3. Permutaatioista ja symmetrioista

Symmetrioita käytetään usein helpottamaan monimutkaisen ongelman tarkastelua. Jos esimerkiksi tiedetään jonkin kuvion olevan tietyllä tavalla symmetrinen, on kuvion muodolle olemassa vähemmän vaihtoehtoja.

Symmetriaryhmät koostuvat permutaatioista, jotka liikuttelevat jonkin rakenteen perusosia säilyttäen kuitenkin niiden väliset suhteet. Tällainen yleinen määritelmä voi oikeastaan kuvata mitä tahansa ryhmää – kunhan säilytettävät "osasten väliset suhteet" valitaan oikein – ja joskus sanotaankin, että ryhmäteoria on nimenomaan symmetrioiden tutkimista. Se, millä tavalla symmetrioiden sallitaan muutella rakennetta, vaihtelee tapauskohtaisesti. Esimerkiksi neliön symmetriaryhmään lasketaan sellaisetkin permutaatiot, jotka peilaavat neliön jonkin lävistäjän suhteen, vaikka tällaista muunnosta varten neliö täytyy "nostaa tasosta irti" ja kääntää ympäri.[9] Sen sijaan kuution symmetriaryhmään ei yleensä 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, miten symmetrioita voidaan käsitellä ja millaista hyötyä niistä voi olla. Koska symmetriat ovat permutaatioita, aloitetaan tutustumalla tarkemmin näihin kuvauksiin. Lisäksi rajoitutaan äärellisiin joukkoihin.

3.1. Symmetriset ryhmät ja permutaation etumerkki. Merkitään n ensimmäisen positiivisen kokonaisluvun joukkoa $N_n = \{1, 2, \ldots, n\}$. Tämän joukon kaikkien permutaatioiden muodostama ryhmä on *symmetrinen ryhmä* S_n. 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 tapana merkitä listaamalla kaikkien alkioiden kuvat:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix} \in S_n.$$

Usein kätevämpi merkintätapa on niin sanottu *sykliesitys*. Jos $a_1, \ldots, a_m$ ovat joukon N_n eri alkioita, niin *m-sykli* $\rho = (a_1 \quad \ldots \quad a_m)$ 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. Pienellä vaivalla nähdään, että jokainen permutaatio voidaan kirjoittaa erillisten syklien tulona, esimerkiksi

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

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

[9] 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 lopulta siitä, että peilauksen determinantti on -1.

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

$$(a_1 \quad a_2 \quad \cdots \quad a_m) = (a_1 \quad a_2)\,(a_2 \quad a_3)\cdots(a_{m-1} \quad a_m)\,.$$

Tästä seuraa, että mielivaltainen permutaatio voidaan kirjoittaa vaihtojen tulona. Permutaation esitys vaihtojen tulona 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.

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

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

Jos $\sigma \in S_n$ on m-sykli, niin sen esityksessä erillisten syklien tulona on yksi m-sykli ja $n-m$ kappaletta 1-syklejä. Määritelmän perusteella pätee täten

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

Syklin etumerkki on siis 1, jos ja vain jos sen pituus on pariton. Esimerkiksi jokaisen vaihdon etumerkki on -1.

Osoitetaan seuraavaksi, että etumerkkikuvaus on ryhmähomomorfismi. Tähän tarvitaan pieni aputulos.

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. $\rho_1 = (a \quad c_1 \quad \ldots \quad c_k \quad b \quad d_1 \quad \ldots \quad d_l)$, niin

$$\tau\rho_1 = (a \quad c_1 \quad \ldots \quad c_k)\,(b \quad d_1 \quad \ldots \quad d_l)\,.$$

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, esimerkiksi $\rho_1 = (a \quad c_1 \quad \ldots \quad c_k)$ ja $\rho_2 = (b \quad d_1 \quad \ldots \quad d_l)$, niin

$$\tau\rho_1\rho_2 = (a \quad c_1 \quad \ldots \quad c_k \quad b \quad d_1 \quad \ldots \quad d_l)\,.$$

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 $\operatorname{sgn}\colon S_n \to (\{1,-1\},\cdot)$ *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 nojalla 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 symbolilla 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 kuvaus 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 yksi. 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 tiedetään, että $b = a'_{1,1}$, joten

$$\tau'(b) = \begin{pmatrix} a'_{1,1} & a'_{1,2} & \dots & a'_{1,k_1} \end{pmatrix}.\, a'_{1,1} = a'_{1,2} = \sigma(a_{1,2}).$$

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

Esimerkki 3.7. Edellisen lauseen avulla on helppo konjugoida mikä tahansa permutaatio sen sykliesityksen avulla. Jos esimerkiksi $\sigma = (13)(425)$, niin

$$\sigma(16)(278)(3495)\sigma^{-1} = (36)(578)(1294).$$

Toisaalta lauseen avulla voidaan todistaa myös yleisempiä tuloksia. Oletetaan esimerkiksi, että ${}^{\tau}\rho = \rho$, missä $\rho = (a_1 \quad \dots \quad a_k)$ on jokin sykli. Nyt τ:n on oltava joukon $\{a_1, \dots, a_k\}$ permutaatio, sillä lauseen perusteella τ ei saa muuttaa syklissä esiintyviä alkioita. Lisäksi τ:n on säilytettävä alkioiden järjestys konjugoitavassa syklissä. Jos siis esim. $\tau(a_1) = a_j$, niin täytyy olla $\tau(a_2) = a_{j+1}$ jne. Tästä nähdään, että itse asiassa täytyy päteä $\tau = \rho^{j-1}$, missä j määräytyy yhtälöstä $\tau(a_1) = a_j$.

Symmetrisen konjugaattiluokat selviävät helposti edellisen lauseen avulla. Samaan konjugaattiluokkaan kuuluvat nimittäin 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 $t_1 \geq t_2 \geq \dots \geq t_m$ ja $\sum_i t_i = n$. (Tällaista jonoa nimitetään luvun n ositukseksi.) Esimerkiksi permutaation $(12)(345)(6)$ syklityyppi on $(3, 2, 1)$.

Esimerkki 3.8. Tarkastellaan ryhmää S_3, joka koostuu 1-, 2- ja 3-sykleistä. Sen konjugaattiluokat ovat

$$K_1 = \{\mathrm{id}\}, \quad K_2 = \{(12), (23), (13)\} \quad \text{ja} \quad K_3 = \{(123), (132)\}.$$

Ainoastaan konjugaattiluokkien yhdiste voi olla normaali aliryhmä. Toisaalta aliryhmän täytyy aina sisältää neutraalialkio, joten epätriviaaleja normaaleja aliryhmiä voivat olla ainoastaan yhdisteet $K_1 \cup K_2$ ja $K_1 \cup K_3$. 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 konjugaattiluokkien määräytyminen on monimutkaisempaa. Esimerkiksi A_3 on vaihdannainen, mistä seuraa, että sen jokainen konjugaattiluokka on yksiö. Edellisen esimerkin luokka $K_3 \subset A_3$ 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 3.9. *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 $\alpha \in C_S$. Alkiolla α konjugointi ei siis saa muuttaa permutaatiota σ. 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. Nyt siis ${}^{\alpha}\rho_i = \rho_i$, joten $\alpha = \rho_i^k$ jollain k (vrt. esim. 3.7). Koska syklin ρ_i pituus on pariton, sen etumerkki on 1. Edelleen $\operatorname{sgn}(\alpha) = 1$, joten $\alpha \in C_A$.

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

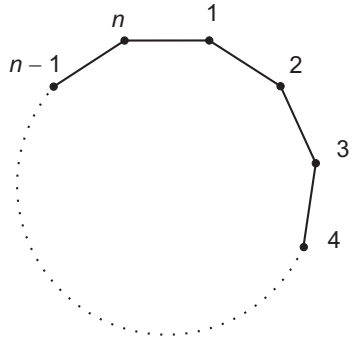
3.3. Diedriryhmät. Tarkastellaan joukosta $N_n = \{1, 2, \ldots, n\}$ muodostettujen järjestämättömien parien joukkoa

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

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 on ryhmän S_n äärellinen alimonoidi, joten se on myös aliryhmä (todistus harjoitustehtävä). Ryhmä G koostuu kaikista mahdollisista verkon solmujen permutaatioista, jotka säilyttävät särmärakenteen, joten kyseessä on monikulmion symmetriaryhmä. Vakauttajaryhmän selvittämiseksi tarkastellaan sen toimintaa vakauttamassaan monikulmiossa.

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

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

missä $k = [n/2]$ (kokonaisosa). Ryhmän G 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 3.10. *Diedriryhmä*[10] D_{2n} on monikulmion E_n vakauttaja.

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

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

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

LAUSE 3.11. *Jos ryhmän G virittää kaksi alkiota r ja s, joille pätee*

$$r^n = 1, \quad s^2 = 1 \quad \textit{ja} \quad srs = r^{-1},$$

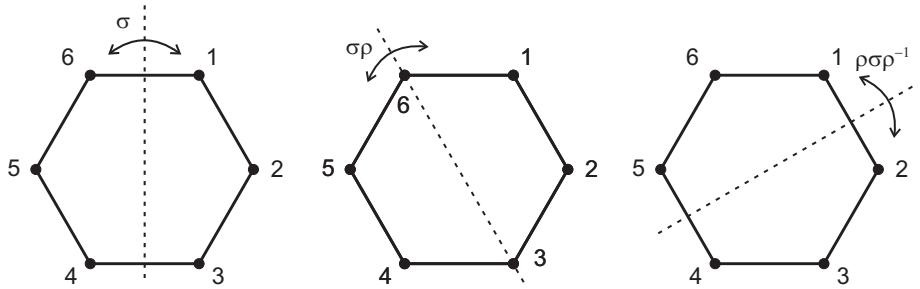
niin $G \cong D_{2n}$.

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 (katso esim. J. Rotman: An Introduction to the Theory of Groups).

LAUSE 3.12. *Jos ryhmän G virittää kaksi alkiota a ja b, joille pätee*

$$a^2 = 1, \quad b^2 = 1 \quad \textit{ja} \quad (ab)^n = 1,$$

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



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

[10]diedri = kaksitahokas (kr.)

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. On jopa mahdollista osoittaa, että sellaisia tason lineaarikuvausten ryhmän äärellisiä 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 3.13. Oletetaan, että G toimii joukossa X. Alkion $g \in G$ *kiintopistejoukko* on

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

LAUSE 3.14 (Ratojenlaskentalause eli Burnsiden lemma). *Oletetaan, että G toimii äärellisessä joukossa G. Tällöin ratojen lukumäärä on*

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

TODISTUS. Se luku, 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 sama termi $1/|Gx|$ luetellaan niin 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

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

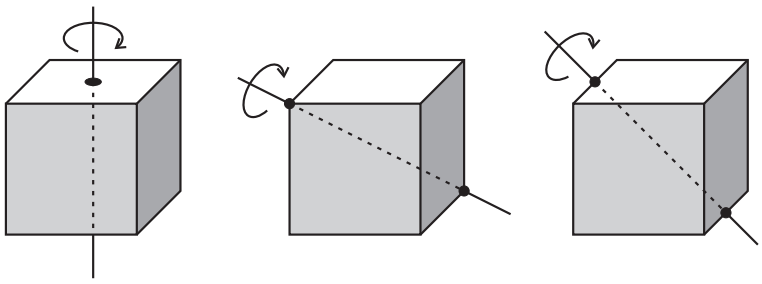
mistä väite seuraa. □

Esimerkki 3.15. 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 $i \in \{1, \ldots, 6\}$.

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 eri 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 $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$. (Näiden väitteiden tarkistaminen jätetään harjoitustehtäväksi.) 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 yhteinen väri.



Kuva 7. Kuution symmetria-akselit

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

symmetria $g \in G$	$\lvert {}^G g\rvert$	$\lvert\operatorname{Fix}(g)\rvert$
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

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

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

3.5. Sisäiset symmetriat. Kuution väritysesimerkissä 3.15 tarkasteltiin yksittäisten alkioiden sijaan niiden konjugaattiluokkia ja esitettiin ajatus, että konjugaattiluokkia vastaisivat luonnollisella tavalla erityyppiset kiertoakselit ja eri kiertokulmat. Tarkastellaan vielä lähemmin tätä konjugointia.

Otetaan esimerkiksi kaksi eri kiertoakselia A ja B, joista kumpikin kulkee eräiden vastakkaisten nurkkien kautta. Kierto B:n ympäri saadaan kääntämällä kuutio ensin symmetrialla g niin, että B siirtyy akselin A paikalle, suorittamalla sitten kierto h akselin A ympäri ja kääntämällä kuutio lopuksi takaisin. Nähdään, että kierto B:n ympäri on itse asiassa $g^{-1}hg$, eli A:n ympäri tapahtuvan kierron konjugaatti.

Ryhmän alkiolla $g \in G$ konjugointi tuottaa ryhmän sisäisen isomorfismin $h \mapsto {}^g h$ eli niin sanotun *automorfismin*. Automorfismit ovat ryhmän itsensä symmetrioita: ne ovat permutaatioita, jotka säilyttävät ryhmän laskutoimitusrakenteen. Konjugoinnista saatavia automorfismeja kutsutaan *sisäisiksi*, ja ne muodostavat ryhmän $\operatorname{Inn}(G)$.

Ryhmällä voi olla muitakin kuin sisäisiä automorfismeja. Kaikkien automorfismien ryhmää merkitään $\operatorname{Aut}(G)$. Sisäiset automorfismit ovat kuitenkin sellaisia, jotka säilyttävät myös ryhmän toiminnan ominaisuudet. Väritysesimerkissä mainittiin, että esimerkiksi $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$, jos alkiot g ja h ovat samassa konjugaattiluokassa eli jos ne saadaan toisistaan jotain sisäistä symmetriaa käyttämällä.

On mahdollista osoittaa, että kuution symmetriaryhmän kaikki automorfismit ovat sisäisiä. Kaikille ryhmille tämä ei kuitenkaan päde. Helppo esimerkki saadaan Kleinin neliryhmästä $V_4 = \{1, a, b, c\}$, jonka kertotaulu näkyy alla.

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Koska V_4 on vaihdannainen, millä tahansa alkiolla konjugointi pitää kaikki alkiot paikallaan, joten $\operatorname{Inn}(V_4) = \{\mathrm{id}\}$. Toisaalta kaikki ryhmän V_4 neutraalialkiosta poikkeavat alkiot ovat keskenään täysin samanarvoisia: kahden eri alkion tulona saadaan aina kolmas. Alkiot a, b ja c voi siis nimetä haluamassaan järjestyksessä ryhmärakenteen siitä muuttumatta. Täten $\operatorname{Aut}(V_4) = S_3$.