11} \wr S_{12}) \times (Z_3^7 \wr S_8) \mid \operatorname{sgn}(\sigma) = \operatorname{sgn}(\rho)\},\end{aligned}$$

missä $Z_2^{11} \cong \mathbb{Z}_2^{11}$ ja $Z_3^7 \cong \mathbb{Z}_3^7$.

Huomataan, että

$$\frac{|\mathcal{K}|}{|R|} = \frac{2^{12} \cdot 12! \cdot 3^8 \cdot 8!}{2^{10} \cdot 12! \cdot 3^7 \cdot 8!} = 2^2 \cdot 3 = 12.$$

Kääntöjonolauseen avulla nähdään, että joukko $\langle S \rangle$ todella säilyttää kuution permutaatiotilojen pariteettien tulon sekä orientaatiosummat. Siis ryhmässä $\mathcal{K}$ on 12 joukon $\langle S \rangle$ määräämää pistevierasta rataa, joista yksi on ryhmä $\mathcal{R}$. Seuraavalla sivulla on taulukko radoista ja niiden määrittelevistä ominaisuuksista.

Rata	$\operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)$	$\sum \nu_i \ (mod\ 3)$	$\sum \omega_i \ (mod\ 2)$
$\mathcal{K}_0 = \mathcal{R}$	1	0	0
$\mathcal{K}_1$	1	0	1
$\mathcal{K}_2$	1	1	0
$\mathcal{K}_3$	1	1	1
$\mathcal{K}_4$	1	2	0
$\mathcal{K}_5$	1	2	1
$\mathcal{K}_6$	-1	0	0
$\mathcal{K}_7$	-1	0	1
$\mathcal{K}_8$	-1	1	0
$\mathcal{K}_9$	-1	1	1
$\mathcal{K}_{10}$	-1	2	0
$\mathcal{K}_{11}$	-1	2	1

Esimerkiksi kaikki kombinaatiot, jotka saadaan ratkaistusta kuutiosta kääntämällä vain yksi reunapala, ovat samassa radassa $\mathcal{K}_1$ ja siten saavutettavissa toisistaan kääntöjonoilla. Huomaa, että järjestysten ketjuoperaatio ($\bullet$) ei yleisesti noudata ratojen rajoitteita, sillä radat ovat kääntöjonojen joukon $\langle S \rangle$ määräämiä. Tämä tarkoittaa sitä, että eri ratojen alkioita voidaan operoida keskenään, mutta näin saatu kombinaatio ei välttämättä ole kummankaan alkion radassa. Esimerkiksi, jos $f \in \mathcal{K}_1$ ja $g \in \mathcal{K}_6$, niin $f \bullet g \in \mathcal{K}_7$.

Radoista vain $\mathcal{R}$ on aliryhmä operaation ($\bullet$) suhteen, sillä vain se sisältää neutraalialkion eli ratkaistun kuution.

Vaikka erilaisia ratkeavia kombinaatioita on noin $4,3 \cdot 10^{19}$ kappaletta, jokaiseen näistä voi päästä ratkaistusta kuutiosta korkeintaan 20 käännöllä. Tämän todistivat Tomas Rokicki, Herbert Kociemba, Morley Davidson ja John Dethridge tietokoneen avulla vuonna 2010 [7]. Eräs 20 kääntöä vaativa ratkeava kombinaatio on niin sanottu superkääntö, joka kääntää kaikki reunapalat, mutta ei siirrä yhtään palaa. Superkääntö voidaan suorittaa esimerkiksi kääntöjonolla

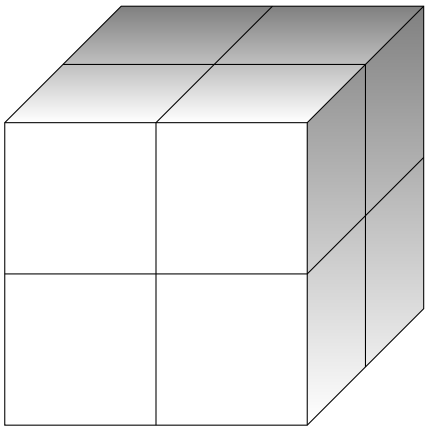
$$U\ R^2\ F\ B\ R\ B^2\ R\ U^2\ L\ B^2\ R\ U^{-1}\ D^{-1}\ R^2\ F\ R^{-1}\ L\ B^2\ U^2\ F^2.$$

4 2x2x2-kuutio

2x2x2-kuutio on eräs Rubikin kuution kanssa täysin saman periaatteen omaava pulmapeli, mutta se koostuu vain kahdeksasta palasta, joista kaikki ovat kulmapaloja. Lisäksi kuution väriteema on sama kuin Rubikin kuution.

2x2x2-kuutiota voidaan lähestyä täsmälleen samalla tavalla kuin tavallista Rubikin kuutiota. Kappaleen 3.1 määritelmiä käyttäen, 2x2x2-kuution järjestys koostuu vain kulmapalojen permutaatio- ja orientaatiotiloista. Tällöin kranssitulon määritelmän nojalla 2x2x2-kuution yleinen ryhmä

$$\mathcal{X} = \mathbb{Z}_3^8 \wr S_8.$$



Kuva 5: 2x2x2-kuutio

2x2x2-kuution orientaatiomerkit asetetaan siten, että jokaisessa palassa on yksi merkki siten, että ratkaistussa kuutiossa merkit ovat kahdella vastakkaisella sivulla. Esimerkiksi ylä- ja alasivun kaikissa tarroissa on merkki. Tällöin merkit ovat samoilla paikoilla kuin Rubikin kuution kulmapaloissa.

Myös tälle kuutiolle voidaan johtaa ratkeavan kombinaation ehdot. Huomataan, että ehdot eivät kuitenkaan ole täysin samat Rubikin kuution kanssa, vaikka reunapalaehto jätetään huomioimatta.

Määritelmä 4.0.1. Olkoon $\circledcirc : \mathbb{Z}_3^8 \wr S_8 \times \mathbb{Z}_3^8 \wr S_8 \longrightarrow \mathbb{Z}_3^8 \wr S_8$ operaatiota $(\bullet)$ vastaava ketjutusoperaatio. Siis, jos $f, g \in \mathbb{Z}_3^8 \wr S_8$, niin

$$(\nu_f, \rho_f) \circledcirc (\nu_g, \rho_g) = (\nu_f . \rho_g +_3 \nu_g,\ \rho_f \rho_g).$$

Nyt $(\mathcal{X}, \circledcirc)$ voidaan todistaa ryhmäksi täsmälleen samalla tavalla kuin Lauseessa 3.3.3. Siten $\mathcal{X}$ on ryhmä. Huomaa, että kääntöjonojen joukko S toimii 2x2x2-kuutiolle vastaavasti kuin Rubikin kuutiolle. Tästä eteenpäin joukolla S tarkoitetaan 2x2x2-kuution kääntöjen joukkoa.

Lemma 4.0.2. *Jos $\mathcal{K}^k$ on Rubikin kuution yleinen kulmapalojen ryhmä, niin*

$$\mathcal{X} \cong \mathcal{K}^k.$$

Todistus. Olkoon

$$\psi : \mathcal{X} \longrightarrow \{id_{\mathcal{K}^r}\} \times \mathcal{K}^k,$$

missä $id_{\mathcal{K}^r}$ on reunapalojen ryhmän identiteettialkio, eli

$$\psi : \mathbb{Z}_3^8 \wr S_8 \longrightarrow (\{\overline{0}\} \wr \{(1)\}) \times (\mathbb{Z}_3^8 \wr S_8),\ \psi((\nu, \rho)) = (\overline{0}, (1), \nu, \rho).$$

Selvästi $\{id_{\mathcal{K}^r}\} \times \mathcal{K}^k \cong \mathcal{K}^k$ ja ψ on bijektio kulmapalojen kombinaation yksikäsitteisyyden nojalla. Osoitetaan, että ψ on myös ryhmähomomorfismi. Olkoon $f, g \in \mathcal{X}$. Tällöin

$$\begin{aligned}
\psi(f \circledcirc g) &= \psi((\nu_f, \rho_f) \circledcirc (\nu_g, \rho_g)) \\
&= \psi(\nu_f.\rho_g +_3 \nu_g,\ \rho_f\rho_g) \\
&= (\overline{0},\ (1),\ \nu_f.\rho_g +_3 \nu_g,\ \rho_f\rho_g) \\
&= (\overline{0},\ (1),\ \nu_f,\ \rho_f) \bullet (\overline{0},\ (1),\ \nu_g,\ \rho_g) \\
&= \psi(\nu_f, \rho_f) \bullet \psi(\nu_g, \rho_g).
\end{aligned}$$

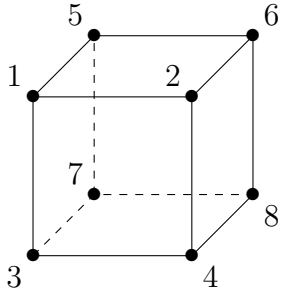
Näin ollen ψ on ryhmäisomorfismi ja siten $\mathcal{X} \cong \mathcal{K}^k$.

□

Koska 2x2x2-kuutiolla ei ole keskuspaloja, niin sillä on symmetrioita. Tämä tarkoittaa sitä, että koko kuution kierto ei muuta 2x2x2-kuution kombinaatiota, mutta kierroilla saatavat kombinaatiot ovat joukon $\mathcal{X}$ eri alkioita. Ajatellaan, että kuutio on ratkaistu. Tällöin jokainen kahdeksasta kulmapalasta voidaan asettaa yläetuoikeaksi palaksi, ja kuutio voi olla näin kolmessa eri asennossa, mutta kuutio on edelleen ratkaistu. Näin ollen 2x2x2-kuutiolla on $8 \cdot 3 = 24$ symmetriaa. Esimerkiksi kääntöjono $R\ L^{-1}$ vastaa kuution kiertämistä 90 astetta siten, että etusivusta tulee uusi yläsivu. Määritellään kuution kiertojen joukko Q.

Määritelmä 4.0.3. Olkoot K_i ja K_j vastakkaisten sivujen käännöt joukossa S. Tällöin ***2x2x2-kuution kiertojen joukko*** $Q = \{K_iK_j^{-1} \in \langle S \rangle\}$. Määritellään lisäksi, että jos $K_i = E$, niin $K_j = E^{-1} = E$.

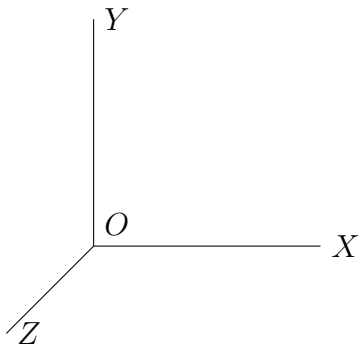
Osoitetaan, että Q generoi kuution kiertosymmetrioiden ryhmän. Merkitään 2x2x2-kuution paloja seuraavasti:



Kuva 6: 2x2x2-kuution palojen indeksointi

Lause 4.0.4. *Olkoon Q kuution kiertojen joukko. Tällöin $\langle Q \rangle$ on ryhmä.*

Todistus. Kuutiota voidaan kiertää kolmen akselin ympäri. Merkitään näitä akseleita kuten kuvassa.



Merkitään kiertoa akselin X suhteen myötäpäivään katsottaessa kuution keskipistettä O akselia X pitkin x, ja vastaavasti y ja z. Tällöin

$$Q = \{(1), x, x^{-1}, y, y^{-1}, z, z^{-1}\},$$

missä

$$\begin{aligned} x &= (1\ 5\ 7\ 3)(2\ 6\ 8\ 4), \\ y &= (1\ 5\ 6\ 2)(3\ 7\ 8\ 4), \\ z &= (1\ 2\ 4\ 3)(5\ 6\ 8\ 7). \end{aligned}$$

Huomataan lisäksi, että $x^3 = x^{-1}, y^3 = y^{-1}, z^3 = z^{-1}$ ja $z = xyx^{-1}$. Nyt

$$Q = \{(1), x, x^{-1}, y, y^{-1}, xyx^{-1}, xy^{-1}x^{-1}\}.$$

Nyt $\langle Q \rangle$ on kaikkien kuution rotaatiosymmetrioiden eli asentojen joukko, sillä kaikki eri asennot saadaan jollakin jonolla akselien X, Y ja Z ympäri tehdyistä kierroista, eli Q generoi kaikki nämä symmetriat. Lisäksi $\langle Q \rangle \subset S_8$. Tällöin jokaista eri asentoa vastaa jokin permutaatio ryhmässä S_8, joka voidaan esittää joukon Q alkioiden tulona.

Nyt S_8 on ryhmä, $\langle Q \rangle \neq \emptyset$ on sen äärellinen osajoukko ja

$$a, b \in \langle Q \rangle \Rightarrow ab \in \langle Q \rangle,$$

jolloin Lauseen 1.1.9 nojalla $\langle Q \rangle \leqslant S_8$.

Siis $\langle Q \rangle$ on ryhmä.

□

Ryhmä $\langle Q \rangle$ voidaan siis esittää kahden alkion, x ja y, generoimana ryhmänä. Koska vastakkaisten sivujen käännöt kommutoivat, niin käyttäen kuvan 6 indeksointia saadaan eksplisiittinen esitys

$$\langle Q \rangle = \langle \{(1\ 5\ 6\ 2)(3\ 7\ 8\ 4),\ (1\ 5\ 7\ 3)(2\ 6\ 8\ 4)\} \rangle \leqslant S_8.$$

Osoitetaan, että ryhmä $\langle Q \rangle$ jakaa ryhmän $\mathcal{X}$ ekvivalenssiluokkiin, joissa kukin alkio saadaan toisistaan kiertämällä kuutiota.

Lause 4.0.5. *Olkoon* $\bowtie$ *sellainen relaatio joukossa* $\mathcal{X}$*, että kaikilla* $a, b \in \mathcal{X}$

$$a \bowtie b \Leftrightarrow a \circledcirc (\nu_q, \rho_q) = b \text{ jollakin } q \in \langle Q \rangle.$$

Tällöin $\bowtie$ *on ekvivalenssirelaatio.*

Todistus. Merkitään $a \circledcirc (\nu_q, \rho_q) = a(\nu_q, \rho_q)$. Nyt

1) $a = a \Leftrightarrow a(\overline{0}, (1)) = a \Leftrightarrow a \bowtie a.$

2) $a \bowtie b \Leftrightarrow a(\nu_q, \rho_q) = b \Leftrightarrow a(\nu_q, \rho_q)((\nu_q +_3 \nu_q).\rho_q^{-1}, \rho_q^{-1}) = b((\nu_q +_3 \nu_q).\rho_q^{-1}, \rho_q^{-1})$
$\Leftrightarrow b((\nu_q +_3 \nu_q).\rho_q^{-1}, \rho_q^{-1}) = a \Leftrightarrow b \bowtie a.$

3) $(a \bowtie b \wedge b \bowtie c) \Leftrightarrow (a(\nu_{q_1}, \rho_{q_1}) = b \wedge b(\nu_{q_2}, \rho_{q_2}) = c) \Leftrightarrow a(\nu_{q_1 q_2}, \rho_{q_1 q_2}) = c$
$\Leftrightarrow a \bowtie c.$

Siis $\bowtie$ on ekvivalenssirelaatio. □

Tällöin Lauseen 4.0.5 nojalla joukko $\mathcal{X}$ jakaantuu ekvivalenssiluokiksi, joissa kussakin on 24 ***kiertoyhtäläistä kombinaatiota*** symmetrioiden lukumäärän mukaisesti.

Lause 4.0.6. *Olkoon* $(\nu, \rho) \in \mathbb{Z}_3^8 \wr S_8 = \mathcal{X}$*. Tällöin pari* (ν, ρ) *vastaa ratkeavaa kombinaatiota jos ja vain jos* $\nu_1 + \nu_2 + ... + \nu_8 \equiv 0 \ (mod\ 3)$.

Todistus. ($\Rightarrow$) Oletetaan, että (ν, ρ) on ratkeava kombinaatio. Tällöin kombinaatiota (ν, ρ) vastaa jokin kääntöjono $f = K_1 K_2 ... K_n \in \langle S \rangle$. Lemman 4.0.2 nojalla kuvan 6 indeksointia käyttäen pätee

K	$\nu(K)$	$\sum \nu_{K,i}\ (mod\ 3)$
F	$(2^1, 1^2, 1^3, 2^4)$	0
B	$(1^5, 2^6, 2^7, 1^8)$	0
L	$(1^1, 2^3, 2^5, 1^7)$	0
R	$(2^2, 1^4, 1^6, 2^8)$	0
U	$\overline{0}$	0
D	$\overline{0}$	0

eli $\nu_1 + \nu_2 + ... + \nu_8 \equiv 0 \ (mod\ 3)$. Tämä tarkoittaa myös sitä, että kääntöjono säilyttää orientaatiosumman.

($\Leftarrow$) Oletetaan seuraavaksi, että ehto $\nu_1 + \nu_2 + ... + \nu_8 \equiv 0 \ (mod\ 3)$ on voimassa kombinaatiolle (ν, ρ). Tällöin $\rho \in S_8$. Olkoon

$$f = U^{-1}\ R\ U\ R^{-1}\ U^{-1}\ F^{-1}\ U^{-1}\ F\ U,$$

jolloin $\rho_f = (1\ 2)$. Vastaavasti kuin Lauseen 3.4.1 ehdon 1) todistuksessa, voidaan vastaavaa menetelmää käyttää tässä tuottamaan kaikki joukon S_8 2-syklit $(i\ j)$, missä $i, j \in \{1, 2, ..., 8\}$ ja $i \neq j$, jolloin nähdään, että kaikki ryhmän S_8 permutaatiot vastaavat ratkeavia permutaatiotiloja. Tämä tapahtuu seuraavasti.

Osoitetaan ensin, että kaikki kuution permutaatiotilat $\rho \in S_8$ ovat ratkeavia, eli että kaikkia permutaatioita $\rho \in S_8$ vastaa jokin kääntöjono. Valitaan mielivaltaiset kulmapalat k_i ja k_j. Alla on listattuna esimerkit kääntöjonoista, jotka siirtävät palan k_i paikalle 1, ja palan k_j paikalle 2 säilyttäen paikan 1.

Siirrettävän palan paikka	$x_1 \in \langle S \rangle$	$x_2 \in \langle \{R, D, B\} \rangle$
1	E	-
2	F^{-1}	E
3	F	$D\ R$
4	F^2	R
5	L	$B\ R^{-1}$
6	U^2	R^{-1}
7	L^2	$D^{-1}\ R^2$
8	$R^2\ U$	R^2

Tällöin, suoritettaessa kääntöjono $x = x_1x_2$ palat k_i ja k_j siirtyvät paikoille 1 ja 2. Siis ρ_x sisältää vaikutuksen $k_i \mapsto 1, k_j \mapsto 2$. Tämän jälkeen kääntöjono f tekee muutoksen $\rho_f = (1\ 2)$, mutta edellisen nojalla tapahtuu $(k_i\ k_j)$. Lopuksi suoritetaan kääntöjono x^{-1}, jolloin kaikki palat palaavat alkuperäisille paikoille, paitsi palat k_i ja k_j palaavat toistensa alkuperäisille paikoille. Näin ollen permutaatiotilojen kokonaismuutos on $\rho_{xfx^{-1}} = (k_i\ k_j)$.

Siis kuutioon voidaan suorittaa mitä tahansa 2-sykliä ryhmästä S_8 vastaava permutaatiotilan muutos. Mutta Lemman 1.2.10 nojalla mikä tahansa ryhmän S_8 alkio voidaan kirjoittaa näiden 2-syklien tulona, jolloin kaikki ryhmän S_8 alkiot vastaavat jotakin ratkeavaa permutaatiotilaa.

Näin ollen kaikki ryhmän S_8 permutaatiot voidaan samaistaa johonkin kääntöjonoon. Tällöin on olemassa sellainen kääntöjono h, että $\rho\rho_h = (1)$. Tämä tarkoittaa sitä, että palat saadaan tällä kääntöjonolla h ratkaistuille paikoilleen. Voidaan myös sanoa, että permutaatiotiloille ei ole mitään erityistä rajoitetta, toisin kuin Rubikin kuutiossa.

Osoitetaan seuraavaksi, että ehdosta $\nu_1 + \nu_2 + ... + \nu_8 \equiv 0\ (mod\ 3)$ seuraa kombinaation ratkeavuus. Edellisen nojalla tiedetään, että palat saadaan ratkaistuille paikoilleen jollakin kääntöjonolla. Lisäksi tiedetään, että kääntöjonot säilyttävät orientaatiosumman. Käytetään tässä hyväksi Lauseen 3.4.1 ehdon 2) todistusta (alk. s. 42). Koska Lemman 4.0.2 nojalla 2x2x2-kuutio voidaan samaistaa täydellisesti Rubikin kuution kulmapaloiksi, lauseen tämän osan todistus on täsmälleen samanlainen kuin Lauseen 3.4.1 ehdon 2) todistus.

Tällöin kaikki 2x2x2-kuution palat saadaan käännettyä oikein päin, sillä kulmapalojen orientaatiosumma on nolla modulo 3. Tämän jälkeen kuutio on ratkaistu, ja kombinaatio (ν, ρ) on siten ratkeava. □

Lemmasta 4.0.2 ja Lauseesta 4.0.6 seuraa, että 2x2x2-kuutio voidaan täydellisesti samaistaa Rubikin kuution kulmapaloiksi.

Lauseesta 4.0.6 seuraa myös se, että joukko $\langle S \rangle$ jakaa ryhmän $\mathcal{X}$ kolmeen pistevieraaseen rataan $\mathcal{X}_0$, $\mathcal{X}_1$ ja $\mathcal{X}_2$, joista $\mathcal{X}_0$ on ratkeava rata. Radan alaindeksi kertoo kyseisen radan palojen orientaatiosumman arvon. Tämä johtuu siitä, että kaikki käännöt, ja siten myös kaikki kääntöjonot, säilyttävät orientaatiosumman.

Nähdään, että eräs suuri ero Rubikin kuution ja 2x2x2-kuution välillä on se, että 2x2x2-kuutiossa voidaan vaihtaa kahden palan paikkaa, ja kombinaatio on edelleen ratkeava. Lauseen 3.4.1 ehto 1) estää tämän Rubikin kuutiolle.

Luonnollisesti vähemmän paloja omaavassa 2x2x2-kuutiossa on vähemmän ratkeavia kombinaatioita kuin Rubikin kuutiossa. Selvitetään niiden lukumäärä.

Lause 4.0.7. *2x2x2-kuution ratkeavien kombinaatioiden lukumäärä huomioiden kiertoyhtäläiset kombinaatiot on* 3 674 160.

Todistus. Vastaavasti kuin Rubikin kuutiolle, Lemman 1.1.5 nojalla

$$|\mathcal{X}| = |\mathbb{Z}_3^8 \wr S_8| = 3^8 \cdot 8!.$$

Lauseen 4.0.6 nojalla joukko $\mathcal{X}$ menettää yhden vapausasteen joukosta $\mathbb{Z}_3^8$. Tämä tapahtuu samasta syystä kuin Rubikin kuutiossa, kahdeksasta kulmapalasta seitsemän voidaan valita vapaasti, ja kahdeksas täytyy valita siten, että orientaatiosumma on nolla, jotta kombinaatio olisi ratkeava. Kulmapalojen ratkeavien orientaatiotilojen joukkoa vastaa siis joukko

$$Z_3^7 = \{(\nu_1, \nu_2, ..., \nu_7, 3 -_3 \sum_{j=1}^{7} \nu_j) \in \mathbb{Z}_3^8\} \cong \mathbb{Z}_3^7.$$

Näin ollen $|\mathcal{X}_0| = 3^7 \cdot 8!$. Lisäksi Lauseen 4.0.5 nojalla kukin kiertoyhtäläisten kombinaatioiden ekvivalenssiluokka sisältää 24 kombinaatiota. Tällöin saadaan

$$|\mathcal{X}_0/\langle Q \rangle| = \frac{|Z_3^7 \wr S_8|}{24} = \frac{3^7 \cdot 8!}{3 \cdot 8} = 3^6 \cdot 7! = 3\ 674\ 160.$$

□

Siis 2x2x2-kuutiossa on 3 674 160 kappaletta merkityksellisesti erilaista ratkeavaa kombinaatiota.

Lähdeluettelo

[1] Bergvall, Olof; Hedberg, Mikael; Hynning, Elin; Masawe, Patrick; Mickelin, Joel: **On Rubik's Cube**, Kuninkaallinen teknillinen korkeakoulu, Ruotsi, 2010.

[2] Daniels, Lindsey: **Group Theory and the Rubik's Cube**, Lakehead University, Kanada, 2014.

[3] Joyner, David: **Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys**, 2008.

[4] Kauppi, Jukka: **80043A Algebra II Markku Niemenmaan luentojen pohjalta**, Matemaattisten tieteiden laitos, Oulun yliopisto, 2008.

[5] Mulholland, Jamie: **Permutation Puzzles: A Mathematical Perspective**, Simon Fraser University, 2016. (Kuva 3.)

[6] Myllylä, Kari; Niemenmaa, Markku; Tirilä, Juha-Matti; Torvikoski, Antti; Törmä, Topi: **802354A Lukuteoria ja ryhmät, luentorunko**, 2015.

[7] Rokicki, Tomas: **God's Number is 20**, http://cube20.org, 2014.