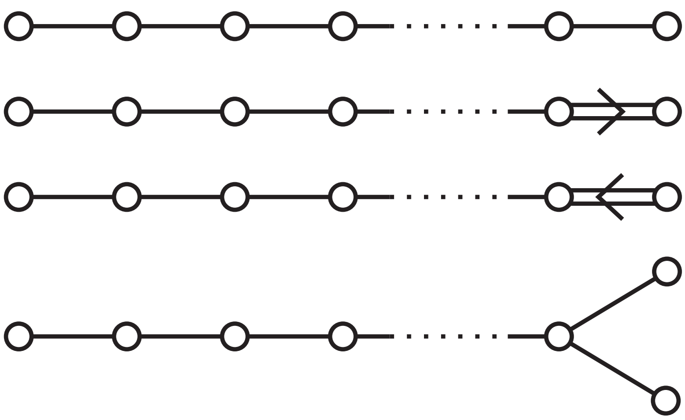
Klassiset ryhmät

Jokke Häsä ja Johanna Rämö

Matematiikan ja tilastotieteen laitos, kevät 2009

Helsingin yliopisto



Sisältö

1 Johdanto

Klassisiksi ryhmiksi nimitetään eräitä matriisiryhmiä, joihin törmää monissa eri tilanteissa matematiikassa ja fysiikassa. Koska klassiset ryhmät koostuvat lineaarikuvauksista, aloitetaan kurssi lineaarialgebran kertauksella. Sen jälkeen esitellään yleinen lineaarinen ryhmä, jonka alkioina ovat vektoriavaruuden kääntyvät lineaarikuvaukset.

Kaikki muut klassiset ryhmät ovat yleisen lineaarisen ryhmän aliryhmiä, jotka säilyttävät jonkin halutun geometrisen rakenteen eli muodon: esimerkiksi ortogonaaliset muunnokset säilyttävät vektoreiden väliset kulmat ja niiden pituudet. Lineaarisen ryhmän jälkeen käsitellään siis erilaisia muotoja ja täman jälkeen määritellään loput klassiset ryhmät eli ortogonaaliset, unitaariset ja symplektiset ryhmät.

Jokaiselle klassiselle ryhmälle voidaan määritellä tietyn kaavan mukaan aliryhmiä ja tekijäryhmiä. Myös näiden ryhmien nimet määräytyvät aina samalla tavalla. Esimerkiksi yleisen lineaarisella ryhmällä on aliryhmänä erityinen lineaarinen ryhmä ja tekijäryhmänä projektiivinen lineaarinen ryhmä. Erityisellä lineaarisella ryhmällä on edelleen tekijäryhmänä erityinen projektiivinen ryhmä.

Allaolevassa taulukossa on lueteltu klassisten ryhmien tyypit mainittuine ali- ja tekijäryhmineen. Ryhmien nimissä symboli V viittaa vektoriavaruuteen, jonka muunnoksista on kyse. Jokaista tyyppiä kohti on olemassa äärettömän monta ryhmää, sillä joitakin isomorfismeja lukuunottamatta jokaista vektoriavaruutta vastaa eri ryhmä.

Ryhmä	Muoto	Erityinen	Projektiivinen	Erityinen projektiivinen
$GL(V)$	(triviaali)	$SL(V)$	$PGL(V)$	$PSL(V)$
$O(V)$	symmetrinen	$SO(V)$	$PO(V)$	$PSO(V)$
$U(V)$	hermiittinen	$SU(V)$	$PU(V)$	$PSU(V)$
$Sp(V)$	alternoiva	$Sp(V)$	$PSp(V)$	$PSp(V)$

Kurssin lopuksi käsitellään hieman Lien teoriaa sekä äärellisiä yksinkertaisia ryhmiä. Nämä kaksi aihetta liittyvät läheisesti klassisiin ryhmiin ja toivon mukaan antavat viitteitä siitä, miksi klassiset ryhmät ovat tärkeitä.

2 Kertausta: Kuntia, lineaarialgebraa ja ryhmäteoriaa

2.1 Kunnat

Tässä luvussa kerrataan kuntien teoriaa ja esitellään joitakin mahdollisesti uusiä käsitteitä.

Määritelmä 2.1. *Kunnaksi* kutsutaan kolmikkoa $(K, +, \cdot)$, missä K on joukko ja $+$ ja $\cdot$ sen laskutoimituksia, jotka toteuttavat seuraavat ehdot:

(K1) $(K,+)$ ja $(K \setminus \{0\}, \cdot)$ ovat vaihdannaisia ryhmiä

(K2) $(a+b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in K$ (osittelulaki).

Ryhmän $(K,+)$ neutraalialkiota merkitään 0 ja ryhmän $(K \setminus \{0\}, \cdot)$ neutraalialkiota 1. Oletamme aina, että $0 \neq 1$.

Usein kuntaan $(K,+,\cdot)$ viitatessa mainitaan vain joukko K. Joukkoa $K \setminus \{0\}$ merkitään tässä tekstissä K^*.

Määritelmä 2.2. Kunnan *karakteristika* on pienin luonnonllinen luku n, jolle pätee $\underbrace{1 + \cdots + 1}_{n} = 0$. Jos tällaista lukua ei ole olemassa, niin sanotaan, että karakteristika on nolla.

Voidaan osoittaa, että kunnan karakteristika on aina joko nolla tai alkuluku.

Kuntaa kutsutaan äärelliseksi, jos joukossa K on äärellisen monta alkiota, muussa tapauksessa äärettömäksi. Kunnat, joiden karakteristika on 0, ovat äärettömiä.

Lause 2.3. *Jos kunta K on äärellinen, niin ryhmä K^* on syklinen.*

Todistus. Todistus sivuutetaan. □

Seuraava lause osoittaa, että äärelliset kunnat tunnetaan hyvin.

Lause 2.4. *Jos äärellisen kunnan K karakteristika on alkuluku p, niin K:n kertaluku on p^n jollakin $n \in \mathbb{N}$. Jokaista alkulukupotenssia p^n kohti on olemassa kunta, jonka kertaluku on p^n. Samaa kertalukua olevat äärelliset kunnat ovat isomorfisia.*

Todistus. Todistus sivuutetaan. □

Tällä kurssilla äärellistä kuntaa, jonka kertaluku on q, merkitään $\mathbb{F}_q$.

Määritelmä 2.5. Kunta K on *algebrallisesti suljettu*, jos jokaisella K-kertoimisella yhden muuttujan polynomilla on nollakohta K:ssa.

Esimerkki 2.6.

1. Kunnat $\mathbb{Q}$ ja $\mathbb{R}$ ovat äärettömiä ja niiden karakteristika on nolla. Ne eivät ole algebrallisesti suljettuja, koska esim. polynomilla $x^2 + 1$ ei ole nollakohtia kummassakaan. Kunnissa $\mathbb{Q}$ ja $\mathbb{R}$ voidaan toisaalta määritellä järjestysrelaatio $\leq$.

2. Kunta $\mathbb{C}$ on ääretön ja sen karakteristika on nolla. Siinä ei voida määritellä luonnollista järjestysrelaatiota (so. laskutoimitusten kanssa yhteensopivaa täyttä järjestystä).

3. Jos p on alkuluku, niin $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ on äärellinen kunta. Sen karakteristika on p. Se ei ole algebrallisesti suljettu eikä järjestetty.

2.2 Vektoriavaruudet

Seuraavissa luvuissa kerrataan kurssin kannalta oleelliset lineaarialgebran käsitteet. Niiden pitäisi olla tuttuja kursseilta Lineaarialgebra ja matriisilaskenta I ja II. Ainona erona on, että tässä luentomateriaalissa vektoriavaruudet määritellään mielivaltaisen kunnan eikä vain reaalilukujen yli. Suurin osa tuloksista ja todistuksista pysyy kuitenkin samoina.

Määritelmä 2.7. Olkoon K kunta. Joukko V on *K-kertoiminen vektoriavaruus*, jos kaikkiin $u, v \in V$ ja $\alpha \in K$ on liitetty yksikäsitteinen summa $u + v \in V$ ja skalaarikertolasku $\alpha v \in V$ siten, että seuraavat ominaisuudet ovat voimassa:

(V1) $(V, +)$ on vaihdannainen ryhmä

(V2) $\alpha(u + v) = \alpha u + \alpha v$ kaikilla $\alpha \in K$ ja $u, v \in V$

(V3) $(\alpha + \beta)v = \alpha v + \beta v$ kaikilla $\alpha, \beta \in K$ ja $v \in V$

(V4) $(\alpha\beta)v = \alpha(\beta v)$ kaikilla $\alpha, \beta \in K$ ja $v \in V$

(V5) $1v = v$ kaikilla $v \in V$.

Vektoriavaruuden alkioita kutsutaan vektoreiksi ja kunnan K alkioita skalaareiksi. Tässä luentomateriaalissa skalaareita merkitään usein kreikkalaisilla kirjaimilla.

Seuraavissa määritelmissä V on jokin K-kertoiminen vektoriavaruus.

Määritelmä 2.8. Joukko $U \subset V$ on V:n *aliavaruus*, jos $(U, +)$ on $(V, +)$:n aliryhmä ja U on suljettu skalaarikertolaskun suhteen.

Määritelmä 2.9. *Vektoreiden* $v_1, v_2, \dots \in V$ *virittämä aliavaruus* on joukko

$$\langle v_1, v_2 \dots \rangle = \{\alpha_1 v_1 + \dots + \alpha_k v_t \mid \alpha_i \in K, t \in \mathbb{N}\}.$$

Sen alkioita kutsutaan vektoreiden $v_1, \dots, v_k$ *lineaarikombinaatioiksi*. Kyseessä on pienin aliavaruus, joka sisältää vektorit $v_1, \dots, v_k$.

Määritelmä 2.10. Vektorit $v_1, v_2, \dots$ ovat *lineaarisesti riippumattomia*, jos yhtälö

$$x_1 v_1, \dots x_k v_t = 0, \quad \text{missä } x_i \in K \text{ ja } t \in \mathbb{Z},$$

toteutuu vain, kun $x_1 = \dots = x_k = 0$.

Vektorijonoa $(v_1, v_2, \dots)$ kutsutaan avaruuden V *kannaksi*, jos se on lineaarisesti riippumaton ja virittää V:n. Luku n on avaruuden V *dimensio*. Käytännössä tämä tarkoittaa sitä, että jokainen avaruuden V vektori voidaan kirjoittaa kantavektorien lineaarikombinaationa täsmälleen yhdellä tavalla.

Tällä kurssilla käsitellään vain äärellisulotteisia vektoriavaruuksia eli avaruuksia, joiden dimensio on äärellinen.

Olkoon $(v_1, \ldots, v_n)$ K-kertoimisen vektoriavaruuden V kanta. Nyt jokainen V:n vektori v voidaan kirjoittaa muodossa $\sum_{i=1}^{n} a_i v_i$, missä $a_i \in K$. Vektorin v ilmaisemiseen riittää siis tietää kertoimien a_i arvo, ja siten kaikki oleellinen tieto v:stä voidaan tiivistää *sarakevektoriin*

$$\hat{v} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}.$$

Vektoriavaruus V voidaan nyt samastaa *sarakeavaruuden* K^n kanssa, joka koostuu kaikista n-ulotteisista K-kertoimisista sarakevektoreista. Jos x on avaruuden K^n vektori, sen i:nnelle komponentille käytetään standardimerkintää x_i. Tilan säästämiseksi sarakevektorit kirjoitetaan tässä luentomateriaalissa useimmiten muodossa $(x_1, \ldots, x_n)$.

Huomaa, että sarakevektorimerkintää käyttäessä on aina tiedettävä, mikä kanta on kyseessä. Jos asiasta voi syntyä epäselvyyttä, voidaan kanta merkitä näkyviin. Jos vektori x halutaan kirjoittaa esimerkiksi kannassa $S = (v_1, \ldots, v_n)$ ja $x = \sum_i x_i v_i$, käytetään merkintää $\hat{x}_S = (x_1, x_2, \ldots, x_n)$.

Sarakevektoriesityksiä voidaan vaihtaa kannasta toiseen *kannanvaihtomatriiseilla*. Olkoot $S = (v_1, \ldots, v_n)$ ja $T = (u_1, \ldots, u_n)$ kaksi V:n kantaa. Kannanvaihtomatriisi P kannasta S kantaan T on matriisi, jonka sarakkeina ovat *kannan S vektorit ilmaistuina sarakevektoreina kannassa T* eli

$$P = [\hat{v}_{1T} \ \ldots \ \hat{v}_{nT}].$$

Nyt kannasta S kantaan T vaihetaan matriisilla P, eli

$$\hat{v}_T = P\hat{v}_S,$$

missä $\hat{v}_T$ ja $\hat{v}_S$ ovat vektoria v vastaavat sarakevektorit kannoissa S ja T. Kannasta T kantaan S vaihdetaan puolestaan P:n käänteismatriisilla.

Kannanvaihto saattaa kuulostaa hieman sotkuiselta, mutta tärkeintä on muistaa, että se tehdään kertomalla sarakevektoreita kannanvaihtomatriisilla. Käytännössä voi yleensä helposti järkeillä, millainen kannanvaihtomatriisin on oltava.

Sarakevektoreiden sijasta voitaisiin yhtä hyvin käyttää rivivektoreita. Silloin matriisit olisi korvattava transpooseillaan. Tässä luentomateriaalissa kaikki vektorit ovat kuitenkin sarakevektoreita.

2.3 Lineaarikuvaukset

Olkoot V ja U K-kertoimisia vektoriavaruuksia.

Määritelmä 2.11. Kuvaus $L : V \to U$ on *lineaarikuvaus*, jos sille pätee

$$L(v + u) = L(v) + L(u) \tag{L1}$$

$$\text{ja} \quad L(\alpha v) = \alpha L(v) \tag{L2}$$

kaikilla $u, v \in V$ ja $\alpha \in K$.

Bijektiivistä lineaarikuvausta kutsutaan *lineaariseksi isomorfismiksi.* Jos lisäksi kuvauksen lähtö- ja kuvajoukko ovat samat, kutsutaan sitä *lineaariseksi automorfismiksi.*

Jokaiseen lineaarikuvaukseen L vektoriavaruudelta V itselleen voidaan liittää matriisi $\hat{L}$, jonka sarakkeet ovat avaruuden kantavektorien arvot kuvauksessa L (kirjoitettuina sarakevektoreina samassa kannassa). Toisin sanoen, jos $(v_1, v_2, \ldots, v_n)$ on avaruuden V kanta, niin

$$\hat{L} = \left[\widehat{L(v_1)}\ \widehat{L(v_2)}\ \cdots\ \widehat{L(v_n)}\right].$$

Nyt vektorin $v \in V$ arvo kuvauksessa L voidaan määrittää matriisikertolaskun avulla: $\widehat{L(v)} = \hat{L}\hat{v}$. Kuvausten yhdistäminen vastaa matriisien kertomista toisillaan, ja käänteiskuvaukset käänteismatriiseja. Vastaavasti jokainen matriisi voidaan tulkita lineaarikuvaukseksi. Tarpeen vaatiessa käytetty kanta voidaan jälleen merkitä näkyviin matriisin alaindeksinä samaan tapaan kuin vektoreilla.

Myös lineaarikuvauksien tapauksessa kannanvaihto tehdään kannanvaihtomatriiseilla. Olkoon L avaruuden V lineaarikuvaus ja S ja T kaksi V:n kantaa. Olkoon P kannanvaihtomatriisi kannasta S kantaan T. Nyt

$$\hat{L}_T = P\hat{L}_S P^{-1},$$

missä $\hat{L}_T$ ja $\hat{L}_S$ ovat L:n matriisit kannoissa T ja S.

Jokainen n-ulotteinen vektoriavaruus V, jonka kerroinkunta on K, voidaan siis samastaa sarakeavaruuden K^n kanssa, ja sen lineaarikuvaukset $n \times n$-matriisien kanssa. Tässä luentomateriaalissa liikumme sulavasti näiden käsitteiden välillä puhuen toisinaan lineaarikuvauksista ja toisinaan matriiseista. Siksi merkinnän $\hat{v}$ sijasta käytetään yleensä yksinkertaisuuden vuoksi merkintää v ja merkinnän $\hat{L}$ sijasta merkintää L. On kuitenkin tärkeää muistaa, että kannalla on vaikutusta siihen, mitä vektoreita ja lineaarikuvauksia tietyt sarakevektorit ja matriisit vastaavat.

2.4 Matriisit ja determinantit

Matriisia A voidaan merkitä $A = (a_{ij})$, missä a_{ij} on rivin i sarakkeessa j oleva alkio. Yksikkömatriisiksi kutsutaan matriisia

$$I_n = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}$$

ja skalaarimatriisiksi matriisia

$$\alpha I_n = \begin{bmatrix} \alpha & 0 & \ldots & 0 \\ 0 & \alpha & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha \end{bmatrix},$$

missä n on kunnan K dimensio, ja $\alpha \in K$.

Määritelmä 2.12. *Determinanttifunktio* on kuvaus $D : (K^n)^n \to K$, jolle pätevät seuraavat ehdot kaikilla $a_1, a_2, \ldots, a_n \in K^n$:

(D1) jokaisella $i \in \{1, \ldots n\}$ ja kiinteillä $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ kuvaus $a_i \mapsto D(a_1, \ldots, a_i, \ldots, a_n)$ on lineaarinen

(D2) jos $a_i = a_{i+1}$ jollakin $i \in \{1, 2, \ldots, n-1\}$, niin $D(a_1, \ldots, a_n) = 0$

(D3) $D(e_1, \ldots, e_n) = 1$, missä $e_i = (0, \ldots, 1, \ldots, 0)$ (ykkönen i:nnellä paikalla).

Lause 2.13. *Jokaisella $n \geq 1$ on olemassa täsmälleen yksi determinattifunktio $D : (K^n)^n \mapsto K$.*

Määritelmä 2.14. Neliömatriisin A *determinantti* $\det(A)$ on $D(a_1, \ldots, a_n)$, missä $a_1, \ldots, a_n$ ovat A:n sarakkeet ja $D : (K^n)^n \mapsto K$ determinanttifunktio.

Olkoon A $n \times n$-matriisi. Sen determinatti $\det(A)$ toteuttaa muun muassa seuraavat ehdot:

(i) $\det(A) = \det(A^T)$

(ii) $\det(AB) = \det(A)\det(B)$

(iii) $\det(A^{-1}) = \det(A)^{-1}$

Ehdoista ii) ja iii) seuraa, että matriisin A determinantin arvo on sama kuin sen konjugaatin $P^{-1}AP$ (P on mikä tahansa kääntyvä matriisi). Determinantin arvo ei siis muutu kannanvaihdossa.

Ehdosta ii) seuraa, että determinanttikuvaus on ryhmähomomorfismi kääntyvien matriisien ryhmältä ryhmälle K^*. Kääntyvien mariisien muodostamaa ryhmää käsitellään seuraavassa luvussa.

Matriisin A determinantin laskemisessa voi käyttää seuraavaa kehityskaavaa.

Lause 2.15. *Olkoon $j \in \{1, \ldots, n\}$. Tällöin*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

missä A_{ij} on matriisi, joka on saatu A:sta poistamalla i:s rivi ja j:s sarake. Kyseessä on kehitys sarakkeen j suhteen. Vastaavasti voidaan determinantti kehittää minkä tahansa rivin i suhteen.

Apuna determinantin laskemisessa kannattaa käyttää apuna myös allaolevia determinantin ominaisuuksia.

(i) Jos matriisin A tiettyyn sarakkeeseen (tai riviin) lisätään jokin toinen sarake (tai rivi) vakiolla kerrottuna, niin sen determinantti ei muutu.

(ii) Jos matriisissa on kaksi samaa saraketta tai riviä tai jokin rivistä on nolla, on matriisin determinantti nolla.

(iii) Matriisin sarakkeen tai rivin kertominen vakiolla vastaa determinantin kertomista samalla vakiolla.

(iv) Matriisin kahden sarakkeen (tai rivin) vaihtaminen keskenään vastaa determinantin kertomista luvulla -1.

(v) Kolmiomatriisin determinatti on sen diagonaalialkioiden tulo.

2.5 Hitunen ryhmäteoriaa

Tässä luvussa esitellään muutamia tällä kurssilla tarvittavia ryhmäteorian tuloksia ja käsitteitä. Lauseiden todistuksia ei esitetä, ja ne ovatkin hyviä harjoitustehtäviä. Todistukset löytyvät myös kaikista algebran perusoppikirjoista.

Ryhmän keskukseksi kutsutaan niiden alkioiden joukkoa, jotka kommutoivat kaikkien ryhmän alkioiden kanssa.

Määritelmä 2.16. Ryhmän G *keskus* on joukko

$$Z(G) = \{z \in G \mid gz = zg\}.$$

Lause 2.17. *Ryhmän G keskus $Z(G)$ on G:n normaali aliryhmä.*

Ryhmähomomorfismin ydin koostuu niistä alkioista, jotka kuvautuvat neutraalialkiolle.

Määritelmä 2.18. Olkoon f ryhmähomomorfismi ryhmältä G ryhmälle H. Kuvauksen f *ydin* on

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1\}.$$

Ryhmien homomorfialause on hyödyllinen väline todistettaessa ryhmien välisiä isomorfismeja.

Lause 2.19. *Olkoon f ryhmähomomorfismi ryhmältä G ryhmälle H. Tällöin ryhmät $G/\mathrm{Ker}(f)$ ja $\mathrm{Im}(f)$ ovat isomorfisia.*

Koska äärellisen kunnan kääntyvät alkiot muodostavat syklisen ryhmän, tulee seuraava lause tarpeeseen.

Lause 2.20. *Olkoon G syklinen ryhmä, jonka kertaluku on k. Olkoon $H = \{g \in G \mid g^l = 1\}$, missä $l \in \mathbb{N}$. Tällöin H on G:n aliryhmä, jonka kertaluku on $\mathrm{syt}(k, l)$.*

3 Lineaariset ryhmät

3.1 Yleinen ja erityinen lineaarinen ryhmä

Seuraavaksi tutustumme klassista ryhmistä ensimmäiseen, yleiseen lineaariseen ryhmään. Tätä ryhmää Hermann Weyl on kutsunut nimellä "Her All-embracing Majesty".

Olkoon V K-kertoiminen n-ulotteinen vektoriavaruus.

Määritelmä 3.1. *Yleinen lineaarinen ryhmä* $GL(V)$ muodostuu avaruuden V lineaarisista automorfismeista. Ryhmän laskutoimituksena on kuvausten yhdistäminen, neutraalialkiona identtinen kuvaus ja käänteisalkioina käänteiskuvaukset.

Kuten edellisessä luvussa todettiin, lineaarikuvaukset voidaan samastaa matriisien kanssa. Yhtä hyvin voidaan siis sanoa, että yleinen lineaarinen ryhmä koostuu kääntyvistä $n \times n$-matriiseista, joiden alkiot ovat kunnassa K. Laskutoimituksena on matriisikertolasku. Tätä ryhmää merkitään $GL_n(K)$. Jos kunta K on äärellinen, voidaan kirjoittaa $GL_n(q)$, missä q on K:n kertaluku.

Lineaarikuvausten ja matriisien välillä ei tehdä tällä kurssilla suurtakaan eroa ja eri merkintöjen välillä saatetaan siirtyä siis melko huolettomasti.

Ne yleisen lineaarisen ryhmän alkiot, joiden determinantti on yksi, muodostavat aliryhmän, jota kutsutaan erityiseksi lineaariseksi ryhmäksi.

Määritelmä 3.2. *Erityinen lineaarinen ryhmä* on

$$SL(V) = \{g \in G \mid \det(g) = 1\}.$$

Samaan tapaan kuin edellä, myös erityiselle lineaariselle ryhmälle voidaan käyttää merkintöjä $SL_n(K)$ tai $SL_n(q)$.

Lause 3.3. *Ryhmä $SL_n(K)$ on $GL_n(K)$:n normaali aliryhmä.*

Todistus. Luvussa 2.4 todettiin, että determinanttikuvaus on homomorfismi ryhmältä $GL_n(K)$ ryhmälle K^*. Sen ydin on ryhmä $SL_n(K)$. Koska ydin on aina normaali aliryhmä, on lause todistettu. □

Lause 3.4. *Ryhmä $GL_n(K)/SL_n(K)$ on isomorfinen ryhmän K^* kanssa.*

Todistus. Todistuksessa käytetään ryhmien homomorfialausetta. Kuten edellä todettiin, on determinanttikuvaus homomorfismi ryhmältä $GL_n(K)$ ryhmälle K^*. Se on surjektio, sillä jos $\alpha \in K^*$, niin esimerkiksi matriisin

$$\begin{bmatrix} \alpha & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

determinantti on α.

Koska kuvauksen ydin on ryhmä $SL_n(K)$, niin ryhmien homomorfialauseen perustella ryhmät $GL_n(K)/SL_n(K)$ ja K^* ovat isomorfisia. □

3.2 Projektiiviset lineaariset ryhmät

Yleisestä lineaarisesta ryhmästä löytyy muitakin kiinnostavia normaaleja aliryhmiä. Sen keskus $Z(GL_n(K))$ muodostuu skalaarimatriiseista ja on siten isomorfinen syklisen ryhmän K^* kanssa.

Lause 3.5. *Yleisen lineaarisen ryhmän keskus on*

$$Z(GL_n(K)) = \{\alpha I_n \mid \alpha \in K\}.$$

Todistus. Osoitetaan ensin, että kaikki skalaarimatriisit kuuluvat ryhmän $GL_n(K)$ keskukseen. Olkoon αI_n skalaarimatriisi ja $J \in GL_n(K)$. Huomataan, että $J(\alpha I_n) = \alpha J = (\alpha I_n)J$, joten $\alpha I_n \in Z(GL_n(K))$.

Osoitetaan seuraavaksi, että jokainen keskuksen alkio on skalaarimatriisi. Jos $n = 1$, niin väite on selvästikin totta, sillä kaikki matriisit ovat silloin skalaarimatriiseja. Voimme siis olettaa, että vektoriavaruuden $V = K^n$ dimensio on suurempi kuin yksi.

Olkoon $L \in Z(GL_n(K))$ jokin matriisi kannan $S = (v_1, \dots, v_n)$ suhteen kirjoitettuna. Osoitetaan aluksi, että L on diagonaalimatriisi, eli että jokaisella $v_i \in S$ on olemassa sellainen $\alpha_i \in K^*$, että $Lv_i = \alpha_i v_i$. Tämä tehdään vastaoletuksen avulla. Oletetaan siis, että $v_i \in S$ on sellainen, että $Lv_i \notin \langle v_i \rangle$. Merkitään $Lv_i = u$. Valitaan kuvaus $M \in GL_n(K)$ niin, että $Mv_i = v_i$ ja $Mu = v_i + u$. Tämä voidaan tehdä, koska vektorit u ja v_i ovat lineaarisesti riippumattomia, kuten myös vektorit v_i ja $v_i + u$. Nyt $LMv_i = Lv_i = u$ ja $MLv_i = Mu = v_i + u$. Siten $MLv_i \neq LMv_i$, mistä seuraa, että $ML \neq LM$. Tämä on ristiriita, sillä $L \in Z(GL_n(K))$. Siispä L on diagonaalimatriisi.

Seuraavaksi osoitamme, että L on skalaarimatriisi. Olkoot $v_i, v_j \in S$. Oletetaan, että $\alpha_i, \alpha_j \in K^*$ ovat sellaisia, että $Lv_i = \alpha_i v_i$ ja $Lv_j = \alpha_j v_j$. Valitaan kuvaus $N \in GL(V)$ niin, että $Nv_i = v_j$, $Nv_j = -v_i$ ja $Nv_k = v_k$ kaikilla $k \neq i, j$. Nyt $LNv_i = Lv_j = \alpha_j v_j$ ja $NLv_i = \alpha_i N v_i = \alpha_i v_j$. Koska $L \in Z(GL_n(K))$, niin $LN = NL$ ja siten $\alpha_i = \alpha_j$. Tästä seuraa, että L on skalaarimatriisi. $\square$

Vastaavasti erityisen lineaarisen ryhmän keskuksen muodostavat skalaarimatriisit, joiden determinantti on yksi.

Lause 3.6. *Erityisen lineaarisen ryhmän keskus on*

$$Z(SL_n(K)) = \{\alpha I_n \mid \alpha \in K, \alpha^n = 1\},$$

missä I_n on yksikkömatriisi

Todistus. Lause todistetaan samalla tavalla kuin ryhmän $GL_n(K)$ tapauksessa. On vain pidettävä huolta siitä, että kuvaukset M ja N voidaan valita ryhmästä $SL_n(K)$. Kuvauksen N determinantti on itse asiassa jo valmiiksi

1. Jos esimerkiksi $v_i = v_1$ ja $v_j = v_2$, niin N:n matriisi on

$$N = \begin{bmatrix} 0 & -1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Tämän matriisin determinantti on 1.

Tutkitaan seuraavaksi kuvausta M. Oletetaan, että $\det(M) = a$. Valitaan uusi kuvaus M' siten, että se on muuten samanlainen kuin kuvaus M, mutta $M'v_i = a^{-1}v_i$. Tämä ei muuta lauseen todistusta mitenkään. Koska kuvaus M' on saatu kuvauksesta M kertomalla sarake i vakiolla a^{-1}, niin $\det(M') = a^{-1}\det(M) = 1$. Siten voimme käyttää ryhmän $SL(V)$ tapauksessa kuvausta M'. □

Koska ryhmän keskus on normaali aliryhmä, voidaan sen suhteen muodostaa tekijäryhmä. Lineaaristen ryhmien tapauksessa tätä tekijäryhmää kutsutaan projektiiviseksi yleiseksi lineaariseksi ryhmäksi.

Määritelmä 3.7. *Projektiivinen yleinen lineaarinen ryhmä* on tekijäryhmä

$$PGL_n(K) = GL_n(K)/Z(GL_n(K)).$$

Merkitään $Z_G = Z(GL_n(K))$. Ryhmä $PGL_n(K) = GL_n(K)/Z_G$ koostuu sivuluokista gZ_G, missä $g \in GL_n(K)$. Tiedämme, että ryhmän $GL_n(K)$ alkiot g_1 ja g_2 ovat samassa sivuluokassa jos ja vain jos $g_1 \in g_2Z_G$ eli jos ja vain jos $g_1 = g_2(\lambda I_n) = \lambda g_2$ jollakin $\lambda \in K^*$.

Tämä tarkoittaa sitä, että tekijäryhmää $PGL_n(K)$ voidaan ajatella ryhmänä $GL_n(K)$, missä alkiot g ja λg on samastettu kaikilla $\lambda \in K^*$. (Käytännössä se on siis kääntyvien $n \times n$-matriisien joukko, jossa on samastettu ne matriisit, jotka saadaan toisistaan jollakin skalaarilla kertomalla.)

Määritelmä 3.8. *Projektiivinen erityinen lineaarinen ryhmä* on tekijäryhmä

$$PSL_n(K) = SL_n(K)/Z(SL_n(K)).$$

Huomaa, että $PSL_n(K)$ ei ole ryhmän $PGL_n(K)$ aliryhmä. Ryhmältä $PSL_n(K)$ voidaan kuitenkin määritellä injektiivinen homomorfistmi ryhmälle $PGL_n(K)$, joten käytännössä ryhmää $PSL_n(K)$ voidaan käsitellä ryhmän $PGL_n(K)$ aliryhmänä.

Esimerkki 3.9. Ryhmän $GL_n(\mathbb{R})$ keskus $Z_G = Z(GL_n(\mathbb{R}))$ koostuu matriiseista αI_n, missä $\alpha \in \mathbb{R}$. Ryhmän $SL_n(\mathbb{R})$ keskuksessa $Z_S = Z(SL_n(\mathbb{R}))$ ovat puolestaan ylläolevista matriiseista ne, joille pätee $\alpha^n = 1$. Jos n on parillinen, niin tällaisia reaalilukuja on täsmälleen kaksi: 1 ja -1. Siten ryhmän $SL_n(\mathbb{R})$ keskus on $\{I_n, -I_n\}$. Jos taas n on pariton, niin ainoa ehdon toteuttava reaaliluku on -1, ja keskus on $\{I_n\}$.

Tutkitaan ensin miltä projektiivinen erityinen lineaarinen ryhmä näyttää, jos n on parillinen. Ryhmä $PSL_n(\mathbb{R}) = SL_n(\mathbb{R})/Z_S$ koostuu sivuluokista gZ_S, missä $g \in SL_n(K)$. Tiedämme, että ryhmän $SL_n(K)$ alkiot g_1 ja g_2 ovat samassa sivuluokassa jos ja vain jos $g_1 \in g_2 Z_S$ eli jos ja vain jos $g_1 = g_2 I_n = g_2$ tai $g_1 = g_2(-I_n) = -g_2$. Tämä tarkoittaa sitä, että tekijäryhmää $PSL_n(\mathbb{R})$ voidaan ajatella ryhmänä $SL_n(\mathbb{R})$, missä alkiot g ja $-g$ on samastettu.

Jos n on pariton, on $SL_n(\mathbb{R})$ keskus triviaali kuten yllä todettiin. Tästä seuraa, että ryhmä $PSL_n(\mathbb{R})$ on isomorfinen ryhmän $SL_n(\mathbb{R})$ kanssa.

Jos kerroinkunnaksi vaihdetaan $\mathbb{C}$, tulee erityisen lineaarisen ryhmän keskukseen lisää alkioita. Kompleksilukujen kunnassa ykkösen n:nnet juuret muodostavat nimittäin n-alkioisen syklisen ryhmän. Ryhmä $Z(SL_n(\mathbb{C}))$ on sen kanssa isomorfinen.

Esimerkki 3.10. Ryhmä $GL_3(7)$ muodostuu 3×3-matriiseista, joiden alkiot ovat kunnassa $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Sen keskus $Z_G = Z(GL_3(7))$ on kuusialkioinen ryhmä $\{\alpha I_n \mid \alpha \in \mathbb{F}_7^*\}$.

Tekijäryhmä $PGL_3(7)$ muodostuu sivuluokista gZ_G, missä $g \in GL_3(7)$. Esimerkiksi matriisit

$$a = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{ja} \quad b = \begin{bmatrix} 3 & 6 & 2 \\ 0 & 3 & 5 \\ 0 & 0 & 3 \end{bmatrix}.$$

kuuluvat samaan sivuluokkaan, sillä $a \cdot (3I_3) = b$. Siten sivuluokat aZ_G ja bZ_G ovat samat, ja ne ovat siis sama $PGL_3(7)$:n alkio.

Ryhmän $SL_3(7)$ keskukseen kuuluvat ryhmän Z_G alkioista αI_3 ne, joille pätee $\alpha^3 = 1$, eli alkiot I_3, $2I_3$ ja $4I_3$.

3.3 Projektiiviset avaruudet

Yleinen lineaarinen ryhmä säilyttää origon kautta kulkevat suorat. Toisin sanoen, jos kaksi vektoria on samalla origon kautta kulkevalla suoralla, niin myös niiden kuvat ovat samalla origon kautta kulkevalla suoralla. Näitä suoria kutsutaan projektiivisiksi pisteiksi ja niiden joukkoa projektiiviseksi avaruudeksi.

Määritelmä 3.11. Vektoriavaruudesta V johdettu *projektiivinen avaruus* on joukko $\mathbb{P}(V) = \{\langle v \rangle \mid v \in V \setminus \{0\}\}$, missä $\langle v \rangle = \{\alpha v \mid \alpha \in K\}$.

Ryhmän $GL(V)$ alkiot voidaan nyt tulkita projektiivisen avaruuden kuvauksiksi seuraavalla tavalla: jos $g \in GL(V)$ ja $\langle v \rangle \in \mathbb{P}(V)$, niin

$$g(\langle v \rangle) = \langle g(v) \rangle.$$

Eri alkiot saattavat kuvata projektiivisen avaruuden alkioita samalla tavalla. Esimerkiksi skalaarimatriisit pitävät projektiivisen avaruuden pisteet paikoillaan eli käyttäytyvät täsmälleen samalla tavalla kuin neutraalialkio I_n.

Tästä seuraa, että myös ryhmän $PGL(V)$:n alkiot voidaan tulkita projektiivisen avaruuden kuvauksiksi. Se tehdään seuraavasti: Olkoot $\langle v\rangle \in \mathbb{P}(V)$ ja $\bar{g} \in PGL(V)$, jolloin $\bar{g} = gZ(GL(V))$ jollakin $g \in GL(V)$. Määritellään

$$\bar{g}(\langle v\rangle) = \langle g(v)\rangle.$$

Ryhmän $PGL(V)$ alkio kuvaa siis projektiivisen avaruuden alkioita samalla tavalla kuin kyseisen alkion edustaja ryhmässä $GL(V)$. (Lukijan tehtäväksi jää osoittaa, että tämä kuvaus on hyvin määritelty. Se seuraa siitä, että skalaarimatriisit, jotka on ryhmässä $PGL(V)$ samastettu neutraalialkion kanssa, kuvaavat projektiivisen avaruuden pisteitä kuten neutraalialkio.)

Seuraava lause osoittaa, että skalaarimatriisit ovat itse asiassa ainoita alkioita, jotka pitävät kaikki projektiivisen avaruuden alkiot paikoillaan.

Lause 3.12. *Olkoon $g \in GL(V) = GL_n(K)$, ja oletetaan, että $g(\langle v\rangle) = \langle v\rangle$ kaikilla $v \in V$. Tällöin $g = \lambda I_n$ jollakin $\lambda \in K^*$.*

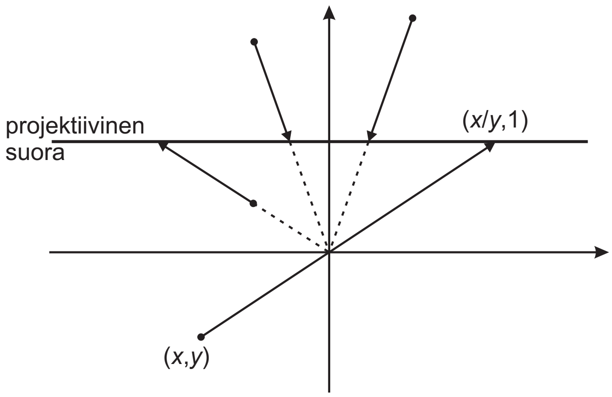
Todistus. Olkoon $v \in V$. Jos V on yksiulotteinen, on väite selvästikin totta. Voidaan siis olettaa, että on olemassa $w \in V$, joka on lineaarisesti riippumaton vektorista v. Koska $g(\langle v\rangle) = \langle v\rangle$ ja $g(\langle w\rangle) = \langle w\rangle$, on olemassa sellaiset skalaarit α ja β, että $g(v) = \alpha v$ ja $g(w) = \beta w$. Lisäksi $g(\langle v + w\rangle) = \langle v + w\rangle$, joten $g(v + w) = \gamma(v + w) = \gamma v + \gamma w$ jollakin $\gamma \in K$. Toisaalta g:n lineaarisuuden nojalla $g(v + w) = g(v) + g(w) = \alpha v + \beta w$. Vektorien v ja w lineaarisesta riippumattomuudesta seuraa, että $\alpha = \gamma = \beta$. Siten $g(v) = \gamma v$ kaikilla $v \in V$, eli g on skalaarimatriisi. □

Ryhmän $GL(V)$ keskus muodostuu siis täsmälleen niistä alkioista, jotka pitävät projektiivisen avaruuden pisteet paikoillaan. Nyt voimmekin tarkastella projektiivista lineaarista ryhmää, jossa kaikki keskuksen alkiot on samastettu. Samastuksesta seuraa, että ryhmässä $PGL(V)$ jokainen alkio on erilainen projektiivisen avaruuden kuvaus. (Tämä jätetään jälleen lukijan osoitettavaksi.)

Siirtymällä tarkastelemaan ryhmää $PGL(V)$ olemme siis päässeet eroon siitä ongelmasta, että ryhmän $GL(V)$ eri alkiot saattavat kuvata projektiivisen avaruuden pisteitä samalla tavalla. Samalla tavoin voidaan ryhmästä $SL(V)$ siirtyä erityiseen projektiiviseen ryhmään $PSL(V)$.

3.3.1 Projektiivinen suora

Aloitetaan projektiivisten avaruuksien tarkastelu kaksiulotteisista avaruuksista johdetuista projektiivisista avaruuksista $\mathbb{P}(K^2)$. Niitä kutsutaan *projektiivisiksi suoriksi.* Projektiivisen suoran alkiot ovat muotoa $\langle(x, y)\rangle$. Jos $y \neq 0$, niin projektiivinen piste $\langle(x, y)\rangle$ on sama piste kuin $\langle(x/y, 1)\rangle$. Siten projektiivinen suora $\mathbb{P}(K^2)$ voidaan samastaa joukon $K \cup \{\infty\}$ kanssa, missä piste $\langle(x, 1)\rangle$ vastaa kunnan alkiota x ja piste $\langle(1, 0)\rangle$ ääretöntä.



Kuva 1: Projektiivinen suora koostuu projektiivisista pisteistä $\langle(x/y, 1)\rangle$

Kuten edellä todettiin, ryhmä $PGL_2(K)$ voidaan tulkita projektiivisen suoran $\mathbb{P}(K^2)$ kuvauksiksi. Matriisin

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

sivuluokka vastaa tällöin projektiivisen suoran kuvausta

$$\langle(x, y)\rangle \mapsto \langle(ax + by, cx + dy)\rangle.$$

Joukossa $K \cup \{\infty\}$ tämä kuvaus taas on muotoa

$$z \mapsto \frac{az + b}{cz + d}$$

ja sitä kutsutaan möbiuskuvaukseksi. Jos $K = \mathbb{C}$, ovat nämä kuvaukset tuttuja funktioteoriasta.

Määritelmä 3.13. *Möbiuskuvaus* on rationaalifunktio $f : K \cup \{\infty\} \to K \cup \{\infty\}$, joka on muotoa

$$f(x) = \frac{ax + b}{cx + d},$$

missä $a, b, c, d \in \mathbb{R}$ ja $ad - bc \neq 0$. Funktion f arvot pisteissä ∞ ja $-\frac{d}{c}$ määritellään seuraavasti: $f(\infty) = \frac{a}{c}$ ja $f(-\frac{d}{c}) = \infty$.

Möbiuskuvausten joukko muodostaa ryhmän, joka on isomorfinen ryhmän $PGL_2(K)$ kanssa. Möbiuskuvaukset, joilla $ad - bc$ on neliö, muodostavat ryhmän, joka on isomorfinen $PSL_2(K)$:n kanssa. Näiden väitteiden todistaminen jätetään harjoitustehtäväksi.

3.3.2 Projektiivinen taso

Projektiivisia avaruuksia, jotka on johdettu kolmiulotteisesta vektoriavaruudesta, kutsutaan *projektiivisiksi tasoiksi.*

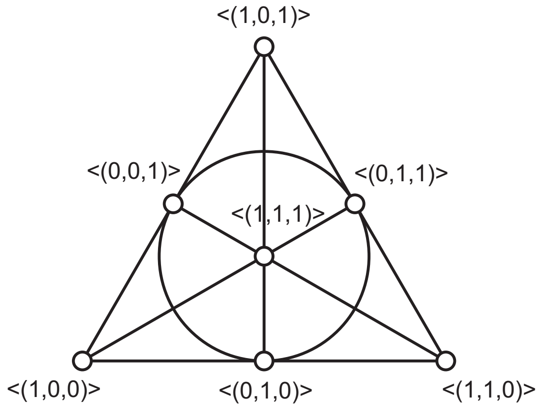
Tutkitaan seuraavaksi projektiivista tasoa $\mathbb{P}(\mathbb{F}_2^3)$, missä $\mathbb{F}_2$ on kaksialkioinen kunta $\{0,1\}$. Avaruudessa $\mathbb{F}_2^3$ on $2^3 = 8$ vektoria, jotka ovat

$$(0,0,0),(1,0,0),(0,1,0),(0,0,1),(0,1,1),(1,0,1),(1,1,0),(1,1,1).$$

Projektiivisen taso koostuu siis seitsemästä alkioista:

$$\begin{aligned}\mathbb{P}(\mathbb{F}_2^3) =\big\{&\langle(1,0,0)\rangle,\ \langle(0,1,0)\rangle,\ \langle(0,0,1)\rangle,\\ &\langle(0,1,1)\rangle,\ \langle(1,0,1)\rangle,\ \langle(1,1,0)\rangle,\ \langle(1,1,1)\rangle\big\}.\end{aligned}$$

Kahden vektorin virittämää aliavaruutta kutsutaan projektiivisen tason suoraksi. Projektiivisen tason pisteen $\langle v\rangle$ sanotaan olevan projektiivisella suoralla $\langle w,u\rangle$, jos suora $\langle v\rangle$ on tasossa $\langle w,u\rangle$. Projektiivisen tason $\mathbb{P}(\mathbb{F}_2^3)$ tapauksessa suoria on seitsemän, ja ne on piirretty allaolevaan kuvaan. Muodostuva diagrammi on kuuluisa Fanon taso.



Kuva 2: Fanon taso eli projektiivinen taso $\mathbb{P}(\mathbb{F}_2^3)$

3.4 Ryhmien kertalukuja

Äärellisten lineaaristen ryhmien kertalukujen laskeminen on melko yksinkertaista.

Lause 3.14. *Ryhmän $GL_n(q)$ kertaluku on*

$$|GL_n(q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}).$$

Todistus. Ryhmän $GL_n(q)$ alkiot vastaavat vektoriavaruuden $\mathbb{F}_q^n$ kannanvaihtoja. Ryhmän kertaluvun selvittämiseen riittää siis kaikkien mahdollisten kannanvaihtojen lukumäärän laskeminen.

Olkoon $(v_1, \ldots, v_n)$ jokin avaruuden $\mathbb{F}_q^n$ kanta. Vektori v_1 voidaan kannanvaihdossa kuvata mille tahansa nollasta poikkeavalle vektorille, joten eri vaihtoehtoja on $q^n - 1$. (Vektoriavaruudessa $\mathbb{F}_q^n$ on q^n vektoria.)

Vektori v_2 taas voidaan kuvata mille tahansa vektorille, joka ei ole vektorin v_1 virittämässä aliavaruudessa. Vaihtoehtoja on siis $q^n - q$. Vektori v_3 puolestaan voidaan kuvata mille tahansa vektorille, joka ei ole vektorien v_1 ja v_2 virittämässä aliavaruudessa. Vaihtoehtoja on siis $q^n - q^2$. Näin jatkaen voidaan todeta, että erilaisia kannanvaihtoja on $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ kappaletta. □

Muiden ryhmien kertalukujen lasku on nyt vaivatonta.

Lause 3.15. *Ryhmän $SL_n(q)$ kertaluku on $|GL_n(q)|/(q-1)$.*

Todistus. Lauseen 3.4 nojalla

$$|SL_n(q)| = \frac{|GL_n(q)|}{|K^*|} = \frac{|GL_n(q)|}{q-1}.$$

□

Lause 3.16. *Ryhmän $PGL_n(q)$ kertaluku on $|GL_n(q)|/(q-1)$.*

Todistus. Koska $PGL_n(q)$ on tekijäryhmä $GL_n(q)/Z(GL_n(q))$, niin sen kertaluku on $|GL_n(q)|/|Z(GL_n(q))|$. Aikaisemmin on osoitettu, että $Z(GL_n(q))$ on isomorfinen ryhmän F_q^* kanssa. Koska $\mathbb{F}_q^*$:n kertaluku on $q-1$, on väite todistettu. □

Lause 3.17. *Ryhmän $PSL_n(q)$ kertaluku on $|SL_n(q)|/\operatorname{syt}(q-1,n)$.*

Todistus. Väitteen todistamiseksi riittää laskea ryhmän $Z(SL_n(q))$ kertaluku. Tämän laskemiseksi taas riittää laskea keskuksen kanssa isomorfisen ryhmän $H = \{\alpha \in \mathbb{F}_q^* \mid \alpha^n = 1\}$ alkioiden lukumäärä. Lauseen 2.3 perusteella $\mathbb{F}_q^*$ on syklinen ryhmä, jonka kertaluku on $q-1$. Siten lauseesta 2.3 seuraa, että aliryhmän H kertaluku on $\operatorname{syt}(q-1,n)$. □

4 Bilineaariset muodot

4.1 Johdanto: sisätulo euklidisessa avaruudessa

Vektoriavaruuden rakenne mahdollistaa monien tavallisten geometristen käsitteiden määrittelemisen. Pisteet, suorat, tasot ym. voidaan määritellä luonnollisesti aliavaruuksien avulla. Kuitenkin esimerkiksi kulman käsitteen määrittelemiseksi tarvitaan jotain lisää.

Tavallisessa euklidisessa avaruudessa $\mathbb{R}^n$ vektorien väliset kulmat voidaan määritellä tutun *pistetulon* avulla:

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = x_1 y_1 + \cdots + x_n y_n.$$

Usein ollaan erityisesti kiinnostuneita siitä, mitkä vektorit ovat *kohtisuorassa* toisiaan vastaan. Tämä tapahtuu euklidisessa avaruudessa täsmälleen silloin, kun pistetulon arvo on 0. Pistetulon määritelmää ei voi kuitenkaan käyttää sellaisenaan esimerkiksi ääretönulotteisissa avaruuksissa. Tällöin turvaudutaan yleisempään *sisätulon* käsitteeseen. Reaalikertoimisen vektoriavaruuden sisätulo on kahden vektorin pareilta kerroinkunnalle (tässä $\mathbb{R}$) määriteltävä kuvaus, joka toteuttaa seuraavat ehdot kaikilla vektoreilla x, y, v ja skalaareilla λ:

$$\langle x + y, v \rangle = \langle x, v \rangle + \langle y, v \rangle \tag{ST1}$$
$$\langle \lambda x, y \rangle = \lambda \langle x, y \rangle \tag{ST2}$$
$$\langle x, y \rangle = \langle y, x \rangle \tag{ST3}$$
$$\langle x, x \rangle \geq 0, \quad \text{ja} \quad \langle x, x \rangle = 0 \iff x = 0. \tag{ST4}$$

Ehtoja (ST1) ja (ST2) kutsutaan lineaarisuusehdoiksi, ehtoa (ST3) symmetrisyydeksi ja ehtoa (ST4) positiiviseksi definiittisyydeksi. Tavallinen pistetulo täyttää kaikki nämä ehdot. Jos sisätulo on olemassa, voidaan määritellä myös vektorin pituus ja vektorien välinen kulma:

$$|v| = \sqrt{\langle v, v \rangle}, \qquad \cos \measuredangle(v, w) = \frac{\langle v, w \rangle}{|v||w|}.$$

Yleisessä tapauksessa vektoriavaruuteen ei voida määritellä minkäänlaista sisätuloa, koska esimerkiksi ehdon (ST4) tarkistamiseksi kerroinkunnassa on oltava järjestysrelaatio $\geq$ (tai vähintään on kyettävä sanomaan mitkä sisätulon arvot ovat positiivisia). Sisätulon käsitettä voidaan kuitenkin edelleen yleistää.

4.2 Määritelmä ja matriisiesitys

Oletetaan jatkossa, että käytetyt vektoriavaruudet ovat äärellisulotteisia.

Määritelmä 4.1. Olkoon V vektoriavaruus, kerroinkuntana K. Kuvausta $B : V \times V \to K$ kutsutaan *bilineaariseksi muodoksi*, jos se täyttää seuraavat ehdot kaikilla vektoreilla x, y, z ja skalaareilla λ:

$$B(x+y,z) = B(x,z) + B(y,z) \tag{B1}$$
$$B(\lambda x, y) = \lambda B(x,y) \tag{B2}$$
$$B(x, y+z) = B(x,y) + B(x,z) \tag{B3}$$
$$B(x, \lambda y) = \lambda B(x,y). \tag{B4}$$

Jos avaruudelle kiinnitetään jokin kanta $(v_1, \ldots, v_n)$, bilineaarinen muoto B voidaan ilmaista matriisina $\hat{B} = [b_{ij}]$, missä $b_{ij} = B(v_i, v_j)$ kaikilla i, j. Tällöin kaikilla vektoreilla x, y pätee

$$B(x,y) = x^\top \hat{B} y.$$

Jos valitusta kannasta ei ole epäselvyyttä, voidaan muoto B ja sitä vastaava matriisi $\hat{B}$ yleensä samastaa.

4.3 Ekvivalenssi

Määritelmä 4.2. Bilineaaristen muotojen B_1 ja B_2 sanotaan olevan *ekvivalentteja*, jos on olemassa jokin vektoriavaruuden lineaarinen automorfismi L, jolle pätee $B_1(x,y) = B_2(Lx, Ly)$.

Esimerkki 4.3. Tarkastellaan $\mathbb{R}^2$ bilineaarista muotoa

$$B(x,y) = x_1 y_1 + 2x_1 y_2 + 2x_2 y_1 + x_2 y_2,$$

missä $x = (x_1, x_2)$ ja $x = (y_1, y_2)$. Suorittamalla vektoriavaruudelle lineaarinen muunnos $x_1' = x_1 + x_2$, $x_2' = x_1 - x_2$, muoto voidaan kirjoittaa yksinkertaisemmin:

$$\begin{aligned} B(x', y') &= (x_1 + x_2)(y_1 + y_2) + 2(x_1 + x_2)(y_1 - y_2) \\ &\quad + 2(x_1 - x_2)(y_1 + y_2) + (x_1 - x_2)(y_1 - y_2) \\ &= 6x_1 y_1 - 2x_2 y_2. \end{aligned}$$

Muunnettu muoto $B'(x,y) = 6x_1y_1 - 2x_2y_2$ on ekvivalentti alkuperäisen kanssa.

Muunnetun muodon matriisiesitys saadaan seuraavasti:

$$x^\top \hat{B}' y = B'(x,y) = B(Lx, Ly) = (Lx)^\top \hat{B}(Ly) = x^\top (L^\top \hat{B} L) y.$$

Koska ylläolevan täytyy päteä kaikilla kantavektoreilla, nähdään, että muunnettua muotoa vastaa matriisi $\hat{B}' = L^\top \hat{B} L$. Tällaista matriisia sanotaan matriisin $\hat{B}$ *kongruentiksi.*

Matriisien tapauksessa ekvivalenssi vastaa *kannanvaihtoa.*

Lause 4.4. *Bilineaariset muodot B_1 ja B_2 avaruudessa V ovat ekvivalentit, jos ja vain jos on olemassa kannat $S = (v_1, \ldots, v_n)$ ja $T = (w_1, \ldots, w_n)$, joiden suhteen matriisiesitykset $\hat{B}_1$ ja $\hat{B}_2$ ovat samat.*

Todistus. Oletetaan ensin, että L on ekvivalenssi muotojen B_1 ja B_2 välillä. Valitaan kanta S mielivaltaisesti ja asetetaan $w_i = Lv_i$ kaikilla i. Nyt $(w_1, \ldots, w_n)$ on kanta (koska L on kääntyvä), ja kaikilla i, j pätee

$$\hat{B}_1(i,j) = B_1(v_i, v_j) = B_2(Lv_i, Lv_j) = B_2(w_i, w_j) = \hat{B}_2(i,j).$$

Täten $\hat{B}_1 = \hat{B}_2$.

Oletetaan sitten, että matriisiesitykset $\hat{B}_1$ ja $\hat{B}_2$ kantojen S ja T suhteen ovat samat. Määritellään lineaarinen isomorfismi L kaavalla $Lv_i = w_i$. Olkoot $x = \sum_i a_i v_i$ ja $y = \sum_j b_j v_j$ kaksi mielivaltaista vektoria. Tällöin

$$\begin{aligned} B_1(x,y) &= B_1\left(\sum_i a_i v_i, \sum_j b_j v_j\right) = \sum_{i,j} a_i b_j B_1(v_i, v_j) = \sum_{i,j} a_i b_j \hat{B}_1(i,j) \\ &= \sum_{i,j} a_i b_j \hat{B}_2(i,j) = \sum_{i,j} a_i b_j B_2(w_i, w_j) = \sum_{i,j} a_i b_j B_2(Lv_i, Lv_j) \\ &= B_2\left(\sum_i a_i Lv_i, \sum_j b_j Lv_j\right) = B_2(Lx, Ly). \end{aligned}$$

□

4.4 Kohtisuoruus

Bilineaarista muotoa B voidaan käyttää kohtisuoruuden eli *ortogonaalisuuden* määrittelemiseen samalla tavoin kuin sisätuloakin, kunhan B on *refleksiivinen*. Tämä tarkoittaa sitä, että

$$B(v,w) = 0 \iff B(w,v) = 0. \tag{R1}$$

Tällöin voidaan määritellä kohtisuoruus.

Määritelmä 4.5. Oletetaan, että B on refleksiivinen bilineaarinen muoto. Vektorien v ja w sanotaan olevan kohtisuorassa toisiaan vastaan, jos $B(v,w) = 0$. Tällöin merkitään $v \perp w$.

Määritelmä 4.6. Olkoon W vektoriavaruuden V aliavaruus. Aliavaruuden W *kohtisuora komplementti* refleksiivisen muodon B suhteen on

$$W^{\perp_B} = \{v \in V \mid B(v,w) = 0 \text{ kaikilla } w \in W\}.$$

Kohtisuora komplementti on myös avaruuden W aliavaruus. Jos käytettävä muoto on asiayhteydestä selvä, kohtisuoraa komplementtia merkitään $W^{\perp}$.

Ne vektorit, jotka ovat kohtisuorassa kaikkia vektoreita vastaan, muodostavat oman aliavaruutensa.

Määritelmä 4.7. Vektoriavaruuden V *radikaali* refleksiivisen muodon B suhteen on joukko

$$\mathrm{rad}_B(V) = \{v \in V \mid B(v,w) = 0 \text{ kaikilla } w \in V\}.$$

Jos asiayhteydestä on selvä, mihin muotoon viitataan, voidaan radikaalia merkitä myös $\mathrm{rad}(V)$.

Määritelmä 4.8. Jos vektoriavaruuden V radikaali muodon B suhteen on epätriviaali ($\neq \{0\}$), niin sanotaan että muoto on *surkastunut*.

Minkä tahansa aliavaruuden kohtisuora komplementti sisältää koko avaruuden radikaalin. Toisaalta, jos radikaali on triviaali, niin vastaava muoto ei ole surkastunut.

4.5 Symmetriset ja alternoivat muodot

Määritellään ensin muutamia bilineaarisen muodon tyyppejä.

Määritelmä 4.9. Bilineaarista muotoa B kutsutaan

(1) *symmetriseksi*, jos $B(v,w) = B(w,v)$ kaikilla vektoreilla v, w

(2a) *alternoivaksi*, jos $B(v,v) = 0$ kaikilla vektoreilla v

(2b) *antisymmetriseksi*, jos $B(v,w) = -B(w,v)$ kaikilla vektoreilla v, w.

Alternoiva muoto on aina myös antisymmetrinen, mutta antisymmetrisyydestä seuraa alternoivuus vain, jos kerroinkunnan karakteristika ei ole 2. Symmetrinen muoto voi olla alternoiva vain, jos $B(v,w) = 0$ kaikilla vektoreilla v, w. Sekä symmetriset että alternoivat muodot ovat refleksiivisiä. Lisäksi osoittautuu, että muunlaisia refleksiivisiä muotoja ei ole olemassa.

Lause 4.10. *Jokainen refleksiivinen bilineaarinen muoto on joko symmetrinen tai alternoiva.*

Lauseen todistus ei ole vaikea mutta sisältää paljon näpertelyä lausekkeiden kanssa. Halukkaat voivat tarkistaa todistuksen esimerkiksi Larry C. Groven kirjasta Classical Groups and Geometric Algebra (propositio 2.7).

Symmetriset bilineaariset muodot eivät poikkea kovin paljon sisätuloista. Ainoastaan ehto (S4) eli positiivinen definiittisyys jää mahdollisesti toteutumatta. Tämä estää vektorien pituuden sekä mielivaltaisten kulmien määrittelemisen tavalliseen tapaan neliöjuuren avulla. Kuitenkin symmetrisillä muodoilla kohtisuoruus käyttäytyy yleensä odotetulla tavalla. Alternoivilla muodoilla sen sijaan kohtisuoruus on jonkin verran eksoottisempi ominaisuus: määritelmän mukaan jokainen vektori on kohtisuorassa itseään vastaan.

4.6 Isometrioista

Olkoon B jokin bilineaarinen muoto vektoriavaruudessa V. Sellaisia kääntyviä lineaarikuvauksia $L : V \to V$, jotka *säilyttävät* muodon B eli joille pätee

$$B(Lx, Ly) = B(x, y) \quad \text{kaikilla } x, y \in V,$$

kutsutaan *B-isometrioiksi*. Nimi tulee siitä, että kuvaus ei muuta sitä geometriaa, jonka B määrittää avaruuteen V. Tämä geometria saattaa esimerkiksi määritellä vektorien pituudet, tai mitkä vektorit ovat kohtisuorassa toisiaan vastaan.

Jonkin muodon suhteen määritellyt isometriat muodostavat aina ryhmän $GL(V)$ aliryhmän. Helposti nimittäin nähdään, että isometrioiden tulot ja käänteiskuvaukset (isometriat ovat määritelmän mukaan kääntyviä) ovat edelleen isometrioita:

$$\begin{aligned} &B\big(L_2(L_1x), L_2(L_1y)\big) = B(L_1x, L_1y) = B(x, y) \quad \text{ja} \\ &B(L^{-1}x, L^{-1}y) = B\big(L(L^{-1}x), L(L^{-1}y)\big) = B(x, y). \end{aligned}$$

Seuraavissa luvuissa käsiteltävät klassiset ryhmät ovat johonkin muotoon liittyvien isometrioiden ryhmiä.

Oletetaan, että $\hat{B}$ on muodon B matriisiesitys ja että $\hat{L}$ on kuvausta L vastaava matriisi. Nyt L on isometria jos ja vain jos

$$v^\top \hat{B} w = (\hat{L}v)^\top \hat{B}(\hat{L}w) = v^\top (\hat{L}^\top \hat{B}\hat{L})w \qquad \text{kaikilla } v, w.$$

Näin saadaan helposti tarkistettava ehto isometrialle: $\hat{B} = \hat{L}^\top \hat{B} \hat{L}$.

Isometrioita tarkasteltaessa ekvivalentit muodot pyritään yleensä samastamaan. On nimittäin niin, että ekvivalentteja muotoja vastaavat isometriaryhmät ovat *isomorfisia*. Tarkemmin sanottuna, jos $B'(v, w) = B(Tv, Tw)$ jollakin lineaarikuvauksella T ja L on jokin B-isometria, niin

$$B'(T^{-1}LTv, T^{-1}LTw) = B(LTv, LTw) = B(Tv, Tw) = B'(v, w).$$

Jokaista B-isometriaa L vastaa siis B'-isometria $T^{-1}LT$. Isometriaryhmien välinen kuvaus $L \mapsto T^{-1}LT$, eli konjugointi alkiolla $T \in GL(V)$, on isomorfismi.

Lause 4.11. *Ekvivalentteja muotoja vastaavat isometriaryhmät ovat toistensa konjugaatteja kääntyvien lineaarikuvausten ryhmässä $GL(V)$.*

5 Ortogonaaliset ryhmät

Tässä luvussa tarkastellaan symmetristen bilineaaristen muotojen isometriaryhmiä. Yksinkertaistuksen vuoksi tapaus, jossa kerroinkunnan karakteristika on 2, käsitellään lopuksi erillisessä kappaleessa, ja siihen asti oletetaan, että kyseinen karakteristika ei ole 2.

5.1 Määritelmä ja perusominaisuudet

Määritelmä 5.1. Oletetaan, että B on surkastumaton symmetrinen bilineaarinen muoto vektoriavaruudessa V. Jos lineaarikuvaus g säilyttää muodon B, niin sanotaan että g on *ortogonaalinen* (muodon B suhteen). Ortogonaalisten kuvausten ryhmää kutsutaan *ortogonaaliseksi ryhmäksi* ja merkitään $O^{(B)}(V)$.

Ortogonaalisen ryhmän rakenne riippuu muodosta B, mutta jos muoto on asiayhteydestä selvä, voidaan ryhmää merkitä $O(V)$. Toisaalta äärellisulotteisen vektoriavaruuden määrittävät isomorfiaa vaille sen kerroinkunta K ja dimensio n, joten ortogonaalista ryhmää voidaan merkitä myös $O_n^{(B)}(K)$ tai $O_n(K)$. Lisäksi erilaisissa erikoistapauksissa tavataan vielä lukuisia muita merkintätapoja.

Ortogonaaliset kuvaukset jakautuvat kahteen tyyppiin determinantin perusteella. Nimittäin, jos $g \in O^{(B)}(V)$, niin $B = g^\top Bg$, ja

$$\det(B) = \det(g^\top Bg) = \det(g^\top)\det(B)\det(g) = \det(g)^2\det(B),$$

sillä $\det(A^\top) = \det(A)$ kaikilla matriiseilla A. Jakamalla yllä olevan yhtälön molemmat puolet luvulla $\det(B)$ saadaan $\det(g)^2 = 1$, josta puolestaan $\det(g) = \pm 1$. Ortogonaalisia kuvauksia, joiden determinantti on 1, kutsutaan *kierroiksi*. Ne muodostavat ortogonaalisen ryhmän normaalin aliryhmän, mikä nähdään esimerkiksi siitä, että determinanttikuvaus on homomorfismi kerroinkunnan multiplikatiiviselle ryhmälle (tai sitten suoraan tarkistamalla normaalin aliryhmän ehdot). Tätä aliryhmää nimitetään *erityiseksi ortogonaaliseksi ryhmäksi* ja merkitään $SO^{(B)}(V)$. Erityisen ortogonaalisen ryhmän indeksi $[O(V) : SO(V)]$ on korkeintaan 2, mistä saadaan seuraava lause.

Lause 5.2. *Oletetaan, että $O(V) \neq SO(V)$, ja kiinnitetään jokin $p \in O(V) \setminus SO(V)$. Joukko $SO(V) \cup \{p\}$ virittää ryhmän $O(V)$, ja jokainen $g \in O(V)$ on joko muotoa r tai $r \cdot p$, missä $r \in SO(V)$.*

Todistus. Jos $g \in SO(V)$, niin tulos on selvä. Voidaan siis olettaa, että $g \in O(V) \setminus SO(V)$. Koska aliryhmällä $SO(V)$ on vain kaksi sivuluokkaa: $SO(V)$ ja $SO(V)\cdot p$, niin g kuuluu sivuluokkaan $SO(V)\cdot p$. Näin ollen $g = r\cdot p$ jollain kierrolla r. □

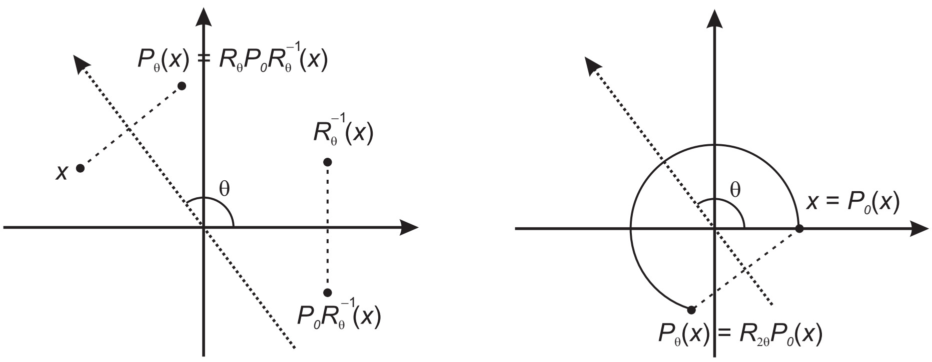
Itse asiassa myöhemmin nähdään, että $O(V) \neq SO(V)$. Siis aliryhmän $SO(V)$ indeksi ryhmässä $O(V)$ on aina 2, ja edellisen lauseen oletus oli tarpeeton.

Esimerkki 5.3. Tarkastellaan avaruutta $\mathbb{R}^n$ ja siinä muotona tavallista pistetuloa $x \cdot y$. Lineaarialgebrasta tiedetään, että kunkin vektorin euklidinen pituus saadaan kaavasta $\sqrt{x \cdot x}$ ja kahden vektorin välinen kulma kaavasta $(x \cdot y)/(|x||y|)$. Koska ortogonaaliset kuvaukset säilyttävät pistetulon, ne siis säilyttävät vektorien pituudet ja niiden väliset kulmat. Geometrisessä mielessä tällaiset kuvaukset ovat *kiertoja* tai *peilauksia* tai niiden yhdistelmiä.

Tasossa $\mathbb{R}^2$ kiertoa kulman φ verran origon ympäri vastaa matriisi

$$R_\varphi = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}.$$

Tällaisen matriisin determinantti on $\cos^2\varphi + \sin^2\varphi = 1$, joten kierrot kuuluvat ryhmään $SO_2(\mathbb{R})$. Tasossa tämä kiertoryhmä on vaihdannainen, koska $R_\varphi \cdot R_\psi = R_{\varphi+\psi}$.



Kuva 3: Peilauksen kaavan johtaminen kahdella eri tavalla

Tarkastellaan peilauksia origon kautta kulkevan suoran yli. Peilaus x-akselin yli hoituu matriisilla $P_0 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Olkoon θ jonkin mielivaltaisen suoran ja positiivisen x-akselin välinen kulma. Peilaus tämän suoran yli saadaan peilauksesta P_0 konjugoimalla sitä sopivalla kierrolla:

$$P_\theta = R_\theta P_0 R_\theta^{-1} = R_\theta P_0 R_{-\theta} = \begin{bmatrix} \cos^2\theta - \sin^2\theta & 2\sin\theta\cos\theta \\ 2\sin\theta\cos\theta & \sin^2\theta - \cos^2\theta \end{bmatrix}.$$

Tästä nähdään jo, että kaikkien suoran yli tapahtuvien peilausten determinantti on -1, koska konjugointi ei vaikuta determinanttiin ja $\det P_0 = -1$. Kuitenkin edellä esitetyn lauseen nojalla tiedetään, että P_θ voidaan lausua myös tulona peilauksesta P_0 ja jostain kierrosta R_φ. Tämä kierto saadaan selville, kun huomataan, että $P_\theta(1,0) = (R_\varphi \cdot P_0)(1,0) = R_\varphi(1,0)$ ja toisaalta $P_\theta(1,0) = R_{2\theta}(1,0)$ (ks. kuva 3). Näin ollen

$$P_\theta = R_{2\theta} P_0 = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}.$$

Tuloksista voidaan lukea trigonometristen funktioiden kaksinkertaisen kulman kaavat.

Kuten yleisen lineaarisen ryhmän tapauksessa, voidaan myös ortogonaalisessa ryhmässä samastaa kuvaukset, jotka eroavat toisistaan vain skalaarikertoimella. Näin saadaan *projektiivinen ortogonaalinen ryhmä* $PO^{(B)}(V)$, jonka alkiot toimivat projektiivisessa avaruudessa. Vastaavasti, jos lähtökohtana ovat vain kierrot eli ryhmän $SO^{(B)}(V)$ alkiot, saadaan *erityinen projektiivinen ortogonaalinen ryhmä* $PSO^{(B)}(V)$.

5.2 Ortogonaaliset kannat

Tässä kappaleessa kuvaillaan, miten symmetrinen muoto voidaan aina ilmaista tietyssä normaalimuodossa. Todetaan ensin eräs ortogonaalisia komplementteja koskeva hyödyllinen tulos.

Lemma 5.4. *Oletetaan, että B on refleksiivinen bilineaarinen muoto avaruudessa V, ja että aliavaruudelle W pätee* $\mathrm{rad}(W) = \{0\}$. *Tällöin jokaisella $v \in V$ on yksikäsitteinen esitys muodossa $v = w + u$, missä $w \in W$ ja $u \in W^\perp$ (eli V on aliavaruuksien W ja $W^\perp$ suora summa).*

Todistus. Olkoon $(v_1, \dots, v_r)$ aliavaruuden W kanta. Jatketaan sitä vektoreilla $v_{r+1}, \dots, v_n$ niin, että siitä tulee kanta koko avaruudelle V. Olkoon $\hat{B} = [b_{ij}]$ muodon V matriisi tässä kannassa, ja olkoon $x = \sum_i x_i v_i \in V$ mielivaltainen. Nyt $x \in W^\perp$ jos ja vain jos kaikilla i pätee $B(v_i, x) = 0$ eli

$$\sum_{j=1}^{r} b_{ij} x_j = 0.$$

Siispä x on yhtälöryhmän $B'X = 0$ ratkaisu, missä B' on $r \times n$-matriisi, jonka rivit ovat samat kuin B:n r ensimmäistä riviä. Lineaarialgebrasta tiedetään, että tällöin $\dim W^\perp = \dim \mathrm{Null}(B') = n - \mathrm{rank}(B') \geq n - r$. Näin ollen $V \subset W + W^\perp$, joten jokainen V:n vektori voidaan kirjoittaa summana avaruuksien W ja $W^\perp$ vektoreista.

Toisaalta, jos $v = w + u = w' + u'$, missä $w, w' \in W$ ja $u, u' \in W^\perp$, niin $w - w' = u - u' \in W \cap W^\perp$. Oletuksen mukaan $\mathrm{rad}(W) = W \cap W^\perp = \{0\}$, joten $w = w'$ ja $u = u'$. $\square$

Lause 5.5. *Olkoon B symmetrinen bilineaarinen muoto vektoriavaruudessa V. Tällöin on olemassa kanta $(v_1, \dots, v_n)$, jonka suhteen B:n matriisiesitys on muotoa*

$$\hat{B} = \begin{bmatrix} b_1 & 0 & & \cdots & & 0 \\ 0 & \ddots & & & & \\ & & b_r & & & \\ \vdots & & & 0 & & \vdots \\ & & & & \ddots & \\ 0 & & & \cdots & & 0 \end{bmatrix},$$

missä $b_i \neq 0$ kaikilla $i \in \{1, \dots, r\}$. Lisäksi jono $(v_{r+1}, \dots, v_n)$ on avaruuden $\mathrm{rad}(V)$ *kanta.*

Todistus. (Hahmotelma.) Jos $B(v,w) = 0$ kaikilla $v, w \in V$, niin voidaan asettaa $r = 0$. Muussa tapauksessa löytyy jokin $v_1 \in V$, jolle $B(v_1, v_1) \neq 0$ (osoitettu harjoitustehtävässä). Nyt avaruus $W = \langle v_1 \rangle$ ei ole surkastunut, joten $W \cap W^{\perp} = \{0\}$. Jos $n > 1$, niin $\dim W^{\perp} > 0$ edellisen lemman nojalla. Tällöin konstruktiota voidaan jatkaa valitsemalla $v_2 \in W^{\perp}$, jolloin v_1 ja v_2 ovat lineaarisesti riippumattomat. Kuten aiemmin, jos $B(v,w) \neq 0$ joillakin $v, w \in W^{\perp}$, niin voidaan olettaa, että $B(v_2, v_2) \neq 0$.

Kun konstruktiota on jatkettu r askelta, niin on saatu jono $(v_1, \ldots, v_r)$, joka virittää jonkin surkastumattoman aliavaruuden U. Lisäksi $B(v_i, v_i) \neq 0$ kaikilla $i \leq r$, ja $B(v_i, v_j) = 0$ kun $i \neq j$. Jos $r < n$, niin konstruktio on pysähtynyt ennen aikojaan, mikä tapahtuu vain, jos $B(v,w) = 0$ kaikilla $v, w \in U^{\perp}$. Tällöin jono $(v_1, \ldots, v_r)$ voidaan täydentää avaruuden V kannaksi lisäämällä mitkä tahansa lineaarisesti riippumattomat vektorit $v_{r+1}, \ldots, v_n \in U^{\perp}$. Koska $U \cap U^{\perp} = \{0\}$, avaruuden $U^{\perp}$ dimensio on $n - r$, joten jono $(v_{r+1}, \ldots, v_n)$ on sen kanta. Edelleen on helppo nähdä, että $U^{\perp} = \mathrm{rad}(V)$. □

Huomautus 5.6. Edellisen lauseen todistuksen konstruktiota voi sellaisenaan käyttää ortogonaalisen kannan löytämiseksi. Oletetaan, että avaruudella on kanta $(v_1, \ldots, v_n)$. Valitaan ensin $u_1 = v_1$. Jos on voitu valita kantavektorit $u_1, \ldots, u_k$ siten, että $B(u_i, u_i) \neq 0$ kaikilla $i \leq k$, seuraava kantavektori saadaan kaavasta

$$u_{k+1} = v_{k+1} - \sum_{i=1}^{k} \frac{B(u_i, v_{k+1})}{B(u_i, u_i)} u_i.$$

Tällöin nimittäin $u_{k+1} \perp u_i$ kaikilla $i \leq k$. Tätä rekursiivista menetelmää kutsutaan *Gram-Schmidtin ortogonalisointimenetelmäksi*. On kuitenkin mahdollista, että jossain vaiheessa $B(u_{k+1}, u_{k+1}) = 0$ (voi olla jopa $B(v_1, v_1) = 0$). Tällöin yllä olevaa kaavaa ei voi soveltaa, vaan täytyy esimerkiksi pyrkiä vaihtamaan vektorien järjestystä alkuperäisessä kannassa.

Edellisessä lauseessa valitut kantavektorit voidaan tarpeen vaatiessa *normalisoida* valitsemalla $v_i' = c_i v_i$ jollain skalaarilla c_i, jolloin matriisimuodon diagonaalilla oleva alkio b_i muuttuu alkioksi $c_i^2 b_i$. Näin saadaan seuraavat tärkeät korollaarit.

Korollaari 5.7. *Olkoon B symmetrinen bilineaarinen muoto vektoriavaruudessa K^n. Jos kerroinkunnan K kaikilla alkioilla on neliöjuuri (esim. jos kunta on algebrallisesti suljettu kuten $\mathbb{C}$), niin on olemassa sellainen kanta, jossa B:n matriisiesitys on*

$$\hat{B} = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0_{n-r} \end{array}\right].$$

Korollaari 5.8. *Euklidisessa avaruudessa $\mathbb{R}^n$ jokaiselle symmetriselle bilineaariselle muodolle löytyy kanta, jossa sen matriisimuoto on*

$$\hat{B} = \left[\begin{array}{c|c|c} I_r & 0 & 0 \\ \hline 0 & -I_s & 0 \\ \hline 0 & 0 & 0_{n-r+s} \end{array}\right].$$

5.3 Peilauksista

Tässä luvussa tarkastellaan lähemmin peilauksia jonkin *hypertason* suhteen. Hypertasoksi kutsutaan n-ulotteisen avaruuden $n-1$-ulotteista aliavaruutta. Peilauksia varten tarvitaan vektoreita, joilla $B(v, v) \neq 0$.

Määritelmä 5.9. Vektoria $u \neq 0$ kutsutaan *isotrooppiseksi*, jos $B(u, u) = 0$.

Jos $u \in V$ ei ole isotrooppinen, niin $u^\perp$ on perusesimerkki hypertasosta.

Määritelmä 5.10. Olkoon $u \in V$ jokin epäisotrooppinen vektori. Kuvausta p, jolle pätee $p(u) = -u$ ja $p(w) = w$ kaikilla $u \perp w$, kutsutaan *(ortogonaaliseksi) peilaukseksi vektorin u suuntaan* tai, toisin sanoin, *hypertason $u^\perp$ yli.*

Peilaus vektorin u suuntaan on yksikäsitteinen, koska voidaan valita ortogonaalinen kanta niin, että u on yksi kantavektoreista, jolloin peilaus määräytyy kantavektorien arvoista. Peilaukselle voidaan johtaa seuraava kaava:

$$p_u(v) = v - 2\frac{B(v, u)}{B(u, u)}u.$$

Kaavasta voidaan tarkistaa, että peilaukset ovat ortogonaalisia kuvauksia:

$$\begin{aligned} B(p_u(v), p_u(w)) &= B\left(v - 2\frac{B(v, u)}{B(u, u)}u,\ w - 2\frac{B(w, u)}{B(u, u)}u\right) \\ &= B(v, w) - 4\frac{B(v, u)B(w, u)}{B(u, u)} + 4\frac{B(v, u)B(w, u)B(u, u)}{B(u, u)^2} \\ &= B(v, w). \end{aligned}$$

Esimerkki 5.11. Tarkastellaan tasoa $\mathbb{R}^2$, jossa bilineaarisena muotona on

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

Tällaista avaruutta kutsutaan *hyperboliseksi tasoksi.* Vektorin $x = (x_1, x_2)$ "pituus" on tässä avaruudessa

$$B(x, x) = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1^2 - x_2^2.$$

Jos $x_1 = \pm x_2$, niin $B(x, x) = 0$, ja x on isotrooppinen. Tällaisen vektorin suhteen ei peilauksia voi tehdä. Sen sijaan esimerkiksi vektori $u = (1, 2)$

ei ole isotrooppinen: $B(u,u) = -3$. Ratkaistaan u:ta vastaan kohtisuoran hypertason $u^\perp$ yhtälö:

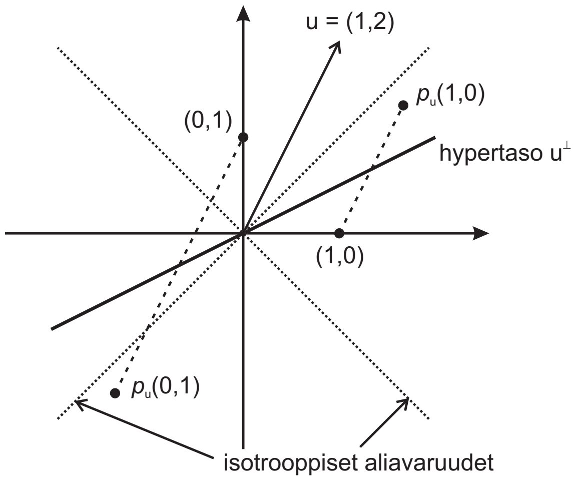
$$B(u,x) = 0 \iff \begin{bmatrix} 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 - 2x_2 = 0.$$

Hypertaso on siis suora, jonka yhtälö on $x_2 = \frac{1}{2}x_1$ (ks. kuva 4). Vektorin u suhteen tehtävän peilauksen kaava saadaan yllä esitetystä lausekkeesta:

$$\begin{aligned} p_u(x) &= x - 2\frac{B(x,u)}{B(u,u)}u = x - 2 \cdot \frac{x_1 - 2x_2}{-3}u \\ &= \frac{1}{3}(5x_1 - 4x_2, 4x_1 - 5x_2). \end{aligned}$$

Peilauksen matriisi on

$$\hat{p}_u = \begin{bmatrix} 5/3 & -4/3 \\ 4/3 & -5/3 \end{bmatrix}.$$



Kuva 4: Peilaus hyperbolisessa tasossa

Peilauksen p_u determinantti on aina -1. Tämä nähdään esimerkiksi valitsemalla ortogonaalinen kanta $(u, v_2, \ldots, v_n)$. Nyt $p_u(u) = -u$ ja $p(v_i) = 1$ kaikilla $i \in \{2, \ldots, n\}$, joten peilauksen matriisi näyttää seuraavalta:

$$p_u = \begin{bmatrix} -1 & 0 \\ 0 & I_{n-1} \end{bmatrix}.$$

Tämän matriisin determinantti on selvästi -1. Nyt voidaan vihdoin todistaa, että $O(V) \setminus SO(V)$ on epätyhjä.

Lause 5.12. *Olkoon B surkastumaton symmetrinen bilineaarinen muoto avaruudessa V. Tällöin löytyy jokin $g \in O^{(B)}(V) \setminus SO^{(B)}(V)$, mistä seuraa $[O^{(B)}(V) : SO^{(B)}(V)] = 2$.*

Todistus. Koska symmetrinen muoto B ei ole surkastunut, on olemassa jokin epäisotrooppinen vektori $u \in V$. Olkoon p_u vastaava ortogonaalinen peilaus. Koska kaikkien peilausten determinantti on -1, niin $u \notin SO^{(B)}(V)$. □

Peilausten merkitys korostuu siinä, että ne *virittävät* ortogonaalisen ryhmän. Tämä tärkeä seikka mainitaan seuraavassa lauseessa, jonka monivaiheinen todistus joudutaan sivuuttamaan.

Lause 5.13. *(Cartan-Dieudonné) Olkoon B surkastumaton bilineaarinen muoto n-ulotteisessa avaruudessa V. Jos $g \in O^{(B)}(V)$, niin g on tulo korkeintaan n kappaleesta peilauksia.*

Yllä olevasta lauseesta saadaan helppona seurauksena muun muassa tuttu kolmiulotteisia kiertoja koskeva lause, joka euklidisen avaruuden tapauksessa tunnetaan nimellä Eulerin lause. Merkitään tässä yhteydessä kuvauksen g *kiintopistealiavaruutta* $\mathrm{Fix}(g) = \{v \in V \mid g(v) = v\}$.

Korollaari 5.14. *Jos* $\dim V = 3$ *ja* $r \in SO(V)$, $r \neq \mathrm{id}$, *niin kiintopisteavaruuden dimensio on* $\dim \mathrm{Fix}(r) = 1$. *Toisin sanoen, g:tä vastaa jokin yksiulotteinen "kiertoakseli".*

Todistus. Kuvaus on r on tulo korkeintaan kolmesta peilauksesta. Koska peilausten determinantti on -1 ja $r \in SO(V)$, niin peilauksia on täsmälleen kaksi. Voidaan siis merkitä $r = p_1 p_2$, missä p_1 ja p_2 ovat peilauksia, jotka kiinnittävät 2-ulotteiset hypertasot W_1 ja W_2. Nyt $W_1 \cap W_2 \subset \mathrm{Fix}(r)$.

Koska $W_1 + W_2 \subset V$ ja

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2),$$

nähdään, että $\dim(W_1 \cap W_2) \geq 1$. Siispä myös $\dim \mathrm{Fix}(r) \geq 1$. Toisaalta, jos avaruuden $\mathrm{Fix}(r)$ dimensio olisi 2 tai 3, niin r kiinnittäisi jonkin hypertason H, ja jokaisella $v \in H^\perp$ pätisi $r(v) \in H^\perp$ (koska r on ortogonaalinen) eli $r(v) = \lambda v$ jollain skalaarilla λ. Sopivassa kannassa olisi siis

$$r = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \lambda \neq 0.$$

Tämä on mahdotonta, koska $\det(r) = 1$ ja $r \neq I$. Siispä täytyy päteä $\dim \mathrm{Fix}(r) = \dim(W_1 \cap W_2) = 1$. □

Peilausten avulla voidaan määritellä myös eräs kiinnostava erityisen ortogonaalisen ryhmän aliryhmä. Seuraavassa määritelmässä $SO(V)$ on erityinen ortogonaalinen ryhmä avaruudessa, jonka kerroinkunta on K.

Määritelmä 5.15. Jokainen $g \in SO^{(B)}(V)$ voidaan kirjoittaa tulona $g = p_1 \cdots p_r$, missä kukin p_i on peilaus vektorin v_i suuntaan. Nyt sanotaan, että kuvaus g kuuluu *omegaryhmään* $\Omega^{(B)}(V)$, jos ja vain jos tulo $\prod_i B(v_i, v_i)$ on neliö kunnassa K.

Omegaryhmän määritelmä näyttäisi riippuvan siitä, minkälaisena tulona alkio g kirjoitetaan. Voidaan kuitenkin osoittaa, että tulo $\prod_i B(v_i, v_i)$ joko on aina neliö tai sitten ei, riippumatta siitä, miten peilaukset valitaan. Lisäksi on melko helppo todistaa, että omegaryhmä tosiaan on ryhmä, vieläpä ryhmän $SO(V)$ normaali aliryhmä.

5.4 Muodot $\mathbb{R}^n$:ssä, definiittisyys ja Sylvesterin lause

Tässä kappaleessa tarkastellaan avaruutta $\mathbb{R}^n$, mutta tarkastelu voidaan monilta osin yleistää sellaisiin avaruuksiin, joiden kerroinkunta on *täysin järjestettävissä*. Tämä tarkoittaa sitä, että kerroinkunnassa K on olemassa sellainen järjestysrelaatio $<$, että kaikilla alkioilla $a, b, c \in K$ pätee

1) joko $a < b$ tai $b < a$ tai $a = b$

2) jos $a < b$, niin $a + c < b + c$

3) jos $a < b$ ja $c > 0$, niin $ca < cb$.

Äärellisiä kuntia tai kompleksilukujen kuntaa $\mathbb{C}$ ei voi järjestää.

Määritelmä 5.16. Oletetaan, että B on symmetrinen bilineaarinen muoto vektoriavaruudessa, jonka kerroinkunta on täysin järjestetty. Muotoa B sanotaan *positiivisesti definiitiksi*, jos $B(v, v) > 0$ aina kun $v \neq 0$.

Vastaavasti voidaan määritellä *negatiivinen definiittisyys*. Positiivisesti definiittiä symmetristä bilineaarista muotoa kutsutaan *sisätuloksi*. Seuraavassa luvussa nähdään, että definiittisyyden käsite voidaan yleistää myös kompleksiluvuille, kunhan muodon bilineaarisuus korvataan muilla ehdoilla.

Reaaliavaruudessa positiivisesti (tai yhtä hyvin negatiivisesti) definiitit muodot ovat siitä mielenkiintoisia, että niiden avulla voidaan määritellä vektorien (aidot) pituudet ja niiden väliset kulmat tutuilla kaavoilla

$$|v| = \sqrt{B(v, v)} \qquad \text{ja} \qquad \cos \measuredangle(v, w) = \frac{B(v, w)}{|v||w|}.$$

Positiivinen definiittisyys vaaditaan neliöjuurten ottamista varten. Negatiivisesti definiitin muodon tapauksessa voidaan määritellä $|v| = \sqrt{-B(v, v)}$ jne.

Korollaarin 5.8 mukaan jokainen avaruuden $\mathbb{R}^n$ surkastumaton muoto voidaan esittää matriisilla

$$B = \begin{bmatrix} I_r & 0 \\ 0 & -I_s \end{bmatrix},$$

missä $r + s = n$. Paria (r, s) kutsutaan avaruuden *metriseksi merkinnäksi*. Seuraavan lauseen mukaan metrinen merkintä on avaruuden invariantti.

Lause 5.17 (Sylvesterin inertialause). *Olkoon B surkastumaton symmetrinen bilineaarinen muoto avaruudessa $\mathbb{R}^n$. Oletetaan, että avaruudella on kannat $V_1 = (v_1, \ldots, v_n)$ ja $V_2 = (w_1, \ldots, w_n)$, joiden suhteen muodon B matriisit ovat*

$$\hat{B}_1 = \begin{bmatrix} I_r & 0 \\ 0 & -I_{n-r} \end{bmatrix} \quad \textit{ja} \quad \hat{B}_2 = \begin{bmatrix} I_s & 0 \\ 0 & -I_{n-s} \end{bmatrix},$$

missä $0 < r \leq s$. Tällöin $r = s$.

Todistus. Olkoot $W_1 = \langle v_1, \ldots, v_r \rangle$ ja $W_2 = \langle w_{s+1}, \ldots, w_n \rangle$. Olkoon $x = \sum_{i=1}^{r} x_i v_i \in W_1 \setminus \{0\}$, jolloin $B(x,x) = \sum_{i=1}^{r} x_i^2 > 0$. Toisaalta, jos $y = \sum_{i=s+1}^{n} y_i w_i \in W_2$, niin $B(y,y) = -\sum_{i=s+1}^{n} y_i^2 \leq 0$. Näin ollen $W_1 \cap W_2 = \{0\}$, joten $\dim W_1 + \dim W_2 \leq n$ eli $r + (n-s) \leq n$, josta $s \leq r$. $\square$

Reaaliavaruudessa jokainen positiivisesti definiitti symmetrinen bilineaarinen muoto on ekvivalentti tavallisen pistetulon kanssa. *Jokainen $\mathbb{R}^n$:n sisätulo on siis ekvivalentti pistetulon kanssa.* Tähän muotoon liittyvää ortogonaalista ryhmää merkitään monissa lähteissä yksinkertaisesti $O(n)$. On helppo tarkistaa, että mikäli kuvaus säilyttää muodon B, se säilyttää myös muodon $-B$, joten negatiivisesti definiitteihin muotoihin liittyy sama ortogonaalinen ryhmä. Myös epädefiniiteillä muodoilla on omat sovelluksensa, kuten seuraavasta esimerkistä nähdään.

Esimerkki 5.18. Suppean suhteellisuusteorian aika-avaruus on neliulotteinen reaaliavaruus. Sen vektorit ovat siis muotoa (t, x_1, x_2, x_3), missä t-komponentti kuvaa aikaa ja muut paikkaa. Näitä *nelivektoreita* kutsutaan myös *tapahtumiksi*. Aika-avaruus noudattaa geometriaa, jota kuvaa symmetrinen bilineaarinen muoto

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

Tällaista avaruutta kutsutaan *Minkowskin avaruudeksi*. Minkowskin avaruuden ortogonaalinen ryhmä $O_4^{(M)}(\mathbb{R})$ on niin sanottu *Lorentzin ryhmä*. Suhteellisuusteorian mukaan Lorentzin ryhmän alkiot kuvaavat muunnoksia sellaisten koordinaatistojen välillä, jotka liikkuvat tasaisella nopeudella toistensa suhteen. Lorentzin ryhmä sisältää paikka-aliavaruuden $\langle (x_1, x_2, x_3) \rangle$ kierrot ja peilaukset eli tavallisen ortogonaalisen ryhmän $O(3) = O_3(\mathbb{R})$ (pistetulon suhteen).

Lorentzin muunnokset säilyttävät tapahtuman v *nelipituuden* $M(v,v)$. Nelipituuden perusteella tapahtumat voidaan jakaa kolmeen tyyppiin. Jos arvo on positiivinen, tapahtumaa sanotaan *ajanluonteiseksi*, jos se on negatiivinen, *paikanluonteiseksi*, ja jos se on 0, *valonluonteiseksi*. Ajanluonteiset vektorit kuvaavat niitä tapahtumia, joista tieto voi päästä origossa olevaan tapahtumaan valoa hitaammin (tai joihin tieto voi päästä origossa olevasta tapahtumasta). Valonluonteisiin tapahtumiin voi origosta päästä ainoastaan valon nopeudella, ja paikanluonteisiin ei ole mahdollista päästä lainkaan.

Jos rajoitutaan tarkastelemaan yhtä paikkakoordinaattia, Minkowskin avaruus kutistuu hyperboliseksi tasoksi. Isotrooppiset aliavaruudet muodostavat niin kutsutun *valokartion*, joka kuvaa valonsäteen mahdollisia reittejä origosta (tai origoon). Valoa hitaammat kappaleet voivat edetä vain valokartion sillä puolella oleviin pisteisiin v, joissa $M(v, v) > 0$.

5.5 Neliömuodot

Jokaista symmetristä bilineaarista muotoa vastaa tietty *neliömuoto*, joka on sukua vektorin pituudelle eli normille.

Määritelmä 5.19. Olkoon B symmetrinen bilineaarinen muoto avaruudessa V, jonka kerroinkunta on K. Muotoa B vastaava *neliömuoto* on kuvaus $Q : V \to K$, jolle pätee $Q(v) = B(v, v)$.

Ortogonaaliset kuvaukset säilyttävät neliömuodon. Seuraavat neliömuodon ominaisuudet on helppo osoittaa määritelmästä lähtien:

$$Q(v + w) = Q(v) + 2B(v, w) + Q(w) \tag{Q1}$$

$$Q(av) = a^2 Q(v). \tag{Q2}$$

Ortogonaaliset ryhmät voidaan määritellä yhtä hyvin neliömuodon kuin bilineaarisen muodon avulla, koska jos neliömuoto tunnetaan, bilineaarisen muodon arvot saadaan kaavasta

$$B(v, w) = \frac{1}{2}\big(Q(v + w) - Q(v) - Q(w)\big). \tag{5.20}$$

Jos bilineaarisena muotona on tavallinen euklidisen avaruuden pistetulo, niin neliömuoto on $Q(v) = v \cdot v$, ja tämän neliöjuuri on vektorin *normi* eli pituus.

Huom. Kaavassa (5.20) on olennaista, että kerroinkunnan karakteristika ei ole 2, sillä muuten kahdella jakoa ei voida suorittaa. Karakteristikan ollessa kaksi neliömuodot ja ortogonaaliset ryhmät määritellään kuitenkin hieman eri tavalla, mihin palataan tämän luvun lopussa.

Esimerkki 5.21. Tasossa $\mathbb{R}^2$ mahdolliset symmetriset bilineaariset muodot ovat muotoa

$$B = \begin{bmatrix} a & b \\ b & c \end{bmatrix}, \quad a, b, c \in \mathbb{R}.$$

Tällaista muotoa vastaa neliömuoto

$$Q(x) = ax_1^2 + 2bx_1x_2 + cx_2^2.$$

Yhtälön $Q(x) = r$ ratkaisujoukko on siis jokin toisen asteen käyrä, ja käänteen jokainen toisen asteen käyrä on jonkin yhtälön $Q(x) = r$ ratkaisujoukko. Lauseesta 5.17 seuraa, että kannanvaihdolla jokainen neliömuoto voidaan palauttaa joko muotoon

$$x_1^2 + x_2^2 \qquad \text{tai} \qquad x_1^2 - x_2^2.$$

Erityisesti tästä seuraa, että jokainen toisen asteen käyrä on joko ellipsi tai hyperbeli.

5.6 Äärelliset kunnat

Jos vektoriavaruuden kerroinkunta on äärellinen, siinä voidaan määritellä korkeintaan kaksi epäekvivalenttia symmetristä bilineaarista muotoa. Seuraavissa lauseissa oletetaan, että B on symmetrinen bilineaarinen muoto avaruudessa V, jonka kerroinkunta on äärellinen. (Kunnan karakteristika on edelleen eri kuin 2.) Molempien lauseiden todistukset sivuutetaan.

Lause 5.22. *Jos V:n dimensio on pariton, löytyy ortogonaalinen kanta, jossa B:n matriisi on diagonaalinen ja diagonaalialkiot ovat järjestyksessä $(1,-1,1,-1,\dots,1,-1,-1)$.*

Lause 5.23. *Jos V:n dimensio on parillinen, löytyy ortogonaalinen kanta, jossa B:n matriisi on diagonaalinen ja diagonaalialkiot ovat joko*

a) $(1,-1,1,-1,\dots,1,-1)$ ($+$-tyyppi) tai

b) $(1,-1,1,-1,\dots,1,-d)$, missä d ei ole neliö ($-$-tyyppi).

Äärellisen kerroinkunnan tapauksessa avaruus voidaan siis jakaa suoraksi summaksi kahdesta aliavaruudesta U ja W ($U \cap W = \{0\}$), joista U koostuu pelkästään hyperbolisista tasoista ja sen dimensio on siis välttämättä parillinen. Lisäksi voidaan osoittaa, että W, jonka dimensio on 0, 1 tai 2, ei sisällä yhtään isotrooppista vektoria.

Jos avaruuden dimensio on parillinen, niin $+$-tyypin muotoa vastaavaa ortogonaalista ryhmää merkitään $O^+(V)$ ja $-$-tyypin muotoa vastaavaa ryhmää $O^-(V)$. Parittoman dimension ryhmää merkitään $O^0(V)$.

Esimerkki 5.24. Tarkastellaan tasoa $\mathbb{F}_3^2$, jossa muotona käytetään pistetuloa $B(x,y) = x_1y_1 + x_2y_2$. Tämän muodon matriisi on $B = \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$, ja koska -1 ei ole neliö kunnassa $\mathbb{F}_3$, niin muoto on edellisen lauseen kohdassa (b) mainittua tyyppiä.

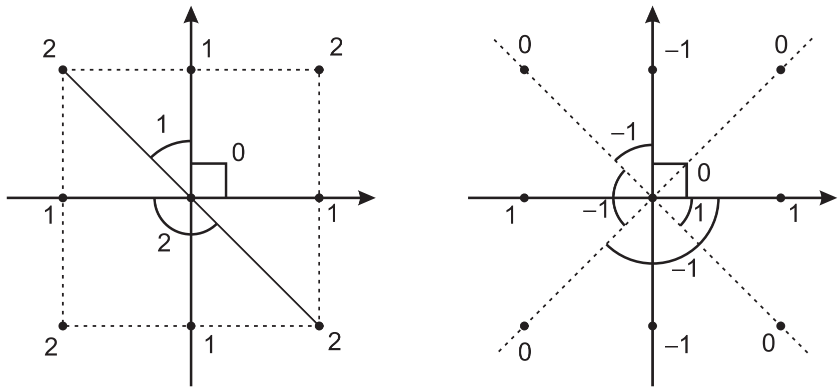
Neliömuodon arvot eli "vektorien pituudet" ovat

$$Q(0,0) = 0, \quad Q(\pm1,0) = Q(0,\pm1) = 1 \quad \text{ja} \quad Q(\pm1,\pm1) = 2.$$

Oletetaan nyt, että $g \in O_2^-(3)$. Koska ortogonaaliset kuvaukset säilyttävät neliömuodon arvot, on kullakin vektorilla (paitsi nollavektorilla) vain neljä mahdollista tapaa kuvautua. Esimerkiksi $g(1,0)$ voi olla joko $(1,0)$, $(-1,0)$, $(0,1)$ tai $(0,-1)$.

Kun yhden kantavektorin v_1 kuva on valittu, toisen kantavektorin v_2 kuvaksi jää tasan kaksi mahdollisuutta arvojen $g(v_1) \neq \pm g(v_2)$ lineaarisen riippumattomuuden vuoksi. Kumpikin valinta on mahdollinen. Jos esimerkiksi $g(1,0) = (0,1)$, niin $g(0,1)$ voi olla joko $(-1,0)$ tai $(1,0)$; edellisessä tapauksessa $g \in SO_2^-(3)$, jälkimmäisessä $\det g = -1$.

Nähtiin, että ryhmässä $O_2^-(3)$ on 8 alkiota. Itse asiassa bilineaarisen muodon arvoja eli "vektorien välisiä kulmia" tarkkailemalla nähdään, että ortogonaalisten kuvausten on säilytettävä kuvassa 5 näkyvän neliön nurkat nurkkina ja särmät särminä, mistä seuraa, että $O_2^-(3)$ on isomorfinen neliön symmetriaryhmän D_8 kanssa.



Kuva 5: Neliömuodon ja bilineaarisen muodon arvoja −- ja +-tyypin tasoissa

Jos muotona on $B = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, niin kyseessä on hyperbolinen taso. Tällöin kummallakin kantavektorilla on vain yksi vaihtoehto mihin kuvautua, koska neliömuodon arvot ovat

$$Q(\pm 1, 0) = 1, \quad Q(0, \pm 1) = -1 \quad \text{ja} \quad Q(\pm 1, \pm 1) = Q(0,0) = 0.$$

Tuloksena saadaan neljän alkion ortogonaalinen ryhmä, jossa kaikkien alkioiden kertaluku on kaksi. Onkin niin, että $O_2^+(3)$ on isomorfinen Kleinin neliryhmän kanssa.

5.7 Karakteristikan ollessa 2

Kun kerroinkunnan karakteristika on kaksi, tapahtuu ortogonaalisten ryhmien kannalta kaksi merkittävää asiaa. Ensinnäkin neliömuodosta ei voi johtaa bilineaarisen muodon arvoja, koska kaavaa (5.20) ei voida soveltaa. Toisaalta jokainen determinantti on 1, joten kaikki ortogonaaliset kuvaukset ovat aikaisemman määritelmän mukaisesti kiertoja.

Karakteristikan ollessa kaksi lähdetään bilineaarisen muodon sijasti liikkeelle neliömuodosta, joka määritellään nyt hieman aikaisemmasta poikkeavalla tavalla.

Määritelmä 5.25. *(Kun karakteristika on 2.)* K-kertoimisen avaruuden V *neliömuoto* on funktio $Q : V \to K$, jolle pätee kaikilla $x, y \in V$

$$Q(ax + by) = a^2 Q(x) + abB(x, y) + b^2 Q(y), \tag{5.26}$$

missä B on jokin (tavanomainen) bilineaarinen muoto avaruudessa V.

Nyt neliömuotoa vastaava bilineaarinen muoto on yksikäsitteinen, mutta bilineaarisesta muodosta ei voida johtaa neliömuodon arvoja. Ortogonaaliset kuvaukset määritellään niin, että ne säilyttävät jonkin neliömuodon, eli

$$g \in O(V) \iff Q(g(v)) = Q(v).$$

Jokaisen kuvauksen determinantti on 1, joten $O(V) = SO(V)$. Peilauksia ei voida määritellä, koska $-v = v$ kaikilla vektoreilla v. Peilauksien paikalla voidaan käyttää niin kutsuttuja *transvektioita.* Omegaryhmää vastaava aliryhmä määritellään myös näiden transvektioiden avulla. (Toisinaan tällä tavoin määriteltyä omegaryhmää kutsutaan myös erityiseksi ortogonaaliseksi ryhmäksi, kun karakteristika on 2.)

Kuten aikaisemmin, jos avaruuden kerroinkunta on äärellinen ja dimensio pariton, on kannanvaihtoa vaille olemassa vain yksi neliömuoto. Jos dimensio on parillinen, muotoja on kaksi. Nämä muodot poikkeavat kuitenkin monelta osin niistä muodoista, jotka saadaan parittoman karakteristikan tapauksessa.

6 Unitaariset ryhmät

Unitaariset ryhmät ovat sukua ortogonaalisille ryhmille, ja monilla tässä luvussa esiteltävillä asioilla on vastineensa ortogonaalisten ryhmien teoriassa. Unitaariset ryhmät määritellään hermiittisten muotojen avulla, jotka muun muassa hoitavat sisätulon tehtävää kompleksikertoimisissa avaruuksissa. Hermiittisten muotojen isometrioina unitaariset kuvaukset säilyttävät kompleksiavaruudessa vektorien pituudet ja niiden väliset kulmat samoin kuin ortogonaaliset tekevät euklidisessa avaruudessa.

6.1 Seskvilineaariset[1] muodot

Ennen muotojen määrittelyä on rajoitettava tarkasteltavien vektoriavaruuksien joukkoa. Koko tässä luvussa oletetaan, että vektoriavaruuden kerroinkunnassa K voidaan määritellä *automorfismi* σ, jonka kertaluku on 2. Tämä tarkoittaa sitä, että kuntaan K voidaan liittää kuntaisomorfismi $\sigma : K \to K$, jolle pätee $\sigma \circ \sigma = \mathrm{id}$. Automorfismin arvoa luvulla a merkitään

$$\sigma(a) = \bar{a}$$

ja kutsutaan luvun a *konjugaattiluvuksi* tai *konjugaatiksi*. Itse automorfismia kutsutaan *konjugoinniksi*. Tavallisin esimerkki konjugoinnista on kompleksikonjugointi $a + bi \mapsto a - bi$. Kaikissa kunnissa konjugointia ei voida määritellä.

Konjugointiin liittyy läheisesti *normikuvaus* N, joka määritellään kaavalla

$$N(a) = a\bar{a} \qquad \text{kaikilla } a \in K.$$

Kompleksiluvuilla normi vastaa luvun modulin neliötä.

Konjugoinnin avulla voidaan määritellä tässä luvussa käytettävät muodot, jotka poikkeavat hieman bilineaarisista muodoista. Oletetaan seuraavassa, että V on K-kertoiminen vektoriavaruus ja että kunnassa K on määritelty konjugointiautomorfismi.

Määritelmä 6.1. Kuvausta $S : V \times V \to K$ kutsutaan *seskvilineaariseksi muodoksi*, jos se täyttää seuraavat ehdot kaikilla $x, y, z \in V$ ja $\lambda \in K$:

$$S(x + z, y) = S(x, y) + S(z, y) \tag{S1}$$
$$S(\lambda x, y) = \lambda S(x, y) \tag{S2}$$
$$S(x, y + z) = S(x, y) + S(x, z) \tag{S3}$$
$$S(x, \lambda y) = \bar{\lambda} S(x, y) \tag{S4}$$

Seskvilineaariset kuvaukset poikkeavat bilineaarisesta vain ehdon (S4) kohdalla. Jos avaruudelle V on valittu kanta $T = (v_1, \ldots, v_n)$, niin seskvilineaarisen muodon S matriisi $\hat{S} = [s_{ij}]$ määritellään tuttuun tapaan kaavalla

[1] Etuliite *sesqui-* tarkoittaa latinassa "...ja puoli", esimerkiksi *sesquimensis* = "puolitoista kuukautta".

$s_{ij} = S(v_i, v_j)$. Tällöin kaikilla sarakevektoreilla x ja y pätee

$$S(x,y) = x^\top \hat{S}\bar{y} \qquad \text{(huomaa konjugointi)}.$$

Isometrialle L saadaan siis ehto $L^\top \hat{S}\bar{L} = \hat{S}$.

Tässä luvussa ollaan kiinnostuneita vain tietynlaisista seskvilineaarisista muodoista.

Määritelmä 6.2. Jos avaruuden V seskvilineaarinen muoto S toteuttaa lisäksi ehdon

$$S(x,y) = \overline{S(y,x)} \quad \text{kaikilla } x, y \in V, \tag{H}$$

muotoa S kutsutaan *hermiittiseksi.*

Hermiittistä muotoa vastaavalle matriisille pätee $S^\top = \bar{S}$. Tällaista matriisia kutsutaan *hermiittiseksi matriisiksi.* Voidaan myös osoittaa, että jokainen hermiittinen matriisi vastaa jotain hermiittistä muotoa (kannasta riippumatta).

Jokaisella kunnalla K, jolla on konjugointiautomorfismi σ, on myös alikunta

$$K_0 = \mathrm{Fix}(\sigma) = \{a \in K \mid \sigma(a) = a\}.$$

Kompleksilukujen tapauksessa $\mathbb{C}_0 = \mathbb{R}$. Hermiittiselle muodolle S pätee aina $S(x,x) = \overline{S(x,x)}$, joten $S(x,x) \in K_0$ kaikilla vektoreilla x.

Määritelmä 6.3. Oletetaan, että S on hermiittinen muoto K-kertoimisessa avaruudessa V. Kuvausta $Q : V \to K$, $Q(v) = S(v,v)$ kutsutaan *(hermiittiseksi) neliömuodoksi.*

Hermiittiselle neliömuodolle pätee

$$Q(\lambda v) = \lambda\overline{\lambda}Q(v) \qquad \text{kaikilla } v \in V \text{ ja } \lambda \in K.$$

Lisäksi tietysti $Q(v) = S(v,v) \in K_0$ kaikilla $v \in V$.

6.2 Kohtisuoruus

Hermiittiselle muodolle S pätee $S(x,y) = 0$ jos ja vain jos $S(y,x) = 0$, eli muoto on refleksiivinen. Samoin kuin refleksiivisten bilineaaristen muotojen tapauksessa määritellään vektorien x ja y kohtisuoruus ehdolla $S(x,y) = 0$. Myös kohtisuorat komplementit ja avaruuden radikaali määritellään kuten aikaisemmin. Jos $\mathrm{rad}(V) \neq \{0\}$, sanotaan että V on surkastunut.

Samoin kuin symmetrisen bilineaarisen muodon tapauksessa, voidaan hermiittinen muoto aina esittää tietyssä perusmuodossa. Olkoon S surkastumaton hermiittinen muoto K-kertoimisessa avaruudessa V, ja olkoon Q sitä vastaava neliömuoto.

Lemma 6.4. *Jollakin $v \in V$ pätee $Q(v) \neq 0$.*

Todistus. Oletetaan vastoin väitettä, että $Q(v) = 0$ kaikilla $v \in V$. Koska S ei ole surkastunut, löydetään vektorit v ja w, joille pätee $S(v, w) = 1$. (Jos $S(v, w) = \mu \neq 0$, vaihdetaan $v \mapsto \mu^{-1}v$.) Tällöin kaikilla $\lambda \in K$ pätee

$$0 = Q(v + \lambda w) = \underbrace{Q(v)}_{=0} + S(v, \lambda w) + S(\lambda w, v) + \underbrace{Q(w)}_{=0} = \lambda + \bar{\lambda}.$$

Jos $\lambda = 1$, niin $1 + \bar{1} = 2 = 0$, joten kerroinkunnan karakteristika on 2. Tällöin kuitenkin $\bar{\lambda} = -\lambda = \lambda$ kaikilla $\lambda \in K$, joten konjugointiautomorfismi on identtinen kuvaus. Tämä on ristiriita, koska konjugointiautomorfismin kertaluku on kaksi. $\square$

Lause 6.5. *Avaruudella V on kanta $(v_1, \dots, v_n)$, jonka suhteen $\hat{S}$ on diagonaalimatriisi. Lisäksi $Q(v_i) = \hat{S}_{ii} \in K_0^*$ kaikilla $i \in \{1, \dots, n\}$.*

Todistus. Todistus etenee samalla tavalla kuin lauseessa 5.5. $\square$

Samoin kuin symmetrisillä bilineaarisilla muodoilla, myös hermiittisillä muodoilla voidaan matriisiesityksen diagonaalialkioita skaalata. Nyt kuitenkin kantavektorin muunnos $v_i' = c_i v_i$ aiheuttaa diagonaalialkion muunnoksen $b_i' = c_i \bar{c}_i b_i$, eli diagonaalialkioita voi skaalata vain sellaisilla luvuilla, jotka ovat muotoa $\lambda\bar{\lambda} \in K_0^*$. Esimerkiksi kompleksiluvuilla $\lambda\bar{\lambda}$ on aina positiivinen, joten päädytään samanlaiseen tilanteeseen kuin Sylvesterin inertialauseessa, jossa muodon määrittää diagonaalilla olevien lukujen 1 ja -1 määrät. Toisaalta, jos kerroinkunta on äärellinen, muotoja on vain yksi.

Lause 6.6. *Jos avaruuden V kerroinkunta K on äärellinen, niin V:llä on kanta $(v_1, \dots, v_n)$, jonka suhteen $\hat{S} = I_n$.*

Todistus. Sivuutetaan. $\square$

6.3 Unitaarisen ryhmän määritelmä

Määritelmä 6.7. Oletetaan, että S on surkastumaton hermiittinen muoto vektoriavaruudessa V. Jos lineaarikuvaus g säilyttää muodon S, niin sanotaan että g on *unitaarinen* (muodon S suhteen). Unitaaristen kuvausten ryhmää kutsutaan *unitaariseksi ryhmäksi* ja merkitään $U^{(S)}(V)$.

Jos S on hermiittinen muoto ja $g \in U^{(S)}(V)$, niin $g^\top \hat{S} \bar{g} = \hat{S}$. Laskemalla determinantit ja jakamalla luvulla $\det \hat{S}$ nähdään, että

$$\det g \cdot \overline{\det g} = 1.$$

Toisin kuin ortogonaalisten ryhmien tapauksessa, determinantin arvot eivät ole yleensä rajoitettuja äärelliseen joukkoon. Kuitenkin $N(\det g) = 1$ kaikilla $g \in U(V)$, missä N on kerroinkunnan normikuvaus.

Määritelmä 6.8. *Erityinen unitaarinen ryhmä* on

$$SU^{(S)}(V) = \{g \in U^{(S)}(V) \mid \det g = 1\}.$$

Erityinen unitaarinen ryhmä on ryhmän $U(V)$ normaali aliryhmä. Voidaan osoittaa, että $U(V)/SU(V) \cong \operatorname{Ker} N$, missä N on kerroinkunnan normikuvaus. Todistus on harjoitustehtävänä.

Kuten aiemmin, projektiiviset unitaariset ryhmät $PU(V)$ ja projektiiviset erityiset unitaariset ryhmät $PSU(V)$ määritellään ottamalla tekijäryhmät ryhmistä $U(V)$ ja $SU(V)$ skalaarimatriisien suhteen.

6.4 Kerroinkuntana $\mathbb{C}$

Kun vektoriavaruus on kompleksikertoinen, automorfismina σ toimii kompleksikonjugointi, alikunta $\operatorname{Fix}(\sigma)$ on $\mathbb{R}$, ja luvun λ normi $N(\lambda)$ on sen modulin neliö $|\lambda|^2$.

Koska jokaiselle hermiittiselle neliömuodolle Q pätee $Q(v) \in \mathbb{R}$, niin voidaan määritellä positiivinen definiittisyys.

Määritelmä 6.9. Hermiittinen muoto S on *positiivisesti definiitti*, jos kaikilla vektoreilla $v \neq 0$ pätee $S(v, v) > 0$.

Positiivisesti definiittiä hermiittistä neliömuotoa kutsutaan *sisätuloksi*. Sen avulla voidaan määritellä vektorien pituudet ja niiden väliset kulmat aivan samoin kuin bilineaarisen sisätulon tapauksessa. Tavallisesti avaruuden $\mathbb{C}^n$ pistetulo määritellään myös hermiittisen muodon mukaisesti:

$$v \cdot w = \sum_i v_i \bar{w}_i.$$

Tämä pistetulo on sisätulo, toisin kuin tavallinen pistetulo (kompleksiavaruudessa).

Esimerkki 6.10. Tarkastellaan sarakevektoriavaruuksia $\mathbb{C}^n$, joissa on muotona hermiittinen pistetulo $x \cdot y = \sum_i x_i y_i$.

Ryhmä $U(1) = U_1(\mathbb{C})$ koostuu 1×1-matriiseista eli kompleksiluvuista $z = a + bi$, joille pätee $z\bar{z} = 1$ kaikilla $z \in U(1)$. Koska $z\bar{z} = a^2 + b^2$, nämä kompleksiluvut sijaitsevat kompleksitason yksikköympyrällä. Vastaava erityinen unitaarinen ryhmä on triviaali, koska kaikilla $z \in SU(1)$ täytyy pätea $z = \det z = 1$.

Ryhmä $U(2) = U_2(\mathbb{C})$ koostuu kaksiulotteisista matriiseista g, joilla $g^\top \bar{g} = I$. Merkitään $g = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, jolloin unitaarisuusehdosta saadaan yhtälöryhmä

$$\begin{cases} a\bar{a} + c\bar{c} &= |a|^2 + |c|^2 = 1 \\ b\bar{b} + d\bar{d} &= |b|^2 + |d|^2 = 1 \\ a\bar{b} + c\bar{d} &= 0 \end{cases}.$$

Ensimmäisistä ehdoista nähdään, että pisteet (a, c) ja (b, d), jotka ovat siis kantavektorien arvot, sijaitsevat avaruudessa $\mathbb{C}^2$ yksikköpallon pinnalla. Kolmas ehto puolestaan voidaan kirjoittaa muodossa $d = -\bar{a}b/\bar{c}$, mikä tarkoittaa sitä, että lukujen a, b ja c arvot määräävät myös luvun d (kunhan $c \neq 0$).

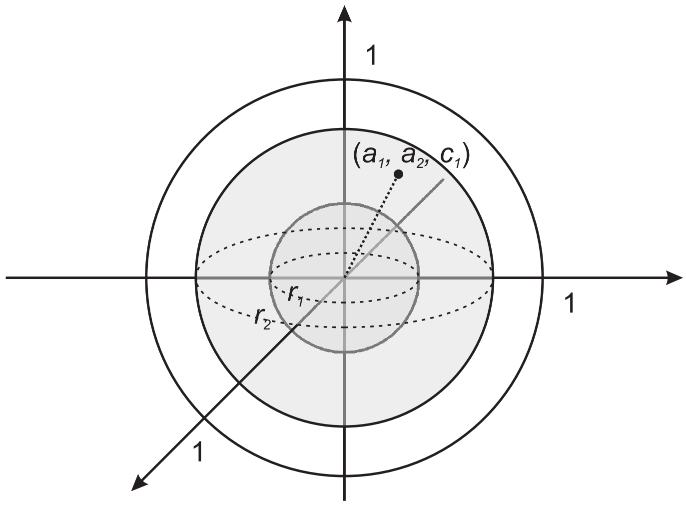
Erityisessä unitaarisessa ryhmässä $SU(2)$ saadaan vielä yksi lisäehto, nimittäin $ad - bc = 1$. Ratkaisemalla tästä $d = (bc + 1)/a$ ja käyttämällä ylempänä mainittua ehtoa $d = -\bar{a}b/\bar{c}$, saadaan yhtälöt $b = -\bar{c}$ ja $d = \bar{a}$. Siispä jokainen erityisen unitaarisen ryhmän matriisi on itse asiassa muotoa

$$g = \begin{bmatrix} a & -\bar{c} \\ c & \bar{a} \end{bmatrix}, \qquad \text{missä} \quad |a|^2 + |c|^2 = 1.$$

Jos nyt merkitään $a = a_1 + a_2 i$ ja $c = c_1 + c_2 i$, voidaan kirjoittaa

$$a_1^2 + a_2^2 + c_1^2 + c_2^2 = 1.$$

Samastamalla $\mathbb{C}^2 = \mathbb{R}^4$ huomataan, että jokainen ryhmän $SU(2)$ alkio vastaa itse asiassa jotain 3-ulotteisen pallonkuoren pinnan pistettä avaruudessa $\mathbb{R}^4$. Toisaalta, jos esimerkiksi $c_2 \in [-1, 1]$ on kiinnitetty, mahdolliset alkiot vastaavat sellaisen $\mathbb{R}^3$:n kaksiulotteisen pallonkuoren pisteitä, jonka säde on $\sqrt{1 - c_2^2}$. Kun luku c_2 käy läpi kaikki luvut -1:stä 1:een, pallonkuori kasvaa origosta 1-säteiseksi ja takaisin, täyttämällä kahdesti koko suljetun yksikkökuulan.



Kuva 6: Ryhmän $SU(2)$ alkiot vastaavat pisteitä pallonkuorilla, joiden säde on $r = \sqrt{1 - c_2^2}$. Jokaista nollasta poikkeavaa sädettä vastaa kaksi identtistä pallonkuorta, joista toisella $c_2 > 0$, toisella $c_2 < 0$.

Kompleksikertoimisten avaruuksien unitaariset ryhmät ovat erityisen tärkeitä kvanttimekaniikassa.

Esimerkki 6.11. Kvanttimekaniikassa mitä tahansa hiukkasta, kuten elektronia, voidaan kuvata *aaltofunktiolla* ψ, joka on ajan ja paikan funktio. Aaltofunktion arvot ovat kompleksilukuja, joilla ei sinänsä ole mitään fysikaalista merkitystä. Kuitenkin *todennäköisyys*, jolla aallon ψ kuvaama hiukkanen on tietyllä hetkellä t paikassa x, on $|\psi(t, x)|^2$.

Olkoon ψ elektronia kuvaava aaltofunktio. Jos c on nyt jokin kompleksiluku, jolle $|c| = 1$, niin

$$|\psi(t,x)| = |c\psi(t,x)|.$$

Todennäköisyys, että hiukkanen löytyy tietystä paikasta ei siis muutu, vaikka aaltofunktiota kerrottaisiin vakiolla c. Koska $c \in U(1)$, sanotaan, että elektronin aaltofunktion symmetriaryhmä on $U(1)$.

Liikkuvan elektronin tapauksessa voidaan ajatella, että termi c on itse asiassa paikan x funktio, eli että aaltofunktion arvot ovat muotoa $c(x)\psi(t,x)$. Tämä lisäoletus ei edelleenkään vaikuta elektronin sijainnin todennäköisyyksiin. Johtamalla tästä elektronin liikeyhtälöt, nähdään, että elektroni itse asiassa vuorovaikuttaa sähkömagneettista vuorovaikutusta välittävien *fotonien* kanssa. Lisäksi voidaan määrittää tämän vuorovaikutuksen voimakkuus.

Sama ajattelu voidaan toistaa muidenkin hiukkasten tapauksessa muita symmetrioita käyttämällä. Nykyfysiikan mukaan protonit ja neutronit koostuvat kvarkeista, joilla on ominaisuus, jota kutsutaan *väriksi*. Värejä on kolme erilaista, ja erivärisillä kvarkeilla on täsmälleen samat fysikaaliset ominaisuudet. Kvarkkien värin symmetriaryhmä on $SU(3)$, jonka alkiot “vaihtavat erivärisiä kvarkkeja toisikseen”. Edelleen voidaan olettaa, että kvarkkien värijakauma on paikasta riippuva funktio, ja liikeyhtälöt johtamalla nähdään, että kvarkit vuorovaikuttavat vahvaa vuorovaikutusta välittävien *gluonien* kanssa.

Erityistä yllä mainituissa esimerkeissä on se, että tapa, jolla liikeyhtälöt johdetaan, perustuu vain kyseessä olevan symmetriaryhmän ominaisuuksiin sekä joihinkin yleisiin fysikaalisiin periaatteisiin. Hiukkasfyysikot pyrkivät yhtenäistämään kaikki luonnossa havaittavat perusvuorovaikutukset, ja eräs tapa lähestyä tätä tehtävää on tutkia, minkälainen ryhmä voisi sopivalla tavalla sisältää kaikki yksittäisiin vuorovaikutuksiin liittyvät symmetriaryhmät.

6.5 Äärelliset kunnat

Äärellisissä kunnissa tilanne on hyvin rajoitettu. Ensinnäkin lauseen 6.6 mukaan on kannanvaihtoa vaille olemassa vain yksi hermiittinen muoto. Toisaalta voidaan osoittaa, että läheskään kaikissa kunnissa ei voida määritellä tarvittavaa automorfismia.

Lause 6.12. *Äärellisessä kunnassa voidaan määritellä konjugoiva automorfismi σ jos ja vain jos kunnan kertaluku q on neliö. Myönteisessä tapauksessa saatava automorfismi on muotoa $\sigma(a) = a^{\sqrt{q}}$.*

Lauseen todistus ei ole vaikea, mutta se vaatii esitietoja kuntalaajennosten teoriasta. Ideana on, että jos kunnassa K on konjugaatioautomorfismi σ, niin K on kaksiulotteinen vektoriavaruus, jonka kertoimet ovat alikunnassa $K_0 = \mathrm{Fix}(\sigma)$. Tällöin nimittäin pätee $|K| = |K_0|^2$. Yksityiskohdat sivuutetaan.

Yllä olevasta lauseesta seuraa muun muassa, että alkukunnissa $\mathbb{F}_p$ ei voida määritellä konjugointia. Tarkastellaan seuraavassa esimerkissä sitä, miten ylipäänsä voidaan määritellä muita äärellisiä kuntia.

Esimerkki 6.13. Tiedetään, että on olemassa yhdeksänalkioinen kunta $\mathbb{F}_9$, jonka karakteristika on kolme. Tämä kunta voidaan määritellä lähtemällä alkukunnasta $\mathbb{F}_3 = \{0, 1, -1\}$. Aluksi etsitään $\mathbb{F}_3$-kertoiminen toisen asteen polynomi, jolla ei ole juuria kunnassa $\mathbb{F}_3$. Tällainen on esimerkiksi

$$x^2 + 1,$$

sillä $(\pm 1)^2 + 1 = -1 \neq 0$. Lisätään nyt tähän kuntaan kyseisen polynomin juuret seuraavasti: Koska polynomi $x^2 + 1$ ei jakaudu tekijöihin (sillä ei ole juuria) polynomirenkaassa $\mathbb{F}_3[x]$, niin sen virittämä pääideaali $\langle x^2 + 1\rangle$ on maksimaalinen. Tämä tarkoittaa sitä, että tekijärengas $\mathbb{F}_3[x]/\langle x^2 + 1\rangle$ on kunta. Kyseisessä tekijärenkaassa on alkioina sivuluokat $a + \langle x^2 + 1\rangle$, missä a on jokin polynomeista

$$0, \quad 1, \quad -1, \quad x, \quad x+1, \quad x-1, \quad -x, \quad -x+1 \quad \text{ja} \quad -x-1.$$

Toisaalta $x^2+1 \in \langle x^2+1\rangle$, joten polynomin x^2+1 sivuluokka on $0+\langle x^2+1\rangle$. Näin ollen $x + \langle x^2 + 1\rangle$ on tekijärenkaassa polynomin $x^2 + 1$ juuri.

Nimetään nyt tekijärengas $\mathbb{F}_3[x]/\langle x^2 + 1\rangle$ kunnaksi $\mathbb{F}_9$ ja merkitään polynomia x symbolilla i. Näin on saatu kunta

$$\mathbb{F}_9 = \{0,\ 1,\ -1,\ i,\ i+1,\ i-1,\ -i,\ -i+1,\ -i-1\},$$

jossa $i^2 = -1$. Konjugoivana automorfismina on $\bar{a} = a^3$, jolla $\bar{i} = i^2 \cdot i = -i$.

Koska vain niissä kunnissa, joiden kertaluku on neliö, on mahdollista määritellä konjugaatioautomorfismi, äärellisiä unitaarisia ryhmiä on tapana merkitä $U_n(\mathbb{F}_{q^2}) = U_n(q)$ ja vastaavasti $SU_n(\mathbb{F}_{q^2}) = SU_n(q)$. Kirjallisuudessa tapaa kuitenkin tästä poikkeavia käytäntöjä.

7 Symplektiset ryhmät[2]

Symplektiset ryhmät ovat alternoivien muotojen isometriaryhmiä. Alternoivan muodon määrittämä geometria ei ole yhtä intuitiivisesti selkeä kuin esimerkiksi symmetrisen muodon, mutta laskennallisesti se on sitä vastoin helpompi käsitellä. Myös isometriaryhmässä kuvastuu tämä laskennallinen vaivattomuus.

7.1 Symplektiset kannat

Oletetaan tässä kappaleessa, että B on alternoiva bilineaarinen muoto K-kertoimisessa vektoriavaruudessa V.

Jos $u, v \in V$ ja $B(u,v) = b \neq 0$, niin u ja v ovat lineaarisesti riippumattomia. Muuten nimittäin $B(u,v) = B(u, \lambda u) = \lambda B(u,u) = 0$ jollain $\lambda \in K^*$. Valitaan $u_1 = u$ ja $v_1 = b^{-1}v$, jolloin $B(u_1, v_1) = 1$. Nyt vektorit u_1 ja v_1 muodostavat kannan jollekin V:n kaksiulotteiselle aliavaruudelle W. Tuossa aliavaruudessa muoto B on kyseisen kannan suhteen kirjoitettuna

$$\hat{B} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Tällaista kaksiulotteista avaruutta kutsutaan *hyperboliseksi tasoksi* (symplektisessä avaruudessa).

Määritelmä 7.1. Jos kaksiulotteisella avaruudella V on kanta (u,v), jonka vektoreille pätee $B(u,v) = 1$, niin avaruutta V kutsutaan *hyperboliseksi tasoksi*. Sen kantavektorit puolestaan muodostavat *hyperbolisen parin*.

Symplektiset avaruudet koostuvat kokonaan hyperbolisista tasoista.

Lause 7.2. *Oletetaan, että B on alternoiva bilineaarinen muoto avaruudessa V. Tällöin avaruudella V on kanta $(u_1, v_1, \ldots, u_r, v_r, w_1, \ldots, w_{n-2r})$, jonka suhteen muodon B matriisi on muotoa*

$$\hat{B} = \begin{bmatrix} M & & 0 \\ & \ddots & \\ & & M & \\ 0 & & & 0_{n-2r} \end{bmatrix}, \qquad \textit{missä} \quad M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Lisäksi jono $(w_1, \ldots, w_{n-2r})$ on radikaalin $\mathrm{rad}(V)$ kanta.

Todistus. Jos $B(u,v) = 0$ kaikilla $u, v \in V$, niin $\mathrm{rad}(V) = V$, joten asetetaan $r = 0$. Muuten voidaan yllä esitetyllä tavalla valita hyperbolinen pari

[2] Nimitys "symplektinen" tulee sanasta *symplektikos*, joka on suora käännös latinasta kreikkaan sanalle *complexus*. Käännös heijastaa symplektisen geometrian ja kompleksiavaruuksien välistä suhdetta, ja sen kehittäjäksi on esitetty Hermann Weylia. Kuitenkin esim. R.A. Wilson mainitsee Sylvesterin sanan ensimmäisenä käyttäjänä.

(u_1, v_1). Olkoon W_1 tämän parin virittämä aliavaruus. W_1 on surkastumaton, joten lemman 5.4 perusteella V on suora summa aliavaruuksista W_1 ja $W_1^\perp$. Lisäksi $\operatorname{rad} V = V^\perp = W_1^\perp \cap (W_1^\perp)^\perp = \operatorname{rad} W_1^\perp$. Konstruktiota voidaan siis jatkaa aliavaruudessa $W_1^\perp$. Lopulta $B(u, v) = 0$ kaikilla $u, v \in W_{2r}^\perp$, jolloin konstruktio pysähtyy, ja $\operatorname{rad}(V) = \operatorname{rad}(W_{2r}^\perp) = W_{2r}^\perp$. □

Kutsutaan tästä lähtien yllä olevassa lauseessa esitettyä kantaa *symplektiseksi kannaksi*. Lauseesta saadaan heti seuraavat korollaarit.

Korollaari 7.3. *Jos vektoriavaruudessa on surkastumaton alternoiva muoto, niin avaruuden dimensio on parillinen.*

Korollaari 7.4. *Vektoriavaruuden kaikki surkastumattomat alternoivat bilineaariset muodot ovat ekvivalentteja.*

Korollaari 7.5. *Alternoivaa muotoa esittävän matriisin determinantti on aina neliö kerroinkunnassa.*

Todistus. Jos matriisi $\hat{B}$ on lauseessa mainittua muotoa $\hat{B}_0$, sen determinantti on 1. Muuten löytyy jokin kannanvaihtomatriisi L, jolla $\hat{B} = L^\top \hat{B}_0 L$, jolloin $\det \hat{B} = (\det L)^2$. □

Mainittakoon tässä yhteydessä, että alternoivan muodon matriisilla on muitakin esitystapoja, joita käytetään ahkerasti kirjallisuudessa. Ehkä tavallisin yllä olevasta poikkeava surkastumattoman muodon esitystapa on

$$\hat{B} = \left[\begin{array}{c|c} 0_r & I_r \\ \hline -I_r & 0_r \end{array}\right].$$

Tämä esitys saadaan yllä olevasta yksinkertaisesti kantavektoreiden järjestystä vaihtamalla.

7.2 Symplektisen ryhmän määritelmä

Symplektiset ryhmät ovat alternoivan muodon isomorfiaryhmiä.

Määritelmä 7.6. Oletetaan, että B on surkastumaton alternoiva bilineaarinen muoto vektoriavaruudessa V. Jos lineaarikuvaus g säilyttää muodon B, niin sanotaan että g on *symplektinen*. Symplektisten kuvausten ryhmää kutsutaan *symplektiseksi ryhmäksi* ja merkitään $Sp^{(B)}(V)$.

Merkinnässä $Sp(V)$ muotoa ei yleensä tarvitse merkitä näkyviin, koska kaikki avaruuden alternoivat muodot ovat keskenään ekvivalentteja. Matriisiyhtälöstä $g^\top \hat{B} g = \hat{B}$, missä B on alternoiva muoto, nähdään helposti, että $\det g = \pm 1$ kaikilla $g \in Sp(V)$. Myöhemmin kuitenkin voidaan todeta, että symplektisten kuvausten determinantti on aina 1. Mitään erityistä symplektistä ryhmää "SSp(V)" ei siis ole tarvetta määritellä.

Projektiivinen symplektinen ryhmä $PSp(V)$ määritellään tuttuun tapaan tekijäryhmänä skalaarimatriisien suhteen. Symplektisiä skalaarimatriiseja ovat vain I ja $-I$. Nämä itse asiassa muodostavat ryhmän $Sp(V)$ keskuksen, joten $PSp(V) = Sp(V)/Z(Sp(V))$.

Esimerkki 7.7. Vektoriavaruuden V *pinta-alamuoto* on bilineaarinen kuvaus $A : V \times V \to K$, jolle pätee $A(v, w) = 0$ aina, kun v ja w ovat lineaarisesti riippuvia. Pinta-alamuoto ilmoittaa kahden vektorin virittämän suunnikkaan *suunnatun pinta-alan*. Bilineaarisuusehto takaa, että esimerkiksi skaalatun suunnikkaan ala skaalautuu myös oikeassa suhteessa. Toisaalta, jos v ja w sijaitsevat samalla suoralla (eli ovat lineaarisesti riippuvia), niin ne virittävät janaksi surkastuneen suunnikkaan, jonka pinta-ala on 0. Suunnatulla tarkoitetaan tässä yhteydessä sitä, että pinta-alamuoto voi olla positiivinen tai negatiivinen, ja jos suunnikas "käännetään" vaihtamalla sen virittävät vektorit keskenään, pinta-alamuoto vaihtaa merkkiä. Esimerkki pinta-alamuodosta on kaksiulotteisen avaruuden determinanttikuvaus.

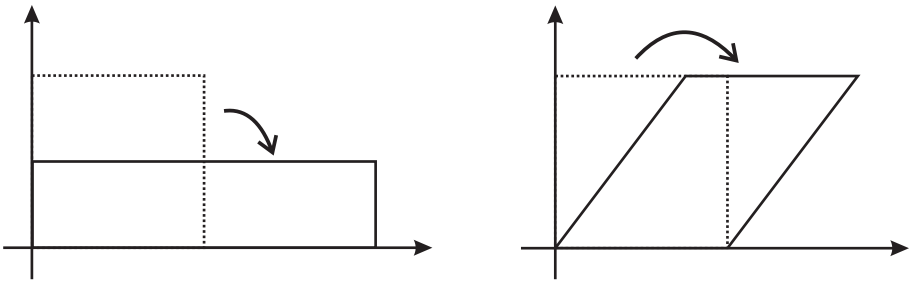
Koska pinta-alamuoto on itse asiassa alternoiva bilineaarinen muoto, sen säilyttävät lineaarikuvaukset ovat symplektisiä kuvauksia. Esimerkiksi tasossa $\mathbb{R}^2$ tällaiset kuvaukset ovat *kiertoja*, *litistyksiä*, *transvektioita* tai niiden yhdistelmiä. Kierrot ovat tuttuja erityisen ortogonaalisen ryhmän alkioina. Litistyksen matriisi on sopivassa kannassa

$$L_\beta = \begin{bmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{bmatrix}.$$

Transvektiot puolestaan ovat kuvauksia, jotka muuttavat jonkin kiinnitetyn suoran suuntaiset suorakulmiot suunnikkaiksi niiden korkeutta muuttamatta. Sellaisen matriisi on sopivassa kannassa muotoa

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

Kaikki nämä kuvaukset säilyttävät kahden vektorin virittämän suunnikkaan pinta-alan ja lisäksi kyseisten vektorien järjestyksen niiden muodostaman kulman kylkinä. Voidaan itse asiassa osoittaa, että kaikki symplektiset kuvaukset voidaan ilmaista transvektioiden avulla.



Kuva 7: Litistys ja transvektio ovat tason symplektisiä kuvauksia

Symplektiset kuvaukset esittävät merkittävää osaa myös teoreettisessa fysiikassa.

Esimerkki 7.8. Klassisessa mekaniikassa on tapana hankkiutua eroon kappaleeseen vaikuttavista tuki- ja sidosvoimista korvaamalla tavalliset paikkakoordinaatit *yleistetyillä koordinaateilla* q_i. Esimerkiksi vaijerin päässä pyörivä moukari voi liikkua ainoastaan ympyrän kehällä, jolloin sen liikkeen kuvaamiseen riittää tuntea kiertokulma q. Kun koordinaatit valitaan sopivasti, liikeyhtälöt tulevat muotoon

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_i}\right) - \frac{\partial L}{\partial q_i} = 0,$$

missä $\dot{q}_i$ merkitsee q_i:n aikaderivaattaa ja L on niin sanottu *Lagrangen funktio*, joka määritellään systeemin potentiaali- ja kineettisen energian erotuksena.

Yllä oleva liikeyhtälö sisältää toisen asteen derivaattoja. Hamiltonilaisessa muotoilussa otetaan käyttöön kutakin yleistettyä koordinaattia vastaa *yleistetty liikemäärä* $p_i = \partial L/\partial \dot{q}_i$. Kun lisäksi määritellään *Hamiltonin funktio* $H = \dot{q}_i p_i - L$, liikeyhtälöt tulevat muotoon

$$\dot{q}_i = \frac{\partial H}{\partial p_i} \qquad \text{ja} \qquad -\dot{p}_i = \frac{\partial H}{\partial q_i}.$$

Tässä muotoilussa yhtälöt sisältävät vain ensimmäisen asteen derivaattoja, mutta toisaalta vapaita muuttujia on kaksinkertainen määrä aikaisempaan verrattuna.

Kirjoitetaan nyt yleistetyt koordinaatit ja liikemäärät samaan vektoriin $\eta = (q_1, \ldots, q_n, p_1, \ldots, p_n)$. Tällöin Hamiltonin liikeyhtälöt tulevat muotoon

$$\dot{\eta} = J\frac{\partial H}{\partial \eta}, \qquad \text{missä} \quad J = \begin{bmatrix} 0_n & I_n \\ -I_n & 0_n \end{bmatrix}.$$

Voidaan osoittaa, että Hamiltonin funktio säilyy ajasta riippumattomissa koordinaatistonmuunnoksissa. Tällöin, jos L on muunnoksen $\eta \mapsto \zeta$ Jacobin matriisi, niin

$$L^\top J L = J.$$

Antisymmetrisenä matriisina J määrittää jonkin alternoivan muodon, joten koordinaatistonmuunnoksen Jacobin matriisin on oltava symplektinen.

7.3 Transvektiot eli murroskuvaukset

Olkoon W jokin hypertaso vektoriavaruudessa V. Transvektioksi kutsutaan lineaarikuvausta T, jolle pätee $Tw = w$ kaikilla $w \in W$ ja $Tv - v \in W$ kaikilla $v \in V$.

Määritelmä 7.9. Olkoon B alternoiva muoto K-kertoimisessa avaruudessa V. Olkoot lisäksi $u \in V \setminus \{0\}$ ja $\alpha \in K$. Lineaarikuvausta

$$\tau_{u,\alpha}(v) = v + \alpha B(u,v)u$$

kutsutaan *symplektiseksi transvektioksi*.

On helppo nähdä, että $\tau_{u,\alpha}$ kiinnittää hypertason $u^\perp$ ja että $\tau_{u,\alpha}(v) - v$ on vektorin u suuntainen. Täten $\tau_{u,\alpha}(v) - v \in u^\perp$, ja kuvaus $\tau_{u,\alpha}$ on transvektio. Lisäksi kaikilla $v, w \in V$ pätee

$$\begin{aligned} B\big(\tau_{u,\alpha}(v), \tau_{u,\alpha}(w)\big) &= B\big(v + \alpha B(u,v)u,\ w + \alpha B(u,w)u\big) \\ &= B(v,w) + \alpha B(u,w)B(v,u) + \alpha B(u,v)B(u,w) \\ &\quad + \alpha^2 B(u,v)B(u,w)B(u,u) \\ &= B(v,w). \end{aligned}$$

Siispä kuvaus $\tau_{u,\alpha}$ on myös symplektinen. Symplektiset transvektiot hoitavat tietyssä mielessä ortogonaalisten peilausten virkaa symplektisissä ryhmissä.

Lause 7.10. *Avaruuden V symplektiset transvektiot virittävät koko symplektisen ryhmän $Sp(V)$.*

Todistus. Sivuutetaan. □

Korollaari 7.11. *Kaikilla $g \in Sp(V)$ pätee* $\det g = 1$.

Todistus. Olkoon $\tau = \tau_{u_1,\alpha}$ avaruuden V mielivaltainen symplektinen transvektio. Valitaan avaruudelle $u_1^\perp$ jokin kanta $(u_1, u_2, \ldots, u_{n-1})$ ja täydennetään se vektorilla u_n avaruuden V kannaksi. Nyt kaikilla $i \in \{1, \ldots, n-1\}$ pätee $\tau(u_i) = u_i$, ja lisäksi $\tau(u_n) = u_n + \lambda u_1$, missä $\lambda = \alpha B(u_1, u_n)$. Valitussa kannassa transvektion matriisi on siis

$$\hat{\tau} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \lambda \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 1 & 0 \\ 0 & & \cdots & 0 & 1 \end{bmatrix}.$$

Nähdään, että mielivaltaisen symplektisen transvektion determinantti on 1. Jokainen $g \in Sp(V)$ on puolestaan transvektioiden tulo, joten $\det g = 1$. □

7.4 Yhteys kompleksikertoimisiin avaruuksiin

Tarkastellaan kompleksikertoimista avaruutta $\mathbb{C}^n$, jossa on määritelty hermiittinen pistetulo $x \cdot y = \sum_k x_k \bar{y}_k$. Jos merkitään $x_k = a_k + b_k i$ ja $y_k = c_k + d_k i$, niin

$$x \cdot y = \sum_{k=1}^{n} \big[(a_k c_k + b_k d_k) + i(b_k c_k - a_k d_k)\big].$$

Samastetaan nyt $\mathbb{C}^n = \mathbb{R}^{2n}$ kuvauksella

$$\iota(a_1 + b_1 i, \ldots, a_n + b_n i) = (a_1, b_1, \ldots, a_n, b_n).$$

Tällöin hermiittiselle pistetulolle pätee

$$x \cdot y = B_1\big(\iota(x), \iota(y)\big) + iB_2\big(\iota(x), \iota(y)\big),$$

missä B_1 on tavallinen ortogonaalinen pistetulo avaruudessa $\mathbb{R}^{2n}$ ja B_2 on alternoiva muoto

$$\begin{bmatrix} 0 & -1 & & 0 & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & -1 \\ & 0 & & 1 & 0 \end{bmatrix}.$$

Hermiittisen sisätulon arvot ovat siis kompleksilukuja, joiden imaginaariosa saadaan tietyn reaaliavaruuden alternoivan muodon arvoista. Kuvausten, jotka säilyttävät kompleksiavaruudessa esimerkiksi vektorien pituudet, täytyy siis olla tuossa reaaliavaruudessa symplektisiä kuvauksia. Tällä tavoin symplektisen geometrian tutkiminen liittyy läheisesti kompleksikertoimisten vektoriavaruuksien geometriaan.

8 Äärelliset yksinkertaiset ryhmät

Tässä luvussa tarkastellaan äärellisiä yksinkertaisia ryhmiä. Kaikki äärelliset ryhmät koostuvat niistä, ja äärellisiä yksinkertaisia ryhmiä kutsutaankin usein äärellisten ryhmien rakennuspalikoiksi. Ryhmäteorian suuri voimanponnistus on ollut luokittelulause, joka listaa kaikki äärelliset yksinkertaiset ryhmät. Matemaatikoilla on siis käytössään tarkka lista äärellisen ryhmäteorian rakennuspalikoista!

Tämän kurssin kannalta äärelliset yksinkertaiset ryhmät ovat kiinnostavia sen vuoksi, että valtaosa niistä saadaan klassisista ryhmistä.

Määritelmä 8.1. Ryhmä on G *yksinkertainen*, jos sillä on täsmälleen kaksi normaalia aliryhmää: $\{1\}$ ja G.

Huomaa, että määritelmän mukaan ryhmä $\{1\}$ ei ole yksinkertainen.

8.1 Kompositiojonot

Jotta voidaan puhua tarkemmin siitä, mitä äärellisten ryhmien rakennuspalikoilla tarkoitetaan, on esiteltävä kompositiojonon käsite.

Määritelmä 8.2. Olkoon G äärellinen ryhmä. Sen *kompositiojono* on äärellinen jono

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G,$$

jota ei voida pidentää lisäämällä siihen normaaleja aliryhmiä. Tekijäryhmiä G_i/G_{i-1} kutsutaan jonon *kompositiotekijöiksi*.

Merkintä $G_{i-1} \lhd G_i$ tarkoittaa, että G_{i-1} on ryhmän G_i normaali aliryhmä, joka on lisäksi G_i:n aito osajoukko.

Äärellisillä ryhmillä on aina olemassa jokin kompositiojono. Voidaan nimittäin aloittaa jonosta $\{1\} \lhd G$. Sen jälkeen jonoa pidennetään niin paljon kuin mahdollista lisääämällä siihen normaaleja aliryhmiä. Tätä ei kuitenkaan voida jatkaa äärettömän kauan, sillä ryhmä on äärellinen. Siten saatu jono on kompositiojono.

Ryhmällä saattaa olla useita kompositiojonoja, mutta ne ovat kaikki pohjimmiltaan samanlaisia.

Lause 8.3. *(Jordan-Hölder) Valitaan kaksi G:n kompositiojonoa, ja oletetaan, että niiden kompositiotekijöiden joukot ovat S ja T. Nyt on on olemassa bijektio $\sigma : S \to T$, jolla pätee $x \cong \sigma(x)$ kaikilla $x \in T$.*

Todistus. Lauseen todistus löytyy mistä tahansa ryhmäteorian perusteoksesta. $\square$

Lause 8.4. *Jono*

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G,$$

on kompositiojono jos ja vain jos sen tekijät G_i/G_{i-1} ovat yksinkertaisia.

Todistus. Oletetaan aluksi, että kyseessä on kompositiojono. Jos on olemassa tekijä G_i/G_{i-1}, joka ei ole yksinkertainen, niin silloin sillä on jokin epätriviaali normaali aliryhmä. Tämä aliryhmä on muotoa H_i/G_{i-1}, missä $G_{i-1} \triangleleft H_i \triangleleft G_1$. Tämä tarkoittaa sitä, että kompositiojonoon voidaan lisätä ryhmä H_i, mikä on ristiriita. Siten kaikki kompositiotekijät ovat yksinkertaisia.

Oletetaan sitten, että kaikki tekijät G_i/G_{i-1} ovat yksinkertaisia. Jos jonoon nyt lisätään ryhmä H_i siten, että $G_{i-1} \triangleleft H_i \triangleleft G_i$, niin silloin H_i/G_{i-1} on ryhmän G_i/G_{i-1} epätriviaali normaali aliryhmä. Siten on päädytty ristiriitaan, ja jonon on oltava kompositiojono. □

Nyt siis tiedämme, että jokainen äärellinen ryhmä voidaan hajottaa kompositiojonoksi, jonka tekijät ovat äärellisiä yksinkertaisia ryhmiä. Nämä kompositiotekijät ovat tavallaan ryhmien rakennuspalikoita, ja kompositiojonot kertovat meille paljon ryhmän rakenteesta. Ne eivät kuitenkaan määrää ryhmän rakennetta täysin, ja kahdella ryhmällä saattaakin olla samanlainen kompositiojono, vaikka ryhmät eivät olisi isomorfisia. Jos ryhmän rakenne halutaan määrittää tarkasti, on rakennuspalikkojen lisäksi tiedettävä, miten ne kiinnittyvät toisiinsa.

Esimerkki 8.5. Etsitään symmetrisen ryhmälle S_3 jokin kompositiojono. Merkitään $A_3 = \{1, (123), (132)\}$. Nyt jono

$$\{1\} \triangleleft A_3 \triangleleft S_3$$

on kompositiojono, ja sen tekijät ovat

$$S_3/A_3 \cong C_2 \quad \text{ja} \quad A_3/\{1\} \cong A_3 \cong C_3,$$

missä C_2 ja C_3 ovat syklisiä ryhmiä.

Tarkastellaan sitten syklistä ryhmää C_6. Sille löydetään kompositiojono

$$\{1\} \triangleleft C_3 \triangleleft C_6,$$

jonka kompositiotekijät ovat

$$C_6/C_3 \cong C_2 \quad \text{ja} \quad C_3/\{1\} \cong C_3,$$

Näiden kahden ryhmän kompositiojonot ovat siis samat, mutta ryhmät eivät kuitenkaan ole isomorfiset.

8.2 Äärellisten yksinkertaisten ryhmien luokittelu

Eräs ryhmäteorian huomattavimmista tuloksista on äärellisten yksinkertaisten ryhmien luokittelu. Luokittelulauseen nojalla tiedämme tarkalleen, millaisia äärellisten ryhmien rakennuspalikat ovat.

Lause 8.6. *Seuraavat äärelliset ryhmät ovat yksinkertaisia eikä muita äärellisiä yksinkertaisia ryhmiä ole:*

(1) sykliset ryhmät C_p, missä p on alkuluku

(2) alternoivat ryhmät A_n, missä $n \geq 5$

(3) klassiset ryhmät (nämä on lueteltu tarkemmin alla)

(4) poikkeukselliset Lie-tyypin ryhmät

(5) sporadiset ryhmät.

8.2.1 Sykliset ryhmät

Syklistä ryhmää, jonka virittäjän kertaluku on n, merkitään C_n. Koska sykliset ryhmät ovat vaihdannaisia, ovat niiden kaikki aliryhmät normaaleja. Siten syklinen ryhmä on yksinkertainen jos ja vain jos sillä ei ole epätriviaaleja aliryhmiä. Koska syklisellä ryhmällä C_n on aina yksi aliryhmä kutakin luvun n jakajaa kohden, niin ryhmä on yksinkertainen jos ja vain jos n on alkuluku.

8.2.2 Alternoivat ryhmät

Alternoivat ryhmät ovat symmetristen ryhmien aliryhmiä. Symmetrinen ryhmä S_n koostuu kaikista joukon $\{1, \ldots, n\}$ permutaatioista. Jokainen S_n:n alkio voidaan kirjoittaa vaihtojen tulona. Ne permutaatiot, joiden ilmaisemiseen tarvitaan parillinen määrä vaihtoja, muodostavat aliryhmän A_n.

8.2.3 Klassiset ryhmät

Yksinkertaiset klassiset ryhmät saadaan projektiivisista ryhmistä. Ryhmät $PSL_n(q)$, $PSU_n(q)$ ja $PSp_n(q)$ ovat muutamaa poikeusta luukun ottamatta yksinkertaisia. Ortogonaalisissa ryhmissä tämä ei toimi, sillä $PSO_n(q)$ ei yleensä ole yksinkertainen. Tällöin onkin tarkasteltava aliryhmän $\Omega_n(q)$ tekijäryhmää $P\Omega_n(q)$, joka pienimpiä dimensioita lukuun ottamatta on yksinkertainen.

Lause 8.7. *Seuraavat klassiset ryhmät ovat yksinkertaisia:*

(1) $PSL_n(q)$, jos $n \geq 2$, poikkeuksina $PSL_2(2)$ ja $PSL_2(3)$

(2) $PSU_n(q)$, jos $n \geq 3$, poikkeuksena $PSU_3(2)$

(3) $PSp_n(q)$, jos $n \geq 2$, poikkeuksena $PSp_4(2)$

(4a) $P\Omega_{2n+1}(q)$, jos $n \geq 3$ ja q on pariton

(4b) $P\Omega^+_{2n}(q)$, jos $n \geq 4$

(4b) $P\Omega^-_{2n}(q)$, jos $n \geq 4$.

Todistus. Ryhmien yksinkertaisuus todistetaan niin kutsutun Iwasawan lemman avulla. Tällöin on tutkittava ryhmien toimintaa jossakin joukossa eli tulkittava ne tämän joukon kuvauksiksi. Esimerkiksi ryhmän $PSL_n(q)$ tapauksessa voidaan joukoksi valita projektiivinen avaruus.

Todistukset löytyvät esimerkiksi kirjasta L. C. Grove: Classical Groups and Geometric Algebra. □

Omegaryhmä Tarkastellaan seuraavaksi hieman tarkemmin omegaryhmiä, joiden määritelmä on hyvin erilainen parillisen ja parittoman karakteristikan tapauksessa.

Oletetaan ensin, että kerroinkunnan karakteristika on pariton. Tällöin omegaryhmä $\Omega_n(q)$ voidaan määritellä ortogonaalisen ryhmän peilauksien avulla. (Katso määritelmä 5.15.) Ryhmä $P\Omega_n(q)$ saadaan tuttuun tapaan muodostamalla tekijäryhmä skalaarien suhteen eli

$$P\Omega_n(q) = \Omega_n(q)/(\Omega_n(q) \cap \{I_n, -I_n\}).$$

Parillisessa karakteristikassa ei voida käyttää samaa määritelmää kuin parittomassa, sillä peilauksia ei ole. Jos karakteristika on parillinen ja avaruuden dimensio pariton, niin määritellään $\Omega_n(q) = O_n(q)$ ja $P\Omega_n(q) = PO_n(q)$. Tämä tapaus ei kuitenkaan ole mielenkiintoinen, sillä ryhmä $O_n(q)$ on isomorfinen symplektisen ryhmän $Sp_{n-1}(q)$ kanssa. Siksi ryhmää ei myöskään tarvitse mainita äärellisten yksinkertaisten ryhmien luokittelulauseessa.

Jos sekä karakteristika että avaruuden dimensio ovat parillisia, niin omegaryhmä määritellään seuraavasti: Olkoon $g \in O_n(q)$ ja olkoon k g:n kiinnittämän aliavaruuden dimensio eli

$$k = \dim \mathrm{Fix}(g) = \dim\{v \in K^n \mid gv = v\}.$$

Nyt $g \in \Omega_n(q)$ jos ja vain jos k on parillinen. Projektiivinen ryhmä $P\Omega_n(q)$ on parillisen karakteristikan tapauksessa isomorfinen ryhmän $\Omega_n(q)$ kanssa.

On hyvä tiedostaa, että kirjallisuudessa esiintyy rutkasti erilaisia omegaryhmän määritelmiä.

8.2.4 Poikkeukselliset Lie-tyypin ryhmät

Klassiset ryhmät ovat osa suurempaa kokonaisuutta, jota kutsutaan Lie-tyypin ryhmiksi. Muita Lie-tyypin ryhmiä kutsutaan poikkeuksellisiksi Lie-tyypin ryhmiksi. Muutamia poikkeuksia lukuun ottamatta ne ovat yksinkertaisia.

8.2.5 Sporadiset ryhmät

Sporadiset ryhmät muodostuvat niistä äärellisistä ryhmistä, jotka eivät mahdu mihinkään ylläolevista luokista. Niitä on yhteensä 26 kappaletta.

8.3 Klassisten ryhmien kompositiojonot

Tarkastellaan seuraavaksi klassisten ryhmien kompositiojonoja. Nämä jonot eivät ole erityisen monimutkaisia, sillä ne koostuvat yksinkertaisesta klassisesta ryhmästä sekä syklisistä ryhmistä.

Yleisen lineaarisen ryhmän kompositiojono on

$$\{1\} \lhd \underset{(1)}{\cdots} \lhd Z(SL_n(q)) \underset{(2)}{\lhd} SL_n(q) \lhd \underset{(3)}{\cdots} \lhd GL_n(q).$$

Jonon kompositiotekijät ovat seuraavat:

(1) Jos ryhmä $Z(SL_n(q))$ on yksinkertainen, on tässä välissä vain yksi kompositiotekijä. Muussa tapauksessa kompositiotekijät ovat ryhmän $Z(SL_n(q))$ aliryhmien tekijäryhmiä. Kompositiotekijät ovat syklisiä, sillä ryhmä $\mathbb{F}_q^*$ on syklinen.

(2) Kompositiotekijä on $SL_n(q)/Z(SL_n(q)) = PSL_n(q)$, kunhan $PSL_n(q)$ on yksinkertainen.

(3) Jos ryhmä $GL_n(q)/SL_n(q) \cong \mathbb{F}_q^*$ on yksinkertainen, on tässä välissä vain yksi kompositiotekijä $\mathbb{F}_q^*$. Muussa tapauksessa kompositiotekijät ovat ryhmän $\mathbb{F}_q^*$ aliryhmien tekijäryhmiä ja siten syklisiä.

Unitaarisen ryhmän kompositiojono on

$$\{1\} \lhd \underset{(1)}{\cdots} \lhd \{SU_n(q)\text{:n skalaarit}\} \underset{(2)}{\lhd} SU_n(q) \lhd \underset{(3)}{\cdots} \lhd U_n(q).$$

Jonon kompositiotekijät ovat seuraavat:

(1) Jos ryhmä $\{SU_n(q)\text{:n skalaarit}\}$ on yksinkertainen, on tässä välissä vain yksi kompositiotekijä. Muussa tapauksessa kompositiotekijät ovat tämän ryhmän aliryhmiä. Ne ovat syklisiä.

(2) Kompositiotekijä on $SU_n(q)/\{\text{skalaarit}\} = PSU_n(q)$, kunhan $PSU_n(q)$ on yksinkertainen.

(3) Jos ryhmä $U_n(q)/SU_n(q) \cong \mathrm{Ker}(N)$ on yksinkertainen, on tässä välissä vain yksi kompositiotekijä $\mathbb{F}_q^*$. Muussa tapauksessa kompositiotekijät ovat ryhmän $\mathrm{Ker}(N)$ aliryhmien tekijäryhmiä. Ne ovat syklisiä.

Jos $PSp_n(q)$ on yksinkertainen, niin symplektisen ryhmän kompositiojonoksi saadaan

$$\{1\} \underset{C_2}{\lhd} \{1,-1\} \underset{PSp_n(q)}{\lhd} Sp_n(q),$$

missä kompositiotekijät on merkitty kolmioiden alle.

Jos q on pariton, niin ortogonaalisen ryhmän kompositiojono on

$$\{1\} \underset{1 \text{ tai } C_2}{\lhd} \{1,-1\} \cap \Omega_n(q) \underset{P\Omega_n(q)}{\lhd} \Omega_n(q) \underset{1 \text{ tai } C_2}{\lhd} SO_n(q) \underset{C_2}{\lhd} O_n(q),$$

kunhan vain $P\Omega_n(q)$ on yksinkertainen.

Jos q ja n ovat parillisia, niin ortogonaalisen ryhmän kompositiojono on

$$\{1\} \underset{\Omega_n(q)}{\lhd} \Omega_n(q) \underset{C_2}{\lhd} O_n(q),$$

kunhan vain $\Omega_n(q)$ on yksinkertainen.

8.4 Äärellisten yksinkertaisten ryhmien historia

Äärellisten yksinkertaisten ryhmien historia ulottuu ainakin 1830-luvulle asti. Niihin aikoihin ranskalainen matemaatikko Évariste Galois selvitti ryhmien merkityksen polynomiyhtälöiden ratkaisemisessa ja loi pohjan ryhmäteorialle. Galois ymmärsi, että yksinkertaiset ryhmät ovat tärkeitä, ja tiesi alternoivan ryhmän A_n olevan yksinkertainen, kun $n \geq 5$. Lisäksi Galois konstruoi ainakin ryhmät $PSL_2(p)$, missä p on alkuluku.

Muutamia kymmeniä vuosia myöhemmin 1870-luvulla Galoisin maanmies Camille Jordan löysi loputkin lineaarisista yksinkertaisista ryhmistä $PSL_n(q)$. Hän myös kehitti menetelmiä, joita voitiin myöhemmin käyttää äärellisten yksinkertaisten ryhmien luokittelussa. Samohin aikoihin Émile Mathieu konstruoi viisi sporadista ryhmää, joita kutsutaan Mathieun ryhmiksi. (Mathieukin oli ranskalainen.)

1900-luvulla klassisten ryhmien teoria pääsi toden teolla vauhtiin. Saksalainen matemaatikko Wilhelm Killing oli luokitellut yksinkertaiset Lien algebrat, ja kävi ilmi, että niihin liittyvät niin kutsutut Lie-tyypin ryhmät ovat yksinkertaisia. (Klassiset ryhmät kuuluvat näihin.) Tässä työssä merkittävä osuus oli ranskalaisella Claude Chevalleylla, joka kehitti systemaattisen menetelmän Lie-tyypin ryhmien konstruoimiseksi.

1960-luvulla kaikki Lie-tyypin ryhmät oli löydetty ja matemaatikot alkoivat olla sitä mieltä, että äärellisiä yksinkertaisia ryhmiä ei enää olisi enempää. Luokittelulauseelle ryhdyttiin toiveikkaina kokoamaan todistusta, mutta pian huomattiin, ettei se ollutkaan aivan helppoa. Vuonna 1964 ryhmäteoreetikkoja järkytti kroatialaisen Zvonimir Jankon löydös: uusi yksinkertainen sporadinen ryhmä. Tutkijoille alkoi valjeta, että tehtävä saattaisi hyvin vaikea. Ehkäpä äärellisiä yksinkertaisia ryhmiä olikin jäjellä vielä sadoittain?

Seuraavalla vuosikymmenellä löytyivät loputkin 20 sporadista ryhmää, mutta sen jälkeen alkoi näyttää siltä, että äärellisiä yksinkertaisia ryhmiä ei enää löytyisi enempää. 1980-luvulla alettiin uskoa, että luokittelulause todistuksineen olisi viimeinkin valmis.

Äärellisiä yksinkertaisia ryhmiä ei tähän päivään mennessä ole löytynyt lisää. Luokittelulauseen todistus koostuu useiden eri ihmisten kokoamista palasista, ja sitä on jouduttu moneen otteeseen korjaamaan ja paikkailemaan. Tuhansia sivuja pitkä todistus koostuu sadoista artikkeleista, ja tuskinpa kukaan pystyy sitä kokonaisuudessaan ymmärtämään. Tämä onkin herättänyt kritiikkiä, eivätkä kaikki ole aina olleet sitä mieltä, että tulosta ylipäänsä voi kutsua lauseeksi ja sen todistusta todistukseksi. Todistuksen eri osaset on kuitenkin tarkastettu moneen otteeseen ja eri ihmiset ovat saaneet eri menetelmillä samoja tuloksia, joten vain harva enää nykyään epäilee lauseen todistuksessa olevan vakavia virheitä.

Luokittelulause on eräs ryhmäteorian huikeimmista saavutuksista. Jo pituudeltaankin sen todistus on omaa luokkaansa. Gorenstein, Lyons ja Solomon aloittivat kokoamaan todistusta yksiin kansiin, ja siitä on muodostumassa yksitoistaosainen kirjasarja, josta tähän mennessä on ilmestynyt kuusi osaa. Luokittelulauseen todistusta pyritään edelleen kehittämään ja yksinkertaistamaan, ja tälläkin hetkellä monet ryhmäteoreetikot työskentelevät sen parissa.

Lähde: R. A. Wilson: Finite Simple Groups

9 Lien teoria

9.1 Tausta

Norjalaisella matemaatikolla Sophus Marius Liellä (1842–1899) oli unelma. Hän oli kuullut Evariste Galois'n teoriasta, jossa tämä liitti kuhunkin polynomiyhtälöön tietyn symmetriaryhmän, joka permutoi yhtälön ratkaisuja pitäen kerroinkunnan paikallaan. Galois oli onnistunut tämän symmetriaryhmän avulla määrittämään tarkat ehdot sille, milloin polynomiyhtälö voidaan ratkaista analyyttisesti, ja tätä keksintöä pidetään ryhmäteorian ja modernin algebran alkuna. Ottaen mallia Galois'n teoriasta, Lie halusi löytää differentiaaliyhtälöihin liittyvät symmetriaryhmät, jotka auttaisivat yhtälön ratkaisujen löytämisessä.

Lien oivallus, jonka hän mainitsi 1871 väitöskirjassaan "Über eine Classe geometrischer Transformationen", perustui hänen aikaisempiin differentiaaligeometrian tutkimuksiinsa. Hän huomasi, että reaaliluvuilla parametrisoitu muunnosryhmä säilyttää differentiaaliyhtälön muodon vain jos ryhmän *tangenttiavaruudella* on tietty rakenne. Lien pyrkimys oli luokitella kaikki tällaiset tangenttiavaruudet, ja käyttää sitten tätä luokittelua differentiaaliyhtälöiden ratkaisemiseksi.

Vaikka Lien tavoite ei koskaan täysin toteutunut, Lie tuli kehittäneeksi "jatkuviksi" kutsumiensa ryhmien teorian, joka on vieläkin pääasiallinen työkalu näiden ryhmien tutkimisessa. Hänen mukaansa näitä ryhmiä kutsutaan nykyisin *Lien ryhmiksi.*

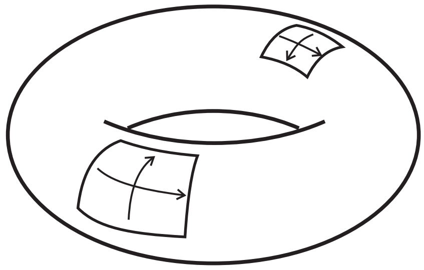
9.2 Differentiaaligeometriaa

Lien ryhmien määrittelemiseksi tarvitsemme *derivoituvia monistoja.* Emme määrittele tässä tällaisia monistoja täsmällisesti; riittää ajatella, että n-ulotteinen monisto on topologinen avaruus[3], jonka jokaisella pisteellä on avaruutta $\mathbb{R}^n$ muistuttava ympäristö (homeomorfinen sen kanssa). Tällaista ympäristöä kutsutaan *kartaksi*, ja sille saadaan koordinaatisto avaruudesta $\mathbb{R}^n$. Koko monisto voidaan peittää kartoilla, jotka menevät osaksi limittäin. Derivoituvuus tarkoittaa tässä yhteydessä sitä, että koordinaatistonmuunnos kahden limittäin menevän kartanosan välillä on derivoituva[4]. Jos M on derivoituva monisto, niin kuvausten $f : M \to \mathbb{R}$, $g : M \to M$ ja $\gamma : \mathbb{R} \to M$ derivaatat pisteessä x voidaan määritellä jokin sopivan x:n sisältävän kartan koordinaatiston avulla.

Määritelmä 9.1. *Lien ryhmä* on derivoituva monisto M, joka on samalla ryhmä jonkin laskutoimituksen suhteen, ja jonka kuvaukset $\mu : (x, y) \mapsto xy$ ja $\iota : x \mapsto x^{-1}$ ovat derivoituvia.

[3] Oikeastaan Hausdorff-avaruus, jolla on numeroituva kanta.

[4] Lien ryhmien yhteydessä derivoituvalla kuvauksella tarkoitetaan reaalianalyyttistä kuvausta eli kuvausta, jolla on kaikkien kertalukujen derivaatat.



Kuva 8: Kaksiulotteinen monisto, jolla kaksi karttaa

Esimerkki 9.2. Tarkastellaan tason yksikköympyrää S. Jokaisella yksikköympyrän pisteellä on ympäristö, joka on homeomorfinen lukusuoran $\mathbb{R}$ kanssa. Ympyrä voidaan peittää kahdella kartalla esimerkiksi seuraavasti: Kuvaus $h_1 : (0, 2\pi) \to S$, $h_1(t) = (\cos t, \sin t)$ peittää koko ympyrän pistettä $(1, 0)$ lukuunottamatta. Vastaavasti kuvaus $h_2 : (0, 2\pi) \to S$, $h_2(t) = (\cos(t - \pi), \sin(t - \pi))$ peittää ympyrän pistettä $(-1, 0)$ lukuunottamatta. Alueella, jossa kartat menevät limittäin, koordinaatistonmuunnos kahden kartan välillä tapahtuu kuvauksella $t \mapsto t - \pi$, joka on selvästi derivoituva.[5]

Tason kierrot voidaan parametrisoida reaaliparametrilla φ, joka kertoo kiertokulman origon ympäri. Jokaista kulmaa välillä $[0, 2\pi)$ vastaa oma kiertonsa. Kiertoryhmä $SO(2)$ voidaan samastaa yksikköympyrän kanssa siten, että jokainen ympyrän piste vastaa kiertoa sen kulman ympäri, jonka piste muodostaa positiivisen x-akselin kanssa. Tällaisen kierron matriisi on

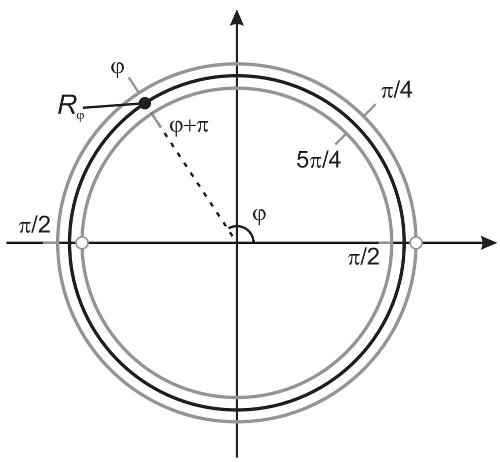
$$R_\varphi = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}.$$

Tällä tavoin ryhmälle $SO(2)$ saadaan yksikköympyrältä topologia ja derivoituvan moniston rakenne.

Tarkistetaan, että alkion kääntäminen on monistolla derivoituva kuvaus. Olkoon R_φ jokin kierto, jolla $\varphi \neq 0$. Tätä kiertoa vastaa ympyrällä piste $(\cos\varphi, \sin\varphi)$, joka on kuvauksen h_1 määrittämällä kartalla. Tällä kartalla kierron koordinaatti on φ. Kierron käänteisalkio $\mathbb{R}_{-\varphi}$ on samalla kartalla kuin kierto itse, ja sen koordinaatti on $-\varphi$. Siispä koordinaatistossa (avoimella välillä $(0, 2\pi)$) alkion R_φ kääntävä kuvaus on $\varphi \mapsto -\varphi$, joka on selvästi derivoituva.

Jos taas $\varphi \neq \pi$, niin kiertoa vastaava piste on kuvauksen h_2 määrittämällä kartalla, ja sen koordinaatti on $\varphi + \pi$. Kierron käänteisalkio on jälleen samalla kartalla, koordinaattinaan $-\varphi + \pi$. Alkion kääntäminen on siis myös tässä koordinaatistossa derivoituva kuvaus $\varphi \mapsto -\varphi$. Vastaavasti voidaan

[5]Tässä käytettiin karttoina avoimen välin kuvia koko lukusuoran $\mathbb{R}$ sijasta. Tällä ei ole kuitenkaan merkitystä, koska koko lukusuora voidaan kuvata avoimelle välille sopivalla derivoituvalla bijektiolla.



Kuva 9: Yksikköympyrä voidaan peittää kahdella avoimella välillä. Kierrot vastaavat ympyrän pisteitä.

tarkistaa, että alkioiden tulo on derivoituva kuvaus, joten $SO(2)$ on Lien ryhmä.

Lien aliryhmä H on Lien ryhmän G aliryhmä, joka on samalla moniston G alimonisto. Niin kutsutun *Cartanin lauseen* mukaan jokainen G:n (topologisesti) suljettu aliryhmä on Lien ryhmä.

Kompleksiset monistot määritellään täsmälleen samalla tavalla kuin reaaliset: jokaisella pisteellä täytyy olla ympäristö, joka on homeomorfinen avaruuden $\mathbb{C}^n$ kanssa. Derivoituvuus tarkoittaa tällöin kompleksista derivoituvuutta. Myös Lien ryhmät voivat olla kompleksisia monistoja, mutta ellei toisin sanota, pitäydymme jatkossa reaalisissa monistoissa.

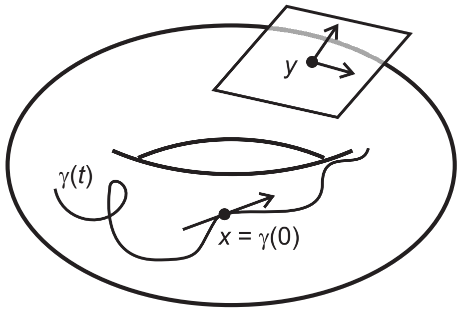
9.3 Tangenttivektorit ja kommutaattorit

Olkoon x jokin piste n-ulotteisella derivoituvalla monistolla M. Pisteen x kautta kulkevalla *derivoituvalla käyrällä* tarkoitetaan derivoituvaa kuvausta $\gamma : \mathbb{R} \to M$, jolla pätee $\gamma(0) = x$. Käyrän γ derivaatta pisteessä x kertoo polun *suunnan pisteessä x* ja sitä kutsutaan *tangenttivektoriksi pisteessä x*. Jos tarkastellaan kaikkia pisteen x kautta kulkevia käyriä ja samastetaan samansuuntaiset keskenään, muodostuu tangenttivektoreista vektoriavaruus, jota kutsutaan *tangenttiavaruudeksi pisteessä x*.

Olkoon M Lien ryhmä, ja olkoon γ neutraalialkion 1 kautta kulkeva käyrä. Differentiaalilaskennasta tiedetään, että kun $h \in \mathbb{R}$ on riittävän pieni, voidaan arvioida

$$\gamma(h) \approx \gamma(0) + \gamma'(0)h = 1 + \gamma'(0)h.$$

Termiä $\gamma'(0)h$ voidaan pitää ryhmän M *infinitesimaalisena alkiona.*



Kuva 10: Polun γ tangenttivektori pisteessä x sekä tangenttitaso pisteessä y.

Jos M on Lien ryhmä, pisteessä $g \in M$ voidaan määritellä tangenttitaso kahdella tavalla: joko määritellään tangenttitaso suoraan pisteen g kautta kulkevien käyrien avulla, tai sitten siirretään kuvauksen $h \mapsto gh$ avulla neutraalialkio 1 pisteeseen g, ja käytetään neutraalialkion kohdalla määriteltyä tangenttitasoa. Osoittautuu, että nämä tuottavat saman tuloksen. Sanotaan, että moniston M tangenttivektorien muodostama vektorikenttä[6] on *invariantti vasemmalta kertomisen suhteen.*

Tärkeä tangenttivektorien välinen operaatio on *kommutaattori* $[x, y]$, jota kutsutaan myös *Lien derivaataksi.* Sen täsmällinen määritelmä sivuutetaan, mutta se kuvaa tangenttivektorin y hetkellistä muutosnopeutta, kun sitä siirretään tangenttivektorin x suunnassa. Kommutaattorilla on läheinen yhteys ryhmän M konjugointiin. Lisäksi vektorien $[x, y]$ muodostama vektorikenttä on invariantti vasemmalta kertomisen suhteen, aivan kuten tangenttivektorien muodostamat kentät, joten kommutaattorivektoreita voidaan siirrellä vapaasti pitkin monistoa ryhmän alkioilla kertomalla.

9.4 Lien matriisiryhmät

Monet Lien ryhmistä ovat itse asiassa lineaarikuvausten ryhmiä, joten niiden alkioita voidaan ajatella matriiseina. Tarkastellaan helpoimpana esimerkkinä kaikkien kääntyvien matriisien ryhmää $GL_n(\mathbb{R})$. Matriisia $X = [x_{ij}]$ voidaan ajatella avaruuden $\mathbb{R}^{n^2}$ vektorina $(x_{11}, x_{12}, \ldots, x_{nn})$. Kääntyvät eli ehdon $\det(X) \neq 0$ toteuttavat matriisit muodostavat tällöin koko avaruuden avoimen osajoukon, joka on n^2-ulotteinen derivoituva monisto (kartat saadaan suoraan ympäröivästä avaruudesta $\mathbb{R}^{n^2}$). Yksikkömatriisin kautta kulkeva käyrä on muotoa $\Gamma(t) = [\gamma_{ij}(t)]$, ja tangenttivektori pisteessä I_n on vastaavasti $\Gamma'(0) = [\gamma'_{ij}(0)]$. Osoittautuu, että koska $GL_n(\mathbb{R})$ on avaruuden $\mathbb{R}^{n^2}$ avoin osajoukko, voidaan missä tahansa pisteessä määritellä kaikensuuntaisia käyriä, joten luvuilla $\gamma'_{ij}(0)$ ei ole mitään ulkoisia rajoitteita. Näin ollen pisteeseen x liitettävä tangenttiavaruus on itse asiassa kaikkien $n \times n$-matriisien muodostama avaruus $L_n(\mathbb{R})$.

[6]Vektorikenttä on kuvaus, joka liittää moniston jokaiseen pisteeseen tietyn vektorin.

Cartanin lauseen avulla voidaan osoittaa, että kaikki klassiset ryhmät ovat Lien ryhmiä. Tarkastellaan esimerkiksi $\mathbb{R}^n$:n tavallisten kiertojen muodostamaa erityistä ortogonaalista ryhmää $SO(n) = SO_n(\mathbb{R})$. Tangenttivektorit voidaan laskea seuraavasti: Olkoon $\Gamma'(t) = [\gamma'_{ij}(t)]$ jokin yksikkömatriisi kautta kulkeva käyrä. Ortogonaalisuuden määritelmän mukaan $\Gamma(t)^\top \Gamma(t) = I_n$ eli

$$\left(\Gamma(t)^\top \Gamma(t)\right)(i,j) = \sum_{k=1}^{n} \gamma_{ki}(t)\gamma_{kj}(t) = \delta_{ij},$$

missä $\delta_{ij} = 1$ jos $i = j$, muuten $\delta_{ij} = 0$. Derivoimalla yhtälö puolittain pisteessä $t = 0$ saadaan

$$\sum_{k=1}^{n} \left(\gamma'_{ki}(0)\gamma_{kj}(0) + \gamma_{ki}(0)\gamma'_{kj}(0)\right) = \gamma'_{ji}(0) + \gamma'_{ij}(0) = 0, \tag{9.3}$$

sillä $\gamma(0) = I_n$ (joten $\gamma_{jk}(0) = 0$ jos $j \neq k$) ja $D(I_n) = 0$ (vakion derivaatta). Yhtälöstä (9.3) nähdään, että ortogonaalisen ryhmän tangenttitaso pisteessä I_n koostuu antisymmetrisistä matriiseista.

Yllä olevassa esimerkissä ei itse asiassa käytetty determinanttiehtoa lainkaan. Voidaankin osoittaa, että ryhmillä $O_n(\mathbb{R})$ ja $SO_n(\mathbb{R})$ on samat tangenttiavaruudet. Erona näiden Lien ryhmien välillä on se, että $SO_n(\mathbb{R})$ on monistona yhtenäinen, kun taas $O_n(\mathbb{R})$ koostuu kahdesta erillisestä komponentista, joista toisella $\det g = 1$, toisella $\det g = -1$.

Kommutaattoreille saadaan matriisiryhmien tapauksessa yksinkertainen yhtälö: jos $X, Y \in L_n(\mathbb{R})$ ovat tangenttivektoreita, niin

$$[X, Y] = XY - YX.$$

Tämän yhtälön avulla on helppo johtaa kommutaattoreiden ominaisuuksia, kuten $[X, X] = 0$ ja $[X, Y] = -[Y, X]$.

9.5 Eksponenttikuvaus ja yksiparametriset aliryhmät

Matriiseilla voidaan määritellä *eksponenttikuvaus* sarjakehitelmän avulla:

$$\exp A = e^A = I_n + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots .$$

Voidaan osoittaa, että tämän sarjan osasummilla on raja-arvo, joten eksponenttikuvaus on hyvin määritelty. Ei vaadi paljon vaivaa tarkistaa, että $\exp(0) = I_n$ ja $(\exp A)^{-1} = \exp(-A)$. Kuitenkin $\exp(A+B) = \exp A \cdot \exp B$ pätee vain, jos $AB = BA$.

Eksponenttikuvauksen avulla voidaan määritellä halutunsuuntaisia käyriä, jotka ovat samalla Lien ryhmän aliryhmiä. Tällaista käyrää sanotaan yksiparametriseksi aliryhmäksi. Jos G on Lien matriisiryhmä ja A on jokin tangenttivektori pisteessä I_n, niin käyrälle $\gamma(t) = \exp(tA)$ pätee $\gamma(0) = I_n$, ja joukko $\{\gamma(t)\}$ on G:n aliryhmä. Lisäksi

$$\gamma'(0) = A\exp(0 \cdot A) = A,$$

joten A on käyrän $\gamma(t)$ tangenttivektori. Voidaan myös osoittaa, että muita yksiparametrisiä aliryhmiä, joilla olisi sama ominaisuus, ei ole.

Yksiparametrisia aliryhmiä voidaan käyttää muodostamaan Lien ryhmän alkioita annetuista tangenttivektoreista. Jos Lien ryhmä G on yhtenäinen, niin jokainen sen alkio on muotoa $\exp(x_1)\cdots\exp(x_r)$, missä $x_1, \ldots, x_r$ ovat tangenttiavaruuden vektoreita neutraalialkion kohdalla.

9.6 Lien algebrat

Lien ryhmien ominaisuuksia voidaan hyvin pitkälle selvittää neutraalialkion kohdalla määriteltyjen tangenttivektorien avulla. Nämä muodostavat struktuurin, jota kutsutaan *Lien algebraksi*. Saksalainen matemaatikko Wilhelm Killing (1847–1923) oli Liestä riippumatta keksinyt Lien algebran käsitteen, ja onnistui myöhemmin luokittelemaan kaikki niin sanotut *yksinkertaiset* Lien algebrat. Killingin sekavan esityksen siisti väitöskirjassaan ranskalainen Élie Cartan (1869–1951), joka oli itse Lien oppilas.

Määritelmä 9.4. Olkoon $\mathfrak{g}$ vektoriavaruus, jossa on määritelty laskutoimitus $(x, y) \mapsto [x, y]$, nimeltään *Lien tulo*. Oletetaan lisäksi, että kaikilla vektoreilla x, y, z ja skalaareilla λ pätevät seuraavat ehdot:

$$[x + z, y] = [x, y] + [z, y] \quad \text{ja} \quad [\lambda x, y] = \lambda[x, y] \tag{L1}$$
$$[x, y + z] = [x, y] + [x, z] \quad \text{ja} \quad [x, \lambda y] = \lambda[x, y] \tag{L2}$$
$$[x, x] = 0 \tag{L3}$$
$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0. \tag{L4}$$

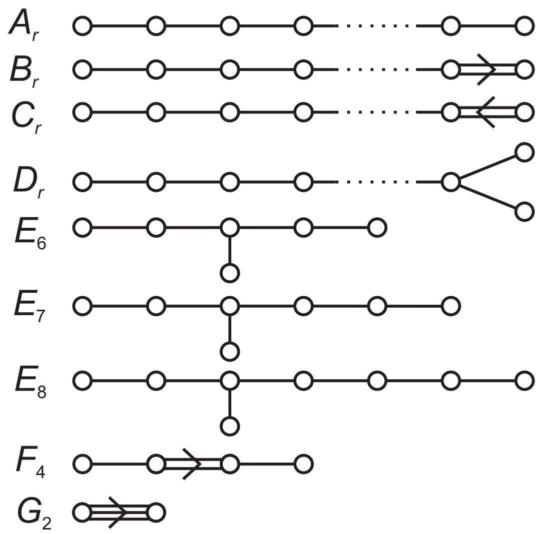
Tällöin avaruutta $\mathfrak{g}$ kutsutaan *Lien algebraksi*.

Ehdot (L1) ja (L2) määrittelevät *bilineaarisuuden* ja ehto (L3) *alternoivuuden*. Ehtoa (L4) kutsutaan *Jacobin identiteetiksi*. Esimerkki reaalikertoimisesta Lien algebrasta on $\mathbb{R}_3$, jossa laskutoimituksena on ristitulo eli $[x, y] = x \times y$.

Lien algebraa sanotaan yksinkertaiseksi, jos sillä ei ole tiettyjä epätriviaaleja alistruktuureja, joita kutsutaan *ideaaleiksi* (sama kuin renkaan ideaali). Killing ja Cartan selvittivät, että yksinkertaiset kompleksikertoimiset Lien algebrat koostuvat alialgebrasta $\mathfrak{h}$, jota kutsutaan *Cartanin alialgebraksi*, sekä joukosta yksiulotteisia alialgebroja, joita kutsutaan *juurialgebroiksi*. Kun juurialgebrojen alkioita kerrotaan Cartanin alialgebran alkioilla, ne pysyvät edelleen samassa juurialgebrassa. Tällä tavoin voidaan jokaiselle juurialgebralle $\mathfrak{l}_i$ määritellä kuvaus $r_i : \mathfrak{h} \to \mathbb{C}$, jolle pätee

$$[h, x] = r_i(h)x, \qquad \text{kun } x \in \mathfrak{l}_i.$$

Yllä määriteltyjä kuvauksia r_i sanotaan *juuriksi*, ja ne muodostavat niin kutsutun *juurijärjestelmän*. Juurten väliset kulmat voidaan määrittää negatiivisesti definiitin *Killingin muodon* avulla. Yksinkertaisen Lien algebran juuret voivat olla neljässä eri kulmassa toisiinsa nähden, ja kaikki mahdolliset juurijärjestelmät voidaan listata seuraavien *Dynkinin diagrammien* muodossa.



Kuva 11: Dynkinin diagrammit

Diagrammeja tulkitaan siten, että jokainen piste vastaa tiettyä perusjuurta, joiden avulla kaikki muut juuret voidaan muodostaa. Jos kahden perusjuuren välinen kulma on 90°, niin niiden välille ei piirretä viivaa. Yksi viiva juurten välillä tarkoittaa 120 asteen kulmaa, kaksi viivaa 135:tä astetta ja kolme viivaa 150:tä astetta. Nuolen suunta osoittaa pidemmästä juuresta lyhyempään, jos pituuksissa on eroa.

Juurijärjestelmiä A_r, B_r, C_r ja D_r vastaavia Lien algebroja kutsutaan *klassisiksi*, muita *poikkeuksellisiksi*. Klassiset järjestelmät vastaavat klassisten Lien ryhmien tangenttiavaruuksia seuraavasti:

Diagrammi	Lien ryhmät
A_r	$SL_{r+1}(\mathbb{C})$ ja $SU_{r+1}(\mathbb{C})$
B_r	$O_{2r+1}(\mathbb{C})$ ja $SO_{2r+1}(\mathbb{C})$
C_r	$Sp_{2r}(\mathbb{C})$
D_r	$O_{2r}(\mathbb{C})$ ja $SO_{2r}(\mathbb{C})$

Kaikki ryhmät on määritelty kompleksikertoimisissa avaruuksissa. Reaalikertoimisten ryhmien tangenttiavaruudet ovat reaalikertoimisia Lien algebroja, joiden kerroinkunta voidaan laajentaa *kompleksifioimalla*, minkä jälkeen ne voidaan sovittaa samoihin diagrammeihin. Erityiset unitaariset ryhmät ovat Lien ryhminä reaalimonistoja(!), ja niiden Lien algebrat vastaavat tyyppiä A_r.

9.7 Äärelliset kerroinkunnat

Ranskalainen matemaatikko Claude Chevalley (1909–1984) löysi tavan yleistää Lien algebrat äärellisiin kerroinkuntiin niin, että Cartanin alialgebrat ja juurijärjestelmät säilyvät. Chevalley pystyi systemaattisesti konstruoimaan niin sanotut *Lie-tyypin ryhmät*, jotka koostuvat äärellisten Lien algebrojen automorfismeista. Lie-tyypin ryhmät jakautuvat klassisiin ja poikkeuksellisiin vastaavan Lien algebran juurijärjestelmän mukaan, ja ne muodostavat suuren osan äärellisistä yksinkertaisista ryhmistä.

Myöhemmin on yksinkertaisia Lie-tyypin ryhmiä löydetty lisää, kun huomattiin, että Dynkinin diagrammien automorfismeista saadaan aliryhmiä jo tunnetuille Lie-tyypin ryhmille.

9.8 Loppusanat

Sophus Lie ei saanut kehitettyä Galois'n teorian veroista työkalua differentiaaliyhtälöiden tutkimiseen, mutta hänen panoksensa ryhmäteoriassa hakee silti vertaistaan. Myöhemmin Lien ryhmät ovat tulleet korvaamattomiksi esimerkiksi kvanttimekaniikan kuvailussa, ja Lien keksimät menetelmät ovat näiden ryhmien analysoimisessa välttämättömiä.

Lien terveys alkoi heiketä vuoden 1889 tienoilla. Häneltä diagnosoitiin pernisiöösi anemia, jossa elimistö ei kykene absorboimaan B12-vitamiinia. Lien viimeiset elinvuodet olivat taudin vuoksi vaikeita, sillä hoitokeinoa ei ollut vielä löydetty. Edes lukuisat palkinnot ja huomionosoitukset eivät pystyneet ilahduttamaan häntä. Lie kuoli tautiin 56-vuotiaana, jättäen jälkeensä paljon julkaisematonta materiaalia.

Lähteet:

- Sigurdur Helgason: Sophus Lie, the mathematician, *Proceedings of The Sophus Lie Memorial Conference, Oslo, August, 1992*, Scandinavian University Press, ss. 3–21
- Louis Auslander & Robert E. MacKenzie: Introduction to Differentiable Manifolds, Dover Publications, 1977
- Roger W. Carter: Simple Groups of Lie Type, Wiley-Interscience, 1989

LOPPU