Agnesa Ujkani

RYHMÄT JA SYMMETRIA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2020

Tiivistelmä

Agnesa Ujkani: Ryhmät ja symmetria
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Joulukuu 2020

Tässä tutkielmassa esitellään ryhmät ja symmetria sekä niiden välinen yhteys.

Tutkielman alussa käsitellään ryhmiä. Ensiksi määritetään binäärinen operaatio, ryhmä ja Abelin ryhmä, josta esitetään myös esimerkki. Lisäksi esitetään ryhmien ominaisuuksia.

Tämän tutkielman seuraavassa luvussa esitetään käsitteitä, jotka auttavat pääaiheen eli symmetrian tarkastelemisessa. Ensiksi tutustutaan isometriaan ja sen määritelmään. Isometria on siis metristen avaruuksien välinen funktio, joka säilyttää etäisyyden kaikilla pisteillä avaruudessa $\mathbb{R}^2$. Seuraavaksi esitetään muutama esimerkki isometrioista. Esitetään peilaus, kierto eli rotaatio sekä siirto eli translaatio. Seuraavaksi tutkielmassa esitetään ja todistetaan lause, jonka mukaan jokainen kierto origon suhteen eli rotaatio on lineaarikuvaus. Tästä seuraa, että jokainen isometria on bijektio ja jokainen isometria origon suhteen on epäsingulaarinen lineaarikuvaus. Tämän jälkeen määritellään ortogonaalinen ryhmä. Ortogonaalinen ryhmä on joukko, jossa kaikki tason isometriat kiinnittävät origon. Lopuksi esitetään lause, jonka mukaan ortogonaalinen ja isometrinen ryhmä ovat ryhmiä kuvausten yhdistämisen suhteen.

Tutkielman lopuksi esitellään symmetriaryhmä ja diedriryhmä. Tasokuvion symmetriaryhmä on kaikkien tason isometrioiden joukko eli kaikki symmetriaryhmän alkiot ovat isometrioita, jotka säilyttävät kuvion. Symmetriaryhmän alkioita kutsutaan tasokuvion symmetrioiksi. Lukijalle selventämiseksi esitetään myös muutama esimerkki symmetria- ja diedriryhmistä. Tutkielma on kirjoitettu Rotmanin kirjaa A First Course in Abstract Algebra ja Gilbertin kirjaa Modern algebra with applications mukaillen.

Avainsanat: ryhmä, isometria, symmetria, symmetriaryhmä

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisältö

1 Johdanto

Tässä tutkielmassa käsitellään ryhmiä ja symmetriaa ja niiden välistä yhteyttä. Lähdetään liikkeelle käsitteistä, joita tarvitsemme aiheen tarkestelemiseen.

Alussa esitetään ryhmän määritelmä ja ryhmän perusominaisuudet. Tutkielman luvussa 3 määritellään symmetriaan liittyviä käsitteitä, kuten isometria ja esitetään myös muutama esimerkki isometrioista.

Luvussa 4 päästään esittämään ryhmän ja symmetrian yhtenäisyyttä. Tässä pykälässä määritetään symmetriaryhmä ja diedriryhmä. Seuraavaksi esitetään myös muutama esimerkki.

Lukijalta edellytetään hallitsevan Algebra 1A:n ja Algbera 1B:n perusasioiden tuntemista. Oletetaan myös, että lukija hallitsee abstraktia lineaarialgebrallista tuntemusta. Edellytetään muun muassa, että lukija tuntee lineaarikuvauksen. Lähdeteoksena tutkielmassa on käytetty Rotmannin kirjaa A first course in absrtact algebra.

2 Ryhmät

2.1 Ryhmän määritelmä

Luvussa 2 esitetään ryhmän ja Abelin ryhmän määritelmät ja esitetään myös ryhmän perusominaisuudet. Tässä pykälässä esitetään kolme määritelmää: Binäärisen operaation sekä ryhmän ja Abelin ryhmän määritelmät (vrt. [2, s. 121–122]).

Määritelmä 2.1. *(Binäärinen)* operaatio $\bullet$ joukossa G, on funktio: $G \times G \rightarrow G$. $\bullet(a, b)$ merkitään yleensä $a \bullet b$ tai ab.

Määritelmä 2.2. Olkoon G epätyhjä joukko, joka on varustettu binäärioperaation $\bullet$ kanssa. Pari $(G, \bullet)$ on *ryhmä*, jos seuraavat aksioomat täyttyvät:

(i) G on suljettu operaation suhteen, eli $a \bullet b \in G$ kaikilla $a, b \in G$.

(ii) Operaatio $\bullet$ on *liitännäinen* (*assosiatiivinen*): $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ kaikilla $a, b, c \in G$.

(iii) On olemassa *neutraalialkio* $e \in G$: $e \bullet a = a \bullet e = a$ kaikilla $a \in G$.

(iv) Kaikilla $a \in G$ on olemassa *käänteisalkio* $a^{-1} \in G$: $a^{-1} \bullet a = a \bullet a^{-1} = e$.

Määritelmä 2.3. Jos operaatio on *vaihdannainen* (*kommutatiivinen*): $a \bullet b = b \bullet a$, kaikilla $a, b \in G$, niin ryhmää kutsutaan *Abelin ryhmäksi*.

Esimerkki 2.1. Ryhmä $(\mathbb{Z}, +)$ on *Abelin ryhmä*, koska $a+b = b+a$ kaikilla $a, b \in \mathbb{Z}$.

2.2 Ryhmistä

Tässä pykälässä esitetään ryhmän ominaisuuksia. Määritelmät, lauseet ja lauseiden todistukset ovat lähteistä [2, s. 124 – 133] ja [1, s. 53 – 54].

Lause 2.1. *Olkoon operaatio $\bullet$ liitännäinen joukossa G ja olkoon neutraalialkio $e \in G$. Jos alkiolla a on käänteisalkio, niin se on yksikäsitteinen.*

Todistus (vrt. [1, s. 53]). Oletetaan, että b ja c ovat alkion a käänteisalkiota.

Näin ollen
$$a \bullet b = b \bullet a = e \quad \text{ja} \quad a \bullet c = c \bullet a = e.$$

Nyt, koska e on neutraalialkio ja operaatio $\bullet$ on liitännäinen, niin

$$b = b \bullet e = b \bullet (a \bullet c) = (b \bullet a) \bullet c = e \bullet c = c,$$

joten alkion a käänteisalkio on yksikäsitteinen. $\square$

Lause 2.2. *Jos a, b ja c ovat ryhmän* $(G, \bullet)$ *alkioita, niin*

(i) $(a^{-1})^{-1} = a$,

(ii) $(a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$.

(iii) *Jos* $a \bullet b = a \bullet c$ *tai* $b \bullet a = c \bullet a$, *niin* $b = c$.

Todistus. Ks. [1, s. 54]. $\square$

Tästä lähtien ryhmään $(G, \bullet)$ viitataan merkitsemällä sitä kyseiseen ryhmään liitettävällä joukolla, eli käytetään merkinnällistä lyhennettä G. Merkitään yleensä jatkossa myös esimerkiksi alkioiden a ja b tuloa $a \bullet b$ merkinnällä ab eli operaatio jätetään merkitsemättä.

Kun ryhmä on Abelin ryhmä, niin yleensä ryhmä merkitään additiivisella tavalla. Seuraavassa määritelmässä esitellään ryhmä, joka on merkitty additiivisella tavalla.

Määritelmä 2.4. *Adiitiivinen ryhmä* on sellainen joukko G, joka on varustettu operaation $+$ kanssa ja neutraalialkiona on $0 \in G$ siten, että

(i) $a + (b + c) = (a + b) + c$ jokaiselle $a, b, c \in G$;

(ii) $0 + a = a$ kaikilla $a \in G$;

(iii) jokaista $a \in G$ kohti on sellainen $-a \in G$, että $(-a) + a = 0$.

Määritelmä 2.5. Olkoon G ryhmä ja $a \in G$. Määritellään potenssit a^n, jossa $n \geq 1$,

$$a^1 = a, \quad a^{n+1} = aa^n, \quad a^0 = 1, \quad a^{-n} = (a^n)^{-1}.$$

Lause 2.3. *Olkoon G ryhmä ja olkoot* $a, b \in G$. *Olkoot n ja m kokonaislukuja.*

(i) *Jos a ja b kommutoivat, niin* $(ab)^n = a^n b^n$.

(ii) $(a^n)^m = a^{mn}$.

(iii) $a^m a^n = a^{m+n}$.

Todistus.

1º Olkoon $n = 0$, tällöin

$$(ab)^0 = 1 = a^0 b^0.$$

2º Olkoon $n \in \mathbb{Z}^+$, tällöin

$$(ab)^n = \underbrace{(ab)\cdots(ab)}_{n \text{ kertaa}} = \underbrace{(a\cdots a)}_{n \text{ kertaa}}\underbrace{(b\cdots b)}_{n \text{ kertaa}} = a^n b^n,$$

jossa a ja b voidaan järjestää uudelleen, sillä $ab = ba$ eli a ja b kommutoivat.

3º Olkoon $n \in \mathbb{Z}^-$, tällöin

$$\begin{aligned}
(ab)^n &= ((ab)^{|n|})^{-1} && \text{(määritelmä 2.5)} \\
&= (a^{|n|}b^{|n|})^{-1} && \text{(kohta 2°)} \\
&= b^{-|n|}a^{-|n|} && \text{(lause 2.2 ja määritelmä 2.5)} \\
&= \underbrace{(b^{-1}\cdots b^{-1})}_{n \text{ kertaa}}\underbrace{(a^{-1}\cdots a^{-1})}_{n \text{ kertaa}}.
\end{aligned}$$

Kommutatiivisuuden nojalla nähdään, että

$$(ab)^n = \underbrace{(a^{-1}\cdots a^{-1})}_{|n| \text{ kertaa}}\underbrace{(b^{-1}\cdots b^{-1})}_{|n| \text{ kertaa}} = a^n b^n.$$

Kohdat (ii) ja (iii) voidaan todistaa samankaltaisella menetelmällä. □

Määritelmä 2.6. Olkoon G ryhmä ja $a \in G$. Jos $a^k = 1$ jollakin $k \geq 1$, niin pienintä tällaista eksponenttia $k \geq 1$ kutsutaan alkion a *kertaluvuksi*. Jos tällaista eksponenttia ei ole olemassa, niin sanotaan, että alkiolla a on *ääretön kertaluku*.

Esimerkki 2.2. Olkoot a ja b ryhmän G alkioita. Oletetaan, että alkion a kertaluku on 5 ja $a^3 b = ba^3$. Osoitetaan, että $ab = ba$.

Todistus. Koska alkion a kertaluku on 5, niin $a^5 = e$ ja $a^3 b = ba^3$. Kerrotaan a^3 puolittain. Saadaan $a^3(a^3 b) = a^3(ba^3) = (ba^3)a^3$. Näin ollen, $a^6 b = ba^6$.

Tällöin $a^6 = a^5 a = ea = a$ ja saadaan $ab = ba$. □

Lause 2.4. *Olkoon S_n symmetrinen ryhmä ja $\alpha \in S_n$.*

(i) *Jos α on r-sykli, niin alkion α kertaluku on r.*

(ii) *Jos $\alpha = \beta_1 \dots \beta_t$ on erillisten r_i-syklien β_i tulo, niin alkiolla α on kertaluku $m = pyj(r_1, \dots, r_t)$.*

(iii) *Jos p on alkuluku, niin alkion α kertaluku on p, jos ja vain jos se on $p-$sykli tai erillisten $p-$syklien tulo.*

Todistus. Ks. [2, s.134]. $\square$

3 Isometria

Tässä pykälässä esitetään isometrian määritelmä ja esitetään esimerkkejä isometrioista. Tämän pykälän määritelmät, lauseet ja todistukset ovat lähteestä [2] sivuilta 135 –139.

3.1 Isometrian määritelmä

Määritelmä 3.1. Tason *isometria* on funktio $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$, joka säilyttää etäisyyden kaikilla pisteillä $P = (a, b) \in \mathbb{R}^2$ ja $Q = (c, d) \in \mathbb{R}^2$,

$$\|\varphi(P) - \varphi(Q)\| = \|P - Q\|,$$

jossa $\|P - Q\| = \sqrt{(a - c)^2 + (b - d)^2}$ on pisteiden P ja Q etäisyys.

Merkitään pistetulo:

$$P \cdot Q = ac + bd.$$

Nyt

$$\begin{aligned}(P - Q) \cdot (P - Q) &= P \cdot P - 2(P \cdot Q) + Q \cdot Q \\ &= (a^2 + b^2) - 2(ac + bd) + (c^2 + d^2) \\ &= (a^2 - 2ac + c^2) + (b^2 - 2bd + b^2) \\ &= \|P - Q\|^2.\end{aligned}$$

Tästä seuraa, että jokainen isometria φ säilyttää pistetulot:

$$\varphi(P) \cdot \varphi(Q) = P \cdot Q,$$

koska

$$\varphi(P) \cdot \varphi(Q) = \|\varphi(P) - \varphi(Q)\|^2 = \|P - Q\|^2 = P \cdot Q.$$

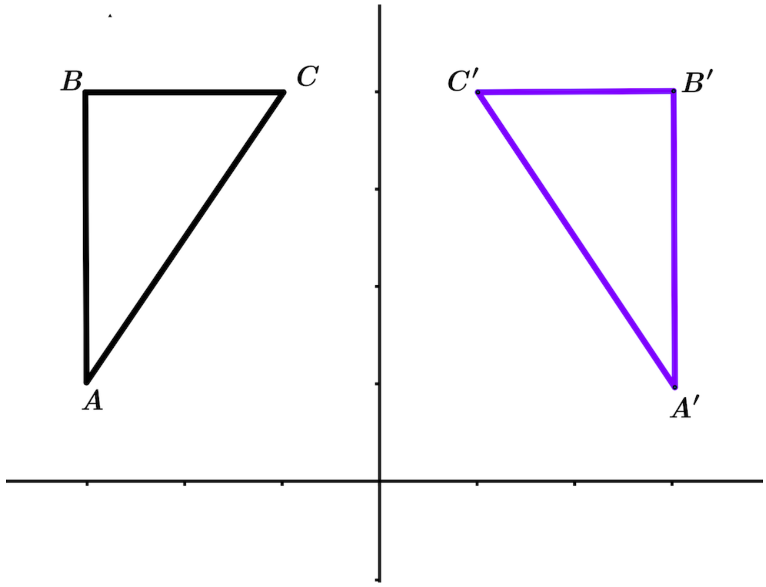
Pistetulon geometrinen tulkinta:

$$P \cdot Q = \|P\|\,\|Q\| \cos\theta,$$

jossa θ on pisteiden P ja Q välinen kulma. Tästä seuraa, että jokainen isometria säilyttää kulmat. Etenkin P ja Q ovat ortogonaalisia, jos ja vain jos $P \cdot Q = 0$, joten isometriat säilyttävät kohtisuoruuden. Käänteisesti, jos φ säilyttää pistetulot, eli jos $\varphi(P) \cdot \varphi(Q) = P \cdot Q$, niin kaava $(P - Q) \cdot (P - Q) = \|P - Q\|^2$ osoittaa, että funktio φ on isometria.

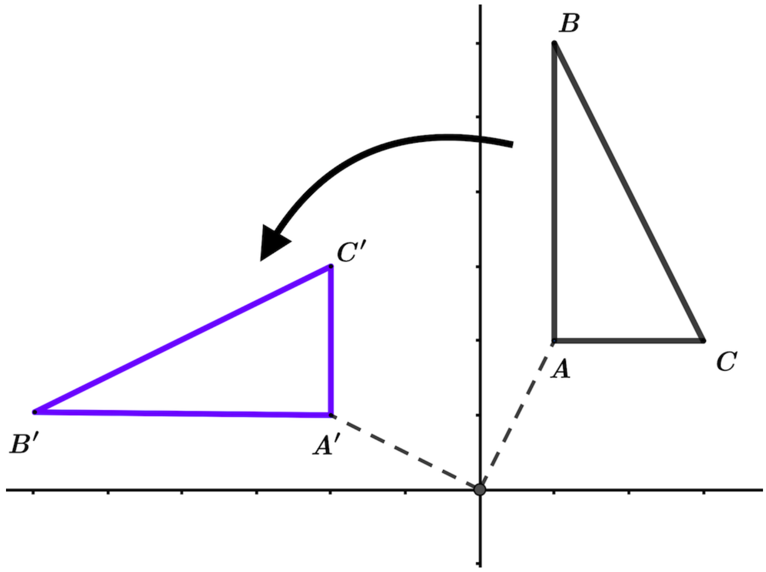
Seuraavaksi esitetään muutama esimerkki isometrioista. Esitetään peilaus, kierto ja siirto. Olkoon $\triangle$ kolmio ja olkoot A, B ja C sen kärkipisteet.

Esimerkki 3.1. Kuvassa 3.1 nähdään, että $\triangle ABC$ ja sen peilikuvalla $\triangle A'B'C'$ on samat etäisyydet. Näin ollen peilaus on isometria.



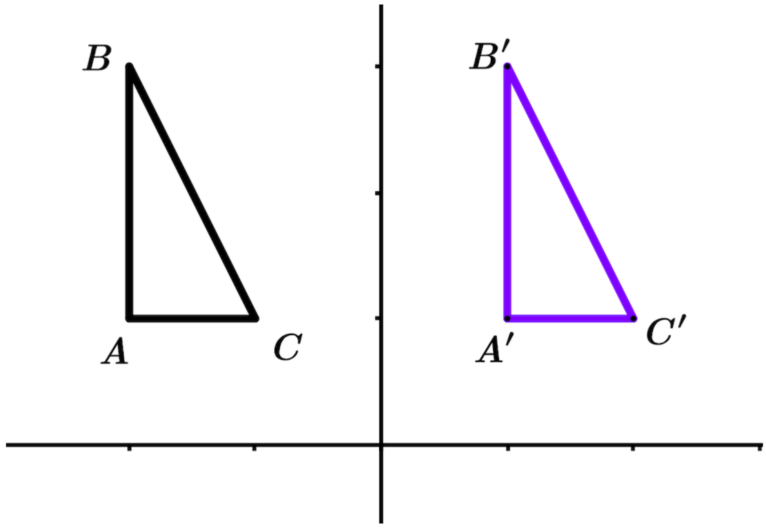
Kuva 3.1. Peilaus

Esimerkki 3.2. Seuraavassa kuvassa 3.2 nähdään, että kuvilla $\triangle ABC$ ja $\triangle A'B'C'$ on samat etäisyydet. Näin ollen kierto eli rotaatio on myös isometria.



Kuva 3.2. Kierto (rotaatio)

Esimerkki 3.3. Seuraavassa kuvassa 3.3 nähdään, että myös kuvilla $\triangle ABC$ ja $\triangle A'B'C'$ on samat etäisyydet. Näin ollen siirto eli translaatio on isometria.



Kuva 3.3. Siirto (translaatio)

3.2 Isometrioista

Tässä pykälässä määritellään ortogonaalinen ryhmä ja esitetään sekä todistetaan pari lausetta seurauksineen.

Lause 3.1. *Jokainen kierto origon suhteen eli rotaatio φ on* lineaarikuvaus.

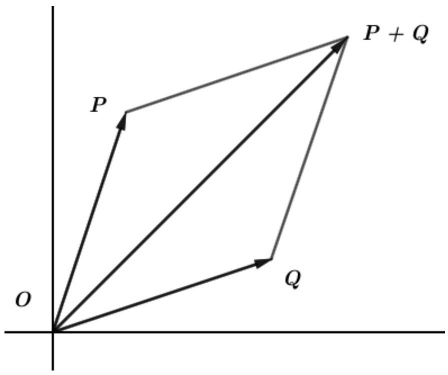
Todistus (vrt. [2, s. 137–138]). Olkoon $C_d = \{Q \in \mathbb{R}^2 \mid \|Q - 0\| = d\}$ ympyrä, jonka säde on $d > 0$ ja keskipiste on 0. Väitämme, että $\varphi(C_d) \subseteq C_d$. Jos $P \in C_d$, niin $\|P - 0\| = d$. Koska φ säilyttää etäisyyden, niin $d = \|\varphi(P) - \varphi(0)\| = \|\varphi(P) - 0\|$. Näin ollen $\varphi(P) \in C_d$.

Olkoon $P \neq O$ piste avaruudessa $\mathbb{R}^2$ ja olkoon $r \in \mathbb{R}$. Jos $\|P - O\| = p$, niin $\|rP - O\| = |r|p$. Tällöin $rP \in L[O, P] \cap C_{|r|p}$ eli $\varphi(rP) = \pm r\varphi(P)$ (sillä suora leikkaa ympyrän enintään kahdessa pisteessä). Tässä L[O,P] on pisteiden O ja P kautta kulkeva suora.

Jos voidaan osoittaa, että $\varphi(rP) \neq -r\varphi(P)$, niin voidaan päätellä, että $\varphi(rP) = r\varphi(P)$. Kun $r > 0$, niin origo O sijaitsee pisteiden $-rP$ ja P välillä. Tällöin pisteiden $-rP$ ja P välinen etäisyys on $rp + p$. Toisaalta rP ja P välinen etäisyys on $|rp - p|$. (Kun $r > 1$, niin etäisyys on $rp - p$ ja kun $0 < r < 1$ etäisyys on $p - rp$). Nähdään, että $r + rp \neq |rp - p|$, joten $\varphi(rP) \neq -r\varphi(P)$, sillä φ säilyttää etäisyyden. Samankaltainen argumentti pätee myös, kun $r < 0$. Näin ollen $\varphi(rP) = r\varphi(P)$.

Seuraavaksi todistetaan, että $\varphi(P + Q) = \varphi(P) + \varphi(Q)$. Jos O,P ja Q ovat kollineaarisia eli samalla suoralla. Valitaan suoralta $L[O, P]$ piste U, jonka etäisyys origosta on 1. Näin ollen $P = pU$, $Q = qU$ ja $P + Q = (p + q)U$. Pisteet $O = \varphi(O)$, $\varphi(U)$, $\varphi(P)$ ja $\varphi(Q)$ ovat kollineaarisia. Koska φ säilyttää skalaarilla kertomisen, niin

$$\begin{aligned}
\varphi(P) + \varphi(Q) &= \varphi(pU) + \varphi(qU) \\
&= p\varphi(U) + q\varphi(U) \\
&= (p + q)\varphi(U) \\
&= \varphi((p + q)U) \\
&= \varphi(P + Q).
\end{aligned}$$



Kuva 3.4. Translaatio

Jos O, P ja Q eivät ole kollineaarisia, niin suunnikassäännön mukaan $P + Q$ on piste S siten, että O, P, Q ja S ovat suunnikkaan kärkipisteet. Koska φ säilyttää etäisyyden, myös pisteet $O = \varphi(U)$, $\varphi(P)$, $\varphi(Q)$ ja $\varphi(S)$ ovat suunnikkaan kärkipisteet, joten $\varphi(S) = \varphi(P) + \varphi(Q)$. Mutta koska $S = P + Q$, niin $\varphi(P + Q) = \varphi(P) + \varphi(Q)$. □

Seuraus 3.1. *Jokainen isometria φ: $\mathbb{R}^2 \to \mathbb{R}^2$ on bijektio ja jokainen origon kiinnittävä isometria on epäsingulaarinen lineaarikuvaus.*

Todistus (vrt. [2, s. 138]). Oletetaan, että φ kiinnittää origon, $\varphi(0) = 0$. Lauseen 3.1 nojalla φ on lineaarikuvaus. Koska φ on injektiivinen, $P = \varphi(e_1)$ ja $Q = \varphi(e_2)$ on avaruuden $\mathbb{R}^2$ kanta, jossa $e_1 = (1, 0)$ ja $e_2 = (0, 1)$ ovat avaruuden $\mathbb{R}^2$ luonnollinen kanta. Tällöin ψ: $\mathbb{R}^2 \to \mathbb{R}^2$, ψ: $aP + bQ \mapsto ae_1 + be_2$, on (yksiarvoinen)funktio, ja ψ ja φ ovat toistensa käänteisfunktioita. Näin ollen φ on bijektio, ja siksi myös epäsingulaarinen.

Oletetaan, että φ on isometria niin, että $\varphi(0) = U$. Olkoon τ_{-U} siirto eli translaatio pistessä $-U$. Nyt $\tau_{-U} \circ \varphi\colon 0 \mapsto U \mapsto 0$ niin, että $\tau_{-U} \circ \varphi = \theta$, missä θ on epäsingulaarinen lineaarikuvaus. Näin ollen $\varphi = \tau_U \circ \theta$ on bijektio, joka on bijektioiden yhdistelmä. □

Määritelmä 3.2. *Ortogonaalinen ryhmä* $O_2(\mathbb{R})$ koostuu origon kiinnittävistä tason isometrioista.

Lause 3.2. *Joukot* $\mathrm{Isom}(\mathbb{R}^2)$ *ja* $O_2(\mathbb{R})$ *ovat ryhmiä kuvausten yhdistämisen suhteen.*

Todistus. Ks. [2, s. 139]. Näytetään, että $\mathrm{Isom}(\mathbb{R}^2)$ on ryhmä. Huomataan, että $1_{\mathbb{R}}$ on isometria ja että $1_{\mathbb{R}} \in \mathrm{Isom}(\mathbb{R}^2)$. Olkoot φ' ja φ isometrioita. Tällöin kaikilla pisteillä P ja Q:

$$\begin{aligned}\|(\varphi'\varphi)(P) - (\varphi'\varphi)(Q)\| &= \|\varphi'(\varphi(P)) - \varphi'(\varphi(Q))\| \\ &= \|\varphi(P) - \varphi(Q)\| \\ &= \|P - Q\|,\end{aligned}$$

joten $\varphi'\varphi$ on myös isometria eli kuvausten yhdiste on binäärioperaatio ryhmässä $\mathrm{Isom}(\mathbb{R}^2)$. Jos $\varphi \in \mathrm{Isom}(\mathbb{R}^2)$, niin Seurauksen 3.1 nojalla φ on bijektio. Näin ollen isometrialla φ on käänteinen isometria φ^{-1}:

$$\|P - Q\| = \|\varphi(\varphi^{-1}(P)) - \varphi(\varphi^{-1}(Q))\| = \|\varphi^{-1}(P) - \varphi^{-1}(Q)\|.$$

Funktioiden yhdiste on liitännäinen, joten $\mathrm{Isom}(\mathbb{R}^2)$ on ryhmä.

Joukko $O_2(\mathbb{R})$ voidaan osoittaa ryhmäksi samalla menetelmällä. □

Seuraus 3.2. *Jos pisteet O, P ja Q eivät ole samalla suoralla ja jos φ ja ψ ovat sellaisia tason isometrioita, että $\varphi(P) = \psi(P)$ ja $\varphi(Q) = \psi(Q)$, niin $\varphi = \psi$.*

Todistus. Ks. [2, s. 139]. □

4 Symmetria

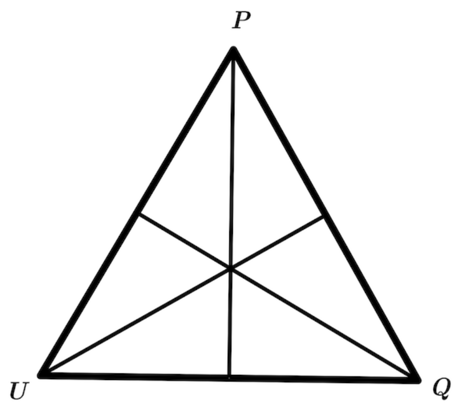
Luvussa 4 esitetään ryhmien ja symmetrian välistä yhteyttä. Tässä pykälässä määritetään symmetriaryhmä ja diedriryhmä. Tämän pykälän määritelmät, lause ja todistus ovat lähteestä [2] sivuilta 140 –142.

Määritelmä 4.1. Tasokuvion Ω *symmetriaryhmä* $\sum(\Omega)$ on kaikkien tason isometrioiden φ joukko. Symmetriaryhmän alkiot ovat isometrioita, jotka säilyttävät kuvion eli $\varphi(\Omega) = \Omega$. Symmetriaryhmän $\sum(\Omega)$ alkioita kutsutaan tasokuvion Ω symmetrioiksi.

Nähdään ,että $\sum(\Omega)$ on aina ryhmä.

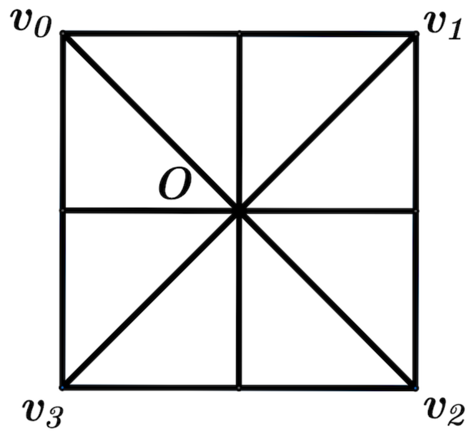
Esimerkki 4.1. (vrt. [2, s. 140 – 141]).

(i) Säännöllinen monikolmio π_3 on tasasivuinen kolmio, ja $|\sum(\pi_3)| = 6$.



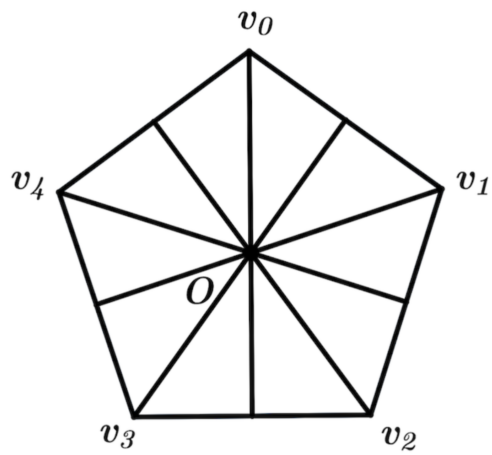
Kuva 4.1. π_3

(ii) Olkoon π_4 neliö, jonka kärkipisteet ovat $\{v_0, v_1, v_2, v_3\}$. Piirretään π_4 niin, että sen keskipiste on origossa O ja niin, että sen sivut ovat akselien suuntaiset. Huomataan, että jokainen $\varphi \in \sum(\pi_4)$ permutoi kärkipisteet. Neliön π_4 symmetria φ määräytyy seuraavasti: $\{\varphi(v_i) : 0 \leq i \leq 3\}$, näin ollen on enintään $24 = 4!$ mahdollista symmetriaa. Kaikki symmetrisen ryhmän S_4 permutaatiot eivät kuitenkaan johdu neliön π_4 symmetriasta. Jos kärkipisteet v_i ja v_j ovat vierekkäisiä, niin $\|v_i - v_j\| = 1$, mutta $\|v_0 - v_2\| = \sqrt{2} = \|v_1 - v_3\|$. Tästä seuraa, että kuvauksen φ on säilytettävä vierekkäisyys. Lauseessa 4.1 tullaan osoittamaan, että neliöllä π_4 on vain kahdeksan symmetriaa. Ryhmää $\sum(\pi_4)$ kutsutaan diedriryhmäksi, jossa on 8 alkiota. Merkitään D_8.



Kuva 4.2. π_4

(iii) Säännöllisen viisikulmion π_5 symmetriaryhmässä $\sum(\pi_5)$, jonka kärkipisteet ovat $v_0, \ldots, v_4$ ja keskipiste O, on 10 alkiota eli säännöllisellä viisikulmiolla π_5 on kymmenen symmetriaa. Lauseen 4.1 nojalla muita symmetrioita ei ole. Ryhmää $\sum(\pi_5)$ kutsutaan diedriryhmäksi, jossa on 10 alkiota. Merkitään D_{10}.



Kuva 4.3. π_5

Määritelmä 4.2. Ryhmää D_{2n}, jolla on tasan $2n$ alkiota, kutsutaan *diedriryhmäksi*, jos ryhmä sisältää sellaisen alkoin a, jonka kertaluku on n, ja sellaisen alkion b, joka kertaluku on 2, ja $bab = a^{-1}$.

Jos $n = 2$, niin diedriryhmä D_4 on Abelin ryhmä. Jos $n \geq 3$, niin D_{2n} ei ole Abelin ryhmä.

Lause 4.1. *Säännöllisen n-kulmion π_n symmetriaryhmä $\sum(\pi_n)$ on diedriryhmä, jossa on $2n$ alkiota.*

Todistus. Ks. [2, s. 142]. Olkoon π_n säännöllinen monikulmio, jonka kärkipisteet ovat $v_0, \ldots, v_{n-1}$ ja jonka keskipiste on O. Määritellään, että a on rotaatio keskipisteen O ympäri kulman $(360/n)^\circ$ verran:

$$a(v_i) = \begin{cases} v_{i+1} & \text{jos } 0 \leq i < n-1 \\ v_0 & \text{jos } i = n-1. \end{cases}$$

On selvää, että rotaatiolla a on kertaluku n. Määritellään seuraavaksi, että b on peilaus akselilla $L[O, v_0]$;

$$b(v_i) = \begin{cases} v_0 & \text{jos } i = 0 \\ v_{n-i} & \text{jos } 1 \leq i \leq n-1. \end{cases}$$

On selvää, että peilauksella b on kertaluku 2. Koska rotaatiolla a on kertaluku n, niin $1, a, a^2, \ldots, a^{n-1}$ ovat erillisiä symmetrioita. Lauseen 2.2 kohdan (iii) nojalla, myös $b, ab, a^2b, \ldots, a^{n-1}b$ ovat erillisiä symmetriota. Jos $a^s = a^r b$, missä $0 \leq r \leq n-1$ ja $s = 0, 1$, tällöin $a^s(v_i) = a^r b(v_i)$ jokaista lukua i kohti. Nyt $a^s(v_0) = v_s$ kun taas $a^r b(v_0) = v_{r-1}$. Näin ollen $s = r - 1$. Jos $i = 1$, niin $a^{r-1}(v_1) = v_{r+1}$ kun taas $a^r n(v_1) = v_{r-1}$. Näin ollen, $a^s \neq a^r b$ kaikilla luvuilla r, s. Tällöin, on löydetty $2n$ eri symmetriaa symmetriaryhmässä $\sum(\pi_n)$.

Näytetään seuraavaksi, että ei ole muita säännöllisen monikulmion π_n symmetrioita. Voidaan olettaa, että säännöllisen monikulmion π_n keskipiste O on origossa, ja niin jokainen symmetria φ kiinnitttää keskipisteen O. Tällöin lauseen 3.1 nojalla symmetria φ on lineaarikuvaus. Kärkipisteen v_0 vieressä olevat kärkipisteet eli v_1 ja v_{n-1} ovat lähimpänä kärkipistettä v_0. Toisin sanoen, jos $2 \leq i \leq n-2$, niin $\|v_i - v_0\| > \|v_1 - v_0\|$. Tällöin, jos $\varphi(v_0) = v_j$, niin $\varphi(v_1) = v_{j+1}$ tai $\varphi(v_1) = v_{j-1}$. Ensimmäisessä tapauksessa $a^j(v_0) = \varphi(v_0)$ ja $a^j(v_1) = \varphi(v_1)$ siten, että seurauksen 3.2 nojalla $\varphi = a^j$. Toisessa tapauksessa $a^j b(v_0) = v_j$ ja $a^j b(v_1) = v_{j-1}$ ja seurauksen 3.2 nojalla $\varphi = a^j b$. Näin ollen, $|\sum(\pi_n)| = 2n$.

Ollaan siis osoitettu, että $\sum(\pi_n)$ on ryhmä, jolla on täsmälleen $2n$ alkiota ja joka sisältää alkiot a ja b, joilla on kertaluvut n ja 2. Lopuksi näytetään, että $bab = a^{-1}$. Seurauksen 3.2 nojalla riittää, että tutkitaan yhtälöä kärkipisteissä v_0 ja v_1. Mutta $bab(v_0) = v_{n-1} = a^{-1}(v_0)$ ja $bab(v_1) = v_0 = a^{-1}(v_1)$. Näin ollen $bab = a^{-1}$. □

Lähteet

[1] Gilbert, W. Nicholson K. *Modern algebra with applications, 1st edition*. New Jersey: Hoboken, 2003.

[2] Rotman, J. *A first course in abstract algebra, 3rd edition*. New Jersey: Prentice Hall, 2006.