

### 3.4 Alternoivat ryhmät

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Näin ollen  $\sigma$  voidaan kirjoittaa 3-syklien tulona. □

## 4 Konjugointi

### 4.1 Konjugoinnin määritelmä

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

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

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

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

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

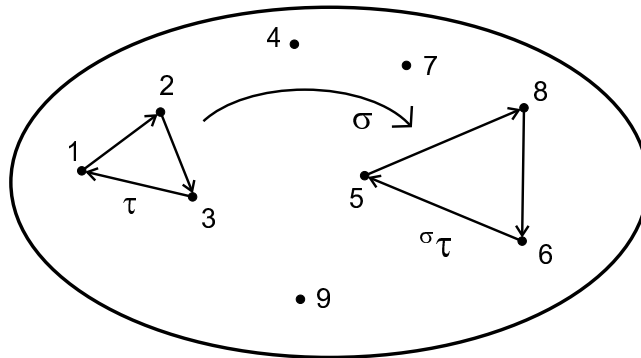
on *joukon  $X$  konjugaattijoukko*.

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

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

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

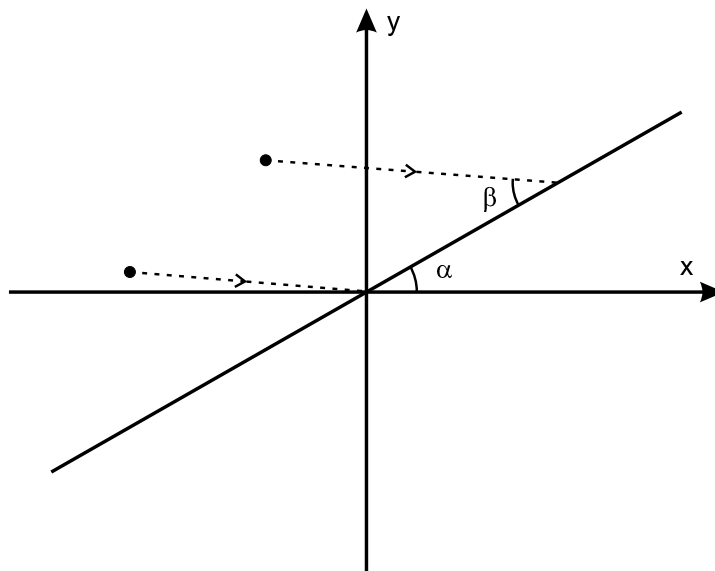
Esimerkin 3-sykli saatiin siis konjugoimalla siirrettyksi toimimaan lukujen 1, 2 ja 3 sijasta luvuilla 5, 8 ja 6.



Kuva 10: Syklin siirto konjugoimalla

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

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



Kuva 11: Projisointikuvaus

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

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

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

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

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

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

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

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

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

Mikäli ryhmän alkiot nimittäin toimivat jossain joukossa, niiden konjugointi siirtää kyseisen toiminnan johonkin toisaalle samassa joukossa. Jos nyt pätee  $\sigma_\tau = \tau$ , tämä tarkoittaa sitä, että alkio  $\tau$  toimii *jo alun perinkin* siellä, mihin  $\sigma$

sen toiminnan siirtää. Vaihdannaisen ryhmän jokaisen alkion toiminta ulottuu siis joka puolelle joukkoa, eikä konjugointia siksi tarvita mihinkään. Tämä nähdään hyvin esimerkin ryhmässä  $T$ , sillä jokainen  $T$ :n alkio siirtää kaikkia kokonaislukuja samalla tavalla, ja siksi alkion konjugoiminen on tarpeetonta.

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

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

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

## 4.2 Konjugointi permutaatioryhmissä

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

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

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

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

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

*Todistus.* Merkitään väitteessä esiintyvää tuloa

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

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

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

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

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

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

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

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

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

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

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

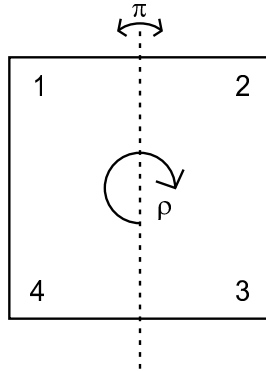
$${}^\sigma\tau = (x_2 x_1 x_3 \dots x_n).$$

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

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

**Esimerkki 4.9.** Tarkastellaan ryhmän  $S_4$  aliryhmää

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



Kuva 12: Neliön kierto ja peilaus

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

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

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

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

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

Alkiot  $\rho$  ja  $\pi$  siis virittävät neliön symmetriaryhmän.

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

$$\pi(1234) = (1432),$$

joten yhden konjugaattiluokan muodostavat 4-syklit  $(1234)$  ja  $(1423)$ . Konjugoinnilla on tässä erityinen geometrinen merkitys. Kun neliöön käytetään peilausta, neliö ikään kuin kääntyy nurin päin, taustapuoli eteen. Tällöin neljänneskierto myötä-



päivään muuttuukin alkuperäisessä neliössä neljänneskierroksi vastapäivään. Sama toimii millä tahansa peilauksella, ja kaikki nämä tuottavatkin saman konjugaatin.

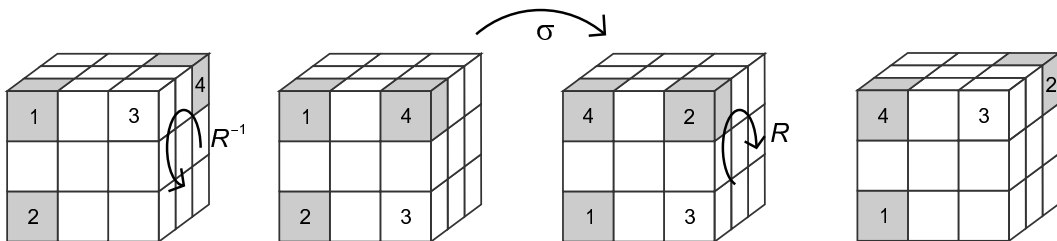
Pystypeilaus  $(12)(34)$  taas voidaan muuttaa vaakapeilaukseksi  $(14)(23)$  kiertämällä neliötä ensin neljänneskierroksen verran. Niinpä  ${}^{\rho}(12)(34) = (14)(23)$ . Myös diagonaali-peilaukset  $(24)$  ja  $(13)$  toimivat tässä konjugoivina alkioina. Samalla tavoin nähdään vielä, että esimerkiksi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

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

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

### 4.3 Konjugointi Rubikin ryhmässä

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



Kuva 13: Opitun siirron konjugointi