3. Symmetriaryhmiä

Symmetrioita käytetään usein helpottamaan monimutkaiseen struktuuriin liittyviä ongelmia. Symmetriaryhmät koostuvat permutaatioista, jotka säilyttävät jonkin tietyn rakenteen. Tällainen yleinen määritelmä voi oikeastaan kuvata mitä tahansa ryhmää (kaikki ryhmät ovat isomorfisia jonkin permutaatioryhmän kanssa), ja joskus sanotaankin, että ryhmäteoria on nimenomaan symmetrioiden tutkimista. Lisäksi se, mitä rakennetta symmetrioiden sallitaan muuttaa, vaihtelee hyvin paljon. Esimerkiksi neliön symmetriaryhmään lasketaan sellaisetkin permutaatiot, jotka peilaavat neliön jonkin lävistäjän suhteen, vaikka tällaista muunnosta varten neliö täytyy "nostaa tasosta irti" ja kääntää ympäri.[7] Sen sijaan kuution symmetriaryhmään ei lasketa muita kuin kolmiulotteisessa avaruudessa tapahtuvia kiertoja; kuutiota ei saa peilata poikkileikkaavan tason suhteen, niin että etusivu ja takasivu vaihtuisivat päittäin.

Tässä luvussa tarkastellaan esimerkinomaisesti, mitä symmetrioista saadaan tietää ja mihin niitä voidaan käyttää. Koska symmetriat ovat permutaatioita, aloitetaan tutustumalla tarkemmin permutaatioihin.

3.1. Symmetriset ryhmät ja permutaation etumerkki. Merkitään n ensimmäisen positiivisen kokonaisluvun joukkoa $N_n = \{1, 2, \ldots, n\}$. *Symmetrinen ryhmä* S_n on tämän joukon kaikkien permutaatioiden muodostama ryhmä. Sopivalla alkioiden numeroinnilla voidaan määritellä ryhmän S_n luonnollinen toiminta missä tahansa äärellisessä joukossa $X = \{x_1, \ldots, x_n\}$ kaavalla $\sigma x_n = x_{\sigma(n)}$.

Symmetrisen ryhmän alkioita on yleensä kätevintä merkitä syklien avulla. Jos $a_1, \ldots, a_m$ ovat joukon N_n eri alkioita, niin *m-sykli* $\rho = \begin{pmatrix} a_1 & \ldots & a_m \end{pmatrix}$ on sellainen permutaatio, että

$$\rho(a_i) = \begin{cases} a_{i+1}, & \text{jos } i < m, \\ a_1, & \text{jos } i = m. \end{cases}$$

Muut alkiot ρ pitää paikallaan. On helppo nähdä, että jokainen permutaatio voidaan kirjoittaa erillisten syklien tulona, esimerkiksi

$$S_6 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix} = (12)(3)(465).$$

Tämä esitys on syklien järjestystä sekä kirjoitusasua vaille yksikäsitteinen, esimerkiksi $(123)(45) = (54)(231)$. Usein yhden alkion syklit jätetään merkitsemättä.

Kahden alkion syklejä nimitetään *vaihdoiksi* tai *transpositioiksi.* Jokainen sykli voidaan kirjoittaa vaihtojen tulona, sillä

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}.$$

Tästä seuraa, että mielivaltainen permutaatio voidaan kirjoittaa vaihtojen tulona. Tällainen esitys ei ole millään muotoa yksikäsitteinen, mutta osoittautuu, että saman permutaation esityksessä vaihtojen lukumäärä on aina joko parillinen tai pariton. Tämän osoittamiseksi määritellään ensin permutaation etumerkki.

[7] Tarkemmin sanoen, jos L on peilaus, ei ole olemassa jatkuvasti parametrisoitua tason etäisyydet säilyttävien lineaarikuvausten perhettä (A_t), missä $t \in [0, 1]$ ja $A_0 = \mathrm{id}$, $A_1 = L$. Tämä johtuu siitä, että peilauksen determinantti on -1.

MÄÄRITELMÄ 3.1. Oletetaan, että permutaation $\sigma \in S_n$ esityksessä erillisten syklien tulona on t sykliä (1-syklit mukaanluettuina). Tällöin permutaation σ *etumerkki* on

$$\operatorname{sgn}(\sigma) = (-1)^{n-t}.$$

Määritelmän perusteella esimerkiksi m-syklin etumerkki on 1, jos ja vain jos m on pariton. Vaihdon etumerkki on siis -1. Osoitetaan seuraavaksi, että etumerkkikuvaus on ryhmähomomorfismi.

LEMMA 3.2. *Jos $\beta \in S_n$ ja τ on jokin vaihto, niin* $\operatorname{sgn}(\tau\beta) = -\operatorname{sgn}(\beta)$.

TODISTUS. Merkitään $\tau = (a\ b)$. Olkoon $\rho_1 \cdots \rho_t$ permutaation β esitys erillisten syklien tulona (1-syklit mukana). Jos a ja b esiintyvät samassa syklissä, esim. $\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}$, niin

$$\tau\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k \end{pmatrix} \begin{pmatrix} b & d_1 & \dots & d_l \end{pmatrix}.$$

Tässä tapauksessa permutaatiolla $\tau\beta$ on sykliesitys $(\tau\rho_1)\rho_2 \cdots \rho_t$, jossa on yhteensä $t+1$ sykliä. Etumerkin määritelmän mukaan $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\operatorname{sgn}(\beta)$. Toisaalta, jos a ja b esiintyvät eri sykleissä, esim. $\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k \end{pmatrix}$ ja $\rho_2 = \begin{pmatrix} b & d_1 & \dots & d_l \end{pmatrix}$, niin

$$\tau\rho_1\rho_2 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}.$$

Tällöin permutaation $\tau\beta$ sykliesityksessä on yksi sykli vähemmän kuin β:n esityksessä, joten $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\operatorname{sgn}(\beta)$. □

LAUSE 3.3. *Kaikilla $\alpha, \beta \in S_n$ pätee*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta),$$

eli kuvaus $\operatorname{sgn} : S_n \to (\{1, -1\}, \cdot)$ *on ryhmähomomorfismi.*

TODISTUS. Oletetaan, että α voidaan kirjoittaa vaihtojen tulona $\tau_1 \cdots \tau_m$, missä m on pienin mahdollinen. Käytetään induktiota tulon pituuden m suhteen. Jos $m = 1$, niin α on itse vaihto, jolloin tulos seuraa edellisestä lemmasta. Oletetaan sitten, että $m > 1$ ja väite pätee kaikilla m:ää pienemmillä luvuilla. Nyt $\tau_2 \cdots \tau_m$ on erään permutaation minimaalinen esitys vaihtojen tulona. Jos nimittäin $\tau_2 \cdots \tau_m = \sigma_1 \cdots \sigma_r$, missä $r < m - 1$, niin $\alpha = \tau_1\sigma_1 \cdots \sigma_r$, mikä on ristiriidassa luvun m minimaalisuuden kanssa. Näin ollen edellisestä lemmasta ja induktio-oletuksesta seuraa

$$\begin{aligned} \operatorname{sgn}(\alpha\beta) &= \operatorname{sgn}(\tau_1 \cdots \tau_m\beta) = -\operatorname{sgn}(\tau_2 \cdots \tau_m\beta) \\ &\overset{\text{i.o.}}{=} -\operatorname{sgn}(\tau_2 \cdots \tau_m)\operatorname{sgn}(\beta) \\ &= \operatorname{sgn}(\tau_1 \cdots \tau_m)\operatorname{sgn}(\beta) \\ &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta). \end{aligned}$$

Tämä todistaa induktioaskeleen. □

Yllä olevan lauseen mukaan permutaation etumerkki voidaan selvittää kirjoittamalla permutaatio vaihtojen tulona: etumerkki on 1, jos ja vain jos vaihtojen lukumäärä on parillinen, sillä $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_m) = (-1)^m$. Tällöin permutaatiota kutsutaan *parilliseksi*, muuten *parittomaksi*. Parilliset permutaatiot muodostavat tärkeän normaalin aliryhmän.

Määritelmä 3.4. Etumerkkihomomorfismin ydintä

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \sigma \text{ on parillinen}\}$$

kutsutaan *alternoivaksi ryhmäksi* ja merkitään A_n.

Lause 3.5. *Jos $n \geq 2$, niin $[S_n : A_n] = 2$.*

Todistus. Koska $n \geq 2$, niin vaihto (12) kuuluu ryhmään S_n. Täten sgn on surjektio kahden alkion joukolle $\{1, -1\}$. Homomorfialauseen nojalla löytyy bijektio $S_n/A_n \to \{1, -1\}$. □

3.2. Konjugointi symmetrisessä ryhmässä. Symmetrisessä ryhmässä alkion konjugaatit löydetään helpoiten sykliesityksen avulla. Konjugointi yksinkertaisesti permutoi sykliesityksen symboleja.

Lause 3.6. *Olkoot $\sigma, \tau \in S_n$. Oletetaan, että τ:n esitys erillisten syklien tulona on*

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

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

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

Todistus. Merkitään väitteessä esiintyvää tuloa

$$\tau' = \left(a'_{1,1} \quad \dots \quad a'_{1,k_1}\right) \cdots \left(a'_{m,1} \quad \dots \quad a'_{m,k_m}\right)$$

ja osoitetaan, että $\sigma\tau\sigma^{-1} = \tau'$. Olkoon sitä varten $b \in N_n$ mielivaltainen. Koska σ on bijektio, löydetään jokin $a \in N_n$, jolle $b = a'$. Jos τ pitää a:n paikallaan, niin τ' pitää puolestaan b:n paikallaan. Tällöin $\sigma\tau\sigma^{-1}(b) = \sigma\tau(a) = \sigma(a) = b = \tau'(b)$.

Oletetaan sitten, että a esiintyy jossain syklissä, jonka pituus on suurempi kuin 1. Järjestelemällä syklejä tarvittaessa uudestaan, voidaan valita, että $a = a_{1,1}$. Tällöin pätee

$$\tau\sigma^{-1}(b) = \tau(a) = (a_{1,1} \quad a_{1,2} \quad \dots \quad a_{1,k_1}) \,.\, a_{1,1} = a_{1,2}.$$

Lisäksi nähdään, että $b = a'_{1,1}$, joten

$$\tau'(b) = \left(a'_{1,1} \quad a'_{1,2} \quad \dots \quad a'_{1,k_1}\right) . \, a'_{1,1} = a'_{1,2} = \sigma(a_{1,2}).$$

Saatiin, että mielivaltaisella alkiolla $b \in N_n$ pätee $\tau'(b) = \sigma(a_{1,2}) = \sigma\tau\sigma^{-1}(b)$. Siispä väite on todistettu. □

Symmetrisessä ryhmässä samaan konjugaattiluokkaan kuuluvat siis täsmälleen ne alkiot, joilla on sama *syklityyppi*, eli joiden sykliesityksessä on sama lukumäärä samanpituisia syklejä. Syklityyppiä voidaan merkitä jonolla $(t_1, t_2, \dots, t_m)$, missä $t_1 \geq t_2 \geq \cdots t_m$ ja $\sum_i t_i = n$. Tällaista jonoa nimitetään luvun n ositukseksi. Esimerkiksi permutaation (12)(345)(6) syklityyppi on $(3, 2, 1)$.

Esimerkki 3.7. Tarkastellaan ryhmää S_3, joka koostuu 1-, 2- ja 3-sykleistä. Sen konjugaattiluokat ovat

$$C_1 = \{\mathrm{id}\}, \quad C_2 = \{(12), (23), (13)\} \quad \text{ja} \quad C_3 = \{(123), (132)\}.$$

Ainoastaan konjugaattiluokkien yhdiste voi olla normaali aliryhmä. Toisaalta aliryhmän täytyy aina sisältää neutraalialkio, joten epätriviaaleja normaaleja aliryhmiä voivat olla ainoastaan yhdisteet $C_1 \cup C_2$ ja $C_1 \cup C_3$. Ensimmäisessä on 4 alkiota, joten se ei voi olla aliryhmä, koska $4 \nmid 6$. Jälkimmäinen yhdiste on alternoiva ryhmä A_3, joka on tunnetusti normaali aliryhmä.

Alternoivassa ryhmässä tilanne on monimutkaisempi. Esimerkiksi A_3 on vaihdannainen, mistä seuraa, että sen jokainen konjugaattiluokka on yksiö. Edellisen esimerkin luokka $C_3 \subset A_3$ siis jakautuu A_3:n toiminnassa kahdeksi eri luokaksi. Tämä johtuu siitä, että ainoa alkio, joka konjugoisi alkion (123) alkiolle (132), sattuu olemaan transpositio. Seuraavan lauseen avulla voidaan päätellä, milloin jokin konjugaattiluokka jakautuu siirryttäessä alternoivaan ryhmään. Oletetaan, että alkiolla $\sigma \in S_n$ on esitys $\rho_1 \cdots \rho_m$ erillisten syklien tulona, ja että syklit on järjestetty pituuden mukaan laskevaan järjestykseen.

LAUSE 3.8. *Olkoon K_S alkion σ konjugaattiluokka ryhmässä S_n ja vastaavasti K_A saman alkion konjugaattiluokka ryhmässä A_n. Nyt $K_S \neq K_A$, jos ja vain jos*

$$(*) \qquad \textit{syklien } \rho_i \textit{ pituudet ovat parittomia ja erillisiä.}$$

Tällöin $|K_A| = \frac{1}{2}|K_S|$.

TODISTUS. Tarkastellaan alkion σ keskittäjiä. Merkitään $C_S = C_{S_n}(\sigma)$ ja $C_A = C_{A_n}(\sigma) = C_S \cap A_n$. Koska $C_A \leq C_S$, löytyy Lagrangen lauseen jokin positiivinen kokonaisluku k, jolle $k \cdot |C_A| = |C_S|$. Lauseen 2.11 mukaan taas

$$n! = |C_S| \cdot |K_S| \qquad \text{ja} \qquad \frac{n!}{2} = |C_A| \cdot |K_A|.$$

Näistä yhtälöistä voidaan lopulta päätellä, että $|K_A| = k/2 \cdot |K_S|$. Toisaalta, koska $K_A \subset K_S$, niin k on joko 1 tai 2.

Tarvitsee siis vain todistaa, että ehto $(*)$ pätee, jos ja vain jos $C_A = C_S$. Oletetaan, että $\alpha \in C_S$. Lauseen 3.6 perusteella jokaisella i löytyy jokin sellainen j, että ${}^{\alpha}\rho_i = \rho_j$. Jos ehto $(*)$ pätee, täytyy olla $i = j$, koska syklit ovat eri pituisia ja ne on järjestetty pituuden mukaan. Tällöin $\alpha = \rho_i^k$ jollain k. Koska syklin ρ_i pituus on pariton, sen etumerkki on 1. Edelleen $\mathrm{sgn}(\alpha) = 1$, joten $\alpha \in C_A$.

Oletetaan sitten, että ehto $(*)$ ei päde. Tällöin voidaan löytää sellainen $\alpha \in C_S$, että $\mathrm{sgn}(\alpha) = -1$ (harjoitustehtävä). Näin ollen $C_S \neq C_A$, ja väite on todistettu. □

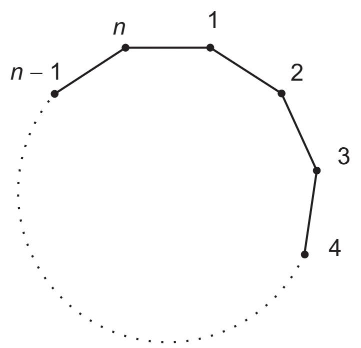
3.3. Diedriryhmät. Tarkastellaan joukosta $N_n = \{1, 2, \ldots, n\}$ muodostettujen järjestämättömien parien joukkoa

$$X = \{\{a, b\} \mid a, b \in N_n,\ a \neq b\}.$$

Määritellään tässä joukossa ryhmän S_n toiminta kaavalla $\sigma.\{a, b\} = \{\sigma(a), \sigma(b)\}$. Joukon X osajoukkoja voidaan ajatella *verkkoina*, joissa solmuina ovat joukon N_n alkiot ja särminä parit $\{a, b\}$. Verkkoa

$$E_n = \{\{1, 2\},\ \{2, 3\},\ \ldots,\ \{n-1, n\},\ \{n, 1\}\}.$$

nimitetään *monikulmioksi*.



KUVA 5. Monikulmio E_n

Etsitään monikulmion E_n vakauttaja G. Tämä koostuu kaikista mahdollisista verkon solmujen permutaatioista, jotka säilyttävät särmärakenteen, joten se on monikulmion symmetriaryhmä. Vakauttaja G toimii nyt vakauttamassaan monikulmiossa samalla tavalla kuin S_n.

Särmän $\{1, n\}$ kiinnittäjä aliryhmän G toiminnassa sisältää kaksi alkiota: identtisen kuvauksen ja *peilauksen*

$$\sigma = (1 \quad n)\,(2 \quad n-1)\ldots(k \quad n-k)\,,$$

missä $k = [n/2]$ (kokonaisosa). Toiminta on selvästi transitiivista, joten lauseen 2.7 perusteella $|G| = |G_{\{1,n\}}||E_n| = 2n$. Etsitään nuo $2n$ symmetriaryhmän alkiota. Sykli $\rho = (1\ 2\ \ldots\ n)$ eli *kierto* on vakauttajassa G, ja sen potensseista saadaan jo n alkiota. Koska mikään kierron positiivinen potenssi ei kiinnitä särmiä, σ ei kuulu aliryhmään $\langle\rho\rangle$, ja täten kyseinen aliryhmä ja sen sivuluokka $\sigma\langle\rho\rangle$ ovat erillisiä. Näistä saadaan jo yhteensä $2n$ alkiota, joten jokainen symmetriaryhmän alkio on joko muotoa ρ^j tai $\sigma\rho^j$ jollain $j \in \{0, 1, \ldots, n-1\}$.

MÄÄRITELMÄ 3.9. *Diedriryhmä*[8] D_{2n} on monikulmion E_n vakauttaja.

Edellä todettiin, että alkiot ρ ja σ virittävät diedriryhmän, ja jokainen diedriryhmän alkio voidaan kirjoittaa muodossa ρ^j tai $\sigma\rho^j$. Suoraviivaisella laskulla nähdään, että

$${}^{\sigma}\rho = (n \quad n-1 \quad \ldots \quad 2 \quad 1) = \rho^{-1},$$

josta sitten seuraa, että ${}^{\sigma}(\rho^j) = \rho^{-j}$. Erityisesti $\rho\sigma = \sigma\rho^{-1}$. Tämän tiedon avulla voidaan rekonstruoida koko ryhmän laskutoimitustaulu, mikä johtaa seuraavaan havaintoon.

LAUSE 3.10. *Jos ryhmän G virittää kaksi alkiota r ja s, joille pätee*

$$r^n = 1, \qquad s^2 = 1 \qquad \text{ja} \qquad srs = r^{-1},$$

niin $G \cong D_{2n}$.

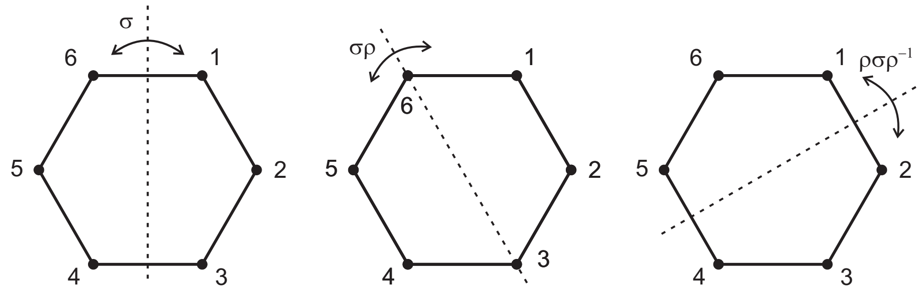
Diedriryhmässä $(\sigma\rho)^2 = \sigma\rho\sigma\rho = \rho^{-1}\rho = \mathrm{id}$, ja toisaalta $\sigma \cdot \sigma\rho = \rho$. Näin ollen diedriryhmän virittää kaksi *involuutiota* eli kertalukua kaksi olevaa alkiota, joiden tulon kertaluku on n. Osoittautuu, että myös tämä ominaisuus karakterisoi diedriryhmän täydellisesti. Seuraavan lauseen todistus sivuutetaan (ks. esim. Rotman: An Introduction to the Theory of Groups).

[8]diedri = kaksitahokas (kr.)

LAUSE 3.11. *Jos ryhmän G virittää kaksi alkiota a ja b, joille pätee*

$$a^2 = 1, \qquad b^2 = 1 \qquad ja \qquad (ab)^n = 1,$$

niin $G \cong D_{2n}$.



KUVA 6. Peilauksia eräässä diedriryhmässä. Huomaa, että peilauksen konjugaatille pätee $\rho\sigma\rho^{-1} = \sigma\rho^{-1}\rho^{-1} = \sigma\rho^{-2}$.

Diedriryhmät ovat säännöllisten monikulmioiden symmetriaryhmiä. Kiinnittämällä säännöllinen monikulmio keskipisteestään tason origoon ja valitsemalla sopivat lineaarikuvaukset kuvaamaan kiertoa ja peilausta, voidaan helposti näyttää, että diedriryhmä on isomorfinen erään äärellisen lineaarikuvausryhmän kanssa. Koska $D_6 = S_3$ (niissä on yhtä monta alkiota), tällä tavoin saadaan jo aiemmin mainittu ryhmän S_3 esitys tason lineaarikuvausten joukkona. Voidaan osoittaa, että sellaisia äärellisiä tason lineaarikuvausten ryhmän aliryhmiä, jotka säilyttävät pisteiden väliset etäisyydet, ovat ainoastaan sykliset ryhmät C_n ja diedriryhmät D_{2n}.

3.4. "Burnsiden" kaava. Esimerkkinä symmetriaryhmien sovelluksista esitetään seuraavassa niin sanottu Burnsiden lemma. William Burnside (1852–1927) oli huomattava brittimatemaatikko, joka loi perustan ryhmäteorian tutkimukselle Englannissa. Hän todisti lukuisia keskeisiä ryhmäteorian lauseita, mutta Burnsiden lemmaksi nimitettävä lause ei itse asiassa kuulu niihin. Burnside esittää kyseisen lemman kirjassaan "The Theory of Groups of Finite Order" mainiten sen löytäjäksi saksalaisen Ferdinand Frobeniuksen, mutta myöhemmistä painoksista lähdeviite on jostain syystä poistettu. Traditioon on sittemmin iskostunut viitata tulokseen Burnsiden lemmana, mutta erityisesti ryhmäteoreetikot tapaavat vitsailla aiheesta kutsuen lausetta "Ei-Burnsiden lemmaksi".

MÄÄRITELMÄ 3.12. Oletetaan, että G toimii joukossa X. Alkion $g \in G$ *kiintopistejoukko* on

$$\mathrm{Fix}(g) = \{x \in X \mid gx = x\}.$$

LAUSE 3.13 (Ratojenlaskentalause eli Burnsiden lemma). *Oletetaan, että G toimii äärellisessä joukossa G. Tällöin*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)|.$$

Todistus. Se lukumäärä, kuinka monta kertaa jokin tietty $x \in X$ luetellaan summassa $\sum_g |\operatorname{Fix}(g)|$, on täsmälleen $|G_x|$, sillä x on kiintopistejoukossa $\operatorname{Fix}(g)$ jos ja vain jos $g \in G_x$. Täten

$$\sum_{g \in G} |\operatorname{Fix}(g)| = \sum_{x \in X} |G_x|,$$

ja rata-vakauttajalauseen seurauslauseen 2.7 perusteella

$$\sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|Gx|}.$$

Oikeanpuoleisessa summassa tietty termi $1/|Gx|$ luetellaan yhtä monta kertaa, kuin radassa Gx on alkioita. Näistä termeistä koostuva osasumma on selvästi $|Gx| \cdot 1/|Gx| = 1$, ja koska radat muodostavat osituksen, kokonaissummaksi tulee ratojen lukumäärä $|X/G|$. Siispä

$$\sum_{x \in X} |G_x| = |G| \cdot |X/G|,$$

josta väite seuraa. □

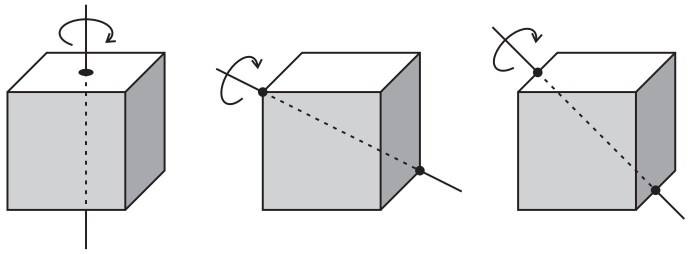
Esimerkki 3.14. Lasketaan, kuinka monella tavalla kuution tahkot voidaan värittää n eri väriä käyttämällä. Väritykset lasketaan samaksi, jos ne saadaan toisistaan kuutiota kiertämällä.

Värityskysymys voidaan formalisoida seuraavasti. Numeroidaan kuution tahkot yhdestä kuuteen ja käytettävät värit yhdestä n:ään. Tällöin jokainen väritys on kuuden alkion jono $(a_1, a_2, a_3, a_4, a_5, a_6)$, missä $a_i \in N_n$ kaikilla i, ja kaikkien väritysten joukko on N_n^6. Kuution symmetriaryhmä G toimii tässä joukossa luonnollisella tavalla: jos $g \in G$ tuottaa kuution tahkojen permutaation $\sigma \in S_6$ ja $a \in N_n^6$ on jokin väritys, niin $(g.a)_i = a_{\sigma(i)}$ kaikilla i.

Kaksi väritystä a ja b samastetaan, jos pätee $g.a = b$ jollain kuution kierrolla $g \in G$. Tämä tarkoittaa sitä, että a ja b kuuluvat samaan rataan. Kysymyksessä halutaan siis selvittää ratojen lukumäärä. Ratojenlaskentalauseen perusteella riittää selvittää kaikki kiintopistejoukot.

Tehtävää helpottaa, jos jaetaan symmetriat konjugaattiluokkiin. "Samantyyppiset" kierrot kuuluvat samaan konjugaattiluokkaan, ja jos g ja h ovat konjugaatteja, niin $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$. Tarkastellaan esimerkiksi neljännesympyrän kiertoa vastakkaisten tahkojen keskipisteiden kautta kulkevan akselin ympäri. Tällaisia akseleita on yhteensä 3, ja kierto voidaan tehdä joko myötä- tai vastapäivään. Kyseiseen konjugaattiluokkaan kuuluu siis 6 kiertoa. Jokainen tällainen kierto kiinnittää täsmälleen ne väritykset, joissa akselin suuntaiset tahkot ovat samanväriset. Näitä värityksiä on tuloperiaatteen mukaan n^3 kappaletta, sillä akselin lävistämille tahkoille voidaan valita mitkä tahansa värit, ja muille tahkoille valitaan jokin kolmas väri.

Alla olevassa taulukossa esitetään kaikki tarpeelliset laskelmat konjugaatioluokittain. Symmetriat on ilmoitettu kiertoakselin ja kiertokulman avulla.



Kuva 7. Kuution symmetria-akselit

symmetria $g \in G$	$\lvert {}^G g \rvert$	$\lvert \mathrm{Fix}(g) \rvert$
identtinen kuvaus	1	n^6
tahkojen keskipisteiden ympäri 90°	6	n^3
tahkojen keskipisteiden ympäri 180°	3	n^4
nurkan ympäri 120°	8	n^2
särmän keskipisteen ympäri 180°	6	n^3

Tuloksena saadaan nyt ratojenlaskentalauseen mukaan

$$|X/G| = \frac{1}{24} \sum_{g \in G} |\mathrm{Fix}(g)| = \frac{1}{24} \left(n^6 + 3 \cdot n^4 + 12 \cdot n^3 + 8 \cdot n^2 \right).$$

Jos värejä on esimerkiksi kolme, saadaan $1368/24 = 57$ erilaista väritystä.