4 Konjugointi

4.1 Konjugoinnin määritelmä

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

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

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

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

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

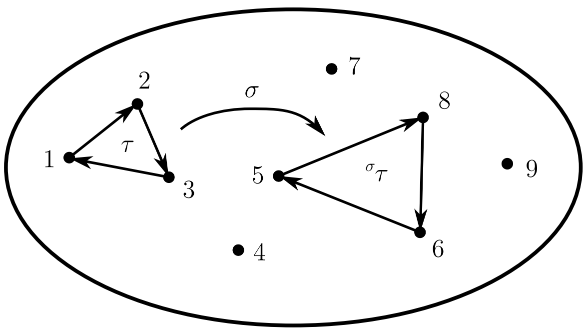
on joukon X *konjugaattijoukko*.

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

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

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

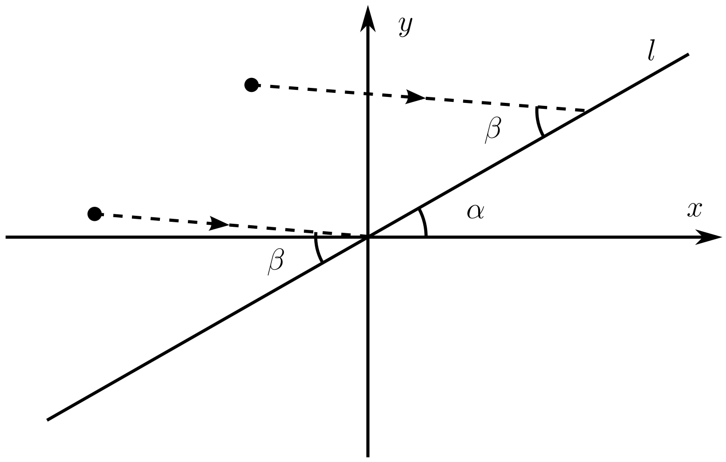
Konjugointi siirsi siis syklin τ toimimaan lukujen 1, 2 ja 3 sijasta luvuilla 5, 8 ja 6.



Kuva 11: Syklin siirto konjugoimalla.

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

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



Kuva 12: Projektiokuvaus.

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

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

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

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

Nyt siis alkuperäinen lineaarikuvaus on saadun diagonaalimatriisin konjugaatti:

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

Kuvauksen L matriisi voitaisiin helposti laskea tästä yhtälöstä.

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

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

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

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

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

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

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

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

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

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

4.2 Konjugointi permutaatioryhmissä

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

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

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

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

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

Todistus. Merkitään väitteessä esiintyvää tuloa

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

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

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

Oletetaan sitten, että x esiintyy τ:n sykliesityksessä. Järjestämällä syklit tarvittaessa uudelleen voidaan olettaa, että $x = x_{1,1}$. Kun 1-syklit on jätetty pois, nähdään, että

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

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

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

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

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

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

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

Esimerkki 4.8. Valitaan jokin n-sykli $\tau = (x_1\ x_2\ \ldots\ x_n)$ ryhmästä S_n, missä $n > 3$. Tämä n-sykli virittää aliryhmän $H = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}\}$. 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 lauseen 4.6 mukaan

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

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

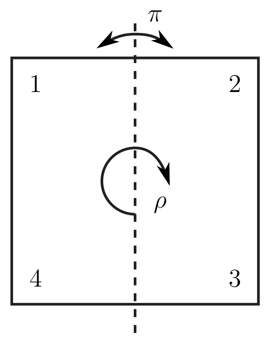
Tässä oletus $n > 3$ on välttämätön, sillä ryhmässä S_3 aliryhmä $\langle(123)\rangle = A_n$ on normaali.

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

Esimerkki 4.9. Tarkastellaan ryhmän S_4 aliryhmää

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

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



Kuva 13: Neliön kierto ja peilaus.

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

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

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

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

Alkiot ρ ja π siis virittävät neliön symmetriaryhmän.

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

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

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

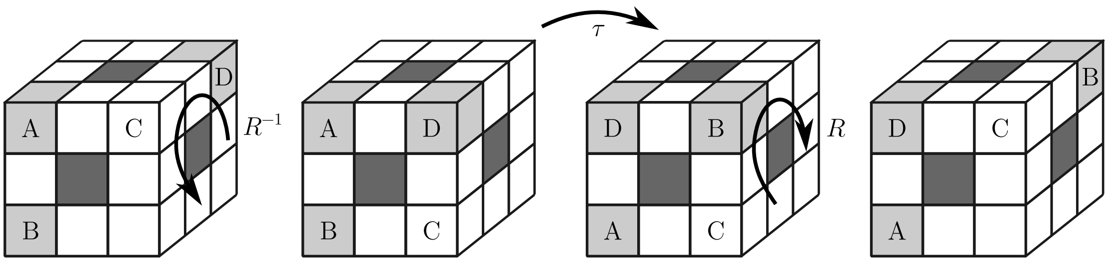
Pystypeilaus (12)(34) taas voidaan muuttaa vaakapeilaukseksi (14)(23) kiertämällä neliötä ensin neljänneskierroksen verran. Niinpä $^{\rho}(12)(34) = (14)(23)$. Myös diagonaalipeilaukset (24) ja (13) toimivat tässä konjugoivina alkioina. Samalla tavoin nähdään vielä, että esimerkiksi $^{\rho}(13) = (24)$.

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

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

4.3 Konjugointi Rubikin ryhmässä

Konjugointi auttaa Rubikin kuution ratkaisussa merkittävästi, sillä sen avulla voidaan opittu siirtosarja siirtää kuution toiseen osaan. Oletetaan esimerkiksi, että halutaan suorittaa paikkaryhmässä $\mathbb{R}_p$ luvussa 3.3 esitetyn syklin asemesta kuvan 14 mukainen 3-sykli, joka liikuttaa paloja A, B ja D. Tällöin voidaan ensin suorittaa perussiirto R^{-1}, joka tuo palan D palan C paikalle (ja liikuttaa toki samalla muitakin paloja). Tämän jälkeen suoritetaan aiemmin opittu 3-sykli τ ja lopuksi palautetaan pala C paikalleen perussiirrolla R. On siis suoritettu konjugaattisiirto ${}^{R}\tau$. Aiemman teoreettisen tarkastelun perusteella tiedetään, että kyseinen konjugaatti todella on 3-sykli eikä liikuta muita kuin haluttuja paloja.



Kuva 14: Opitun siirron konjugointi.

Jotta kaikki nurkkapalat saataisiin paikoilleen tunnettua 3-sykliä ja sen konjugaatteja soveltamalla, täytyisi kahden ehdon täyttyä: ensinnäkin nurkkapalojen permutaation pitäisi aina olla parillinen. Tämä johtuu siitä, että 3-syklit ja niiden tulot ovat parillisia. Toiseksi kaikkien konjugointiin tarvittavien permutaatioiden pitäisi olla laillisia siirtoja.

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

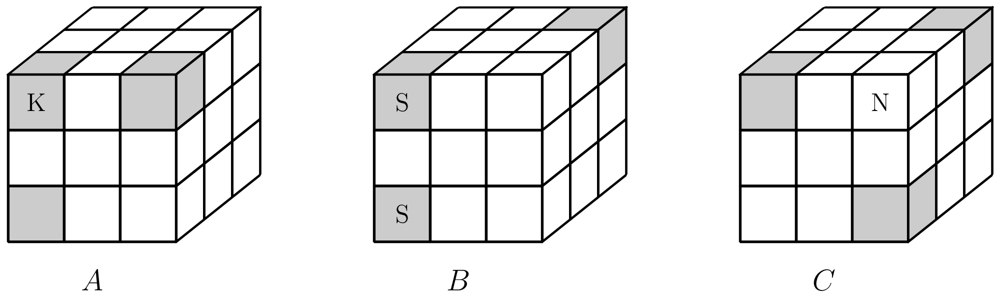
Käydään nyt läpi kaikki mahdolliset kolmen nurkkapalan kombinaatiot ja osoitetaan, että näistä jokaista kohti löytyy permutaatio σ, joka vie tunnettuun 3-sykliin τ osallistuvat palat noiden kolmen nurkkapalan paikalle. Tällöin voidaan mikä tahansa 3-sykli suorittaa konjugaattina ${}^{\sigma}\tau$.

Lasketaan ensin, kuinka monta erilaista kolmen nurkkapalan kombinaatiota kuutiosta yhteensä löytyy. Koska nurkkapaloja on yhteensä kahdeksan, lukumäärä on $\binom{8}{3} = 56$. Nämä kombinaatiot jakautuvat kolmeen joukkoon A, B ja C, jotka näkyvät kuvassa 15. Jokaisen joukon sisällä kombinaatiot saadaan johonkin kuvan kolmesta asennosta koko kuutiota kiertämällä.

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

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

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



Kuva 15: Kolmen nurkkapalan kombinaatiot.

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

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

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

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

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

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

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

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

1. Saatetaan koko kuutiota kiertämällä kuutio johonkin kuvan 15 kolmesta asemasta, minkä jälkeen nimetään siirrot uudestaan niin, että kuvan ylätahkon kiertäminen on U, etutahkon kiertäminen F jne.

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

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

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

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

Käytännössä vaiheiden 2A, 2B ja 2C konjugointeja ei tarvitse muistaa ulkoa vaan niiden sijaan voi keksiä kuhunkin tilanteeseen sopivan konjugointisiirron.

4.4 Ryhmän keskus

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

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

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

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

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

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

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

Vaikka keskittäjän määritelmä on annettu siinä muodossa, että sen alkioilla konjugoiminen ei vaikuta alkioon x, voidaan sama ajatella myös niin, että x:llä konjugoiminen ei vaikuta keskittäjän alkioihin. Tämä nähdään seuraavasta:

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

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

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

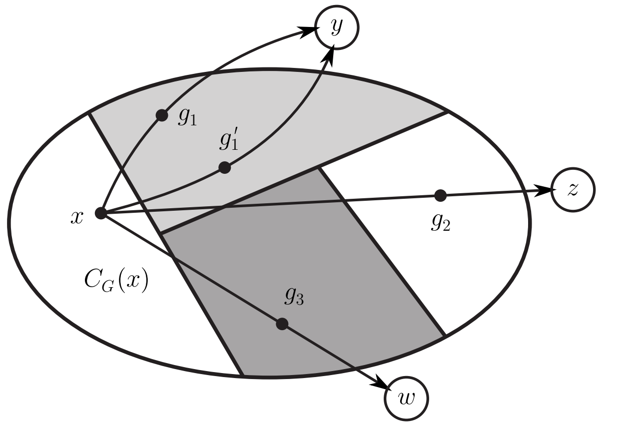
Lause 4.12. *Olkoon G äärellinen ryhmä ja olkoon $x \in G$. Keskittäjän $C_G(x)$ sivuluokkien lukumäärä $[G : C_G(x)]$ on sama kuin alkion x konjugaattiluokan koko.*

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

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

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

Oheisessa kuvassa on havainnollistettu keskittäjäaliryhmän ja konjugaattiluokan suhdetta. Alkion x konjugaattiluokka on neljän alkion joukko $\{x, y, z, w\}$. Saman alkion keskittäjällä puolestaan on neljä sivuluokkaa $C_G(x)$, $g_1C_G(x)$, $g_2C_G(x)$ ja $g_3C_G(x)$. Kustakin eri sivuluokasta otettu alkio tuottaa eri konjugaatin, esimerkiksi ${}^{g_1}x = y$, toisaalta saman sivuluokan alkiot tuottavat aina saman konjugaatin. Huomaa, että konjugaatin sijaintia ryhmässä ei tunneta; ei esimerkiksi päde välttämättä $y \in g_1C_G(x)$.



Kuva 16: Keskittäjän sivuluokat ja konjugaatit.

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

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

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

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

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

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

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

Todistetun lauseen seurauksena saadaan nk. *luokkayhtälö*. Numeroidaan äärellisen ryhmän G konjugaattiluokat $A_1, A_2, \ldots, A_m$ ja valitaan jokaisesta luokasta edustaja $x_i \in A_i$. Koska konjugaattiluokan A_i koko on edellisen lauseen mukaan $[G : C_G(x_i)]$ ja konjugaattiluokat muodostavat toisaalta koko ryhmän osituksen, pätee yhtälö

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

Tätä yhtälöä nimitetään luokkayhtälöksi.

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

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

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

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

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

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

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

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

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

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

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

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