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

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

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 $x_1 = \cdots = x_k = 0$.

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 $\mathrm{syt}(k, l)$.*