Lineaarialgebra 2

Kevät 2014

Kerkko Luosto
Informaatiotieteiden yksikkö, Tampereen yliopisto

I Skalaarit ja vektorit

1. Kerroinrenkaat

Kun euklidisten vektoriavaruuksien teoriaa yleistetään mielivaltaisiin vektoriavaruuksiin ja moduleihin, on tärkeätä mieltää, mitä algebrallisia sääntöjä vektoreiden ja skalaareiden on edellytettävä noudattavan, jotta avaruuksille saataisiin todistettua toimiva teoria. Koulustakin tutut vektorikuviot säilyvät abstraktissa mielessä, kunhan vektorit vektorisummalla varustettuna muodostavat Abelin ryhmän. Skalaareilta vaaditaan enemmän rakennetta, koska sekä skalaareiden summia että tuloja tarvitaan vektorialgebrassa. Käytännössä on huomattu, että skalaareiden on syytä muodostaa rengas näillä laskutoimituksilla varustettuna. Usein tulon vaihdannaisuuden puuttuminen on kiusallista, ja jokseenkin täysin euklidisia avaruuksia vastaava teoria saadaan toimimaan, kun skalaarit muodostavat kunnan. Tässä luvussa esitellään nopeasti tarvittavat algebralliset käsitteet, joista useimmat ovat tuttuja opiskelijoille jo algebran peruskurssilta.

1.1. Määritelmä. Olkoon S epätyhjä joukko ja $*$ sen laskutoimitus, ts. $*$ on kuvaus $S \times S \to S$. Laskutoimitus $*$ on *liitännäinen*, jos kaikilla $x, y, z \in S$ pätee

$$(x * y) * z = x * (y * z).$$

Se on *vaihdannainen*, jos kaikilla $x, y \in S$ on voimassa

$$x * y = y * x.$$

Alkio $e \in S$ on laskutoimituksen $*$ *neutraalialkio*, jos kaikilla $x \in S$ pätee

$$x * e = e * x = x.$$

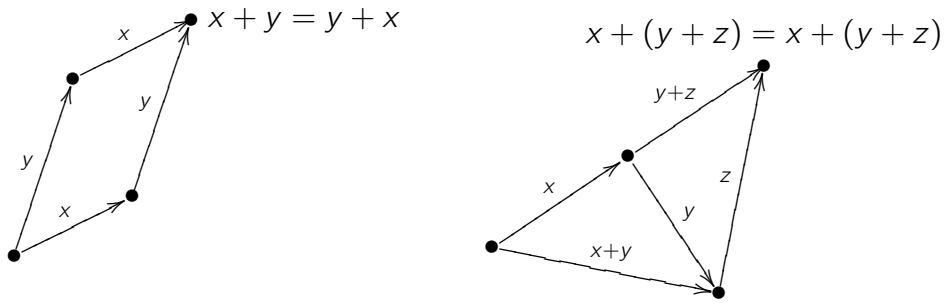
Jos laskutoimituksella $*$ on neutraalialkio e, niin alkiolla $x \in S$ on *käänteisalkio* $y \in S$, jos

$$x * y = y * x = e.$$

Käänteisalkiota nimitetään myös *vasta-alkioksi*, jos laskutoimitukselle käytetään yhteenlaskumerkintää. Alkion x käänteisalkiota merkitään x^{-1} tai $-x$ sen mukaan, mielletäänkö se käänteis- vai vasta-alkioksi.

Huomautus. Laskutoimituksella $*$ voi olla korkeintaan yksi neutraalialkio, joten käänteisalkion käsite on hyvinmääritelty. Myös käänteisalkiot ovat yksikäsitteisiä.

1.2. Määritelmä. Yhden laskutoimituksen rakenne $(S, *)$ on *puoliryhmä*, jos $\cdot$ on liitännäinen. Puoliryhmä $(S, *)$ on *monoidi*, jos laskutoimituksella $*$ on neutraalialkio. Monoidi $(S, *)$ on *ryhmä*, jos jokaisella $x \in S$ on käänteisalkio. *Vaihdannaista ryhmää* $(S, *)$, ts. ryhmää, jossa laskutoimitus $*$ on vaihdannainen, kutsutaan *Abelin ryhmäksi*. Abelin ryhmän laskutoimitus on siten liitännäinen ja vaihdannainen, sillä on neutraalialkio, ja jokaisella Abelin ryhmän alkiolla on käänteisalkio.



Vektorien vaihdannaisuus ja liitännäisyys havainnollistettuna

1.3. Määritelmä. Kahden laskutoimituksen rakenne $(R, +, \cdot)$ on *rengas*, jos
1) $(R, +)$ on Abelin ryhmä,
2) $(R, \cdot)$ on monoidi ja
3) osittelulaki on voimassa, ts.

$$x(y + z) = xy + xz \text{ ja } (x + y)z = xz + yz,$$

kun $x, y, x \in R$.
Rengas on *vaihdannainen*, jos sen kertolasku on vaihdannainen.

1.4. Määritelmä. Kahden laskutoimituksen rakenne $(K, +, \cdot)$ on *kunta*, jos
1) $(K, +)$ on Abelin ryhmä, ns. *kunnan yhteenlaskuryhmä*, jonka neutraalialkiota merkittäköön symbolilla 0,
2) $(K^*, \cdot)$, jossa $K^* = K \setminus \{0\}$, on Abelin ryhmä (*kunnan kertolaskuryhmä*), jonka neutraalialkiota merkitään yleensä symbolilla 1, ja
3) Yhteen- ja kertolasku osittelevat (oikealta) eli

$$(x + y)z = xz + yz,$$

kun $x, y, z \in K$.

1.5. Määritelmä. Kunnan $\boldsymbol{K} = (K, +, \cdot)$ *karakteristika* on pienin $p \in \mathbb{Z}_+$, jolle pätee $p \cdot 1$ kunnassa $\boldsymbol{K}$, jos tällainen on olemassa, muuten 0.

Kunnista todistetaan algebrasta seuraavia perustuloksia:

1) Kunnan karakteristika on aina joko nolla tai alkuluku.
2) Alkulukukarakteristikaa olevat kunnat ovat kaikki äärellisiä.
3) Äärellisen kunnan koko on alkulukupotenssi.
4) Samankokoiset äärelliset kunnat ovat isomorfisia.

2. Modulit

Puhtaasti matemaattis-tekniseltä kannalta katsoen euklidinen vektoriavaruus $V = \mathbb{R}^n$ on lähtökohtaisesti monimutkainen olio: Se ovat rakenne, joka on varustettu peräti neljällä laskutoimituksella. Kun korostetaan näiden erilaisia rooleja sopivilla alaindekseillä, ne ovat

$$\begin{array}{cc} +_V\colon V \times V \to V & \text{(vektorisumma)}, \\ +_{\mathbb{R}}\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} & \text{(reaalilukujen yhteenlasku)}, \\ \cdot_{\mathbb{R}}\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} & \text{(reaalilukujen kertolasku) ja} \\ \cdot \mathbb{R} \times V \to V & \text{(skalaarikerronta)}. \end{array}$$

Modulin käsite kasataan vastaavalla tavalla edellisessä luvussa määriteltyjen algebrallisten käsitteiden avulla.

2.1. Määritelmä. Olkoon $(M, +_M)$ Abelin ryhmä ja $(R, +_R, \cdot_R)$ epätriviaali rengas, jossa siis $0_R \neq 1_R$. Tällöin M:stä muodostuu *R-moduli*, jos se varustetaan lisäksi *skalaarikerronnalla* $\cdot$, jolle ovat voimassa seuraavat laskulait: Kun $x, y \in M$ ja $a, b \in R$, niin

1) $a(x +_M y) = ax +_M ay$,
2) $(a +_R b)x = ax +_M bx$,
3) $a(bx) = (a \cdot_R b)x$

   ja
4) $1 \cdot x = x$.

   Muodollisesti siis *moduli* on kolmikko $\big((M, +_M), (R, +_R, \cdot_R), \cdot\big)$, jossa

a) $(M, +_M)$ on Abelin ryhmä,
b) $(R, +_R, \cdot_R)$ on yksiköllinen rengas, jossa $0_R \neq 1_R$, ja
c) laskulait 1–4 ovat voimassa.

Rengasta $(R, +_R, \cdot_R)$ kutsutaan tämän modulin *kerroinrenkaaksi*. Joukon M alkioita kutsutaan *vektoreiksi* ja joukon R alkioita *skalaareiksi*.

Huomautus.

1) Skalaarikerronta ei ole varsinaisesti minkään perusjoukon laskutoimitus, sillä se on kuvaus $R \times M \to M$, missä yleensä $R \neq M$. Sitä on kuitenkin käytännöllistä myös nimittää laskutoimitukseksi, kuten modulin kolmea muuta (aitoa) laskutoimitusta.
2) Käytännössä alaindeksejä ei käytetä, jolloin vektorien ja skalaarien yhteenlaskuja merkitään (hieman hämäävästi) molempia symbolilla $+$, ja skalaarikerrontaa ja skalaarien kertolaskua molempia symbolilla $\cdot$. Varsinkin skalaarikerronnan symboli jätetään useimmiten kokonaan pois merkinnästä.

2.2. Määritelmä. Jos modulin V kerroinrengas $(K, +, \cdot)$ on kunta, niin K-modulia V kutsutaan K-vektoriavaruudeksi.

3. Viritys ja vapaus

3.1. Merkintä. Kun $(M, +)$ on Abelin ryhmä ja $S \subseteq M$ äärellinen, niin joukon S alkioiden summaa voidaan merkitä

$$\sum_{x \in S} x = \sum_{i=0}^{n-1} s_i,$$

missä joukon S alkiot on lueteltu toistotta: $S = \{s_0, \ldots, s_{n-1}\}$. Koska M:n yhteenlasku on vaihdannainen, lopputulos ei riipu siitä, missä järjestyksessä alkiot on lueteltu. Huomattakoon, että erikoistapauksessa $S = \emptyset$ määritellään

$$\sum_{x \in \emptyset} x = \bar{0}_M,$$

mikä edellyttää neutraalialkion olemassaoloa. Vastaavasti jos $(x_i)_{i \in I}$ on äärellinen jono M:n alkioita, summa

$$\sum_{i \in I} x_i$$

on yksikäsitteisesti määritelty riippumatta siitä, onko indeksijoukolla I luonnollista järjestystä.

Oletetaan nyt, että M on jopa R-moduli, $S \subseteq M$ mahdollisesti ääretön ja $(\lambda_s)_{s \in S}$ jono R:n alkioita. Summa

$$\sum_{s \in S} \lambda_s \cdot s$$

ei ole yleisesti ajatellen mielekäs, mutta jos kerroinjonon *kantaja*

$$S_0 = \operatorname{supt}((\lambda_s)_{s \in S}) = \{\, s \in S \mid \lambda_s \neq 0 \,\}$$

on äärellinen, niin voidaan määritellä

$$x = \sum_{s \in S} \lambda_s \cdot s = \sum_{s \in S_0} \lambda_s \cdot s.$$

Tällaista vektoria x kutsutaan *lineaarikombinaatioksi* S:n vektoreista. Vastaavalla tavalla suhtaudutaan muotoa

$$\sum_{i \in I} \lambda_i x_i$$

oleviin merkintöihin, kun I on ääretön.

3.2. Määritelmä. Joukko S *virittää* R-moduli M, jos jokainen $x \in M$ voidaan kirjoittaa lineaarikombinaationa $x = \sum_{s \in S} \lambda_s \cdot s$ joukon S vektoreista (missä siis $\lambda_s \in R$, kun

$s \in S$, ja supt$((\lambda_s)_{s\in S})$ on äärellinen). Joukkoa S kutsutaan tällöin M:n *virittäjistöksi tai virittäjäjoukoksi*.

Virittäminen voidaan määritellä myös jonoille: Jono $(s_i)_{i\in I}$ modulin M alkioita *virittää* M:n, jos vastaava joukko $\{ s_i \mid i \in I \}$ virittää M:n.

3.3. Määritelmä. R-moduli L on R-modulin M *alimoduli*, jos $L \subseteq M$ ja L perii laskutoimituksensa M:stä.

Sama muodollisemmin: $\big((L,+_L),(R,+_R,\cdot_R),*_L\big)$ on modulin $\big((M,+_M),(R,+_R,\cdot_R),*_M\big)$ *alimoduli*, jos

1) $L \subseteq M$ ja $\big((L,+_L),(R,+_R,\cdot_R),*_L\big)$ on itsekin moduli ja
2) $+_L = +_M\restriction(L\times L)$ ja $*_L = *_M\restriction(R\times L)$.

3.4. Lause. *(Alimodulikriteerit) Olkoon M R-moduli ja $L \subseteq M$. Tällöin L voidaan varustaa M:n alimodulirakenteella, jos ja vain jos seuraavat ehdot ovat voimassa:*

1) $x + y \in L$, kun $x, y \in L$,
2) $ax \in L$, kun $a \in R$ ja $x \in L$
ja
3) $\bar{0} \in L$. □

3.5. Määritelmä. Olkoon M moduli ja $A \subseteq M$. Joukosta A muodostettujen lineaarikombinaatioiden joukkoa merkitään $^{(}A$):lla.

3.6. Lause. *Olkoon M R-moduli ja $A \subseteq M$. Tällöin* sp(A) *on modulin S alimoduli. Itse asiassa* sp(A) *on suppein (eli sisältyvyyden suhteen pienin) M:n alimoduli, joka sisältää A:n, ts.*

$$\mathrm{sp}(A) = \bigcap\{ L \mid L \text{ on } M\text{:n alimoduli}, A \subseteq L \}.$$

□

3.7. Määritelmä. Modulin M osajoukko I on *vapaa*, jos jokaiselle I:n vektoreista muodostetulle lineaarikombinaatiolle pätee seuraava ehto: jos $\sum_{x\in I} \lambda_x \cdot x = \bar{0}$, niin jokaisella $x \in I$ pätee $\lambda_x = 0$.

Vastaavasti jono $(x_i)_{i\in J}$ M:n vektoreita on *vapaa*, jos se on toistoton ja $\{ x_i \mid i \in J \}$ on vapaa. Vektoriavaruuden osajoukkoa tai jonoa nimitetään *sidotuksi*, jos se ei ole vapaa.

4. Kannat

Tässä luvussa esitettävien lauseiden voi hyvällä syyllä väittää olevan lineaarialgebran perustavanlaatuisimpia tuloksia. Joukko-opillisen pohjustuksen jälkeen esitetään kantalause, jonka mukaan jokaisella vektoriavaruudella on kanta. Tähän tulokseen perustuu keskeisiltä osiltaan sekä lineaarialgebran teorian jatkokehitelly että sovelluksissa mallien laskennallinen käsittely. Kantalauseesta nimittäin seuraa, että jokainen vektori voidaan koordinatisoida kannan suhteen, ts. vektoria koskeva informaatio on kantaa vastaavassa kerroinjonossa. Tästä seuraa mm., että vektoriavaruuksien väliset lineaarikuvaukset voidaan esittää matriisien avulla, mikä on tunnetusti tärkeää sovelluksille.

Kantojen käyttöä yksinkertaistaa myös luvun toinen keskeinen tulos, joka kertoo, että vektoriavaruuden kannat ovat yhtämahtavia. Tästä tuloksesta seuraa, että vektoriavaruudelle voidaan määritellä dimensio. Myöhemmin osoitetaan, että vektoriavaruuden tunnistamiseksi isomorfiaa vaille on riittävää tietää kerroinkunta ja dimensio.

4.1. Määritelmä. Joukko $E \subseteq V$ on vektoriavaruuden V *kanta*, jos se on vapaa V:ssä ja virittää V:n. Vastaavasti jonon $(e_i)_{i\in I}$ sanotaan olevan V:n *kanta*, jos se on vapaa V:ssä ja virittää V:n.

4.2. Lause. *(Virityksen perusominaisuudet) Olkoon M R-moduli ja $A, B \subseteq M$. Tällöin:*

1) $A \subseteq \mathrm{sp}(A)$.

2) Jos $A \subseteq B$, *niin* $\mathrm{sp}(A) \subseteq \mathrm{sp}(B)$.

3) $\mathrm{sp}(\mathrm{sp}(A)) = \mathrm{sp}(A)$.

4) (Äärellisluonteisuus) Jokaista $x \in \mathrm{sp}(A)$ *vastaa sellainen äärellinen* $A_0 \subseteq A$, *että* $x \in \mathrm{sp}(A_0)$.

Todistus.

1) Kun $u, v \in M$, merkitään $\delta_{u,v} = \begin{cases} 1, & \text{kun } u = v \\ 0, & \text{kun } u \neq v \end{cases}$, missä $\delta_{u,v} \in R$. Tällöin jokaisella $a \in A$ on voimassa

$$a = \sum_{v\in A} \delta_{a,v} v,$$

joten $a \in \mathrm{sp}(A)$. Siis $A \subseteq \mathrm{sp}(A)$.

2) Jos $x \in \mathrm{sp}(A)$, niin

$$x = \sum_{v\in A} \lambda_v v$$

jollakin äärellisluonteisella kerroinjonolla $(\lambda_v)_{v\in A}$. Kun jonoa täydennetään asettamalla vektorien $v \in B \setminus A$ kohdalla $\lambda_v = 0$, saadaan tietysti

$$x = \sum_{v\in B} \lambda_v v \in \mathrm{sp}(B).$$

3 Koska kohdan 1 perusteella $A \subseteq \mathrm{sp}(A)$, niin kohtaa 2 soveltamalla saadaan $\mathrm{sp}(A) \subseteq \mathrm{sp}(\mathrm{sp}(A))$. Toisaalta jos $x \in \mathrm{sp}(\mathrm{sp}(A))$, niin on olemassa äärellisluonteinen kerroinjono $(\lambda_u)_{u\in\mathrm{sp}(A)}$, jolle

$$x = \sum_{u\in\mathrm{sp}(A)} \lambda_u u,$$

ja jokaisella $u \in \mathrm{sp}(A)$ edelleen on olemassa äärellisluonteinen kerroinjono $(\mu_{u,v})_{v\in A}$, jolle

$$u = \sum_{v\in A} \mu_{u,v} v.$$

Kaikkiaan saadaan

$$x = \sum_{u \in \mathrm{sp}(A)} \lambda_u u = \sum_{u \in \mathrm{sp}(A)} \left(\lambda_u \sum_{v \in A} \mu_{u,v} v \right).$$
$$= \sum_{v \in A} \left(\sum_{u \in \mathrm{sp}(A)} \lambda_u \mu_{u,v} \right) v = \sum_{v \in A} \nu_v v,$$

missä on merkitty $\nu_v = \sum_{u \in \mathrm{sp}(A)} \lambda_u \mu_{u,v}$, kun $v \in A$. Kerroinjono $(\nu_v)_{v \in A}$ on tietenkin myös äärellisluonteinen, koska on olemassa vain äärellisen monta paria $(u, v) \in \mathrm{sp}(A) \times A$, jolle $\lambda_u \mu_{u,v} \neq 0$. Siis $x \in \mathrm{sp}(A)$, mikä osoittaa, että $\mathrm{sp}(\mathrm{sp}(A)) \subseteq \mathrm{sp}(A)$. Siten $\mathrm{sp}(\mathrm{sp}(A)) = \mathrm{sp}(A)$.

4) Jokaista $x \in \mathrm{sp}(A)$ kohti on olemassa äärellisluonteinen kerroinjono $(\lambda_v)_{v \in A}$, jolle

$$x = \sum_{v \in A} \lambda_v v = \sum_{v \in A_0} \lambda_v v,$$

missä $A_0 = \mathrm{supt}\big((\lambda_v)_{v \in A}\big)$ on äärellinen. Siis $x \in \mathrm{sp}(A_0)$. □

4.3. Lause. *(Vektoriavaruuksien vaihto-ominaisuus) Olkoon V K-vektoriavaruus, $A \subseteq V$ ja $x, y \in V$. Tällöin jos $x \in \mathrm{sp}(A \cup \{y\}) \setminus \mathrm{sp}(A)$, niin $y \in \mathrm{sp}(A \cup \{x\}) \setminus \mathrm{sp}(A)$.*

Todistus. Oletetaan, että $x \in \mathrm{sp}(A \cup \{y\}) \setminus \mathrm{sp}(A)$. Tällöin x voidaan kirjoittaa lineaarikombinaationa

$$x = \sum_{v \in A \cup \{y\}} \lambda_v v,$$

missä kerroinjono on äärellisluonteinen. Jos olisi $\lambda_y = 0$, niin saataisiin $x = \sum_{v \in A} \lambda_v v \in \mathrm{sp}(A)$, mikä on vastoin oletusta. Siis $\lambda \neq 0$, joten yo. yhtälöstä voidaan ratkaista y:

$$x = \sum_{v \in A \cup \{y\}} \lambda_v v = \lambda_y y + \sum_{v \in A} \lambda_v v$$
$$\Rightarrow x - \sum_{v \in A} \lambda_v v = \lambda_y y$$
$$\Rightarrow y = (\lambda_y)^{-1} x - \sum_{v \in A} \frac{\lambda_v}{\lambda_y} v.$$

Siis $y \in \mathrm{sp}(A \cup \{x\})$. Ei voi päteä $y \in \mathrm{sp}(A)$, sillä silloin saataisiin $x \in \mathrm{sp}(A \cup \{y\}) \subseteq \mathrm{sp}(A \cup \mathrm{sp}(A)) = \mathrm{sp}(\mathrm{sp}(A)) = \mathrm{sp}(A)$. □

4.4. Lause. *. Olkoon V K-vektoriavaruus ja $I \subseteq V$. Tällöin:*

a) I on vapaa, jos ja vain jos jokaiselle $x \in I$ pätee $x \notin \mathrm{sp}(I \setminus \{x\})$.

b) Jos I on vapaa ja $u \in V \setminus \mathrm{sp}(I)$, niin $I \cup \{u\}$ on vapaa.

Todistus. a) Oletetaan ensin, että jollakin $x \in I$ pätee $x \in \mathrm{sp}(I \setminus \{x\})$. Tällöin on olemassa äärellisluonteinen kerroinjono $(\lambda_v)_{v \in I \setminus \{x\}}$, jolle

$$x = \sum_{v \in I \setminus \{x\}} \lambda_v v,$$

mistä merkitsemällä $\lambda_x = -1$ seuraa

$$\bar{0} = -x + \sum_{v \in I \setminus \{x\}} \lambda_v v = \lambda x + \sum_{v \in I \setminus \{x\}} \lambda_v v = \sum_{v \in I} \lambda_v v.$$

Koska $\lambda_x = -1 \neq 0$, tämä merkitsee, että I on sidottu.

Oletetaan sitten, että kaikilla $x \in I$ on voimassa $x \notin \mathrm{sp}(I \setminus \{x\})$. Testataan joukon I vapautta äärellisluonteisella kerroinjonolla $(\lambda_v)_{v \in I}$. Oletetaan siis, että $\sum_{v \in I} \lambda_v v = \bar{0}$. Jos jollakin $x \in I$ pätisi λ_x, voitaisiin yo. yhtälöstä ratkaista

$$\bar{0} = \sum_{v \in I} \lambda_v v = \lambda_x x + \sum_{v \in I \setminus \{x\}} \lambda_v v \Rightarrow x = -(I a_x)^{-1} \sum_{v \in I \setminus \{x\}} \in \mathrm{sp}(I \setminus \{x\}),$$

mikä on vastoin oletusta. Siis kaikki kertoimet λ_v, $v \in I$, ovat nollia, joten I on vapaa.

b) Oletetaan, että I on vapaa ja $u \notin \mathrm{sp}(I)$. Merkitään $J = I \cup \{u\}$ ja todistetaan joukon J vapaus kohdan a avulla. Olkoon $x \in J$. Jos $x = u$, niin $J \setminus \{u\} = I$, joten $u \notin \mathrm{sp}(I) = \mathrm{sp}(J \setminus \{u\})$. Oletaan siis, että $x \neq u$. Jos pätisi $x \in \mathrm{sp}(J \setminus \{x\})$, niin kohdan a nojalla $x \in \mathrm{sp}(J \setminus \{x\}) \setminus \mathrm{sp}(I \setminus \{x\})$, sillä I on vapaa. Siis

$$x \in \mathrm{sp}((I \setminus \{x\}) \cup \{u\}) \setminus \mathrm{sp}(I \setminus \{x\}),$$

mistä vaihto-ominaisuuden nojalla seuraa

$$u \in \mathrm{sp}((I \setminus \{x\}) \cup \{x\}) = \mathrm{sp}(I),$$

mikä olisi vastoin oletusta. Siis J on vapaa. □

4.5. Lause. *Olkoot E ja E' vektoriavaruuden V kantoja. Tällöin jokaista $e' \in E' \setminus E$ kohti on olemassa $e \in E \setminus E'$, jolle $(E \setminus \{e\}) \cup \{e'\}$ on V:n kanta.*

Todistus. Olkoon $e' \in E' \setminus E$. Koska E on kanta, niin se on virittäjistö, joten $e' \in V = \mathrm{sp}(E)$. Siis e' on lineaarikombinaatio E:n vektoreista:

$$e' = \sum_{f \in E} \lambda_f f,$$

missä kerroinjono on äärellisluonteinen. Jollakin $e \in E \setminus E'$ pätee $\lambda_e \neq 0$, muutenhan saataisiin $e' = \sum_{f \in E \cap E'} \lambda_f f$, ja koska $e' \neq E$, tästä seuraisi $e' \in \mathrm{sp}(E \cap E') \subseteq \mathrm{sp}(E' \setminus \{e'\})$, mikä on vastoin sitä oletusta, että E' on kantana vapaa. Huomattakoon, että $e' \notin \mathrm{sp}(E \setminus \{e\})$, muutenhan e' voitaisiin esittää joukon $E \setminus \{e\}$ lineaarikombinaationa, mikä olisi

vastoin sitä, että kunkin vektorin voi esittää yksikäsitteisellä tavalla kannan (E:n) lineaarikombinaationa.

Tarkastellaan nyt joukkoa $\widetilde{E} = (E \setminus \{e\}) \cup \{e'\}$. Huomataan, että koska

$$e' \in \mathrm{sp}(E) \setminus \mathrm{sp}(E \setminus \{e\}) = \mathrm{sp}((E \setminus \{e\}) \cap \{e\}) \setminus \mathrm{sp}(E \setminus \{e\}),$$

niin vaihto-ominaisuuden vuoksi

$$e \in \mathrm{sp}((E \setminus \{e\}) \cap \{e'\}) = \mathrm{sp}(\widetilde{E}).$$

Siis $E \setminus \{e\} \subseteq \widetilde{E} \subseteq \mathrm{sp}(\widetilde{E})$ ja $e \in \mathrm{sp}(\widetilde{E})$, joten

$$E \subseteq \mathrm{sp}(\widetilde{E}) \;\Rightarrow\; V = \mathrm{sp}(E) \subseteq \mathrm{sp}(\mathrm{sp}(\widetilde{E})) = \mathrm{sp}(\widetilde{E}),$$

joten $\widetilde{E}$ on virittäjistö. Lauseen 4.4 kohdasta b seuraa, ett' $\widetilde{E}$ on vapaa, sillä $E \setminus \{e\}$ on vapaa ja $e' \notin E \setminus \{e\}$. Siis $\widetilde{E}$ on vapaa virittäjistö eli kanta. □

4.6. Esimerkki. $\mathbb{Z}$-modulissa $\mathbb{Z}$ ei päde vaihto-ominaisuus.

4.7. Esimerkki. $\mathbb{Z}$-modulissa $\mathbb{Z}$ joukko $\{2, 3\}$ on sidottu, vaikka $2 \notin \mathrm{sp}(\{3\})$ ja $3 \notin \mathrm{sp}(\{2\})$.

Joukko-opillisia työkaluja

Kantalauseen todistamisessa äärellisulotteisille vektoriavaruuksille selvitään varsin yksinkertaisella kombinatoriikalla, mutta yleisessä tapauksessa kantojen olemassaolon todistamiseen tarvitaan valinta-aksioomaa. Kurssilla Joukko-oppi on todistettu, että valinta-aksioomasta seuraa Zornin lemma. Zornin lemmasta seuraa edellen Tukeyn lemma, joka tässä esitellään ja todistetaan juuri Zornin lemman avulla. Lisäksi kerrataan tarvittavat käsitteet.

4.8. Määritelmä. Rakenne $(P, \leq)$ on *osittaisesti järjestetty joukko*, jos $\leq$ on joukon P relaatio, joka on refleksiivinen, transitiivinen ja antisymmetrinen. Osittaisesti järjestetty joukko $(L, \leq)$ on *lineaarijärjestetty joukko*, jos $\leq$ on lisäksi vertailullinen.

Osittaisesti järjestetyn joukon $(P, \leq)$ osajoukkoa $C \subseteq P$ kutsutaan *ketjuksi*, jos alijärjestys $(C, \leq \cap (C \times C))$ on lineaarijärjestetty joukko. Alkio $a \in P$ on *minimaalinen*, jos kaikille $x \in P$ pätee: jos $x \leq a$, niin $x = a$. Vastaavasti a on *maksimaalinen*, jos kaikille $x \in P$ pätee: jos $x \geq a$, niin $x = a$.

Edellistä määritelmää sovelletaan seuraavanlaisessa tilanteessa:

4.9. Esimerkki. Olkoon $\mathcal{A}$ perhe joukkoja. Tällöin $\mathcal{A}$ varustettuna sisältyvyydellä eli rakenne $(\mathcal{A}, \subseteq)$ on osittaisesti järjestetty joukko, nimittäin seuraavat faktat pätevät kaikilla $A, B, C \in \mathcal{A}$:

refleksiivisyys:	$A \subseteq A$,
transitiivisuus:	$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$,
antisymmetrisyys:	$A \subseteq B \wedge B \subseteq A \Rightarrow A = B$.

Siihen, että $\mathcal{A}$ ei olisi lineaarijärjestetty joukko, riittää, että jotkin joukot $A, B \in \mathcal{A}$ eivät ole vertailullisia, mikä toteutuu täsmälleen silloin, kun $A \setminus B \neq \emptyset$ ja $B \setminus A \neq \emptyset$. Esimerkiksi $\mathcal{P}(\mathbb{N})$ ei ole lineaarijärjestetty sisältyvyydellä varustettuna, sillä $\mathcal{P}(\mathbb{N})$:n joukot $\{2\}$ ja $\{3\}$ eivät ole vertailullisia. Sen sijaan $\mathcal{C} = \{\{2\}, \{2,3\}, \{2,3,5\}\}$ on $\mathcal{P}(\mathbb{N})$:n ketju.

4.10. Zornin lemma. *Olkoon $\mathcal{A}$ perhe joukkoja, joka on ketjujen yhdisteiden suhteen suljettu, ts. jos $\mathcal{K} \subseteq \mathcal{A}$ on ketju, niin $\bigcup \mathcal{K} \in \mathcal{A}$. Tällöin perheessä $\mathcal{C}$ on sisältyvyyden suhteen maksimaalinen alkio.* □

4.11. Määritelmä. Merkitään jokaisella joukolla A

$$[A]^{<\aleph_0} = \{\, B \subseteq A \mid B \text{ on äärellinen} \,\}.$$

Perhe $\mathcal{A} \subseteq \mathcal{P}(X)$ joukkoja on *äärellisluonteinen*, jos jokaisella $A \subseteq X$ pätee, että $A \in \mathcal{A}$ täsmälleen silloin, kun $[A]^{<\aleph_0} \subseteq \mathcal{A}$, ts. A kuuluu perheeseen $\mathcal{A}$, jos ja vain jos kaikki sen äärelliset osajoukot kuuluvat.

4.12. Tukeyn lemma. *Olkoon $\mathcal{A}$ äärellisluonteinen perhe joukkoja. Tällöin perhessä $\mathcal{A}$ on sisältyvyyden suhteen maksimaalinen alkio.*

Todistus. Zornin lemman nojalla riittää osoittaa, että $\mathcal{A}$ on ketjujen yhdisteiden suhteen suljettu. Olkoon siis $\mathcal{K}$ perheen $\mathcal{A}$ ketju. Merkitään $C = \bigcup \mathcal{K}$; väitetään, että $C \in \mathcal{A}$. Olkoon $D \subseteq C$ äärellinen, ts. $D = \{d_0, \ldots, d_{n-1}\}$, missä $n = |D| \in \mathbb{N}$. Koska $D \subseteq C = \bigcup \mathcal{K}$, jokaisella d_i on olemassa $C_i \in \mathcal{K}$, jolle $d_i \in C_i$, kun $i \in \{0, \ldots, n-1\}$. Koska joukkoja D_i on vain äärellisen monta ja ne ovat ketjun alkioina vertailullisia, niin joukossa on suurin, olkoon se C_s. Siis $d_i \in C_i \subseteq C_s$, kun $i \in \{0, \ldots, n-1\}$, mistä seuraa $D = \{d_0, \ldots, d_{n-1}\} \subseteq C_s$. Koska $C_s \in \mathcal{K} \subseteq \mathcal{A}$ ja $\mathcal{A}$ on äärellisluonteinen, tästä seuraa $D \in \mathcal{A}$. Koska $D \in [C]^{<\aleph_0}$ oli mielivaltainen, niin saadaan $[C]^{<\aleph_0} \subseteq \mathcal{A}$. Tästä seuraa jälleen äärellisluonteisuutta soveltamalla $C \in \mathcal{A}$.

Siis $\mathcal{A}$ on ketjujen yhdisteiden suhteen suljettu, joten Zornin lemmasta seuraa, että perheessä $\mathcal{A}$ on maksimaalinen alkio. □

Kantalause ja dimensio

4.13. Lause. *(Kantalause) Jokaisella vektoriavaruudella on kanta. Itse asiassa: Olkoon V vektoriavaruus, I vapaa V:ssä ja S V:n virittäjistö. Oletetaan, että $I \subseteq S$. Tällöin V:llä on kanta E, jolle $I \subseteq E \subseteq S$.*

Todistus. Koska jokaisessa vektoriavaruudessa V tyhjä joukko $\emptyset$ on vapaa ja V virittäjistö sekä triviaalisti $\emptyset \subseteq V$, niin jälkimmäisestä väitteestä seuraa, että on olemassa V:n kanta E, jolle $\emptyset \subseteq E \subseteq V$. Keskitytään siis vahvemman väitteen todistamiseen.

Olkoon I vektoriavaruuden V vapaa osajoukko ja S sen virittäjistö, joille $I \subseteq S$. Tarkastellaan perhettä

$$\mathcal{J} = \{\, J \subseteq V \mid I \subseteq J \subseteq S,\ J \text{ on vapaa} \,\}.$$

Tukeyn lemman soveltamiseksi poistetaan perheen $\mathcal{J}$ joukoista vakio-osa I ja merkitään

$$\mathcal{J}_+ = \{\, D \subseteq V \setminus I \mid I \cup D \in \mathcal{J} \,\}.$$

Perhe $\mathcal{J}_+$ on äärellisluonteinen: Jos nimittäin $D \in \mathcal{J}_+$, niin $I \cup D \in \mathcal{J}$, joten $I \cup D$ on vapaa ja $I \subseteq I \cup D \subseteq S$. Siten jokaisella $A \in [D]^{<\aleph_0}$ pätee selvästi, että $I \subseteq A$ on vapaa ja $I \subseteq I \cup A \subseteq S$, joten $I \cup A \in \mathcal{J}$ ja $A \in \mathcal{J}_+$. Oletetaan sitten, että $D \notin \mathcal{J}_+$, vaikka $D \subseteq V$. Jos $D \cap I \neq \emptyset$, niin on olemassa $a \in D \cap I$, jolloin $\{a\} \in [D]^{<\aleph_0} \setminus \mathcal{J}_+$. Oletetaan siis, että $D \subseteq V \setminus I$. Jos $I \cup D \not\subseteq S$, niin samaten on olemassa yksittäinen piste a, joka sen todentaa, ts. $a \in D \setminus S$, jolloin taas $\{a\} \in [D]^{<\aleph_0} \setminus \mathcal{J}_+$. Jäljelle jää se mahdollisuus, että $I \cup D$ on sidottu. Vapauden äärellisluonteisuus merkitsee, että on olemassa äärellinen $A \subseteq D$, jolle $I \cup A$ on sidottu, jolloin $A \in [D]^{<\aleph_0} \setminus \mathcal{J}_+$. Perhe $\mathcal{J}_+$ on siten todettu äärellisluonteiseksi.

Koska $\mathcal{J}_+$ on äärellisluonteinen, Tukeyn lemman nojalla siinä on maksimaalinen alkio. Valitaan tällainen $D \in \mathcal{J}_+$ ja merkitään $E = I \cup D$. Koska $D \in \mathcal{J}_+$, niin $E \in \mathcal{J}$, joten $I \subseteq E \subseteq S$ ja E on vapaa. Lisäksi on helppo havaita, että E on perheen $\mathcal{J}$ maksimaalinen alkio. Kantalauseen todistuksesta puuttuu siis vain sen osoittaminen, että E on virittäjistö. Toisaalta S on virittäjistö, joten jos näin ei olisi, niin olisi olemassa $s \in S$, jolle $s \notin \mathrm{sp}(E)$. Tällöin lauseen 4.4 mukaan $E \cup \{s\}$ olisi vapaa, sillä E on vapaa ja $s \notin \mathrm{sp}(E)$. Koska $E \cup \{s\}$ olisi vapaa ja $I \subseteq E \cup \{s\} \subseteq S$, saataisiin $E \cup \{s\} \in \mathcal{J}$, mikä on vastoin joukon E maksimaalisuutta. □

4.14. Seuraus. *Vektoriavaruuden V osajoukolle E seuraavat ehdot ovat yhtäpitäviä.*
a) E on kanta.
b) E on maksimaalinen V:n vapaa joukko.
c) E on minimaalinen V:n virittäjistö.

Todistus. Oletetaan ensin, että E on kanta. Suoraan määritelmän nojalla tällöin E on vapaa virittäjistö. Toisaalta minimaalisuuden, toisaalta maksimaalisuuden vuoksi tarkastellaan V:n osajoukkoja A ja B, joille $A \subsetneq E \subsetneq B$. Valitaan $a \in E \setminus A$ ja $b \in B \setminus E$. Koska E on vapaa, niin lauseen 4.4 kohdan a mukaan $a \notin \mathrm{sp}(E \setminus \{a\})$, mistä seuraa myöskin $a \notin \mathrm{sp}(A)$. Siis A ei ole virittäjistö, mikä osoittaa, että E on minimaalinen virittäjistö. Toisaalta koska E on virittäjistö, $b \in \mathrm{sp}(E) \subseteq \mathrm{sp}(B \setminus \{b\})$, sillä $E \subseteq B \setminus \{b\}$. Jälleen lause 4.4 osoittaa, että B ei ole vapaa. Siis E on maksimaalinen vapaa V:n osajoukko. Siis kohdasta a seuraavat kohdat b ja c.

Oletetaan sitten, että E on maksimaalinen V:n vapaa joukko. Koska E on vapaa joukko, V on virittäjistö ja $E \subseteq V$, on olemassa kanta E', jolle $E \subseteq E' \subseteq V$. Koska E' on vapaa, $E \subseteq E'$ ja E on maksimaalinen vapaa joukko, niin $E = E'$. Siis E on kanta.

Kohdasta c seuraa aivan vastaavalla tavalla kohta a. Oletetaan nimittäin, että E on minimaalinen V:n virittäjistö. Koska $\emptyset$ on vapaa joukko, E on virittäjistö ja $\emptyset \subseteq E$, on olemassa kanta E'', jolle $\emptyset \subseteq E'' \subseteq E$. Koska E on minimaalinen virittäjistö ja kannat ovat virittäjistöjä, on oltava $E = E''$. Siis E on kanta. □

4.15. Lemma. *Olkoot E ja S K-vektoriavaruuden V virittäjistöjä. Tällöin jos S on ääretön ja $|S| > |E|$, niin S on sidottu.*

Todistus. Koska S on virittäjistö, niin jokainen $e \in E$ voidaan esittää lineaarikombinaationa S:n vektoreista. Koska nämä lineaarikombinaatiot ovat äärellisiä, on olemassa $S(e)$

ja kertoimet $\lambda_{e,s}$, missä $s \in S(e)$, joille

$$e = \sum_{s \in S(e)} \lambda_{s,e} s \in \mathrm{sp}(S(E)).$$

Merkitään $S_0 = \bigcup_{e \in E} S(e) \subseteq S$. Tarkastellaan kahta eri tapausta.

1) Oletetaan ensin, että E on äärellinen. Tällöin S_0 on äärellinen äärellisenä yhdisteenä äärellisistä joukoista, joten $S_0 \subsetneq S$.
2) Oletetaan sitten, että E on ääretön. Tällöin

$$|S_0| = |\bigcup_{e \in E} S(e)| \leq \sum_{e \in E} |S(e)| \leq |E| \cdot |\mathbb{N}| = \max|E|, |N| = |E| < |S|,$$

missä on käytetty hyväksi peruskardinaaliaritmetiikkaa, mm. sitä, että äärettömien kardinaalien summa ja tulo palautuvat maksimiin. Koska $|S_0| < |S|$, saadaan nytkin $S_0 \subsetneq S$.

Siis joka tapauksessa $S_0 \subsetneq S$. Toisaalta jokaisella $e \in E$ pätee $e \in \mathrm{sp}(S(e)) \subseteq \mathrm{sp}(S_0)$, joten $E \subseteq \mathrm{sp}(S_0)$. Koska E on virittäjistö, seuraa $V = \mathrm{sp}(E) \subseteq \mathrm{sp}(\mathrm{sp}(S_0)) = \mathrm{sp}(S_0)$, joten myös S_0 virittää V:n. Koska $S_0 \subsetneq S$, on olemassa $s \in S \setminus S_0$. Tälle vektorille pätee $s \in \mathrm{sp}(S \setminus \{s\})$, sillä $S_0 \subseteq S \setminus \{s\}$ ja jo S_0 on virittäjistö. Siis S on sidottu. □

4.16. Lause. *Mielivaltaisen vektoriavaruuden V kaikki kannat ovat keskenään yhtämahtavia.*

Todistus. Käsitellään erikseen kaksi tapausta sen mukaan, onko V:llä äärettömiä kantoja.

1) Ainakin jokin vektoriavaruuden V kannoista on ääretön, olkoon E tällainen. Olkoon E' myös V:n kanta. Koska E ja E' ovat kantoina molemmat virittäjistöjä ja E on ääretön mutta vapaa, niin edellisestä lemmasta seuraa, että $|E| \leq |E'|$. Siis myös E' on ääretön, ja vaihtamalla kantojen roolit edellisessä päättelyssä saadaan, että $|E'| \leq |E|$. Schröderin ja Bernsteinin lauseen avulla siis päätellään, että $|E| = |E'|$.

2) Oletetaan, että kaikki V:n kannat ovat äärellisiä. Olkoot E ja E' V:n kantoja. Todistetaan induktiolla symmetrisen erotuksen

$$E \triangle E' = (E \setminus E') \cup (E' \setminus E)$$

koon $n \in \mathbb{N}$ suhteen, että jos $|E \triangle E'| = n$, niin $|E| = |E'|$.

1° Jos $n = 0$ eli $|E \triangle E'| = 0$, niin $E \triangle E = \emptyset$ eli $E = E'$, mistä väite $|E| = |E'|$ seuraa triviaalisti.
2° Oletetaan, että induktioväite pätee, kun kantojen symmetrisen erotuksen koko on pienempi kuin $n > 0$. Oletetaan, että $|E \triangle E'| = n$. Koska $E \triangle E' \neq \emptyset$, voidaan olettaa, että on olemassa $e' \in E' \setminus E$. Kantojen vaihto-ominaisuuden mukaan tätä vektoria vastaa $e \in E \setminus E'$, jolle $\widetilde{E} = (E \setminus \{e\}) \cup \{e'\}$ on V:n kanta. Koska

$$|E' \triangle \widetilde{E}| = |(E \triangle E') \setminus \{e, e'\}| = n - 2 < n,$$

niin induktio-oletuksen mukaan $|E'| = |\widetilde{E}|$. Selvästi $|\widetilde{E}| = |E|$, joten $|E'| = |\widetilde{E}| = |E|$.

Siis molemmissa tapauksissa todetaan, että kaikki kannat ovat yhtämahtavia. □

Edellisten lauseiden nojalla millä tahansa vektoriavaruudella on kanta ja sen koko on yksikäsitteinen, joten seuraava käsite on hyvinmääritelty.

4.17. Määritelmä. Vektoriavaruuden V *dimensio* on $\dim(V) = |E|$, missä E on V:n (mikä tahansa) kanta. V on äärellisulotteinen, jos $\dim(V) \in \mathbb{N}$.

4.18. Lause. *Olkoon V vektoriavaruus.*

a) Jos S virittää V:n, niin $|S| \geq \dim(V)$.

b) Jos I on vapaa V:ssä, niin $|I| \leq \dim(V)$.

Todistus. Sovelletaan molemmissa kohdissa kanta-lausetta.

a) Oletetaan, että S virittää V:n. Tietenkin $\emptyset$ on vapaa ja $\emptyset \subseteq S$, joten kanta-lauseen 4.13 nojalla on olemassa V:n kanta E, jolle $\emptyset \subseteq E \subseteq S$. Sisältyvyyksistä ja dimension määritelmästä seuraa siis

$$|S| \geq |E| = \dim(V).$$

b) Vastaavasti: Jos I on vapaa, niin $I \subseteq V$, missä V on triviaalisti virittäjistö. Kanta-lauseen nojalla V:llä on kanta E', jolle $I \subseteq E'$ ja siis

$$|I| \leq |E'| = \dim(V). \quad \square$$