Luku 2

Äärellisulotteiset modulit ja niiden väliset lineaarikuvaukset

2.1 Perusteiden kertausta

Alamme tutkia lineaarialgebraa, eli modulien teoriaa, tarkemmin. Aloitetaan kertaamalla niihin liittyviä peruskäsitteitä .

Olkoon R rengas. Kolmikko $(M, +, \cdot)$ on R-moduli, jos $+\colon M \times M \to M$ (modulin yhteenlasku), $\cdot\colon R \times M \to M$ (skalaarikertolasku) ovat laskutoimituksia, joille pätee

i) $(a + b) + c = a + (b + c)$ kaikilla $a, b, c \in M$,

ii) $a + b = b + a$ kaikilla $a, b \in M$,

iii) on olemassa alkio $0 \in M$, jolle pätee

$$0 + a = a = a + 0 \tag{2.1}$$

kaikilla $a \in M$,

iv) jokaisella $a \in M$ on olemassa vasta-alkio $-a \in M$, jolle pätee

$$a + (-a) = (-a) + a = 0, \tag{2.2}$$

v) $r(r'a) = (rr')a$ kaikilla $r, r' \in R, a \in M$,

vi) $(r + r')a = ra + r'a$ kaikilla $r, r' \in R, a \in M$,

vii) $r(a + a') = ra + ra'$ kaikilla $r \in R, a, a' \in M$.

Jos R on ykkösellinen, oletamme lisäksi, että

viii) $1a = a$ kaikilla $a \in M$.

Jos $R = K$ on kunta, K-moduleja sanotaan K-vektoriavaruuksiksi.
Rengasta R sanotaan R-modulin M *kerroinrenkaaksi*.

Alkiota $0 \in M$, jolla on ominaisuus (2.1), sanotaan M:n nolla-alkioksi. Ehto (2.1) määrää sen yksikäsitteisesti. Muista, että myös renkaalla R on nolla-alkio, joka merkitään samalla symbolilla 0. Asiayhteydestä pitäisi yleensä olla selvää, kummasta milloinkin on kyse.
Ehdon (2.2) määrittelemä alkion a vasta-alkio $(-a)$ on myös yksikäsitteinen. Oletamme tunnetuksi, että R-modulissa pätevät monet tutut laskusäännöt, esimerkiksi

(2.3) $$0a = 0 \text{ kaikilla } a \in M \text{ ja}$$

(2.4) $$(-r)a = -(ra) \text{ kaikilla } a \in M, r \in R.$$

Näiden kaavojen tarkka perustelu jätetään lukijalle harjoitustehtäväksi.

Jos $R = K$ on kunta eli tarkastellaan K-vektoriavaruutta V, on voimassa seuraavat *supistussäännöt*. Olkoot $a, b \in K, v, w \in V$. Tällöin
1) jos $av = bv$, niin joko $a = b$ tai $v = 0$,
2) jos $av = aw$, niin joko $a = 0$ tai $v = w$.
Todistetaan ensimmäinen sääntö, toinen jää harjoitustehtäväksi.
Yhtälö $av = bv$ on yhtäpitävä yhtälön $(a - b)v = av - bv = 0$ kanssa. Jos $a \neq b$, niin $a - b \neq 0$. Koska K on kunta, on olemassa käänteisalkio $(a-b)^{-1}$. Kertomalla yhtälön $(a-b)v = 0$ molemmat puolet alkiolla $(a-b)^{-1}$, saadaan

$$v = 1 \cdot v = (a - b)^{-1}(a - b)v = (a - b)^{-1}0 = 0.$$

Olkoon M R-moduli. M:n osajoukkoa M' sanotaan M:n *alimoduliksi*, jos

(1) kaikilla $a, a' \in M'$ pätee $a + a' \in M'$,

(2) kaikilla $r \in R$, $m \in M'$ pätee $rm' \in M'$,

(3) M' on epätyhjä,

Näistä ehdoista seuraa, että alimoduli M' on itse R-moduli, laskutoimituksina M:n laskutoimitusten rajoittumat osajoukkoihin $M' \times M'$ ja $R \times M'$.

Huomaa, että nolla-alkio kuuluu joukkoon M', koska M' on epätyhjä ja jokaisella $a \in M'$ pätee $0a = 0 \in M'$ ehdon (2) nojalla yllä.
Samoin M' on suljettu vasta-alkioiden suhteen, sillä jokaisella $a \in M'$ pätee

$$-a = (-1) \cdot a \in M'$$

taas ehdon (2) nojalla.
Vektoriavaruuden V alimodulia sanotaan *(vektori) aliavaruudeksi*.

Olkoot M, M' R-moduleja. Kuvausta $L\colon M \to M'$ sanotaan R-lineaariseksi, jos

1) $L(x + y) = L(x) + L(y)$ kaikilla $x, y \in M$,

2) $L(rx) = rL(x)$ kaikilla $x \in M, r \in R$.

Jos kerroinrengas R on tiedossa, puhutaan lyhyemmin lineaarisesta kuvauksesta modulien välillä.

Olkoon $L\colon M \to M'$ R-lineaarinen kuvaus. Sen ydin on M:n alimoduli

$$\operatorname{Ker} L = \{m \in M \mid L(m) = 0\}.$$

Sen kuva on M' alimoduli

$$\operatorname{Im} L = \{L(m) \mid m \in M\}.$$

Lineaarinen kuvaus on *isomorfismi*, jos se on bijektio. Jos kahden modulin M ja M' välillä on olemassa lineaarinen isomorfismi, modulit ovat *isomorfiset*. Isomorfiset modulit ovat lineaarialgebran näkökulmasta "kopioita" toisistaan, täysin samanlaisia olioita.

Jos M' on modulin M alimoduli, voimme muodostaa *tekijämodulin* M/M'. Sen alkiot ovat ekvivalenssiluokat

$$\bar{x} = x + M' = \{x + m \mid m \in M'\}$$

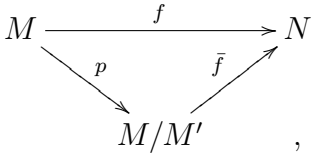
ja laskutoimitukset määritellään kaavoilla

$$\overline{x} + \overline{y} = \overline{x + y},$$

$$r \cdot \overline{x} = \overline{rx}.$$

Tärkeät hajotelma-ja isomorfialauseet ovat voimassa. Nämä ovat erikoistapauksia aikaisemmin todistetuista Lauseista 1.33 ja 1.34. Muotoillaan ne uudestaan modulien tapauksessa.

Lause 2.5. *Olkoon $L\colon M \to N$ R-lineaarinen kuvaus R-modulien välillä. Olkoon $M' \subset M$ alimoduli ja olkoon $p\colon M \to M/M'$ luonnollinen projektio. Tällöin on olemassa R-lineaarinen kuvaus $\bar{L}\colon M/M' \to N$ siten, että $f = \bar{f} \circ p$, eli siten, että seuraava diagrammi kommutoi,*



jos ja vain jos $M' \subset \operatorname{Ker} L$. Jos $\bar{L}$ on olemassa, niin se on yksikäsitteinen ja $\operatorname{Im} \bar{L} = \operatorname{Im} L$. Erityisesti $\bar{L}$ on surjektio jos ja vain jos L on surjektio. Lisäksi $\bar{L}$ on injektio jos ja vain jos $M' = \operatorname{Ker} L$.

Erityisesti L aina indusoi lineaarisen isomorfismin $\bar{L}\colon M/\operatorname{Ker} L \to \operatorname{Im} L$.

Olkoon R ykkösellinen rengas ja M R-moduli. Tällöin R:ssä on määritellyt "renkaan kokonaisluvut " $n = n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ kertaa}}$ (alkion 1 monikerrat Abelin ryhmässä $(R; +)$), joten jokaisella $x \in M$ ja jokaisella $n \in \mathbb{Z}$ on olemassa skalaaritulo $n \cdot x = nx$. Toisaalta $(M, +)$ on Abelin ryhmä, joten siinä on määritelty jokaisen alkion x monikerrat $nx, n \in \mathbb{Z}$. Ottaen huomioon, että molemmat merkitään nyt samalla tavalla, olisi ikävä, jos ne tarkoittaisivat eri asioita. Onneksi näin ei pääse käymään - modulissa lausekkella nx on aina sama merkitys riippumatta sitä, tulkitaanko tämä tulo x:n monikerraksi eli alkioksi $\underbrace{x + x + \ldots + x}_{n \text{ kertaa}}$ vai skalaarituloksi nx, missä $n = n \cdot 1$ on renkaan R ykkösalkion monikerta. Kun $n \geq 0$, tämä nähdään induktiolla n:n suhteen. Tarkemmin $0x = 0$ sekä monikertana (määritelmän mukaan) että skalaaritulona (kts. 2.3). Jos oletetaan, että

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ kertaa}} = (\underbrace{1 + 1 + \ldots + 1}_{n \text{ kertaa}}) \cdot x.$$

Tällöin

$$(n+1)x = \underbrace{x + x + \ldots + x}_{n+1 \text{ kertaa}} = nx + x = n \cdot x + x = n \cdot x + 1 \cdot x = (n+1) \cdot x,$$

missä käytettiin hyväksi induktio-oletus ja modulin ehdot viii) ja vi).

Negatiivisilla $n < 0$ taas saadaan

$$nx = -(-nx) = -(-(n \cdot x) = n \cdot x$$

negatiivisen monikerran määritelmän ja 2.4 nojalla.

Esimerkkejä 2.6. *1) Kokonaislukujen joukko $\mathbb{Z}$ on (ykkösellinen) rengas, joten voimme puhua $\mathbb{Z}$-moduleista. Osoitetaan, että $\mathbb{Z}$-modulien teoria onkin itse asiassa ekvivalentti Abelien ryhmien teorian kanssa. Olkoon M $\mathbb{Z}$-moduli. Tällöin edellisen kappaleen nojalla $n \cdot x$ on jokaisella $n \in \mathbb{Z}, x \in M$ alkion x n's monikerta ryhmässä $(M, +)$,*

$$nx = \underbrace{x + \ldots + x}_{n \text{ kertaa}}.$$

Näin ollen M:n yhteenlaskuryhmän struktuuri määrää $\mathbb{Z}$-modulin struktuurin yksikäsitteisellä tavalla.

Kääntäen olkoon $(M, +)$ mielivaltainen Abelin ryhmä. Yllä läpikäydystä tarkastelusta seuraa, että on olemassa korkeintaan yksi tapa määritellä M:ään $\mathbb{Z}$-skalaarikertolasku, joka tekisi siitä $\mathbb{Z}$-modulin, eli kaavalla

$$nx = \underbrace{x + \ldots + x}_{n \text{ kertaa}} = xtextrm{: } nn\text{:s monikerta}$$

määritelty operaatio.
Koska monikerroille pätee

$$(n + m)x = nx + mx,$$

$$n(mx) = (nm)x,$$

$$1x = x,$$

nähdään, että tämä kaava määritteleekin M:ssä $\mathbb{Z}$-modulin struktuurin. Olkoon $(N, +)$ toinen Abelin ryhmä ja $f\colon M \to N$ Abelin ryhmä. Koska ryhmähomomorfismeille ja monikerroille pätee (todistus induktiolla)

$$f(nx) = nf(x),$$

f on tällöin myös $\mathbb{Z}$-lineaarinen kuvaus.
Jokainen M:n aliryhmä N on suljettu monikertojen suhteen, joten se on myös $\mathbb{Z}$-alimoduli.
Olemme todistaneet, että $\mathbb{Z}$-modulit ja Abelin ryhmät vastaavat toisiaan luonnollisella tavalla. Tämä on hyödyllistä tietoa - voimme käyttää lineaarialgebraa tutkiessamme Abelin ryhmiä.

2) Olkoon $n \geq 1$ ja tarkastelemme kokonaislukujen modulo m renkaan $\mathbb{Z}_n$. Minkälaisessa Abelin ryhmässä $(M, +)$ voidaan määritellä $\mathbb{Z}_n$-modulin struktuurin?

Nähdään samalla tavalla kuin yllä $\mathbb{Z}$:n tapauksessa, että jos tällainen skalaarikertolasku on määritelty, se on yksikäsitteinen, ja

$$\bar{m}x = mx = \underbrace{x + \ldots + x}_{m \text{ kertaa}}$$

kaikilla $m \in Z, x \in M$.
Mutta tällä kertaa tämä kaava ei välttämättä ole edes hyvin määritelty. Nimittäin, jos M on $\mathbb{Z}_n$-moduli, niin jokaisella $x \in M$ tällöin

$$0 = 0x = \bar{n}x = nx.$$

Toisin sanoen $\mathbb{Z}_n$-modulissa jokaisen alkion n:s monikerta (yhteenlaskun suhteen) on modulin nolla-alkio.
Kääntäen olkoon $(M, +)$ sellainen Abelin ryhmä, jossa $nx = 0$ jokaisella $x \in M$ (kiinnitetyllä $n \in \mathbb{N}$). Määrittelemme tällöin $\mathbb{Z}_n$:n skalaarikertolasku M:ssä kaavalla

$$\bar{m}x = mx = \underbrace{x + \ldots + x}_{m \text{ kertaa}}.$$

Tällöin tämä operaatio on hyvin määritelty ja tekee M:stä $\mathbb{Z}_n$-modulin (yksityiskohdat harjoitustehtävänä).

Olemme näyttäneet, että $\mathbb{Z}_n$-modulit vastaavat sellaisia Abelin ryhmiä, joissa $nx = 0$ jokaisella ryhmän alkiolla x.

2.2 Vapaat modulit ja kannat

Lemma 2.7. *Olkoon M R-moduli ja olkoon $\{M_a \mid a \in \mathcal{A}\}$ mielivaltainen perhe M:n alimoduleja. Tällöin leikkaus*

$$M' = \bigcap_{a \in \mathcal{A}} M_a = \{x \in M \mid x \in M_a \text{ kaikilla } a \in \mathcal{A}\}$$

on myös M:n alimoduli

Todistus. Olkoot $x, y \in M'$ ja $r \in R$. Tällöin $x, y \in M_a$ kaikilla $a \in \mathcal{A}$. Koska jokainen M_a on alimoduli, myös $x + y \in M_a$, $rx \in M_a$ jokaisella $a \in \mathcal{A}$. Näin ollen $x + y$ ja rx kuuluvat joukkoon M', joten M' on alimoduli. □

Olkoon M R-moduli ja $A \subset M$ sen mielivaltainen osajoukko. Yleensä A ei tietenkään ole alimoduli. Kuitenkin edellisestä lemmasta seuraa, että on olemassa (sisältyvyysrelaation suhteen) *pienin* M:n alimoduli, joka sisältää joukon A. Tarkemmin sanoen on olemassa sellainen M:n alimoduli M' jolle pätevät seuraavat ehdot,

1. $A \subset M'$,

2. Jos $A \subset L$, missä L on M:n alimoduli, niin $L \subset M'$.

Tätä alimodulia sanotaan A:n *viritetyksi* alimoduliksi ja merkitään symbolilla Span(A) (tulee englanninkielisestä sanasta *span*, joka tässä yhteydessä tarkoittaa juuri *virittää*). Määritelmästä seuraa, että Span(A) on yksikäsitteinen.
Perustellaan tarkemmin miten Lemmasta 2.7 seuraa alimodulin Span(A) olemassaolo. Olkoon $(M_a)_{a\in\mathcal{A}}$ perhe, jonka muodostavat **kaikki** M:n alimodulit, jotka sisältävät A:n. Tällöin Lemmasta 2.7 seuraa, että

$$M' = \bigcap_{a\in\mathcal{A}} M_a$$

on M:n alimoduli. Helposti nähdään, että M' toteuttaa molemmat ehdot 1 ja 2 yllä.
Yllä käytetty tapa osoittaa Span(A):n olemassaolo on "ulkoinen" ja liian "epämääräinen" - se ei kerro suoraan mitkä alkiot kuuluvat joukkoon Span(A). On olemassa myös erittäin hyödyllinen "sisäinen" tapa karakterisoida joukon Span(A) alkiot lineaarisen kombinaation käsitteen kautta.
Olkoon M moduli ja $(x_1, \ldots, x_n)$ *äärellinen* jono sen alkiota. Sanalla "jono" tarkoitamme tässä yhteydessä, että alkiot x_i on laitettu järjestykseen (joukossahan alkioiden listausjärjestyksellä ei ole merkitystä, sen sijaan jonossa on), joka on indeksoitu luonnollisilla luvuilla $1, \ldots, n$.
Mikä tahansa muotoa

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n,$$

oleva lauseke, missä $r_1, r_2, \ldots, r_n$ ovat kerroinrenkaan R alkiot, sanotaan alkioiden $x_1, \ldots, x_n$ *lineaariseksi kombinaatioksi*. Myös sen arvo, eli modulin alkio $x = r_1x_1 + r_2x_2 + \ldots + r_nx_n$ kutsutaan alkioiden $x_1, \ldots, x_n$ lineaariseksi kombinaatioksi. Termit r_ix_i ovat tämän lineaarisen kombinaation *jäsenet*. Alkio $r_i \in R$ on *kombinaatiossa esiintyvän alkion* $x_i \in M$ *kerroin*. Huomaa, että vaikka puhummekin jonosta, alkioiden järjestys ei vaikuta lineaarisen kombinaation $r_1x_1 + r_2x_2 + \ldots + r_nx_n$ arvoon. Tosin sanoen jonon alkiot voidaan permutoida, jolloin saadaan sama lineaarinen kombinaatio.

Teemme myös seuraavan havainnon. Jos kombinaatiossa

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n,$$

kaksi esiintyvää M:n alkiota x_i ja x_j ovatkin sama alkio x', ne voidaan yhdistää jäseneksi $(r_i + r_j)x'$. Tästä seuraa, että lineaaristen kombinaatioiden

tarkastelussa voimme aina olettaa, että kombinaatiossa esiintyvät modulin alkiot $x_1, \ldots, x_n$ ovat *eri* alkiot.
Hyväksymme lineaariseksi kombinaatioksi myös ”tyhjän summan”, jossa on nolla yhteenlaskettavaa termiä. Sovimme, että tällaisen tyhjän summan arvo on aina modulin nolla-alkio 0.
Osoittautuu, että Span(A):n alkiot ovat tasan sellaiset M:n alkiot, jotka voidaan esittää A:n alkioiden lineaarisina kombinaatioina (ainakin silloin kun kerroinrengas on ykkösellinen).

Lemma 2.8. *Olkoon R* **ykkösellinen** *rengas ja M R-moduli. Olkoon $A \subset M$ osajoukko. Tällöin*

$$\text{Span}(A) = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in A, n \geq 0\}.$$

Todistus. Riittää osoittaa, että oikealla puolella esiintyvä joukko

$$N = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in A, n \geq 0\}$$

on M:n alimoduli, joka sisältää A:n, ja lisäksi pienin sellainen. Ensimmäisen väitteen todistaminen jätetään harjoitustehtäväksi.
Kun valitaan $n = 1$ ja $r = 1$ saadaan jokaisella $a \in A$ lineaarinen kombinaatio, jonka arvo on a. Näin ollen $A \subset N$. Huomaa, miten ykkösalkion olemassaolo renkaassa R on olennaista tässä argumentissa.
Olkoon P mikä tahansa M:n alimoduli, joka sisältää A:n. Koska P on suljettu skalaarikertolaskun ja yhteenlaskun suhteen, induktiolla nähdään, että P sisältää kaikki A:n alkioista muodostettuja lineaarisia kombinaatioita, eli $N \subset P$. Näin ollen N on pienen M:n alimoduli, joka sisältää joukon A. □

Jos rengas ei ole ykkösellinen, edellinen tulos ei välttämättä päde. Esimerkiksi olkoon $R = 2\mathbb{Z}$ parillisten kokonaislukujen muodostama rengas. Tällöin R on R-moduli luonnollisella tavalla. Jos otetaan esimerkiksi A:ksi yhden alkion joukko $\{2\}$, niin joukko $\{r2 \mid r \in R\}$ EI sisällä alkioita 2 itse.

Tästä (ja monesta muusta) syystä oletamme tästä lähtien, että kaikki tarkasteltavat modulit ovat määriteltyjä *ykkösellisen renkaan* yli.

Olkoon A R-modulin M osajoukko (missä R on ykkösellinen rengas) ja olkoon $x \in \text{Span}(A)$. Edellisestä lemmasta seuraa, että silloin x voidaan esittää *erilaisten* A:n alkioiden lineaarisena kombinaationa eli muodossa

$$r_1a_1 + r_2a_2 + \ldots + r_na_n,$$

missä $a_i \in A$ ja $r_i \in R$ jokaisella $i = 1, \ldots, n$ ja alkiot a_i ovat kaikki eri alkiot.

Tällainen esitys ei kuitenkaan ole yleensä yksikäsitteinen (järjestystä vaille) eli voi hyvinkin käydä niin, että myös

$$x = r'_1 a'_1 + r'_2 a'_2 + \ldots + r'_n a'_m$$

joka on **oleellisesti erilainen** kuin esitys $r_1 a_1 + r_2 a_2 + \ldots + r_n a_n$. Sana "oleellisesti" tarkoittaa tässä yhteydessä sitä, että kaksi esitystä, jotka eroavat vain yhteenlaskettavien termien $r_i a_i$ järjestyksessä, ajattelemme samaksi esitykseksi, eli jäsenten $r_i a_i$ indeksit voi permutoida. Lisäksi sallimme, että lineaarisen kombinaatioon voi lisätä ns. *nollatermejä*, eli muotoa $0 \cdot a$, $a \in M$ olevia alkiota. Tällainen lisäys ei tietenkään muuta lineaarisen kombinaation arvoa ja sovimme siis, että tällainen nollatermin lisäys ei muuta lineaarista kombinaatiota (vaikka muodollisesti *lausekkeena* kombinaatio on silloin erilainen). Samoin luonnollisesti sovitaan myös, että mahdollisen nollatermin poisjättäminen kombinaatiosta ei muuta sitä.
Näistä määritelmistä seuraa siis, että esitykset $r_1 a_1 + r_2 a_2 + \ldots + r_n a_n$ ja $r'_1 a'_1 + r'_2 a'_2 + \ldots + r'_n a'_m$ ovat oleellisesti erilaiset jos ja vain jos toisesta esityksestä löytyy *nollasta eroava* termi $r_i a_i$, joka **ei** esiinny toisessa.

Esimerkkinä tarkastelemme $\mathbb{Z}$-moduli $\mathbb{Z}^2$. Olkoon $A = \{(1,-1),(2,3),(4,1)\} \subset \mathbb{Z}^2$. Tällöin alkio $(5,0)$ voidaan esittää A:n alkioiden lineaarisena kombinaationa ainakin kahdella eri tavalla, sillä

$$(5,0) = 3 \cdot (1,-1) + 1 \cdot (2,3),$$

$$(5,0) = 1 \cdot (1,-1) + 1 \cdot (4,1).$$

Huomaa, että yhtä hyvin pätee $(5,0) = 3 \cdot (1,-1) + 1 \cdot (2,3) + 0 \cdot (4,1)$, mutta yllä tehdyn sopimuksen nojalla tämä onkin sama kombinaatio kuin $(5,0) = 3 \cdot (1,-1) + 1 \cdot (2,3)$.

Määritelmä 2.9. *Olkoon M R-moduli ja $A \subset M$. Sanomme, että A on* vapaa *joukko (M:ssä), jos jokainen* $\mathrm{Span}(A)$*:n alkio voidaan esittää A:n alkioiden lineaarisena kombinaationa tasan yhdellä tavalla (järjestystä ja nollatermejä vailla).*

Seuraava lemma antaa toisen tavan määritellä vapauden (joka hyvin usein käytetäänkin määritelmänä).

Lemma 2.10. *Olkoon A R-modulin M osajoukko. Tällöin A on vapaa jos ja vain jos seuraava ehto toteutuu aina.*
Olkoot $a_1, \ldots, a_n \in A$ eri alkiot ja $r_1, \ldots, r_n \in R$ siten, että

$$r_1 a_1 + \ldots + r_n a_n = 0.$$

Tällöin $r_1 = r_2 = \ldots = r_n = 0$.

Todistus. Jos A on vapaa, niin erityisesti nolla-alkiolla $0 \in \mathrm{Span}(A)$ on vain yksi lineaarinen kombinaatio - tyhjä summa, eli mikä tahansa kombinaatio, jossa esiintyy ainoastaan nollatermejä. Näin ollen ehto toteutuu.
Oletetaan, että A ei ole vapaa. Tällöin on olemassa kaksi erilaista kombinaatiota A:n alkioista, joilla on sama arvo, eli

$$r_1 a_1 + \ldots + r_n a_n = r'_1 a'_1 + \ldots + r'_m a'_m.$$

Jos jokin a'_j esiintyy vasemmalla puollella kertoimien a_i joukossa, siirretään se vasemmalle puolelle ja yhdistetään vastaavan termin kanssa. Tehdään tämä kaikki molemmilla puolella esiintyvien alkioiden kanssa. Nyt vasemmalla ja oikealla puolella ei esiinny samoja alkioita ja kombinaatiot ovat edelleenkin erilaiset. Lopuksi voimme olettaa (jättämällä pois nollatermit), että kaikki yllä esiintyvät kertoimet r_i, r'_i eroavat nollasta.
Tästä saadaan nollalle lineaarinen esitys

$$r_1 a_1 + \ldots + r_n a_n - r'_1 a'_1 - \ldots - r'_m a'_m = r_1 a_1 + \ldots + r_n a_n + (-r'_1) a'_1 + \ldots + (-r'_m) a'_m = 0.$$

Koska kombinaatiot ovat erilaiset, erityisesti ainakin toinen kombinaatio ei ole tyhjä summa, joten tästä saadaan nollalle *epätriviaali* esitys, mikä on ristiriidassa ehdon kanssa. □

Mikä tahansa lineaarinen kombinaatio

$$r_1 a_1 + \ldots + r_n a_n = 0,$$

jossa ainakin yksi kerroin $r_i \neq 0$, sanotaan siis nolla-alkion *epätriviaaliksi* esitykseksi. Näin ollen $A \subset M$ on vapaa, jos ja vain jos nollalla ei ole epätriviaalia esityksiä A:n alkioilla.
Osajoukkoa, joka ei ole vapaa, sanotaan *sidotuksi*. Välillä puhumme myös vapaista ja sidotuista *jonoista* $(x_1, \ldots, x_n)$. Tällöin tarkoitamme, että jonoa vastaava joukko $\{x_1, \ldots, x_n\}$ on vapaa tai sidottu.
Käydään läpi muutama vapaiden ja sidottujen osajoukkojen perusominaisuuksia.

Lemma 2.11. *Olkoon M R-moduli ja $A \subset V$. Tällöin*

(a) jos A on vapaa ja $B \subset A$, B on myös vapaa,

(b) jos A on sidottu ja $A \subset C$, myös C on sidottu.

Lisäksi, jos R on kunta, eli M on vektoriavaruus, niin seuraavat tulokset pätevät.

(c) *Osajoukko A on sidottu jos ja vain jos on olemassa $a \in A$ jolle $a \in \mathrm{Span}(A \backslash \{a\})$, eli jokin A:n alkio voidaan esittää* **muiden** *A:n alkioiden lineaarisena kombinaationa.*

(d) *Jos $(a_1, \ldots, a_n)$ on äärellinen jono, joka on (joukkona) sidottu, niin on olemassa $i = 1, \ldots, n$ siten, että $a_i \in \mathrm{Span}\{a_1, \ldots, a_{i-1}\}$ eli a_i voidaan esittää jonon* **edellisten** *alkioiden lineaarisena kombinaationa.*

Todistus. (a) Olkoon

$$r_1 b_1 + r_2 b_2 + \ldots + r_n b_n = 0$$

nolla-alkion lineaarinen esitys B:n alkioiden avulla. Koska $B \subset A$ tämä on myös nollan esitys A:n alkioilla. Koska A on vapaa, tämän esityksen kaikki kertoimet r_i ovat nollia. Lemman 2.10 nojalla B on vapaa.
(b) Jos C olisi vapaa, (a)-kohdan nojalla myös A olisi vapaa, mikä on ristiriidassa oletuksen kanssa.
(c) Oletetaan, että A on sidottu. Tällöin on olemassa epätriviaali esitys

$$r_1 a_1 + \ldots + r_n a_n = 0,$$

missä $a_i \in A$ ja jokin kerroin $r_i \neq 0$. Voimme olettaa esim. että $r_n \neq 0$. Tällöin

$$a_n = (-r_1/r_n)a_1 + \ldots + (-r_{n-1}/r_n)a_{n-1},$$

joten $a = a_n$ voidaan esittää joukon $A \setminus \{a\}$ alkioiden lineaarisena kombinaationa. Huomaa, miten oletuksemme "R on kunta" on käytetty tässä hyväksi. Oletetaan kääntäen, että on olemassa $a \in A$ siten, että $a \in \mathrm{Span}(A \setminus \{a\})$. On siis olemassa lineaarinen kombinaatio

$$a = r_1 a_1 + \ldots + r_n a_n,$$

missä $a_i \in A, a_i \neq a$ kaikilla $i = 1, \ldots, n$. Tästä saadaan nollalle epätriviaali esitys

$$0 = r_1 a_1 + \ldots + r_n a_n + (-1) \cdot a,$$

missä esiintyvät vain A:n alkiot. Näin ollen A on sidottu.
(d) Harjoitustehtävä. □

Näytämme esimerkillä, että edellisen lemman kohdassa c) tosiaankin tarvitaan kunta-oletus.
Kokonaislukujen joukko $\mathbb{Z}$ on $\mathbb{Z}$-moduli (eli Abelin ryhmä). Sen osajoukko $\{2, 3\}$ on sidottu, sillä

$$3 \cdot 2 + (-2) \cdot 3 = 0.$$

Kuitenkin ei päde $2 \in \mathrm{Span}(3)$, sillä Span(3) koostuu tasan niistä kokonaisluvuista, jotka ovat jaollisia luvulla 3. Samasta syystä ei päde $3 \in \mathrm{Span}(2)$. Edellisen lemman tapainen todistus ei toimi nyt nimenomaan siitä syystä, että luvuilla 2 ja 3 ei ole käänteisalkioita $\mathbb{Z}$:ssä kertolaskun suhteen.

Olkoon M R-moduli ja $A \subset M$. Jos $\mathrm{Span}(A) = M$ eli A *virittää* koko moduli M, ja lisäksi A on vapaa, sanomme A M:n *kannaksi*. Tällöin M sanotaan *vapaaksi* R-moduliksi. Vapaa moduli on siis sellainen moduli, jolla on kanta.

Jos $M = \mathrm{Span}(A)$, missä $A = \{a_1, \ldots, a_n\}$ on *äärellinen*, sanomme, että M on *äärellisviritteinen* moduli. Jos $M = \mathrm{Span}(A)$, missä A on *äärellinen kanta*, eli sekä äärellinen, että vapaa osajoukko, joka virittää koko M:n, sanomme, että M on *äärellisulotteinen* moduli. Jos M:llä on kanta $\{a_1, \ldots, a_n\}$, jossa on tasan n alkiota, sanomme, että M on n-ulotteinen R-moduli. Teknisistä syistä äärellinen kanta $\{a_1, \ldots, a_n\}$ yleensä esitetään jonona $(a_1, \ldots, a_n)$, ei joukkona. Toisin sanoen kannassa kiinnitetään usein alkioiden järjestystä.

Voidaan osoittaa, että mikä tahansa vektoriavaruus on vapaa, eli sillä on olemassa kanta. Lisäksi tämän kannan "koko" (jolla ymmärretään ns. *mahtavuus* yleisemmin äärettömän kannan tapauksessa) on vakio, joka ei riipu kannan valinnasta. Tästä seuraa, että jokaisella vektoriavaruudella on hyvinmääritelty *ulottuvuus*. Palaamme tähän (ehkä) myöhemmin, tässä vaiheessa palautetaan vain mieleen, miten tämä todistetaan äärellisviritteiselle avaruudelle.

Jos kerroinrengas R ei ole kunta, niin tämä ei ole välttämättä päde - on olemassa modulit, joilla ei ole kanta.

Esimerkkejä 2.12. *1. $\mathbb{Z}_n$ (kokonaisluvut modulo n, $n \geq 1$) on $\mathbb{Z}$-moduli. Lisäksi se on selvästi äärellisviritteinen, sillä se on jopa äärellinen (mikä tahansa moduli selvästi virittää itseään). Kuitenkin se ei ole vapaa. Tämä nähdään seuraavasti. Olkoon A jokin $\mathbb{Z}_n$:n kanta. Tällöin A on selvästi epätyhjä (miksi?), joten on olemassa $a \in A$. Mutta*

$$n \cdot a = 0$$

on nollan epätriviaali esitys. Näin ollen A ei ole edes vapaa, joten se ei voi olla kanta.

2. Edellisessä esimerkissä syy kannan olemattomuuteen on epätriviaalien torsioalkioden *olemassaolo modulissa. R-modulin alkio $x \in M$ sanotaan torsioalkioksi jos on olemassa $r \in R$, $r \neq 0$ jolle $rx = 0$. $\mathbb{Z}_n$:ssä*

itse asiassa mikä tahansa alkio on torsio-alkio. Yleistämällä edellisen esimerkin argumenttia, voidaan osoittaa, että mikä tahansa moduli, jolla on torsioalkio $x \neq 0$, ei voi olla vapaa (harjoitustehtävä).
Annetaan vielä esimerkki ei-vapaasta modulista, jolla ei ole torsioalkioita. Rationaalilukujen joukko $\mathbb{Q}$ on $\mathbb{Z}$-moduli, jolla ei ole torsioalkioita. Kuitenkin $\mathbb{Q}$ ei ole vapaa $\mathbb{Z}$-modilina. Tarkka todistus jätetään harjoitustehtäväksi.

Alamme nyt tutkimaan tarkemmin äärellisulotteisia vektoriavaruuksia. Osa tuloksista on tuttu kurssilta " Lineaarialgebra ja matriisilaskenta", jolla ne tosin todistetaan vain $\mathbb{R}$-kerroinkunnan tapauksessa ja osittain eri tavalla. Ensin osoitetaan että äärellisviritteinen vektoriavaruus on aina äärellisulotteinen, erityisesti aina vapaa.

Lemma 2.13. *Olkoon $V = \mathrm{Span}(A)$ K-vektoriavaruus, missä $A = \{a_1, \ldots, a_n\}$ on äärellinen. Tällöin on olemassa vapaa $B \subset A$, siten, että $V = \mathrm{Span}(B)$.*

Todistus. Jos A on vapaa, valitaan $B = A$. Muuten A on sidottu, joten lemman 2.11, c) nojalla on olemassa $a \in A$ jolle $a \in \mathrm{Span}(A \setminus \{a\})$. Jos merkitään $A' = A \setminus \{a\}$, tästä seuraa, että $V = \mathrm{Span}(A')$.
Jos A' ei ole vapaa, jatketaan samalla tavalla. Koska A on äärellinen, tämä alkioiden vähentäminen joukosta A ei voi jatkua loputtomiin, joten jossakin vaiheessa päästään vapaaseen osajoukkoon, joka virittää koko avaruuden.
Halutessaan sama todistus voi kirjoittaa myös induktio-todistuksena (induktio n:n suhteen). Miten? □

Seuraus 2.14. *Olkoon V K-vektoriavaruus, missä K on mielivaltainen kunta. Tällöin V on äärellisulotteinen jos ja vain jos se on äärellisviritteinen.*

Seuraavaksi osoitamme että vektoriavaruuden kannan koko ei riipu kannan valinnasta, joten voimme puhua avaruuden dimensiosta.

Lemma 2.15. *Olkoon $A = \{a_1, \ldots, a_n\}$ K-vektoriavaruuden V äärellinen osajoukko ja oletamme, että $B = \{b_1, \ldots, b_m\} \subset \mathrm{Span}(A)$ on vapaa osajoukko. Tällöin $m \leq n$.*
(Huomaa, että oletamme, että kaikki alkiot a_i ovat eri alkiot, samoin kaikki alkiot b_j ovat eri alkiot).

Todistus. Osoitetaan väite induktiolla joukon A koon n suhteen. Jos $n = 0$ $\mathrm{Span}(A) = \{0\}$ on triviaali vektoriavaruus. On helppo nähdä, että triviaalissa vektoriavaruudessa ei ole epätyhjiä vapaita osajoukkoja, joten $m = 0$ ja väite on selvä.

Tarkastellaan vielä tapaus $n = 1$, ennen kuin siirrytään induktiovaiheeseen. Nyt $A = \{a\}$, joten

$$\text{Span}(A) = \{ka \mid k \in K\}.$$

Jos $m \geq 2$, on olemassa $k_1, k_2 \in K$ joille $b_1 = k_1 a, b_2 = k_2 a$ ja lisäksi $k_1 \neq k_2$ (muuten olisi $b_1 = b_2$). Voimme olettaa, että $k_2 \neq 0$. Tällöin on olemassa k_2^{-1}, joten

$$b_1 + (-k_1 k_2^{-1})b_2 = 0,$$

mikä on ristiriidassa sen kanssa, että B on vapaa. Näin ollen $m \leq 1$.
Oletamme, että väite on tosi jollakin $n \geq 1$. Olkoon $A = \{a_1, \ldots, a_{n+1}\}$ ja oletamme, että $B = \{b_1, \ldots, b_m\} \subset \text{Span}(A)$ on vapaa. Lemmasta 2.8 seuraa, että jokaisella $j = 1, \ldots, m$ voimme kirjoittaa

$$b_j = r_1^j a_1 + \ldots + r_n^j a_n + r_{n+1}^j a_{n+1}$$

joillakin $r_i^j \in K, i = 1, \ldots, n+1$, $j = 1, \ldots, m$. Jos $r_{n+1}^j = 0$ kaikilla $j = 1, \ldots, m$, joukko B on joukon $A' = \{a_1, \ldots, a_n\}$ virittämässä aliavaruudessa $\text{Span}(A')$. Induktio-oletuksesta seuraa tällöin heti, että $m \leq n \leq n+1$ ja asia on selvä.
Toinen vaihtoehto on, että $r_{n+1}^j = r \neq 0$ jollakin j. Muutamalla B:n alkioiden indeksointia tarvittaessa, voimme olettaa, että $j = m$. Jokaisella $j = 1, \ldots, m-1$ määritellään

$$b'_j = b_j - (r_{n+1}^j r^{-1})b_{n+1}.$$

(Huomaa, miten alkion r^{-1} olemassaolo (eli se, että K on kunta) on olennaista tässä vaiheessa.) Tällöin $b'_j \in \text{Span}(A')$, missä $A' = \{a_1, \ldots, a_n\}$, jokaisella $j = 1, \ldots, m-1$. Osoitetaan, että joukko $B' = \{b'_1, \ldots, b'_{m-1}\}$ on vapaa. Oletamme, että

$$r_1 b'_1 + \ldots + r_{m-1} b'_{m-1} = 0$$

joillakin $r_1, \ldots, r_{m-1} \in K$. Voimme kirjoittaa tämä yhtälö muodossa

$$r_1 b_1 + r_2 b_2 + \ldots + r_{m-1} b_{m-1} + (-r_1 r_{n+1}^1 r^{-1} - r_2 r_{n+1}^2 r^{-1} - \ldots - r_{m-1} r_{n+1}^{m-1} r^{-1}) b_m = 0.$$

Koska oletamme, että B on vapaa, tästä erityisesti seuraa, että $r_1 = r_2 = \ldots = r_{m-1} = 0$. Näin ollen B' on vapaa. Lisäksi $B' \subset \text{Span}(A')$, missä A':n koko on n. Induktio-oletuksen nojalla $m - 1 \leq n$, mistä seuraa $m \leq n + 1$, eli mitä pitikin todistaa. □

Seuraus 2.16. *Olkoon V äärellisulotteinen vektoriavaruus ja $A = \{a_1, \ldots, a_n\}$ sekä $B = \{b_1, \ldots, b_m\}$ sen eri kannat. Tällöin $n = m$.*

Olkoon V äärellisulotteinen K-vektoriavaruus ja olkoon $A = \{a_1, \ldots, a_n\}$ sen eräs kanta. Tällöin sanomme, että V:n *dimensio* eli *ulottuvuus* on n. Merkitsemme tätä myös yhtälönä $\dim V = n$. Edellisen korollaarin nojalla dimensio on tässä tapauksessa hyvin määritelty.

Jos kerroinrengas R ei ole kunta, voi käydä niin, että sen vapaalla äärellisulotteisella modulilla on erikokoisia kantoja, jolloin siis dimensio käsite ei voi vapaille R-moduleille määritellä.

Voidaan osoittaa, että **kommutatiivisen renkaan** vapaalla äärellisulotteisella modulilla on aina hyvin määritelty dimensio. Todistamme tämän väitteen myöhemmin, mutta pidämme tulos tunnettuna jo tässä vaiheessa ja käytämme siis myös R-moduleille dimension käsitettä, kun R on kommutatiivinen rengas. Käytännössä merkintä $\dim M = n$ tarkoittaa siis, että M:llä löytyy kanta $\{a_1, \ldots, a_n\}$, jossa on tasan n alkiota eli sitä, että M on n-ulottinen R-moduli.

Esimerkki 2.17. *Olkoon R ykkösellinen rengas ja $n \in \mathbb{N}$. Tällöin moduli R^n on vapaa ja n-ulotteinen. Näyttääksemme tämän, määrittelemme jokaisella $i = 1, \ldots, n$ alkion*

$$e_i = (0, \ldots, 1, \ldots, 0),$$

missä tasan i's koordinaatti on 1 ja muut ovat nollia. Väitämme, että joukko $\{e_i \mid i = 1, \ldots, n\}$ on R^n:n kanta.
Olkoon $x = (x_1, x_2, \ldots, x_n) \in R^n$ mielivaltainen. Tällöin

$$x = a_1e_1 + a_2e_2 + \ldots + a_ne_n = (a_1, \ldots, a_n)$$

jos ja vain jos $a_i = x_i$ kaikilla $i = 1, \ldots, n$. Tästä nähdään, että jokaisella $x \in R^n$ on tasan yksi lineaarinen esitys muodossa

$$x = a_1e_1 + a_2e_2 + \ldots + a_ne_n.$$

Näin ollen $\{e_i \mid i = 1, \ldots, n\}$ on kanta ja R^n on n-ulotteinen R-moduli.
Näin ollen erityisesti jokaisella $n \in \mathbb{N}$ on olemassa n-ulotteinen R-moduli. Seuravaassa luvussa näemme, että tämä on olennaisesti ainoa n-ulotteinen R-moduli, sillä jokainen n-ulotteinen R-vektoriavaruus on isomorfinen *R^n:n kanssa.*

Viitamme jatkossa juuri konstruoituun R^n:n kantaan $(e_1, \ldots, e_n)$ nimetyksellä standardikanta*. Huomaa, että tässä yhteydessä kanta ajatellaan jo jonona, eli siinä on kiinnitetty alkioiden järjestys.*

Jos R ei ole ykkösellinen, niin R^n ei ole välttämättä edes vapaa (ainakin meidän määritelmän mukaisesti). Esimerkiksi olkoon $R = \{2n \mid n \in \mathbb{Z}\}$ parillisten kokonaislukujen rengas. Tällöin jopa R itse ei ole äärellisulotteinen R-moduli (harjoitustehtävä) ja itse asiassa ei ole olemassa R-moduleita, joilla olisi epätyhjä R-kanta. Tämä havainnollista sen tosi seikan, että meidän tapa määritellä modulin kanta ei sovi ei-ykkösellisen renkaan tapauksessa.

Seuraavaksi tarkastelemme äärellisulotteisen vektoriavaruuden aliavaruuksia ja tekijäavaruuksia.

Lemma 2.18. *Olkoon V äärellisulotteinen K-vektoriavaruus, missä K on kunta ja olkoon $W \subset V$ aliavaruus. Tällöin W on myös äärellisulotteinen. Lisäksi jos $W \subsetneq V$,pätee*

$$\dim W < \dim V.$$

Jokainen W:n kanta $(a_1, \ldots, a_k)$ voi täydentää V:n kannaksi. Pätee jopa seuraava - olkoon $(a_1, \ldots, a_k)$ jokin W:n kanta ja $(e_1, \ldots, e_n)$ jokin V:n kanta. Tällöin jonolla $(e_1, \ldots, e_n)$ on olemassa osajono $(e_{j_1}, e_{j_2}, \ldots, e_{j_{n-k}})$ siten että jono

$$(a_1, \ldots, a_k, e_{j_1}, e_{j_2}, \ldots, e_{j_{n-k}})$$

on V:n kanta.

Todistus. Olkoon $B = \{e_1, \ldots, e_n\}$ jokin V:n kanta. Olkoon $A = \{a_1, \ldots, a_l\}$ mielivaltainen W:n äärellinen vapaa osajoukko. Tällöin erityisesi $A \subset \mathrm{Span}(B)$, joten Lemman 2.15 nojalla $l \leq n$.
Tästä seuraa, että W ei voi sisältää mielivaltaisen isoja vapaita osajoukkoja ja itse asiassa jokaisessa W:n vapaassa osajoukossa on korkeintaan n alkiota. Olkoon $B = \{a_1, \ldots, a_k\}$ W:n *maksimaalinen* vapaa osajoukko, eli sellainen, jota ei voi enää laajentaa. Sellaisen on pakko olla olemassa edellisen nojalla. Lisäksi $k \leq n$. Osoitetaan, että $(a_1, \ldots, a_k)$ on W:n kanta. Riittää osoittaa, että $W = \mathrm{Span}(B)$.
Olkoon $w \in W$ mielivaltainen. Haluamme osoittaa, että $w \in \mathrm{Span}(B)$. Jos $w = a_i$ jollakin i, asia on selvä. Muuten $(a_1, \ldots, a_k, w)$ on W:n eri alkioiden jono, jonka pituus on aidosti isompi kuin joukon B koko. Koska B on maksimaalinen vapaa osajoukko, jono $(a_1, \ldots, a_k, w)$ on sidottu. Lemmasta 2.11, d) seuraa, että jokin tämän jonon jäsen voidaan esittää **edellisten** alkioiden lineaarisena kombinaationa. Mutta mikään a_j ei voida esittää muiden a_i avulla (sillä muuten B olisi sidottu), joten sellaisen alkion täytyy olla w. Olemme näyttäneet, että $W = \mathrm{Span}(B)$. Erityisesti W on äärellisulotteinen ja $\dim W = k \leq n = \dim V$.

Olkoon $(a_1, \ldots, a_k)$ jokin W:n kanta ja $(e_1, \ldots, e_n)$ jokin V:n kanta. Laitetaan ne jonoon $(a_1, \ldots, a_k, e_1, \ldots, e_n)$. Jos $k = 0$ eli W on triviaali aliavaruus $\{0\}$, olemme valmiit. Muuten tämän jonon täytyy olla sidottu (sillä sen pituus on suurempi kuin $n = \dim V$), joten Lemman 2.11, d) nojalla on olemassa sen alkio joka voidaan esittää edellisten lineaarisena kombinaationa. Se ei voi olla mikään alkio a_i W:n kannasta, sillä se on vapaa osajoukko, joten se on yksi alkioista e_j.
Poistetaan se jonosta ja jatketaan samalla tavalla. Jos uusi jono on sidottu, sovelletaan taas sama lemma 2.11, d) ja poistetaan seuraava alkio $e_{j'}$.
Jatketaan näin kunnes jäljelle jäänyt jono $C = (a_1, \ldots, a_k, e_{j_1}, e_{j_2}, \ldots, e_{j_l})$ on vapaa. Konstruktion perusteella jokainen V:n kannan alkio e_i voidaan esittää tämän jonon jäsenten lineaarisena kombinaationa. Koska e_i:t yhdessä virittävät V:n, tästä seuraa, että mikä tahansa V:n alkio on avaruudessa $\mathrm{Span}(C)$. Näin ollen C on V:n kanta, joten täytyy olla myös $k + l = n$ eli $l = n - k$.

Erityisesti, jos W on V aito aliavaruus, täytyy olla $l \geq 1$, sillä muuten W:n kanta olisi samalla myös V:n kanta, mistä seuraisi $W = V$. Toisaalta jos $l \geq 1$, niin tällöin $k = n - l < n$. Näin ollen erityisesti

$$\dim W < \dim V.$$

□

Edellisen lemman tulos ei välttämättä päde äärellisulotteiselle R-modulille, jos R ei ole kunta. Esimerkiksi $\mathbb{Z}$ on vapaa 1-ulotteinen $\mathbb{Z}$-moduli. Helposti nähdään, että $\mathbb{Z}$:n alimodulit ovat muotoa

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

olevia joukkoja, $n \in \mathbb{Z}$ (harjoitustehtävä). Jokainen niistä on myös vapaa 1-ulotteinen $\mathbb{Z}$-moduli. Kun $|n| > 1$, $n\mathbb{Z}$ on aito alimoduli. Myös $n\mathbb{Z}$:n kanta $\{n\}$ ei voi tässä tapauksessa laajentaa koko $\mathbb{Z}$:n kannaksi. Itse asiassa $\mathbb{Z}$:llä on vain kaksi kanta - joukot $\{1\}$ ja $\{-1\}$.
Myöhemmin näytämme, että äärellisulotteisen $\mathbb{Z}$-modulin jokainen alimoduli **on** myös äärellisulotteinen, erityisesti vapaa. On kuitenkin olemassa esimerkkejä renkaista R ja äärellisulotteisista R-moduleista, joilla on ei-vapaa alimoduli.
Esimerkiksi $\mathbb{Z}_4$ on 1-ulotteinen $\mathbb{Z}_4$-moduli. Helposti nähdään, että sen osajoukko $M = \{0, 2\}$ on sen alimoduli. M on siis $\mathbb{Z}_4$-moduli. Se ei kuitenkaan ole vapaa - itse asiassa tässä tapauksessa M:llä ei edes ole epätyhjiä vapaita osajoukkoja. Tämä nähdään seuraavasti - nolla-alkio 0 ei voi kuulua mihinkään vapaaseen osajoukkoon, sillä $0 = 1 \cdot 0$ on epätriviaali nollan esitys.

Mutta samasta syystä alkio 2 ei voi kuulua mihinkään vapaaseen osajoukkoon, sillä $0 = 2 \cdot 2$.
Edellisessä esimerkissä äärellisulotteisen modulin jokainen alimoduli on sentään äärellisviritteinen. Ei tämäkin päde yleisesti - on olemassa tilanteita, joissa äärellisulotteisen modulin alimoduli ei ole edes äärellisviritteinen.
Nämä esimerkit havainnollistavat sen tosiseikan, että vektoriavaruudet ovat paljon ”säännöllisimpiä” ja” hyvin käytytäyttäviä ” kuin yleiset modulit.

Tarkastellaan vielä tekijäavaruuksia.

Lemma 2.19. *Olkoon V äärellisulotteinen K-vektoriavaruus ja V' sen aliavaruus. Tällöin tekijäavaruus V/V' on myös äärellisulotteinen ja*

$$\dim(V/V') = \dim V - \dim V'.$$

Todistus. Olkoon $a_1, \ldots, a_k$ aliavaruuden W kanta. Edellisen lemman nojalla se voidaan täydentää koko avaruuden V kannaksi $a_1, \ldots, a_k, b_1, \ldots, b_{n-k}$, missä $n = \dim V$.
Tarkastellaan tekijäavaruudessa jono $\overline{b_1}, \ldots, \overline{b_{n-k}}$. Riittää osoittaa, että tämä jono on V/V':n kanta.
Olkoon $x \in V$. Tällöin on olemassa esitys

$$x = s_1 a_1 + \ldots + s_k a_k + t_1 b_1 + \ldots + t_{n-k} b_{n-k},$$

missä $s_i, t_j \in K$. Ottamalla tästä ekvivalenssiluokat V/V':ssä saadaan

$$\bar{x} = s_1 \overline{a_1} + \ldots + s_k \overline{a_k} + t_1 \overline{b_1} + \ldots + t_{n-k} \overline{b_{n-k}} =$$

$$= t_1 \overline{b_1} + \ldots + t_{n-k} \overline{b_{n-k}},$$

sillä jokaisen muotoa a_i olevan alkion luokka on $V' = \overline{0}$. Näin ollen alkiot $\overline{b_1}, \ldots, \overline{b_{n-k}}$ virittävät tekijäavaruuden V/V'. Osoitetaan vielä, että tämä jono on vapaa. Oletetaan, että

$$t_1 \overline{b_1} + \ldots + t_{n-k} \overline{b_{n-k}} = \overline{0}$$

joillakin $t_1, \ldots, t_{n-k} \in K$. Tästä seuraa, että $t_1 b_1 + \ldots + t_{n-k} b_{n-k} \in V'$ eli on olemassa esitys

$$t_1 b_1 + \ldots + t_{n-k} b_{n-k} = s_1 a_1 + \ldots + s_k a_k.$$

Tämä voidaan kirjoittaa muodossa

$$(-s_1) a_1 + \ldots + (-s_k) a_k + t_1 b_1 + \ldots + t_{n-k} b_{n-k} = 0.$$

Koska $a_1, \ldots, a_k, b_1, \ldots, b_{n-k}$ on vapaa, tästä seuraa, että erityisesti $t_1 = t_2 = \ldots = t_j = \ldots = t_{n-k} = 0$, eli $\overline{b_1}, \ldots, \overline{b_{n-k}}$ on vapaa. □

Jos kerroinrengas ei ole kunta, edellinen lemma ei taaskaan välttämättä päde. Esimerkiksi $n\mathbb{Z}$ on $\mathbb{Z}$:n $\mathbb{Z}$-alimoduli, ja molemmat ovat vapaita, mutta tekijämoduli $\mathbb{Z}_n$ ei ole edes vapaa. Voidaan osoittaa, että itse asiassa jokainen Abelin ryhmä (eli $\mathbb{Z}$-moduli) on esitettävissä kahden vapaan ryhmän tekijäryhmänä.

2.3 Lineaarikuvaukset ja matriisit

Olkoot M, N molemmat R-modulit (jossa R oletetaan ykköselliseksi renkaaksi, kuten olemme sovineet edellisessä luvussa). Kaikkien R-lineaaristen kuvausten $L\colon M \to N$ joukkoa merkitään $L(M,N)$. Kun $M = N$ on sama moduli, joukkoa $L(M,M)$ merkitään myös lyhyemmin symbolilla $L(M)$.

Olkoot $L, L'\colon M \to N$ kaksi R-lineaarista kuvausta eli kaksi joukon $L(M,N)$ alkiota. Niiden summa $L + L'$ määritellään luonnollisella tavalla pisteittäin kuvauksena $L + L'\colon M \to N$,

$$(L + L')(m) = L(m) + L(m').$$

Helposti nähdään, että $L+L'$ on myös R-lineaarinen. Nimittäin olkoot $m, m_1, m_2 \in M$, $r \in R$. Tällöin

$$(L+L')(m_1+m_2) = L(m_1+m_2)+L'(m_1+m_2) = L(m_1)+L(m_2)+L'(m_1)+L(m_2) =$$

$$(L(m_1) + L'(m_2)) + (L(m_2) + L'(m_2)) = (L + L')(m_1) + (L + L')(m_2),$$

$$(L+L')(rm) = L(rm)+L'(rm) = rL(m)+rL'(m) = r(L(m)+L(m')) = r(L+L')(m).$$

Näin ollen joukossa $L(M,N)$ on hyvin määritelty yhteenlasku-operaatio $+$. Helposti nähdään, että pari $(L(M,N),+)$ on Abelin ryhmä (harjoitustehtävä). Nolla-alkio on nollakuvaus $0\colon M \to N$, joka on määritelty ehdolla $0(m) = 0$ kaikilla $m \in M$. Alkion $L \in L(M,N)$ vasta-alkio $-L$ on määritelty pisteittäin ehdolla $(-L)(m) = -L(m)$.
Voidaanko joukkoon $L(M,N)$ määritellä myös skalaarikertolasku niin että siitä tulee R-moduli? Luonnollinen kandidaatti alkioksi rL, missä $r \in R$ ja $L \in L(M,N)$ on kuvaus joka on määritelty ehdolla $(rL)(m) = r \cdot L(m)$. Mutta onko tällainen skalaarikertolasku hyvin määritelty joukossa $L(M,N)$ eli onko rL myös R-lineaarinen, kun L on? Tarkistetaan tämä. Yhteenlaskun kanssa ei tule ongelmia -

$$(rL)(x+y) = rL(x+y) = r(L(x)+L(y)) = rL(x)+rL(y) = (rL)(x)+(rL)(y).$$

Olkoon $r' \in R$. Tällöin

$$(rL)(r'x) = rL(r'x) = r(r'L(x)) = (rr')L(x),$$

ja $r'(rL)(x) = r'(rL(x)) = (r'r)L(x)$. Tästä näemme, että kun R ei ole vaihdannainen rengas, voi hyvinkin käydä niin, että $(rL)(r'x) \neq r'(rL)(x)$ jolloin rL ei siis ole R-lineaarinen. Kun taas R on kommutatiivinen, pätee $rr' = r'r$, joten rL on silloin myös R-lineaarinen. Ei ole vaikeata verifioida, että tällöin $L(M, N)$ on R-moduli. Itse asiassa helpoin tapa nähdä tämän on huomata, että R:n olleessa kommutatiivinen, $L(M, N)$ on R-modulin $N^M = \{f \colon M \to N\}$ alimoduli (kts. Esimerkki 1.8, 3).
Kootaan kaikki tähän mennessä saadut tulokset seuraavassa Propositiossa yhteen.

Propositio 2.20. *Olkoot M, N R-modulit. Tällöin $L(M, N)$ on Abelin ryhmä. Jos R on kommutatiivinen, $L(M, N)$ on R-moduli.*
Erityisesti jos V, W ovat K-vektoriavaruuksia, missä K on kunta, $L(V, W)$ on myös K-vektoriavaruus luonnollisella tavalla.

Lineaarikuvaus sanotaan *monomorfismiksi* jos se on injektio. Se sanotaan *epimorfismiksi* jos se on surjektio.
Lineaarikuvaus on *isomorfismi* jos se on bijektio eli jos se on sekä mono-, että epimorfismi.

Propositio 2.21. *Olkoon $L \colon M \to N$ R-lineaarinen kuvaus R-modulien välillä. Tällöin*

i) L on epimorfismi jos ja vain jos $\operatorname{Im} L = N$.

ii) L on monomofirmismi jos ja vain jos $\operatorname{Ker} L = \{0\}$.

Todistus. i) Selvä.
ii) Jokaisella R-lineaariselle kuvaukselle pätee $L(0) = 0$. Jos L on injektio, mikään muu alkio ei tällöin voi kuvautua nollalle, joten $\operatorname{Ker} L = \{0\}$. Kääntäen, oletetaan, että $\operatorname{Ker} L = \{0\}$. Olkoot $x, y \in M$ sellaiset, että $L(x) = L(y)$. Tällöin

$$L(x - y) = L(x) - L(y) = 0,$$

joten $x - y \in \operatorname{Ker} L = \{0\}$. Toisin sanoen $x - y = 0$ eli $x = y$. Olemme näyttäneet, että L on injektio. □

Seuraavaksi tarkastellaan vapaiden modulien väliset lineaariset kuvaukset. Aloitetaan tärkeällä tuloksella, jonka mukaan lineaarikuvaus on täysin määrätty, kun sen arvot modulin kannan alkioilla tunnetaan.

Propositio 2.22. *Olkoon M vapaa R-moduli ja olkoon $(e_a)_{a\in\mathcal{A}}$ sen kanta. Olkoon N mielivaltainen R-moduli ja olkoon $(b_a)_{a\in\alpha}$ mielivaltainen perhe N:n alkiota (indeksoitu samalla indeksijoukolla $\mathcal{A}$). Tällöin on olemassa tasan yksi lineaarikuvaus $L\colon M \to N$ jolle pätee $L(e_a) = b_a$.*

Todistus. Modulin M jokainen alkio x voidaan esittää oleellisesti yksikäsitteisellä tavalla muodossa

$$x = r_1 e_{a_1} + r_2 e_{a_2} + \ldots + r_n e_{a_n},$$

missä $a_1, \ldots, a_n \in \mathcal{A}$ äärellinen joukko. Jos kuvaus L on olemassa, tällöin lineaarisuudesta seuraa, että

$$L(x) = r_1 L(e_{a_1}) + r_2 L(e_{a_2}) + \ldots + r_n L(e_{a_n}) = r_1 b_{a_1} + r_2 b_{a_2} + \ldots + r_n b_{a_n},$$

eli $L(x)$ on määrätty yksikäsitteisesti. Tämä todistaa kuvauksen L yksikäsitteisyyden.

Todistaaksemme olemassaolon määrittelemme jokaisella $x \in M$

$$L(x) = r_1 b_{a_1} + r_2 b_{a_2} + \ldots + r_n b_{a_n},$$

missä $x = r_1 e_{a_1} + r_2 e_{a_2} + \ldots + r_n e_{a_n}$. Koska tämä esitys on (permutaatioita ja nollatermejä vailla) yksikäsitteinen, tämä määrää L:n yksikäsitteisesti. Helposti nähdään, että L on R-lineaarinen ja toteuttaa vaadittu ehto. □

Seuraus 2.23. *Olkoon M R-moduli. Tällöin M on m-ulotteinen jos ja vain jos on olemassa isomorfismi $M \cong R^m$.*

Todistus. Jos $M \cong R^m$, niin M on m-ulotteinen, sillä R^m on (kts. esimerkki 2.17).
Kääntäen olkoon M m-ulotteinen Olkoon $(e_1, \ldots, e_m)$ vapaan modulin R^m kanta, joka on konstruoitu esimerkissä (2.17) ja olkoon $(f_1, \ldots, f_m)$ jokin M:n kanta. Edellisen proposition nojalla on olemassa lineaarinen kuvaus $L\colon R^m \to M$, jolle $L(e_i) = f_i$ jokaisella $i = 1, \ldots, m$. Samalla perustelulla on olemassa lineaarinen kuvaus $L'\colon M \to R^m$, jolle $L(f_i) = e_i$ jokaisella $i = 1, \ldots, m$. Yhdistetty kuvaus $A = L' \circ L\colon R^m \to R^m$ on myös lineaarinen (lineaaristen kuvausten yhdistäminen tuottaa aina lineaarisen kuvauksen, tästä tarkemmin hieman myöhemmin), lisäksi $A(e_i) = e_i$. Toisaalta identtinen kuvaus $\mathrm{id}\colon R^m \to R^m$ on lineaarinen kuvaus jolle $\mathrm{id}(e_i) = e_i$ kaikilla $i = 1, \ldots, m$. Koska edellisen Proposition nojalla tällainen kuvaus on yksikäsitteinen, täytyy olla $A = \mathrm{id}$. Toisin sanoen $L' \circ L = \mathrm{id}$.
Samalla tavalla nähdään, että $L \circ L' = \mathrm{id}$. Näin ollen L (ja L') on erityisesti bijektio, eli isomorfismi. □

Propositio 2.22 implikoi erityisesti, että jos M on äärellisulotteinen R-moduli, jolla on kanta $(e_1, \ldots, e_m)$, niin jokainen jono $(b_1, \ldots, b_m)$ N:n alkioita määrittelee yksikäsitteisen lineaarisen kuvauksen $L\colon M \to N$ jolle $L(e_i) = b_i, i = 1, \ldots, m$.
Oletetaan sitten, että myös N on äärellisulotteinen moduli ja olkoon $(f_1, \ldots, f_n)$ sen kanta. Olkoon $L\colon M \to N$ lineaarinen kuvaus. Koska $(f_1, \ldots, f_n)$ on N:n kanta, jokaisella $j = 1, \ldots, m$ on olemassa yksikäsitteinen esitys

$$L(e_j) = a_{1j}f_1 + a_{2j}f_2 + \ldots + a_{nj}f_n = \sum_{i=1}^{n} a_{ij}f_i.$$

Propositiosta 2.22 seuraa, että tuplasti indeksoitu perhe kerroinrengas alkioita $(a_{ij})_{1\leq i\leq n, 1\leq j\leq m}$ määrää kuvauksen L yksikäsitteisesti. Yleensä tämä perhe kirjoitetaan taulukoksi eli *matriisiksi*, jolla on n riviä ja m saraketta, siis muodossa

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix}.$$

Tällainen matriisi sanotaan L:n matriisiksi (kantojen $(e_1, \ldots, e_m)$ ja $(f_1, \ldots, f_n)$ suhteen). Huomaa, miten kannan käsittely **jonona** on olennaista tässä.

Määritellään R-kertoimisen matriisin käsite yleisesti. Merkitään yksinkertaisuuden vuoksi jokaisella $m \in \mathbb{N}$ symbolilla $[m]$ äärellistä indeksijoukkoa $\{1, \ldots, m\}$.

Määritelmä 2.24. *Olkoon R rengas, $m, n \in \mathbb{N}$. R-*kertoiminen $(n \times m)$-matriisi *on mikä tahansa joukolla $[n] \times [m]$ indeksoitu perhe $(a_{ij})_{1\leq i\leq n, 1\leq j\leq m}$, missä $a_{ij} \in R$ kaikilla $i \in [n], j \in [m]$. Matriisi $(a_{ij})_{1\leq i\leq n, 1\leq j\leq m}$ yleensä esitetään taulukkona*

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix},$$

jolla on m riviä ja n saraketta. Alkiot a_{ij} sanotaan matriisien kertoimiksi *tai yksinkertaisesti sen alkioiksi.*

Matriisin

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix}$$

jokainen rivi voi tulkita modulin R^n:n alkiona eli jonoksi $A_i = (a_{i1}, a_{i2}, \ldots, a_{im})$, $i = 1, \ldots, n$. Samoin tulkitsemme jatkossa jokainen matriisin sarake $A^j = (a_{1j}, a_{2j}, \ldots, a_{nj})$, $j = 1, \ldots, m$ modulin R^m alkiona.

Matriisia, jolla on sama määrä riveja ja sarakkeita, eli $(n \times n)$-matriisia sanotaan *neliömatriisiksi*.

Olkoot $m, n \in \mathbb{N}$ ja R rengas. Kaikkien $(n \times m)$-matriisien joukkoa merkitään $M(n \times m; R)$. Tällä joukolla on luonnollinen R-modulin struktuuri, joka on määritelty "komponenteittain" eli

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix}, + \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1} & b_{n2} & \ldots & b_{nm} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \ldots & a_{1m}+b_{1m} \\ a_{21}+b_{21} & a_{22}+b_{22} & \ldots & a_{2m}+b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \ldots & a_{nm}+b_{nm} \end{bmatrix},$$

$$r \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix} = \begin{bmatrix} ra_{11} & ra_{12} & \ldots & ra_{1m} \\ ra_{21} & ra_{22} & \ldots & ra_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ ra_{n1} & ra_{n2} & \ldots & ra_{nm} \end{bmatrix}.$$

Toisin sanoen jos $A = (a_{ij})_{1 \le i \le n, 1 \le j \le m}$ ja $B = (b_{ij})_{1 \le i \le n, 1 \le j \le m}$ ovat $m \times n$ R-kertoimiset matriisit, niiden summa $A + B$ on R-kertoiminen matriisi $(a_{ij}+b_{ij})_{1 \le i \le n, 1 \le j \le m}$. Jos $r \in R$, niin matriisi rA on matriisi $(ra_{ij})_{1 \le i \le n, 1 \le j \le m}$. Ei ole vaikeata tarkistaa, että näin määritellyt operaatiot määrittelevät R-modulin struktuurin $(n \times m)$-matriisien joukossa. Itse asiassa helposti nähdään seuraava väite todeksi.

Lemma 2.25. *$M(n \times m; R)$ on R-modulina isomorfinen modulin R^{nm} kanssa. Erityisesti $M(n \times m; R)$ on nm-ulotteinen R-moduli.*

Todistus. Määritellään kuvaus $L\colon M(n \times m; R) \to R^{nm}$ seuraavasti. Olkoon

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix}$$

matriisi. Asetetaan $L(A)$:ksi jono

$$(a_{11}, a_{12}, \ldots, a_{1m}, a_{21}, a_{22}, \ldots, a_{2m}, a_{31}, ..., a_{i1}, a_{i2}, \ldots, a_{n1}, \ldots, a_{nm}),$$

missä siis ensin kootaan ensimmäisen rivin alkiot, sitten toisen riivin alkiot ja niin edelleen.
Helposti nähdään, että L on lineaarinen isomorfismi.
Koska oletamme, että R on ykkösellinen, moduli R^{nm} on vapaa (esimerkki 2.17) ja nm-ulotteinen. Väite seuraa. □

Olemme edellisessä lemmassa konstruoineet isomofismin $R^{nm} \to M(n \times m; R)$. Koska R^{nm}:llä on standardikanta $(e_1, \ldots, e_n)$ (kts. esimerkki 2.17), $M(n \times m; R)$:llä on vastaava kanta $(e_{ij})_{i=1,\ldots,n, j=1,\ldots,m}$, josta käytämme myös nimitystä *standardikanta*. Huomaa, että e_{ij} on siis tasan sellainen matriisi, jonka (i, j)-alkio on 1 ja muut alkiot nolleja.

Olkoot M ja N äärellisulotteiset R-modulit. Olkoon $\mathbf{e}$ eräs M:n kanta $(e_1, \ldots, e_m)$ (järjestetty jono) ja samoin olkoon $\mathbf{f}$ eräs N:n kanta $(f_1, \ldots, f_n)$. Olkoon $L\colon M \to N$ R-lineaarinen kuvaus. Olemme yllä määritelleet jo *L:n matriisi kantojen $\mathbf{e}$ ja $\mathbf{f}$ suhteen*. Se on matriisi

$$[L]_{\mathbf{f},\mathbf{e}} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix},$$

jonka kertoimet a_{ij} määräytyvät yhtälöistä

$$L(e_j) = \sum_{i=1}^{n} a_{ij} f_i.$$

Siis toisen sanojen matriisin $[L]_{\mathbf{f},\mathbf{e}}$ j'nnes sarake saadaan laitamalla sinne M:n kannan alkion e_j kuvan $L(e_j)$ koordinaatit N:n kannan suhteen.
Propositiosta 2.22 seuraa helposti seuraava väite.

Propositio 2.26. *Olkoot M ja N äärellisulotteiset R-modulit. Olkoon $\mathbf{e}$ eräs M:n kanta $(e_1, \ldots, e_m)$ ja olkoon $\mathbf{f}$ eräs N:n kanta $(f_1, \ldots, f_n)$. Tällöin kuvaus $\Phi\colon L(M, N) \to M(n \times m; R)$, $\Phi(L) = [L]_{\mathbf{f},\mathbf{e}}$ on Abelin ryhmien isomorfismi. Jos R on kommutatiivinen, Φ on R-modulien lineaarinen isomorfismi. Erityisesti, jos R on kommutatiivinen ja ykkösellinen rengas, ja M on m-ulotteinen, N on n-ulotteinen R-modulit, niin $L(M, N)$ on mn-ulotteinen R-moduli.*

Todistus. Olkoon $[L]_{\mathbf{f},\mathbf{e}} = (a_{ij})$ ja $[L']_{\mathbf{f},\mathbf{e}} = (b_{ij})$. Tällöin määritelmän mukaan

$$L(e_j) = \sum_{i=1}^{n} a_{ij} f_i, \text{ ja}$$

$$L'(e_j) = \sum_{i=1}^{n} b_{ij} f_i,$$

joten

$$(L + L')(e_j) = \sum_{i=1}^{n} (a_{ij} + b_{ij}) f_i.$$

Näin ollen

$$\Phi(L + L') = [L + L']_{\mathbf{f},\mathbf{e}} = [L]_{\mathbf{f},\mathbf{e}} + [L']_{\mathbf{f},\mathbf{e}}.$$

Jos R on kommutatiivinen, samalla tavalla nähdään, että

$$\Phi(rL) = r[L]_{\mathbf{f},\mathbf{e}}.$$

Osoitetaan, että Φ on bijektio. Oletetaan, että $A = (a_{ij})$ on $(n \times m)$-matriisi, jonka kertoimet ovat renkaassa R. Proposition 2.22 nojalla on olemassa lineaarinen kuvaus $L\colon M \to N$, jolle

$$L(e_j) = \sum_{i=1}^{n} a_{ij} f_i.$$

Tällöin $\Phi(L) = A$. Näin ollen Φ on surjektio.
Oletetaan, että $\Phi(L) = \Phi(L')$, tällöin kuvauksen Φ määritelmän nojalla jokaisella $i = 1, \ldots, n$ pätee $L(e_i) = L'(e_i)$. Propositiosta 2.22 seuraa tällöin, että $L = L'$. Näin ollen Φ on isomrofismi.

Olemme todistaneet, että $L(M, N)$ on isomorfinen modulin $M(n \times m; R)$ kanssa (edellyttäen, että R on vaihdannainen). Toisaalta Lemman 2.25 nojalla viimeksi mainittu on isomorfinen modulin R^{nm}:n kanssa ja erityisesti nm-ulotteinen. Näin ollen myös $L(M, N)$ on nm-ulotteinen. □

Juuri todistettu propositio sanoo siis, että äärellisulotteisten modulien M, N tapauksessa voimme samaistaa lineaariset kuvaukset $M \to N$ ja $m \times n$-matiisit (missä m on N:n kannan koko ja n on M:n kannan koko). Tämä on hyvin hyödyllinen näkökulma käytännössä - usein kannattaa ajatella lineaariset kuvaukset ja vastaavat matriisit ”samana asiana”, kahtena eri tapana käsitellä ja kuvata ”sama objekti”. Riippuen tilanteesta joskus on kätevämpää ajatella tämä objekti lineaarisena kuvauksena, joskus taas matriisina. Näemme jatkossa paljon esimerkkejä tästä.
Täytyy kuitenkin ehdottomasti muistaa, että tämä vastaavuus lineaaristen kuvausten ja matriisien välillä **riippuu kantojen valinnasta**! Toisin sanoen se ei ole koskaan absoluuttinen ja ennalta kiinnitetty. Vaihtamalla kannat saadaan samalle lineaariselle kuvaukselle erilaisen matriisiesityksen.

Esimerkiksi olemme aikaisemmin konstruoineet matriisiavaruudelle $M(n \times m; R)$ luonnollisen kannan e_{ij}, missä matriisin e_{ij} (i, j)-alkio on tasan $1 \in R$ ja muut alkiot nollia. Käytämällä sitä, että kuvaus Φ on isomorfismi, voimme nyt konstuoida konkrettisen kannan avaruudelle $L(M, N)$.
Olkoon $\mathbf{e}$ eräs M:n kanta $(e_1, \ldots, e_m)$ ja olkoon $\mathbf{f}$ eräs N:n kanta $(f_1, \ldots, f_n)$.

Jokaisella $i = 1, \ldots, n$ ja $j = 1, \ldots, m$ Lemman 2.22 on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varepsilon_i^j \colon M \to N$ siten, että $L_i^j(e_j) = e_i$ ja $L_j^i(e_k) = 0$ kaikilla $k \neq j$. Määritelmästä seuraa heti, että

$$\Phi(\varepsilon_i^j) = [\varepsilon_i^j]_{\mathbf{f},\mathbf{e}} = e_{ij}.$$

Koska Φ on modulien välinen isomorfismi saamme seuraavan tuloksen.

Seuraus 2.27. *Olkoot M ja N äärellisulotteiset R-modulit. Olkoon $\mathbf{e}$ eräs M:n kanta $(e_1, \ldots, e_m)$ ja olkoon $\mathbf{f}$ eräs N:n kanta $(f_1, \ldots, f_n)$. Tällöin*

$$\{\varepsilon_i^j \mid i = 1, \ldots, n, j = 1, \ldots, m\}$$

on $L(M, N)$:n kanta.

Olkoon R ykkösellinen rengas ja olkoon $n \in \mathbb{N}$ mielivaltainen. On olemassa vapaa R-moduli M, jolla on tasan n alkion kokoinen kanta $\mathbf{e} = \{e_1, \ldots, e_n\}$, esimerkiksi R^n. Identtinen kuvaus $I \colon M \to M$ on aina lineaarinen kuvaus. Helposti nähdään, että tämän kuvauksen matriisi $[I]_{\mathbf{e},\mathbf{e}}$ (huom., sama kanta molemmilla puolella!) on niin sanottu *yksikkö-matriisi* $I_n = (\delta_{ij})_{i,j=1,\ldots,n} \in M(n \times n; R)$, jonka kertoimet ovat määriteltyjä ehdoilla

$$\delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Jokaiseen R-kertoimiseen matriisin $A = (a_{ij}) \in M(n \times m; R)$ voidaan liittää tasan yksi lineaarinen kuvaus $L_A \colon R^m \to R^n$, jonka matriisi R^m:n ja R^n:n **standardikantojen** suhteen on A. Tämä on kuvaus, jolle pätee $L(e_j) = \sum_{i=1} a_{ij} e_i$ eli kuvaus, joka on määritelty kaavalla

$$L_A(x_1, \ldots, x_m) = (y_1, \ldots, y_n), \text{ missä}$$

$$y_i = \sum_{j=1}^{n} x_j a_{ij}$$

(tarkista! huomaa järjestys!). Samastuksen $A \leftrightarrow L_A$ kautta voimme ajatella jokainen matriisi lineaarikuvauksena kanonisella tavalla. Tämä on siis tekninen, täsmällinen versio periaatteesta "matriisi on lineaarikuvaus". Huomaa, että pätee

$$L_{A+B} = L_A + L_B$$

ja, vaihdannaisen renkaan R tapauksessa,

$$L_{rA} = rL_A.$$

vastaavuus $A \mapsto L_A$ on siis paitsi bijektio, myös R-lineaarinen (tai ainakin Abelien ryhmien välinen) isomorfismi $M(n \times m; R) \to L(R^m, R^n)$.

Aikaisemmin olemme näyttäneet, miten lineaariseen kuvaukseen liitetään matriisi. Nyt olemme keksineet käänteisen tempun - tavan liittää matriisiin lineaarinen kuvaus. Huomaa, että tässä piilee kuitenkin pieni epäsymmetrisyys - annettuun lineaariseen kuvaukseen voidaan liittää monta erilaista matriisia, mutta matriisiin liitämme yksi tietty fiksattu lineaarinen kuvaus.

- Kuvausten yhdistäminen ja matriisien kertolasku.
Koska lineaariset kuvaukset ovat kuvauksia, niitä voi yhdistää silloin kuin toisen kuvauksen maalijoukko on sama kuin toisen kuvauksen lähtöjoukko. Toisin sanoen jos $L\colon M \to N$ ja $L'\colon N \to P$ ovat R-lineaarisia kuvauksia R-modulien välillä, on olemassa yhdistetty kuvaus $L' \circ L\colon M \to P$. Helposti nähdään, että myös $L' \circ L$ on lineaarinen kuvaus. Usein jätetään symboli $\circ$ kirjoittamatta ja merkitään yhdistetty kuvaus yksinkertaisesti $L'L$.

Kuvausten yhdistäminen määrittelee kuvauksen $\circ\colon L(N,P) \times L(M,N) \to L(M,P)$, joka voidaan ajatella "kertolaskuna". Tämä ei kuitenkaan ole yleisesti ottaen mikään laskutoimitus, sillä joukot $L(N,P), L(M,N)$, ja $L(M,P)$ voivat kaikki olla eri joukot.
Kuvausten yhdistäminen toteuttaa tärkeitä algebrallisia yhtälöitä. Olkoot $L, L_1, L_2\colon M \to N, L', L'_1, L'_2\colon N \to P$ R-lineaariset kuvaukset ja olkoot $r, r' \in R$. Tällöin helposti nähdään (harjoitustehtävä), että

$$L'(L_1 + L_2) = L'L_1 + L'L_2, ja \tag{2.28}$$

$$(L'_1 + L'_2)L = L'_1L + L'_2L. \tag{2.29}$$

Jos R on kommutatiivinen, niin lisäksi

$$r(L'L) = (rL')L = L'(rL). \tag{2.30}$$

Jos $L''\colon P \to Q$, niin selvästi $(L''L')L = L''(L'L)$, sillä kuvausten yhdistäminen on tunnetusti assosiatiivinen operaatio. Jos 1_M:llä merkitään identtistä kuvausta $\mathrm{id}\colon M \to M$, pätee myös

$$L'1_M = L'$$

$$1_{M'}L = L.$$

Kun valitaan $M = M' = M''$ yllä, yhdistämisen operaatiosta tulee kuvaus $\circ\colon L(M) \times L(M) \to L(M)$ eli siis *laskutoimitus* joukossa $L(M)$.

Olettaen, että R on kommutatiivinen rengas, joukossa $L(M)$ on siis määritelty rikas algebrallinen struktuuri - se on R-moduli ja lisäksi sen alkiolle on määritelty assosiatiivinen kertolasku $\circ$, joka toteuttaa ehdot (2.28), (2.29) ja (2.30). Tällä kertolaskulla on neutraalialkio 1_M.
Tämän tyyppisiä algebrallisia olioita sanotaan *algebroiksi*.

Määritelmä 2.31. *Olkoon R rengas. R-algebra on systeemi $(A, +, \cdot, \odot)$, missä $(M, +, \cdot)$ on R-moduli ja $(A, +, \odot)$ on rengas. Lisäksi oletetaan, että kaikilla $r \in R, a, b \in A$ pätee*

$$(ra) \odot b = r(a \odot b) = a \odot (rb).$$

Algebra on ykkösellinen jos se on renkaana ykkösellinen.

Algebran laskutoimitusta $\odot$ sanotaan yleensä algebran *kertolaskuksi* ja merkitään usein $a \odot b = ab$. Algebran kertolaskun ei tarvitse olla kommutatiivinen. Itse asiassa helposti nähdään että yllä määritelty algebra $L(M)$ on yleensä ei-kommutatiivinen.
Joukon $L(M)$ alkio $L\colon M \to M$ on kääntyvä kertolaskun suhteen jos ja vain jos se on isomorfismi eli bijektio. Käänteisalkio on silloin käänteiskuvaus L^{-1} (on helppo nähdä että isomorfismin käänteiskuvaus on myös lineaarinen).

Tutkimme seuraavaksi mikä on yhdistetyn kuvauksen $L' \circ L$ matriisi. Olkoot M, N, P äärellisulotteiset R-modulit. Kiinnitetään M:n kanta $\mathbf{e} = e_1, \ldots, e_n$, N:n kanta $\mathbf{f} = \{f_1, \ldots, f_m\}$ ja P:n kanta $\mathbf{g} = \{g_1, \ldots, g_p\}$. Olkoon $B = (b_{jk})_{1 \le j \le m, 1 \le k \le n}$ L:n matriisi $[L]_{\mathbf{f},\mathbf{e}}$ kantojen $\mathbf{e}$ ja $\mathbf{f}$ suhteen ja vastaavasti olkoon $A = (a_{ij})_{1 \le i \le p, 1 \le j \le m}$ kuvausen L' matriisi $[L]_{\mathbf{f}',\mathbf{f}}$ kantojen $\mathbf{f}$ ja $\mathbf{f}'$ suhteen. Tällöin siis kaikilla $k = 1, \ldots, n$

$$L(e_k) = \sum_{j=1}^{m} b_{jk} f_j,$$

ja kaikilla $j = 1, \ldots, m$

$$L'(f_j) = \sum_{i=1}^{p} a_{ij} g_i.$$

Tästä saadaan, että

$$L'L(e_k) = L'(\sum_{j=1}^{m} b_{jk} f_j) = \sum_{j=1}^{m} b_{jk} L'(f_j) = \sum_{j=1}^{m} b_{jk} (\sum_{i=1}^{p} a_{ij} g_i) = \sum_{i=1}^{p} (\sum_{j=1}^{m} b_{jk} a_{ij}) g_i.$$

Näin ollen $L'L$:n matriisi kantojen $\mathbf{e}$ ja $\mathbf{g}$ suhteen on $(p\times)$-matriisi $(c_{ik})_{1 \le i \le p, 1 \le k \le n}$, missä

$$c_{ik} = \sum_{j=1}^{n} b_{jk} a_{ij}.$$

Tämä lasku motivoi seuraavan määritelmän.

Määritelmä 2.32. *Olkoot R rengas, $n, m, p \in \mathbb{N}$, $A \in M(p \times m; R)$, $B \in M(m \times n; R)$. Tällöin A:n ja B:n* matriisitulo *AB on $(p \times n)$ R-kertoiminen matriisi $C = (c_{ik})$, missä*

$$c_{ik} = \sum_{j=1}^{m} b_{jk} a_{ij}$$

kaikilla $i = 1, \ldots, n, k = 1, \ldots, p$.

Kahden matriisin A ja B tulo AB on siis määritelty täsmälleen silloin kun A:ssä on sama määrä sarakkeita kuin B:ssä on rivejä. Kun R on kommutatiivinen, yllä annettu tulon määritelmä voidaan kirjoittaa myös muotoon

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk},$$

josta lukija tunnistaa tutun "kerro i:s rivi k:nnellä sarakkeella"-säännön. Matriisin tulon määritelmää edeltävä tarkastelu antaa heti seuraavan tärkeän tuloksen.

Propositio 2.33. *Olkoot M, N, P äärellisulotteiset R-modulit. Olkoon $\mathbf{e} = e_1, \ldots, e_n$ M:n kanta, $\mathbf{f} = \{f_1, \ldots, f_m\}$ N:n kanta ja $\mathbf{g} = \{g_1, \ldots, g_p\}$ P:n kanta. Olkoot $L\colon M \to N$ ja $L'\colon N \to P$ R-lineaariset kuvaukset. Tällöin*

$$[L'L]_{\mathbf{g},\mathbf{e}} = [L']_{\mathbf{g},\mathbf{f}} [L]_{\mathbf{f},\mathbf{e}}.$$

Kanoninen vastaavuus $A \mapsto L_A$, $M(n \times m; R) \to L(R^m, R^n)$ "kommutoi" matriisien kertolaskun ja lineaarikuvausten yhdistämisoperaation kanssa. Täsmällisesti sanottuna, olkoon $B \in M(p \times n; R)$. Tällöin voimme muodostaa matriisin $BA \in M(p \times m; R)$, jota vastaa lineaarikuvaus $L_{BA}\colon R^m \to R^p$. Voimme myös muodostaa yhdistetty kuvaus $L_B L_A\colon R^m \to R^p$. Tutkimalla standardikantojen kuvavektoreita molempien kuvausten tapauksessa, nähdään, että ne ovat samat. Näin ollen

$$L_{BA} = L_B L_A.$$

Olkoot M ja N äärellisulotteiset R-modulit ja olkoot $\mathbf{e} = e_1, \ldots, e_n$ M:n kanta, $\mathbf{f} = \{f_1, \ldots, f_m\}$ N:n kanta. Tällöin voimme näiden kantojen avulla identifioida M modulin R^n kanssa ja N modulin R^m kanssa. Täsmällisemmin sanottuna, voimme määritellä lineaarisen isomorfismin $\phi_M\colon M \to R^n$ joka kuvaa kannan $\mathbf{e}$ standardikannaksi. Samoin voimme määritellä isomorfismin $\phi_N\colon N \to R^m$. Voimme kysyä mitä lineaarista kuvausta $R^n \to R^m$ annettu

lineaarinen kuvaus $L\colon M \to N$ vastaa tällöin. Tämä on siis kuvaus $L' = \phi_N \circ L \circ \phi_M^{-1}$, mutta voidaanko ilmaistaa sen matriisin $A = [L]_{\mathbf{f},\mathbf{e}}$ avulla?
Olkoon $x = (x_1, \ldots, x_n) \in R^n$. Tällöin määritelmän mukaan

$$\phi_M^{-1} = \sum_{i=1}^{n} x_i e_i,$$

joten

$$L \circ \phi_M `-1 = \sum_{i=1}^{n} x_i L(e_i) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i a_{ij} f_j = \sum_{j=1}^{m}(\sum_{i=1}^{n} x_i a_{ij})).$$

Isomorfismin ϕ_N määritelmän nojalla saamme siis, että

$$L'(x_1, \ldots, x_n) = (y_1, \ldots, y_m), \text{ missä}$$

$$y_j = (\sum_{i=1}^{n} x_i a_{ij})),$$

toisin sanoen $L' = L_A$.
Nyt, kun käytössämme on matriisien kertolasku, voimme muotoilla L_A:n määritelmän uudestaan sen avulla. Jos tulkitsemme R^n:n alkio $x = (x_1, \ldots, x_n)$ niin sanotuksi "pystyvektoriksi", eli $n \times 1$-matriisina

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix},$$

ja samalla tavalla tulkitsemme $y \in R^m$ $m \times 1$-matriisina

$$y = \begin{pmatrix} y_1 & y_2 & \ldots & y_n \end{pmatrix},$$

voimme kirjoittaa L_A:n määritelmä muodossa $L_A(x) = Ax$.

Vastaavuuden $A \leftrightarrow L_A$ kautta voidaan ajatella matriisi A lineaarisena kuvauksena, voimme myös yleistä kaikki lineaarisiin kuvauksiin liittyvät käsitteet matriiseihin. Voimme siis puhua esim. matriisin A ytimestä, kuvajoukosta, ominaisarvoista jne. Tällöin siis tarkoitamme vastaavan lineaarisen kuvauksen L_A ydintä, ominaisarvoa jne. Teemme näin usein jatkossa.
Joskus haluamme tehdä päinvastaisen asian eli yrittää yleistää matriiseihin liittyviä käsitteittä lineaarisiin kuvauksiin. Tällöin kuitenkin pitää aina tarkistaa, että kyseinen olio on hyvinmääritelty, eli ei riipu siitä, minkälaisten

kantojen, tai millaisen kannan suhteen esitämme kuvaus matriisina. Esimerkiksi vaikka voimme puhua matriisin $(1,1)$-alkiosta a_{11}, mitään vastaava lukua emme voi kuvaukselle määritellä, sillä se riippuisi esityksestä. Sen sijaan esimerkiksi determinantin (joka ensin määritellään matriisille) voimme kuvaukselle määritellä, sillä se on sama riippumatta siitä, missä kannassa kuvaus esitetään (tähän palataan myöhemmin).

Olemme jo aikaisemmin näyttäneet, että vastaavuus $\Psi\colon M(m \times n; R) \to L(R^m, R^n)$, missä $\Psi(A)$ on lineaarinen kuvaus $L_A\colon R^n \to R^m$ säilyttää kaikki laskuoperaatiot, eli matriisien/kuvausten yhteenlasku, skalaarikertolasku, kertolasku (yhdistäminen).
Tätä vastaavuutta käyttämällä voimme heti päätellä, että matriisien laskuoperaatiot, esimerkiksi kertolasku, toteuttavat samoja algebrallisia ominaisuuksia, kuin vastaavat lineaaristen kuvausten operaatiot. Muun muassa seuraavat kaavat pätevät, aina kun siinä esiintyvät symbolit ja laskutoimitukset ovat hyvin määriteltyjä,

$$(AB)C = A(BC) \tag{2.34}$$

$$A(B + C) = AB + AC, \tag{2.35}$$

$$(A + B)C = AC + BC, \tag{2.36}$$

$$1A = A1 = A, \tag{2.37}$$

ja lisäksi

$$r(AB) = (rA)B = A(rB), \tag{2.38}$$

jos rengas R on kommutatiivinen.

Tässä 1 on yksikkömatriisi (δ_{ij}).

Edellä esitetty päättely on mainio esimerkki siitä, miten lineaaristen kuvausten näkökulma matriiseihin helpottaa niiden ominaisuuksien tutkiminen. Esimerkiksi matriisitulon assosiatiivisuuden $(AB)C = A(BC)$ todistus suoraan matriisitulon määritelmästä olisi puuduttava, formaali, ei-motivoitu lasku, täynnä indeksien pyörittelyjä ja monimutkaisen näköisiä välivaiheita. Sen sijaan kun käytetään hyväksi matriisien ja lineaaristen kuvausten vastaavuutta hyväksi, väite on selvä ja luonnollinen, sillä kuvausten yhdistäminen

on liitännäinen operaatio (ja sen todistaminen on yhden rivin helppo lasku).

Kun edellä todistetut matriisilaskutoimitusten ominaisuudet tarkastellaan neliömatriisien erikoistapauksessa, saadaan seuraavat tärkeät tulokset.

Seuraus 2.39. *Olkoon R ykkösellinen rengas ja $n \in N$. Tällöin $(n \times n)$-matriisien joukko $M(n \times n; R)$ on ykkösellinen rengas (matriisien yhteen- ja kertolaskun suhteen). Jos R on kommutatiivinen, $M(n \times n)$ on R-algebra.*

Seuraus 2.40. *Olkoon M äärellisulotteinen vapaa R-moduli ja $\mathbf{e} = (e_1, \ldots, e_n)$ sen kanta. Tällöin kuvaus $\Phi\colon L(M) \to M(n \times n)$, $L \mapsto [L]_{\mathbf{e},\mathbf{e}}$ on bijektio, joka säilyttää kaikki molemmissa joukoissa määritetyt operaatiot. Erityisesti, jos R on vaihdannainen rengas, Φ on R-algebrojen isomorfismi.*

-**Kantojen vaihto**.
Palautetaan vielä mieleen, miten kantojen vaihto vaikuttaa lineaarisen kuvauksen matrisiin.
Olkoon M äärellisulotteinen R-moduli ja olkoot $\mathbf{e} = (e_1, \ldots, e_n)$ ja $\mathbf{f} = (f_1, \ldots, f_n)$ sen (mahdollisesti eri) kannat (periaatteessa voi käydä, että M:llä on eripituisia kantoja, mutta koska meitä kiinnostavissa tapauksissa, esimerkiksi vektoriavaruuksien kohdalla, näin ei voi käydä, oletamme nyt heti, että molemmissa kannoissa on sama määrä alkioita). Olkoon $A = (a_{ij})$ identtisen kuvauksen $\mathrm{id}\colon M \to M$ matriisi $[\mathrm{id}]_{\mathbf{f},\mathbf{e}}$ kantojen $\mathbf{e}$ ja $\mathbf{f}$ suhteen. Tällöin siis kertoimet a_{ij} määräytyvät esityksistä

$$\mathrm{id}(e_j) = e_j = \sum_{i=1}^{n} a_{ij} f_i.$$

Toisin sanoen esitetään ensimmäisen kannan alkiot toisen kannan alkioiden yksikäsitteisenä lineaarisina kombinaatioina ja poimitaan matriisin kertoimet niistä. Tällainen matriisi sanotaan *kannanvaihtomatriisiksi* ja merkitään $[\bar{f} \mid \bar{e}]$.
Samalla tavalla voimme esittää jokainen alkio f_i kannan $\mathbf{e}$ avulla,

$$f_i = \sum_{j=1}^{n} b_{ji} e_j,$$

missä b_{ji} ovat kannavaihtomatriisin $B = [\mathbf{e} \mid \mathbf{f}]$ kertoimet. Propositiosta 2.33 seuraa, että

$$AB = [\mathrm{id}]_{\mathbf{f},\mathbf{e}} \cdot [\mathrm{id}]_{\mathbf{e},\mathbf{f}} = [\mathrm{id} \circ \mathrm{id}]_{\mathbf{e},\mathbf{e}} = [\mathrm{id}]_{\mathbf{e},\mathbf{e}} = I_n.$$

Samoin $BA = \mathrm{id}$. Toisin sanoen kannanvaihtomatriisi $[\bar{f} \mid \bar{e}]$ on aina kääntyvä ja sen käänteismatriisi on itse asiassa kannanvaihtomatriisi $[\bar{e} \mid \bar{f}]$ missä kannat otetaan päinvastaisessa järjestyksessä).

Tarkastellaan nyt yleinen tilanne. Olkoon $L\colon M \to N$ R-lineaarinen kuvaus. Olkoot $\mathbf{e_1}, \mathbf{e_2}$ modulin M eri kannat ja samoin olkoot $\mathbf{f_1}, \mathbf{f_2}$ N:n eri kannat. Tällöin triviaali havainto, että $L = \mathrm{id}_N \circ L \circ \mathrm{id}_M$ ja Propositio 2.33 yhdessä antavat, että

$$[L]_{\mathbf{f_2},\mathbf{e_2}} = [\mathrm{id}]_{\mathbf{f_2},\mathbf{f_1}} \cdot [L]_{\mathbf{f_1},\mathbf{e_1}} \cdot [\mathrm{id}]_{\mathbf{e_1},\mathbf{e_2}} = [\mathbf{f_2} \mid \mathbf{f_1}] \cdot [L]_{\mathbf{f_1},\mathbf{e_1}} \cdot [\mathbf{e_2} \mid \mathbf{e_1}]^{-1}.$$

Toisin sanoen, jos Y on matriisi $[L]_{\mathbf{f_2},\mathbf{e_2}}$ (esitys "uusien" kantojen suhteen), X on matriisi $[L]_{\mathbf{f_1},\mathbf{e_1}}$ (esitys "vanhojen" kantojen suhteen), A on kannanvaihtomatriisi $[\mathbf{e_2}, \mathbf{e_1}]$ (vaihdetaan kannat M:ssä) ja B on kannanvaihtomatriisi $[\mathbf{f_2}, \mathbf{f_1}]$ (vaihdetaan kannat N:ssä), uusi esitys Y saadaan vanhasta esityksestä X kaavalla

$$Y = BXA^{-1}.$$

Erityisen tärkeä erikoistapaus tästä saadaan, kun tarkastellaan lineaarisen kuvauksen $L\colon M \to M$ esityksiä eri kannoissa. Lineaarinen kuvaus $L\colon M \to M$ (jolla siis on samat lähtö- ja maalimoduli) sanotaan modulin M *endomorfismiksi*. Jos $\mathbf{e} = (e_1, \ldots, e_n)$ on M:n kanta, L:n matriisi $[L]_{\mathbf{e},\mathbf{e}}$ (huom., sama kanta molemmilla puoleella!) merkitään yksinkertaisuuden vuoksi vain $[L]_{\mathbf{e}}$.
Oletetaan, että $\mathbf{f}$ on M:n toinen kunta. Tällöin

$$[L]_{\mathbf{f}} = [\mathbf{f} \mid \mathbf{e}][L]_{\mathbf{e}}[\mathbf{f} \mid \mathbf{e}]^{-1}.$$

Jos merkitään $Y = [L]_{\mathbf{f}}$, $X = [L]_{\mathbf{e}}$ ja $A = [\mathbf{f} \mid \mathbf{e}]$, tämä voi kirjoittaa muotoon $Y = AXA^{-1}$.
Kaksi samankokoista neliömatriisia Y ja X sanotaan *similarisiksi* jos on olemassa kääntyvä neliömatriisi A jolle $Y = AXA^{-1}$.

-Yleiset lineaariset ryhmät.
Seuraavaksi tarkastellaan niin sanotut yleiset lineaariset ryhmät.

Lemma 2.41. *Olkoon $(R, +, \cdot)$ ykkösellinen rengas. Merkitään*

$$R^* = \{r \in R \mid \text{ on olemassa } r^{-1}\}.$$

Tällöin $(R^*, \cdot)$ on ryhmä.

Todistus. Harjoitustehtävä. □

Olkoon R rengas ja M R-moduli. Lineaarikuvaukset $L\colon M \to M$ muodostavat renkaan $(L(M), +, \circ)$ kuvausten yhteenlaskun ja yhdistämisen suhteen. Edellisen lemman nojalla kaikki lineaariset bijektiot eli isomorfismit $L\colon M \to M$ muodostavat ryhmän $L(M)^*$ kuvausten yhdistämisen suhteen. Tämä ryhmä merkitään myös $GL(M)$ ja sanotaan modulin M *yleiseksi lineaariseksi ryhmäksi* (engl. general linear group). Se on kaikkien $M \to M$ bijektioiden $\mathrm{Perm}(M)$ ryhmän aliryhmä.

Seuraavaksi oletamme, että R on ykkösellinen, $n \in \mathbb{N}$, ja tarkastellaan $(n \times n)$ R-kertoimisten matriisien muodostamaa rengasta $(M(n \times n; R, +, \cdot)$, missä $\cdot$ on matriisien kertolasku.

Lemmasta 2.41 seuraa, että kääntyvät $(n \times n)$-matriisit muodostavat ryhmän matriisien kertolaskun suhteen. Tätä ryhmää merkitään $GL(n; R)$ ja sanotaan myös *yleiseksi lineaariseksi (matriisi)ryhmäksi*. Yleisen lineaarisen ryhmän aliryhmiä sanotaan renkaan R *matriisiryhmiksi*. Matriisiryhmillä on tärkeä rooli algebrassa, topologiassa, differentiaaligeometriassa ja monissa muissa matematiikan osa-alueissa.
Myöhemmin törmäämme esim. sellaisiin matriisiryhmiin kuin $\mathbb{R}$-kertoimisten ortogonaalien matriisien ryhmään $O(n)$ ($\mathbb{R}^n$ kierrot), unitaristen matriisien ryhmään $U(n)$ ($\mathbb{C}^n$:n kierrot) jne.

Olkoot R ja Q renkaat ja $f\colon R \to Q$ rengasisomorfismi. Tällöin f selvästi määrittelee ryhmäisomorfismin $R^* \to Q^*$. Soveltamalla tämä havainto rengasisomorfismiin $\Phi\colon L(M) \to M(n \times n; R)$, saadaan seuraava tulos.

Seuraus 2.42. *Olkoon M äärellisulotteinen R-moduli, missä R on ykkösellinen rengas. Olkoon $\mathbf{e}$ M:n äärellinen kanta. Tällöin kuvaus $\Phi\colon GL(M) \to GL(n; R)$, $\Phi(L) = [L]_{\mathbf{e},\mathbf{e}}$ on ryhmäisomorfismi.*

Lopuksi tarkastelemme äärellisulotteisten vektoriavaruuksien välisiä lineaarisia kuvauksia ja niihin liittyviä matriiseja.

Propositio 2.43. *Olkoot V ja W äärellisulotteiset K vektoriavaruudet, missä K on kunta. Olkoon $L\colon V \to W$ K-lineaarinen kuvaus. Tällöin* $\operatorname{Ker} L$ *ja* $\operatorname{Im} L$ *ovat myös äärellisulotteiset. Lisäksi*

$$\dim \operatorname{Ker} L + \dim \operatorname{Im} L = \dim V.$$

Todistus. Koska $\operatorname{Ker} L$ ja $\operatorname{Im} L$ ovat äärellisulotteisten vektoriavaruuksien aliavaruudet, ne ovat äärellisulotteisiä (Lemma 2.18).
Lisäksi isomorfialauseesta 2.5 seuraa, että $\operatorname{Im} L$ on isomorfinen tekjämodulin $V/\operatorname{Ker} L$ kanssa, joten $\dim \operatorname{Im} L = \dim(V/\operatorname{Ker} L)$. Mutta Lemman 2.19 nojalla $\dim(V/\operatorname{Ker} L) = \dim V - \dim \operatorname{Ker} L$. Väite seuraa. □

Olkoot A ja B äärelliset joukot, joissa on molemmissa saman verran alkiota ja $f\colon A \to B$ mikä tahansa kuvaus. Tällöin tunnetusti f on injektio jos ja vain jos se on surjektio.
Edellisen tuloksen avulla voidaan helposti osoittaa, että samanlainen ominaisuus on lineaarisilla kuvauksilla äärellisulotteisten vektoriavaruuksien välillä. Voidaan siis ajatella, että äärellisulotteisilla avaruuksilla on vektoriavaruuksien teoriassa ikään kuin "sama rooli" kuin äärellisillä joukoilla on joukkojen teoriassa.

Seuraus 2.44. *Olkoon $L\colon V \to W$ K-lineaarinen kuvaus äärellisulotteisten vektoriavaruuksien välillä. Tällöin*

1) Jos $\dim V < \dim W$, L ei voi olla surjektio.

2) Jos $\dim V > \dim W$, L ei voi olla injektio.

3) Jos $\dim V = \dim W$, L on injektio jos ja vain jos se on surjektio.

Todistus. 1) Edellisen proposition nojalla pätee

$$\dim \operatorname{Ker} L + \dim \operatorname{Im} L = \dim V.$$

Erityisesti tästä seuraa, että $\operatorname{Im} L \leq \dim V$. Näin ollen, jos $\dim V < \dim W$, yhtälö $\operatorname{Im} L = W$ on mahdoton, eli L ei voi olla surjektio.
2) Samasta kaavasta seuraa, että jos L on injektio (eli $\operatorname{Ker} L = \{0\}$), niin $\dim imL = \dim V$. Mutta tällöin $\dim \operatorname{Im} L > \dim W$, mikä on mahdotonta Lemman 2.18 nojalla, sillä $\operatorname{Im} L$ on W aliavaruus.
3) L on injektio jos ja vain jos $\dim \operatorname{Ker} L = \{0\}$ eli jos ja vain jos $\dim \operatorname{Im} L = \dim V$. Kohdan 3) oletuksella tämä on sama asia kuin $\dim \operatorname{Im} L = \dim W$. Lemman 2.18 nojalla tämä voi toteuttua jos ja vain jos $\operatorname{Im} L = W$ eli L on surjektio.

□

Seuraava matriisien ominaisuus on todistettu "Lineaarialgebra ja matriisilaskenta" kurssilla monimutkaisten ja teknisten matriisioperaatioiden avulla. Nyt voimme johtaa sen paljon yksinkertaisemmin lineaaristen kuvausten teorian avulla.

Seuraus 2.45. *Olkoon K kunta ja $n \in \mathbb{N}$. Olkoon $A \in M(n \times n; K)$. Tällöin seuraavat väitteet ovat yhtäpitäviä.*

(1) A on kääntyvä eli sillä on olemassa käänteismatriisi A^{-1}.

(2) A:lla on vasemmanpuoleinen käänteisalkio joukossa $M(n \times n; K)$.

(3) A:lla on oikeanpuoleinen käänteisalkio joukossa $M(n \times n; K)$.

Todistus. Matriisia A vastaa lineaarinen kuvaus $L_A \colon K^n \to K^n$. Tällöin matriisi A on kääntyvä jos ja vain jos kuvaus L_A on bijektio eli isomorfismi. Edellisen korollarin nojalla kuvaus L_A on isomorfismi jos ja vain jos L_A on injektio jos ja vain jos L_A on surjektio.

Oletetaan esimerkiksi, että A:llä on vasemmanpuoleinen käänteisalkio $B \in M(n \times n; K)$ eli $BA = I$. Matriisia B vastaa lineaarinen kuvaus $L_B \colon K^n \to K^n$. Tällöin matriisiyhtälöä $BA = I$ vastaa kuvausten tasolla yhtälö $L_B \circ L_A = \mathrm{id}$. Tästä seuraa, että L_A on injektio, sillä jos $x, y \in K^n$ sellaiset, että $L_A(x) = L_A(y)$, niin

$$x = \mathrm{id}(x) = L_B(L_A(x)) = L_B(L_A(y)) = \mathrm{id}(y) = y.$$

Mutta jos L_A on injektio, se on bijektio (edellisen korollaarin nojalla), joten A on kääntyvä.

Samalla tavalla todistetaan, että (3)⇒(1). □

Korollaarin 2.44, 3) sovelletaan usein sillä tavalla, että huomataan eräs lineaarinen kuvaus olevan injektio, jolloin sen on pakko olla myös surjektio (jos lähtö- ja maaliavaruudet samaa dimensiota, tietysti). Injektiosuuden osoittaminen on yleensä helppo, pitää vain tarkistaa, että ydin on triviaali.
Esimerkiksi tarkastellaan jossakin kunnassa K lineaarista yhtälöryhmää

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n, \end{cases} \tag{2.46}$$

jossa on siis saman verran tuntemattomia ja yhtälöitä. Tähän liitetään K-lineaarinen kuvaus $L \colon K^n \to K^n$, joka on määritelty kaavalla

$$L(x_1, \ldots, x_n) = (y_1, \ldots, y_n),$$

$$y_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n.$$

Korollaarin 2.44 nojalla tämä on surjektio jos ja vain jos se on injektio. Selvästi L on injektio jos ja vain jos yhtälöryhmää 2.46 vastaavalla ns. *homogeenisella yhtälöryhmällä*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = 0 \end{cases} \tag{2.47}$$

on vain triviaali ratkaisu $x_1 = x_2 = \ldots = x_n = 0$. Tässä tapauksessa siis L on myös surjektio, joten yhtälöryhmällä 2.46 on aina ratkaisu, vieläkin yksikäsitteinen. Jos taas tällä homogeenisella yhtölöryhmällä on muitakin kuin triviaali ratkaisu, tästä seuraa, että L ei ole surjektio, joten, jos yhtälöryhmän kertoimet a_{ij} yllä kiinitetään, niin varmasti löytyy sellaset $b_1, \ldots, b_n$ joille yhtälöryhmällä 2.46 ei ole ratkaisuja. Jos taas ratkaisuja on, niitä on aina enemmän kuin yksi, äärettömän K tapauksessa jopa ääretön määrä (miksi?). Samoin voidaan analyysoida yleisempiä yhtälöryhmiä

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_m = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_m = b_2 \\ \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nm}x_m = b_n, \end{cases} \tag{2.48}$$

joissa tuntemattomien m määrä saattaa olla erilainen kuin yhtälöiden määrä n. Voimme taas tarkastella kuvausta $L\colon K^m \to K^n$

$$L(x_1, \ldots, x_m) = (y_1, \ldots, y_n),$$

$$y_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_m.$$

Jos $m > n$, niin L ei voi olla injektio. Näin ollen vastaavalla homogeenisella yhtälöllä on aina epätriviaali ratkaisu, jopa ääretön määrä ratkaisuja, jos kunta K on ääretön. Yleisellä ryhmällä 2.48 ei vältämättä ole ratkaisuja, sillä ei L:n tarvitse olla surjektio, mutta jos sillä on yksikin ratkaisu, sillä on muitakin ratkaisuja (lisätään johonkin ratkaisuun mikä tahansa homogeenisen yhtälöryhmän ratkaisu), eli ratkaisuja on nolla tai enemmän kuin yksi, äärettömän kunnan tapauksessa jopa ääretön määrä.
Jos $m < n$, L ei voi olla surjektio. Näin ollen kun kiinitetään kertoimet a_{ij} yhtälöryhmässä, niin aina löydy luvut $b_1, \ldots, b_n$ joilla yhtälöryhmällä ei ole ratkaisuja.

Annetaan vielä esimerkki äärellisulotteisten modulien välisistä kuvauksista, joille tulos 2.44 ei päde. Esimerkiksi ryhmähomomorfismi eli $\mathbb{Z}$-lineaarinen

kuvaus $L\colon \mathbb{Z} \to \mathbb{Z}, f(n) = 2n$ on injektio, mutta ei ole surjektio, vaikka $\mathbb{Z}$ on äärellisulotteinen. Samoin esim. kuvaus $L\colon \mathbb{Z}^2 \to \mathbb{Z}^2$, $L(x, y) = (2x - 4y, 2x + 4y)$ on injektio, mutta ei ole surjektio (mieti miksi).

2.4 Duaali-avaruus

Olemme kurssin edellisessä osassa törmänneet jatkuvasti tilanteisiin, joissa piti olettaa modulin kerroinrengas R vaihdannaiseksi ja ykköselliseksi, muuten monet hyödylliset tulokset eivät näytä pätevän ja teorian kulku muutenkin monimutkaistuu. Esimerkiksi yleisen renkaan tapauksessa lineaaristen kuvausten joukossa $L(M, M')$ ei pysty määrittelemään R-modulin struktuurin, R^n ei välttämättä ole n-ulotteinen R-moduli ja niin edellinen. Tästä syystä **oletamme tästä lähtien, että kaikki tarkasteltavat modulit ovat määriteltyjä *vaihdannaisen* ja *ykkösellisen* renkaan yli**. Olisimme tietenkin voineet asettaa tämä rajoitus heti alussa, kuten usein tehdäänkin kirjallisuudessa, jolloin monia poikkeustilanteita ei olisi edes syntynyt. Kuitenkin tällöin lukijalle olisi voinut jäädä epäselväksi tällaisen rajoituksen syyt, se ei olisi motivoitu. Tämän tekstin kirjoittaja on esimerkiksi vuosikausia ihmetellyt mistä syystä kaikissa alan teoksissa sovitaan heti alkuun " oletamme kaikki renkaat vaihdannaisiksi" ilman mitään perusteluja ja motivoivia esimerkkejä.

Olkoon M R-moduli. Rengas R on itse R-moduli luonnollisella tavalla, joten voimme muodostaa joukko $L(M, R) = \{L\colon M \to R \text{ on } R\text{-lineaarinen}\}$. Koska oletamme R vaihdannaiseksi, $L(M, R)$ on itse asiassa R-moduli (Propositio 2.20). Tätä modulia sanotaan M:n *duaaliksi* ja merkitään symbolilla M^*.
Olkoon M äärellisulotteinen R-moduli ja olkoon $\mathbf{e} = (e_1, \ldots, e_m)$ sen kanta. Propositiosta 2.22 seuraa, että jokaisella $j = 1, \ldots, m$ voimme määritellä (tasan yhden) R-lineaarisen kuvauksen $\varepsilon^j\colon M \to R$ jolle pätee

$$\varepsilon^j(e_i) = \begin{cases} 1, \text{ jos } j = i, \\ 0, \text{ jos } j \neq i. \end{cases}$$

Lause 2.49. *Olkoot M, $\mathbf{e} = (e_1, \ldots, e_m)$ ja ε^j, $j = 1, \ldots, m$ kuten yllä. Tällöin $\boldsymbol{\varepsilon} = (\varepsilon^1, \ldots, \varepsilon^m)$ on duaalin M^* kanta. Erityisesti M^* on myös äärellisulotteinen ja*

$$\dim M^* = \dim M.$$

Todistus. Tämä on erikoistapaus Korollarin 2.27 tuloksesta, kun valitaan $N = R$ ja sen kannaksi yhden alkion joukko $\{1\}$. □

Olkoon $\mathbf{e} = (e_1, \ldots, e_m)$ R-modulin M kanta. Yllä konstruoitua M^*:n kantaa $\boldsymbol{\varepsilon} = (\varepsilon^1, \ldots, \varepsilon^m)$ sanotaan kannan $\mathbf{e}$ *duaaliksi* kannaksi.

Lineaarikuvauksen duaali ja sen matriisi.
Duaalin konstruktio voidaan suorittaa myös modulien väliselle lineaariselle kuvaukselle. Olkoot M, N molemmat R-modulit ja $L\colon M \to N$ R-lineaarinen kuvaus. Olkoon $A\colon N \to R$ duaalin N^* alkio. Tällöin yhdistetty kuvaus $A \circ L$ on R-lineaarinen kuvaus $M \to R$ eli duaalin M^* alkio. Näin saadaan kuvaus $L^*\colon N^* \to M^*$, $L^*(A) = A \circ L$. Tämä kuvaus on R-lineaarinen, sillä kaikilla $A, B \in N^*$, $r \in R$ pätee

$$L^*(A + B) = (A + B) \circ L = A \circ L + B \circ L = L^*(A) + L^*(B),$$

$$L^*(rA) = (rA) \circ L = r(A \circ L) = rL^*(A).$$

Tämä konstruktio onnistuu jokaisella $L \in L(M, N)$, joten voimme määritellä kuvauksen $^*\colon L(M, N) \to L(N^*, M^*)$, $^*(L) = L^*$(huomaa, että $*$ vaihtaa modulien järjestyksen). Helposti nähdään, että * on R-lineaarinen. Mitä tulee kuvausten yhdistämiseen, niin *-operaatio "kääntää" niiden järjestystä. Täsmällisesti sanoen olkoon P myös R-moduli ja oletetaan, että $L'\colon N \to P$ on R-lineaarinen kuvaus. Tällöin $L'L\colon M \to P$ on myös R-lineaarinen, joten on olemassa $(L'L)^*\colon P^* \to M^*$. Olkoon $A\colon P \to R$ duaalin P^* alkio. Tällöin

$$(L'L)^*(A) = A \circ (L'L) = (A \circ L') \circ L = (L'^*(A)) \circ L = L^*(L'^*(A)) = (L^* \circ L'^*)(A).$$

Näin ollen

$$(L'L)^* = L^*L'^*. \tag{2.50}$$

Olkoot M, N äärellisulotteiset R-modulit ja olkoot $\mathbf{e} = (e_1, \ldots, e_m)$, $\mathbf{f} = (f_1, \ldots, f_n)$ vastaavasti M:n ja N:n kanta. Olkoon $L\colon M \to N$ R-lineaarinen kuvaus. Tällöin sillä on $(n \times m)$-matriisi $A = (a_{ij}) = [L]_{\mathbf{f},\mathbf{e}}$ näiden kantojen suhteen. Matriisin A kertoimet määräytyvät yhtälöistä

$$L(e_j) = \sum_{k=1}^{n} a_{kj} f_k, \;\; j = 1, \ldots, m.$$

Toisaalta on olemassa R-lineaarinen kuvaus $L^*\colon N^* \to M^*$ ja Lauseen 2.49 nojalla modulit N^*, M^* ovat molemmat myös äärellisulotteiset ja kantoja $\mathbf{e}$,$\mathbf{f}$ vastaavat M^*:n duaalikanta $\boldsymbol{\varepsilon}$ ja N^*:n duaalikanta $\boldsymbol{\eta}$. Kuvauksella L^* on

näiden duaalikantojen suhteen $(m \times n)$-matriisi $B = (b_{ji}) = [L^*]_{\boldsymbol{\varepsilon},\boldsymbol{\eta}}$. Mikä on taman matriisin yhteys matriisiin A? Tutkitaan asiaa. Määritelmän mukaan pätee

$$L^*(\eta^i) = \sum_{l=1}^{m} b_{li}\varepsilon^l$$

jokaisella $i = 1, \ldots, n$. Tämän yhtälön molemmalla puolella on lineaarinen kuvaus $M \to R$. Lasketaan tämän kuvauksen arvo modulin M alkiolla e_j, jokaisella $j = 1, \ldots, m$. Vasemmalla puoleella tällöin saadaan

$$(L^*(\eta^i)(e_j) = (\eta^i \circ L)(e_j) = \eta^i(\sum_{k=1}^{n} a_{kj}f_k) = \sum_{k=1}^{n} a_{kj}(\eta^i(f_k)) = a_{ij},$$

sillä $\eta^i(f_k) = \delta_{ik}$. Oikealla puoleella puolestaan saadaan

$$(\sum_{l=1}^{m} b_{li}\varepsilon^l)(e_j)) = \sum_{l=1}^{m} b_{li}\varepsilon_l(e_j) = b_{ji}.$$

Näin ollen kaikilla $i = 1, \ldots, m$, $j = 1, \ldots, n$

$$a_{ij} = b_{ji}.$$

Toisin sanoen matriisi B on matriisin A *transpoosi* A^T! Tästä saadaan siis luonnollinen "lineaarikuvauksellinen" tulkinta matriisin transpoosille.

Kurssilla "lineaarialgebra ja matriisilaskenta" on osoitettu (erikoistapauksessa $R = \mathbb{R}$), että matriisin transpoosi-operaatio toteuttaa seuraavat säännöt,

(2.51) $(A + B)^T = A^T + B^T$, kun A ja B ovat samankokoiset matriisit,

(2.52) $$(rA)^T = rA^T, A \in M(n \times m; R), m, n \in \mathbb{N},$$

(2.53) $(AB)^T = B^T A^T, A \in M(n \times m; R), B \in M(p \times n; R), n, m, p \in \mathbb{N}.$

Näiden todistukset suoraan transpoosin määritelmästä lähtien ovat formaaleja tylsiä indeksien pyöritelyjä (erityisesti viimeisen yhtälön kohdalla). Näytetään miten voimme taas kerran osoittaa niiden paikkansapitävyys yksinkertaisemmin käyttämällä lineaarikuvauksia. Jokaista matriisia $A \in M(n \times m; R)$ vastaa R-lineaarinen kuvaus $L_A \colon R^m \to R^n$. Voimme muodostaa duaali-kuvauksen $L_A^* \colon (R^m)^* \to (R^n)^*$. Käyttämällä duaalikuvauksen ominaisuuksia ja duaalikantoja, saadaan kaavat (2.51), (2.52) ja (2.53) osoitettua. Yksityiskohdat jätetään lukijalle mietittäväksi.

Seuraavaksi tutkitaan duaalikuvauksen L^* ydintä ja kuvajoukkoa.

Lemma 2.54. *Olkoon $L\colon M \to N$ R-lineaarinen kuvaus. Tällöin*

$$\operatorname{Ker} L^* = \{A \in N^* \mid A(x) = 0 \text{ kaikilla } x \in \operatorname{Im} L\}.$$

$$\operatorname{Im} L^* = \{A \in M^* \mid \operatorname{Ker} L \subset \operatorname{Ker} A\}.$$

Todistus. Harjoitustehtävä. □

Seuraus 2.55. *Olkoot V ja W äärellisulotteiset K-vektoriavaruudet, missä K on kunta. Olkoon $L\colon V \to W$ K-lineaarinen. Tällöin*

$$\dim \operatorname{Ker} L^* = \dim W - \dim \operatorname{Im} L, \text{ ja}$$

$$\operatorname{Im} L^* = \dim \operatorname{Im} L. \tag{2.56}$$

Todistus. Osoitetaan ensin, että

$$\dim \operatorname{Ker} L^* = \dim W - \dim \operatorname{Im} L.$$

Osajoukko $\operatorname{Im} L$ on avaruuden W aliavaruus, joten Lemman 2.18 nojalla W:llä on kanta $(e_1, \ldots, e_n)$ siten, että $(e_1, \ldots, e_k)$ on $\operatorname{Im} L$:n kanta. Tällöin W^*:llä on duaalikanta $\boldsymbol{\varepsilon} = (\varepsilon^1, \ldots, \varepsilon^n)$.
Edellisen lemman nojalla $\operatorname{Ker} L^*$ koostuu tasan niistä lineaarisista kuvauksista $A\colon W \to K$, joille $A|\operatorname{Im} L = 0$. Osoitetaan, että $A \in \operatorname{Ker} L^*$ jos ja vain jos $A(e_i) = 0$ kaikilla $i = 1, \ldots, k$ (eli kaikilla $\operatorname{Im} L$:n kannan alkiolla). Jos $A \in \operatorname{Ker} L^*$, eli $A \circ L = 0$, niin $A(x) = 0$ kaikilla $x \in \operatorname{Im} L$, erityisesti kaikilla $A(e_i) = 0$ kaikilla $i = 1, \ldots, k$. Kääntäen, oletetaan, että $A(e_i) = 0$ kaikilla $i = 1, \ldots, k$. Olkoon $x \in \operatorname{Im} L$. Koska $(e_1, \ldots, e_k)$ on $\operatorname{Im} L$:n kanta, on olemassa lineaarinen esitys

$$x = \sum_{i=1}^{k} a_i e_i.$$

Tällöin lineaarisuuden nojalla

$$A(x) = \sum_{i=1}^{k} a_k A(e_i) = 0.$$

Väite on osoitettu.

Seuravaaksi osoitetaan, että $\operatorname{Ker} L^*$ on vapaan jonon $(\varepsilon^{k+1}, \ldots, \varepsilon^n)$ virittämä, mistä seuraa, että $\dim \operatorname{Ker} L^* = n - k = \dim W - \dim \operatorname{Im} L$, eli se mitä

pitikin osoittaa.
Olkoon $A \in W^*$ mielivaltainen, tällöin on olemassa yksikäsitteinen lineaarinen esitys muodossa

$$A = \sum_{j=1}^{n} b_j \varepsilon^j.$$

Olemme edellä osoittaneet, että $A \in \operatorname{Ker} L^*$ jos ja vain jos $A(e_i) = 0$ jokaisella $i = 1, \ldots, k$, mikä on taas yhtäpitävä sen kanssa, että

$$b_i = \sum_{j=1}^{n} b_j \varepsilon^j(e_i) = A(e_i) = 0$$

jokaisella $i = 1, \ldots, k$. Näin ollen $\operatorname{Ker} L^*$ on täsmälleen aliavaruus $\operatorname{Span}\{\varepsilon_{k+1}, \ldots, \varepsilon_n\}$. Ensimmäinen väite on osoitettu. Proposition 2.43 nojalla saadaan

$$\dim \operatorname{Im} L^* = \dim W^* - \dim \operatorname{Ker} L^* = \dim W - (\dim W - \dim \operatorname{Im} L) = \dim \operatorname{Im} L.$$

□

Seuraus 2.57. *Olkoot V ja W äärellisulotteiset K-vektoriavaruudet, missä K on kunta. Olkoon $L\colon V \to W$ K-lineaarinen. Tällöin*

(1) L^* on injektio jos ja vain jos L on surjektio.

(2) L^* on surjektio jos ja vain jos L on injektio.

(3) L^* on bijektio jos ja vain jos L on bijektio.

Todistus. (1) L^* on injektio jos ja vain jos $\dim \operatorname{Ker} L^* = 0$. Edellisen korollaarin nojalla tämä on yhtäpitävä sen kanssa, että $0 = \dim W - \dim \operatorname{Im} L$, eli $\dim \operatorname{Im} L = \dim W$. Lemman 2.18 mukaan tämä on mahdollista jos ja vain jos L on surjektio.
(2) Osoitetaan samalla tavalla.
(3) Seuraa suoraan (1) ja (2):stä. □

Esimerkki 2.58. *Olkoon W vektoriavaruuden V aliavaruus. Tällöin inkluusiokuvaus $i\colon W \hookrightarrow V$ on lineaarinen injektio. Edellisen nojalla $i^*\colon V^* \to W^*$ on surjektio. Tämä on helppo nähdä myös suoraan - kun avataan määritemät auki, nähdään, että tämä väite tarkoittaa sitä, että jokainen lineaarinen muoto $L\colon W \to K$ voidaan jatkaa koko avaruuden lineaariseksi muodoksi $L\colon V \to K$. Tämä puolestaan seuraa siitä, että voimme jatkaa W:n kannan V:n kannaksi, jolloin helposti päästään jatkamaan kuvausta L Proposition 2.22 avulla (mieti yksityiskohdat läpi).*

Sovelluksena yllä osoitetusta näytetään, että matriisin rivi- ja sarakeavaruudet ovat aina samaa dimensiota (kunnan yli). Palautetaan ensin mieleen, miten rivi- ja sarakeavaruus määritellään.
Olkoon $A \in M(n \times m; R)$ matriisi renkaan R yli,

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix}.$$

Kuten olemme jo sovinneet aikaisemmin, jokainen A:n rivi $[a_{i1}, a_{i2}, \dots, a_{in}]$ ajatellaan modulin R^n alkiona $A_i = (a_{i1}, a_{i2}, \dots, a_{in})$. Kaikki rivit $A_1, \dots, A_m$ virittävät erään R^n:n alimodulin, joka merkitään $\mathrm{Row}(A)$ ja sanotaan matriisin A *riviavaruudeksi*. Riviavaruus on siis R^n:n alimoduli.
Samoin jokainen A:n sarake $[a_{1j}, a_{2j}, \dots, a_{mj}]$ on modulin R^m alkio $A^j = (a_{1j}, a_{2j}, \dots, a_{mj})$. Kaikki sarakkeet $A^1, \dots, A^n$ virittävät erään R^m:n alimodulin, joka merkitään $\mathrm{Col}(A)$ ja sanotaan matriisin A *sarakeavaruudeksi*. Sarakeavaruus on siis R^m:n alimoduli. Jos A ajatellaan kuvauksena ${}_A\colon R^n \to R^m$, $\mathrm{Col}(A)$ ei ole itse asiassa mitään muuta, kuin L_A:n kuvajoukko $\operatorname{Im} A$.
A priori siis rivi- ja sarakeavaruudet ovat eri modulin alimodulit eikä niillä näyttää olevan mitään yhteistä keskenään. Silti niillä on sama dimensio, ainakin silloin kun R on kunta.

Propositio 2.59. *Olkoon K kunta ja $A \in M(m \times n; K)$ mielivaltainen matriisi. Tällöin*

$$\dim \mathrm{Row}(A) = \dim \mathrm{Col}(A)$$

Todistus. Olkoon $L_A\colon K^n \to K^m$ A:ta vastaava K-lineaarinen kuvaus. Tällöin $\operatorname{Col} A$ on itse asiassa sama avaruus kuin $\operatorname{Im} L_A$. Korollarin 2.55 nojalla pätee $\dim \operatorname{Im} L_A = \dim \operatorname{Im} L_A^*$.
Toisaalta kuvauksen L_A^* matriisi duaalikantojen suhteen on A:n transpoosi A^T, joten $\operatorname{Im} L_A^* = \operatorname{Col} A^T = \operatorname{Row} A$. Näin ollen

$$\dim \operatorname{Col} A = \dim \operatorname{Im} L_A = \dim \operatorname{Im} L_A^* = \dim \operatorname{Row} A,$$

missä käytimme hyväksi edellä osoitettua yhtälöä 2.56. □

Biduaali ja refleksivisyys.
Olkoon M R-moduli. Tällöin sen duaali M^* on myös R-moduli, joten silläkin on duaali $(M^*)^*$. Tätä modulia merkitään M^{**} ja sanotaan M:n *biduaaliksi* tai yksinkertaisesti M:n toiseksi duaaliksi.

Jos M on äärellisulotteinen R-moduli, pätee

$$\dim M^{**} = \dim M^* = \dim M$$

eli kaikki kolme modulia M, M^*, M^{**} ovat erityisesti isomorfiset. Osoittautuu, että tässä tapauksessa on olemassa jopa niin sanottu *kanoninen* eli *luonnollinen* isomorfismi $M \cong M^{**}$. Tässä yhteydessä "luonnollinen" viittaa siihen, että tämä isomorfismi ei riipu kantojen valinnoista. Jätetään lukijalle harjoitustehtäväksi näyttää, että isomorfismi $M \to M^*$ joka kuvaa kannan $\mathbf{e}$ duaalikannakseen yleensä riippuu kannan valinnasta eikä näin ollen ole "kanoninen".

Kanoninen kuvaus $\Phi\colon M \to M^{**}$ (tässä M mielivaltainen R-moduli, ei vältämättä äärellisulotteinen tai edes vapaa) konstruoidaan seuraavasti. Olkoon $m \in M$. Kuva-alkion $\Phi(m)$ on oltava M^{**}:n alkio, eli lineaarinen kuvaus $\Phi(m)\colon M^* \to R$. Olkoon $L \in M^*$ eli R-lineaarinen kuvaus $L\colon M \to R$. Määritelemme

$$\Phi(m)(L) = L(m).$$

Ensinnäkin on tarkistettavaa, että näin määritelty kuvaus $\Phi(m)$ on M^{**}:n alkio, eli R-lineaarinen kuvaus $M^* \to R$. Olkoot $L, L' \in M^*$, $a \in R$. Tällöin

$$\Phi(m)(L + L') = (L + L')(m) = L(m) + L'(m) = \Phi(m)(L) + \Phi(m)(L'),$$

$$\Phi(m)(aL) = (aL)(m) = aL(m) = a\Phi(m)(L).$$

Kuvaus $\Phi\colon M \to M^{**}$ on siis hyvin määritelty. Tarkistetaan, että se on R-lineaarinen. Olkoot $m, m' \in M$, $r \in R$, $L \in M^*$. Tällöin

$$\Phi(m+m')(L) = L(m+m') = L(m)+L(m') = \Phi(m)(L)+\Phi(m')(L) = (\Phi(m)+\Phi(m'))(L),$$

$$\Phi(rm)(L) = L(rm) = rL(m) = r(\Phi(m)(L)) = (r\Phi(m))(L),$$

joten

$$\Phi(m + m') = \Phi(m) + \Phi(m'),$$

$$\Phi(rm) = r\Phi(m).$$

Seuraavassa propositiossa annetaan täsmällinen, kategoriateorettinen selitys termille "luonnollinen".

Propositio 2.60. *Olkoot M, N R-modulit ja olkoon $L\colon M \to N$ R-lineaarinen kuvaus. Olkoot $\Phi_M\colon M \to M^{**}$, $\Phi_N\colon N \to N^{**}$ kanoniset kuvaukset konstruoitu yllä. Tällöin*

$$L^{**} \circ \Phi_M = \Phi_N \circ L$$

eli diagrammi

(2.61)
$$\begin{array}{ccc} M & \xrightarrow{L} & N \\ \downarrow{\scriptstyle \Phi_M} & & \downarrow{\scriptstyle \Phi_N} \\ M^{**} & \xrightarrow{L^{**}} & N^{**}. \end{array}$$

kommutoi. Tässä L^{**} on kuvauksen $L^*\colon N^* \to M^*$ duaali-kuvaus.

Todistus. Harjotustehtävä. □

Yleisesti ottaen kanoninen kuvaus $\Phi\colon M \to M^{**}$ ei ole isomorfismi. Esimerkiksi olkoon $R = \mathbb{Z}$, $M = \mathbb{Z}_3$. Tällöin mikä tahansa ryhmähomomorfismi (eli $\mathbb{Z}$-lineaarinen kuvaus $L\colon \mathbb{Z}_3 \to \mathbb{Z}$ on nolla-kuvaus. Tämä nähdään seuravaasti. Olkoon $x \in \mathbb{Z}_3$, tällöin $3x = 0$, joten

$$3L(x) = L(3x) = 0.$$

Kuitenkin $L(x)$ on $\mathbb{Z}$:n alkio ja $\mathbb{Z}$:ssä mikä tahansa alkio a jolle $3a = 0$ on nolla-alkio. Näin ollen $L(x) = 0$ kaikilla $x \in \mathbb{Z}_3$. Toisin sanoen $M^* = \{0\}$, joten myös $M^{**} = \{0\}$. Selvästi ainoa lineaarinen kuvaus $\mathbb{Z}_3 \to \{0\}$ on nolla-kuvaus, joten tässä tapauksessa Φ ei ole injektio.

Osoittautuu, että vapaan modulin tapauksessa kanoninen kuvaus on aina injektio. Lisäksi jos moduli on äärellisulotteinen, kuvaus Φ on jopa isomorfismi. Tätä äärellisulotteisten modulien ominaisuutta sanotaan *refleksivisyydeksi.*

Propositio 2.62. *Olkoon M vapaa R-moduli. Tällöin kanoninen kuvaus $\Phi\colon M \to M^{**}$ on injektio. Jos M on äärellisulotteinen, Φ on isomorfismi.*

Todistus. Osoitetaan molemmat väitteet vain erikoistapauksessa $M = V$ on äärellisulotteinen K-vektoriavaruus. Yleinen tapaus jätetään harjoitustehtäväksi.

Osoitetaan, että $\Phi\colon V \to V^{**}$ on injektio. Koska kuvaus on lineaarinen, riittää osoittaa, että sen ydin on triviaali. Olkoon $v \in V$ sellainen, että $\Phi(v) = 0$.
Olkoon $\mathbf{e} = (e_1, \ldots, e_n)$ vektoriavaruuden V kanta ja olkoon $\boldsymbol{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_n\}$ duaaliavaruuden V^* duaalikanta. On olemassa lineaarinen esitys

$$v = \sum_{i=1}^{n} a_i e_i.$$

Nyt

$$a_i = \varepsilon_i(v) = (\Phi(v))(\varepsilon_i) = 0$$

jokaisella $i = 1, \ldots, n$, joten $v = 0$. Näin ollen Φ on injektio.
Koska Φ on lineaarinen injektio äärellisulotteisten avaruuksien V ja V^{**} välillä ja $\dim V = \dim V^{**}$, Korollarin 2.44 nojalla se on myös surjektio. □

Refleksivisyys tarkoittaa, että samalla tavalla kuin ajatelemme M^* M:n duaali-avaruudeksi, voimme myös ajatella M M^*:n duaaliksi (isomofirsmin Φ kautta), joten ne ovat toistensa "duaaleja" hyvin symmetrisella tavalla. M^* alkio L "toimii" alkiolla $x \in M$ - lopputuloksena saadaan skalaari $L(x)$. Yhtä hyvin $x \in M$ toimii M^* alkioilla L - lopputuloksena taas sama skalaari $L(x)$. Usein käytetään merkintää $\langle L, x\rangle$ $L(x)$:n sijaan - näin korostetaan, että L ja x ovat samanarvoisessa asemassa. Kuvaus $(L, x) \mapsto \langle L, x\rangle$ on esimerkki *bilineaarisesta muodosta*, joita käsittelemme luvussa "Multilineaariset kuvaukset ja determinaantit".

Huomautus: Vaikka emme yleisesti ottaen käsittele oikeanpuoleisia moduleita, tehdään pieni sivuhuomatus, joka havainnollista sen, miten oikeanpuoleiset modulit tulevat yleisemmässä teoriassa väistämättä vastaan, vaikka tutkitaankin alunperin vain vasemmanpuoleisia.
Nimittäin, olemme aikaisemmin huomaneet, että jos R ei ole vaihdannainen rengas, rL ei vältämättä ole M^*:n alkio, vaikka L olisi. Mutta renkaassa R alkiot voidaan kertoa myös oikealta, eli voimme yhtähyvin määritellä myös kuvaus Lr kaavalla

$$Lr(x) = L(x)r.$$

Tällöin Lr aina ON R-lineaarinen, sillä kaikilla $r' \in R$ pätee

$$Lr(r'x) = L(r'x)r = r'(L(x)r) = r'(Lr(x)).$$

Operaatio $(L, r) \to Lr$ (kuvausten yhteenlaskun kanssa) määrittelee siis duaalissa M^* luonnollisen **oikeanpuoleisen** R-modulin struktuurin.
Samoin, jos M on *oikeanpuoleinen* R-moduli, niin sen duaalissa M^* voidaan määritellä vasemmanpuoleisen R-modulin struktuurin. Erityisesti jos lähdetään vasemmanpuoleisesta R-modulista, niin M^{**} on myös vasemmanpuoleinen R-moduli. Voimme muodostaa kanoninen kuvaus $\Phi\colon M \to M^{**}$ kuten yllä. Jos M on äärellisulotteinen, tämä kuvaus on isomorfismi.
Sen sijaan moduleista M ja M^* ei voida enää sanoa, että ne olisivat isomorfiset R-modulit, vaikka niillä onkin sama dimensio. Syy tähän on tietenkin se, että niissä ovat määriteltyjä erityyppiset algebralliset struktuurit - toinen on vasemmanpuoleinen ja toinen oikeanpuoleinen moduli, eikä niitä voi verrata keskenään.

2.5 Suora summa

Olkoon M R-moduli ja olkoot N ja N' sen alimodulit. Tällöin niiden *summa*

$$N + N' = \{x + y \mid x \in N, y \in N'\}$$

on myös alimoduli, itse asiassa pienin M:n alimoduli, joka sisältää sekä N:n, että N':n, eli alimoduli $\mathrm{Span}(N \cup N')$.

Summamodulin $N + N'$ jokainen alkio m voidaan määritelmän mukaan kirjoittaa muodossa $m = x + y$ missä $x \in N$ ja $y \in N'$. Yleensä tällainen esitys ei tietenkään ole yksikäsitteinen. Jos se on aina yksikäsitteinen, merkitään $N + N'$ symbolilla $N \oplus N'$ ja sanotaan se alimodulien N, N' *suoraksi summaksi*.

Suoran summan käsitettä voidaan yleistä äärellisen moneen alimoduliin tai jopa mielivaltaiseen perheeseen alimoduleita. Tarkastelemme ensin äärellinen tapaus tarkemmin.

Määritelmä 2.63. *Olkoon M R-moduli ja $N_1, N_2, \ldots, N_n$ alimodulit. Jos alimodulin*

$$N_1 + N_2 \ldots + N_n = \{x_1 + \ldots + x_n \mid x_i \in N_i \text{ kaikilla } i = 1, \ldots, n\}$$

jokainen alkio voidaan kirjoittaa muodossa $x_1 + \ldots + x_n$, $x_i \in N_i$ kaikilla $i = 1, \ldots, n$ **täsmälleen yhdellä tavalla**, *sanomme, että alimodulit $N_1, N_2, \ldots, N_n$ muodostavat* suoran summan. *Tällöin merkitään $N_1 + N_2 \ldots + N_n = N_1 \oplus N_2 \oplus \ldots \oplus N_n$ ja moduli $N_1 \oplus N_2 \oplus \ldots \oplus N_n$ sanotaan modulien $N_1, N_2, \ldots, N_n$* suoraksi summaksi.

Seuraavassa lemmassa annetaan suoran summan vaihtoehtoisia määritelmiä. Sen formulointia varten esitellään seuraava merkintätapa. Jos jossakin summassa, esimerkiksi $a + b + \ldots + \hat{c} + \ldots + d$, jokin termi c esiintyy varustettuna ”hatulla” eli muodossa $\hat{c}$, se tarkoittaa, että se ei oikeasti esiinny tässä summassa, vaan se poistetaan siitä. Tyypillisesti tätä merkintätapaa käytetään seuraavalla tavalla. Olkoon $(x_1, \ldots, x_n)$ jono alkiota. Tällöin merkintä $x_1 + \ldots + \hat{x_i} + \ldots + x_n$ tarkoittaa, että summataan kaikki alkiot paitsi x_i.

Lemma 2.64. *Olkoon M R-moduli ja $N_1, N_2, \ldots, N_n$ alimodulit. Tällöin seuraavat ehdot ovat yhtäpitäviä.*

(i) Summa $N_1 + N_2 \ldots + N_n$ on suora.

(ii) *Jos* $x_1 + \ldots + x_n = 0$ *joillakin* $x_i \in N_i$, $i = 1, \ldots, n$, *niin* $x_i = 0$ *kaikilla* $i = 1, \ldots, n$.

(iii) *Jokaisella* $i = 1, \ldots, n$ *pätee*

$$(N_1 + \ldots + \hat{N}_i + \ldots + N_n) \cap N_i = \{0\}.$$

Todistus. (i)$\Longrightarrow$(ii).
Oletetaan, että summa $N_1 + N_2 \ldots + N_n$ on suora. Tällöin erityisesti sen alkiolla 0 on yksikäsitteinen esitys muodossa $x_1 + \ldots + x_n$ joillakin $x_i \in N_i$, $i = 1, \ldots, n$. Mutta $0 + 0 + \ldots + 0$ on varmasti yksi sellainen esitys, joten se on ainoa.

(ii)$\Longrightarrow$(iii).
Oletetaan, että nollaalkiolla on vain triviaaliesitys muodossa $x_1 + \ldots + x_n$ joillakin $x_i \in N_i$, $i = 1, \ldots, n$. Olkoon $i \in [n]$ ja olkoot $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ sellaiset, että

$$x_1 + \ldots + x_{i-1} + x_{i+1} + \ldots + x_n = x \in N_i.$$

Tällöin

$$0 = x_1 + \ldots + x_{i-1} + (-x) + x_{i+1} + \ldots + x_n,$$

joten oletuksestamme seuraa yrityisesti, että $x = 0$.

(iii)$\Longrightarrow$(i).
Oletetaan, että jokaisella $i \in [n]$ pätee

$$(N_1 + \ldots + \hat{N}_i + \ldots + N_n) \cap N_i = \{0\}.$$

Olkoot x_k, y_k, $k \in [n]$ siten, että

$$x_1 + \ldots + x_n = y_1 + \ldots + y_n.$$

Pitää osoittaa, että $x_i = y_i$ jokaisella $i \in [n]$. Olkoon $i \in [n]$. Voimme kirjoittaa yllä oleva yhtälö muotoon

$$(x_1 - y_1) + \ldots + (x_{i-1} - y_{i-1}) + (x_{i+1} - y_{i+1}) + \ldots + (x_n - y_n) = (y_i - x_i),$$

missä vasemmalla puoleella on summan $N_1 + \ldots + \hat{N}_i + \ldots + N_n$ alkio ja oikealla puoleella alimodulin N_i alkio. Oletuksesta seuraa, että erityisesti $y_i - x_i = 0$ eli $x_i = y_i$. □

Soveltamalla edellisen lemman kohtaa (iii) kahden alimodulin N_1, N_2 tapaukseen, nähdään erityisesti, että summa $N_1 + N_2$ on suora jos ja vain jos $N_1 \cap N_2 = \{0\}$ eli ainoa kahden alimodulin yhteinen alkio on nolla-alkio.

Esimerkki 2.65. *Olkoon $V = \mathbb{R}^{\mathbb{R}}$ kaikkien kuvausten $f\colon \mathbb{R} \to \mathbb{R}$ muodostama $\mathbb{R}$-vektoriavaruus. Määritellään sen aliavaruudet U_1, U_2 seuraavasti.*

$$U_1 = \{f \in V \mid f(x) = f(-x) \text{ kaikilla } x \in \mathbb{R}\},$$

$$U_2 = \{f \in V \mid f(x) = -f(-x) \text{ kaikilla } x \in \mathbb{R}\}.$$

U_1 on siis kaikkien parillisten *kuvausten muodostama joukko ja U_2 on kaikkien* parittomien *kuvausten muodostama joukko. Helposti nähdään, että nämä todellakin ovat V:n aliavaruuksia.*
Osoitetaan edellisen lemman avulla, että summa $U_1 + U_2$ on suora. Riittää osoittaa, että $U_1 \cap U_2 = \{0\}$. Olkoon $f\colon U_1 \cap U_2$ ja olkoon $x \in \mathbb{R}$. Tällöin

$$f(x) = f(-x) = -f(-(-x)) = -f(x),$$

joten $f(x) = 0$. Näin ollen summa $U_1 + U_2$ on suora.

Osoitetaan vielä, että itse asiassa $U_1 \oplus U_2 = V$ eli jokainen funktio $f\colon \mathbb{R} \to \mathbb{R}$ voidaan kirjoittaa parillisen ja parittoman funktion summana. Lisäksi, koska tiedämme jo, että tämä summa on suora, tällainen esitys on tällöin varmasti yksikäsitteinen*. Olkoon $f\colon \mathbb{R} \to \mathbb{R}$. Määritelemme kuvaukset $f_1, f_2\colon \mathbb{R} \to \mathbb{R}$ ehdoilla*

$$f_1(x) = \frac{1}{2}(f(x) + f(-x)),$$

$$f_2(x) = \frac{1}{2}(f(x) - f(-x)).$$

Tällöin $f_i \in U_i, i = 1, 2$ ja $f = f_1 + f_2$.

Esimerkki 2.66. *Olkoon M R-moduli ja olkoon $(e_1, \ldots, e_n)$ vapaa jono M:ssä. Jokaisella $i = 1, \ldots, n$ on olemassa e_i:n virittämä 1-ulotteinen alimoduli*

$$N_i = \{re_i \mid r \in R\} = Re_i.$$

Tällöin summa $N_1 + N_2 + \ldots + N_n$ on suora (tarkista). Näin olleen suoran summan käsite on jossakin mielessä vapauden yleistys.
Jos $(e_1, \ldots, e_n)$ on M:n kanta, pätee

$$N_1 \oplus N_2 \oplus \ldots \oplus N_n = M.$$

Kääntäinen ei päde - jos $(e_1, \ldots, e_n)$ on mielivaltainen M:n alkioiden jono ja summa $N_1 + N_2 + \ldots + N_n$, missä $N_i = Re_i$, on suora, niin jono $(e_1, \ldots, e_n)$ ei ole vältämättä vapaa. Esimerkiksi $\mathbb{Z}_n$ ei ole vapaa $\mathbb{Z}$-moduli, vaikka sen alkio $e_1 = \bar{1}$ virittää sen ja $\mathbb{Z}_n = Re_1$. Pohjimmiltään syys on siinä, että vapaassa jonossa jokaisen alkion e pitää olla **torsiovapaa**, *eli erityisesti $re = 0$ implikoi $r = 0$.*

Olkoon M moduli ja N_1 sen alimoduli. Jos N_2 on jokin L:n alimoduli, jolle pätee $M = N_1 \oplus N_2$, kutsumme N_2 alimodulin N_1 *komplementiksi* modulissa M.
Komplementti ei yleensä ole missään nimessä yksikäsitteinen. Esimerkiksi tasossa $\mathbb{R}^2$, joka on 2-ulotteinen $\mathbb{R}$-vektoriavaruus, aliavaruudella $\mathbb{R}_1 = \{(x, 0) \mid x \in \mathbb{R}\}$ on äärettömän monta erilaista komplementtia - tällaiseksi käy mikä tahansa 1-ulotteinen suora, joka ei ole $\mathbb{R}_1$ itse.
Modulin M alimoduli N sanotaan olevan M:n *suora tekijä* jos sillä on komplementt iM:ssä eli on olemassa M:n alimoduli P siten, että summa $N \oplus P$ on suora ja $N \oplus P = M$.

Esimerkki 2.67. *Modulin alimoduli ei vältämättä ole sen suora tekijä. Esimerkiksi $2\mathbb{Z}$ on $\mathbb{Z}$-modulin $\mathbb{Z}$ alimoduli, mutta ei ole olemassa mitään $\mathbb{Z}$:n alimodulia N jolle pätisi $\mathbb{Z} = 2\mathbb{Z} \oplus N$. Tämä nähdään vaikkapa seuraavasti. $\mathbb{Z}$:n aliryhmät (= $\mathbb{Z}$-alimodulit) ovat muotoa $n\mathbb{Z}$, $n \in \mathbb{N}$. Jos $n \neq 0$, summa $2\mathbb{Z} + n\mathbb{Z}$ ei ole suora, sillä $0 \neq 2n \in 2\mathbb{Z} \cap n\mathbb{Z}$. Jos taas $n = 0$ summa $2\mathbb{Z} + n\mathbb{Z}$ on vapaa, mutta sen arvo on $2\mathbb{Z}$, ei koko moduli $\mathbb{Z}$.*

Vektoriavaruuden jokainen aliavaruus on sen suora tekijä. Todistetaan tämä äärellisulotteiselle avaruudelle.

Lemma 2.68. *Olkoon V äärellisulotteinen K-vektoriavaruus. Olkoon U sen aliavaruus. Tällöin U:llä on olemassa komplementti V:ssä.*

Todistus. Valitaan (Lemma 2.18) V:lle kanta $(e_1, \ldots, e_n)$ siten, että $(e_1, \ldots, e_k)$ on U:n kanta. Tällöin $W = \mathrm{Span}\{e_{k+1}, \ldots, e_n\}$ on U:n komplementti. □

Propositio 2.69. *Olkoon $M = N_1 \oplus N_2 \oplus \ldots \oplus N_n$ suora summa ja oletetaan, että jokainen alimoduli L_i, $i = 1, \ldots, n$, on äärellisulotteinen ja vapaa. Tällöin myös M on äärellisulotteinen ja*

$$\dim M = \sum_{i=1}^{n} \dim L_i.$$

Todistus. Harjoitustehtävä. □

Suoran summan käsitettä on mahdollista yleistää myös äärettömään moneen alimodulin tapaukseen. Olkoon $(N_\alpha)_{\alpha\in\mathcal{A}}$ *mielivaltainen* perhe R-modulin M alimoduleja. Haluamme muodostaa niiden summan $\sum_{\alpha\in\mathcal{A}} N_\alpha$. Tällä kertaa, jos $\mathcal{A}$ on ääretön, emme voi muodostaa summia $\sum_{\alpha\in\mathcal{A}} x_\alpha$, sillä äärettömän monta alkiota ei voi laskea yhteen. Pystymme muodostamaan vain äärellisiä summia. Voisimme siis periaattessa ottaa summaan $\sum_{\alpha\in\mathcal{A}} N_\alpha$ mukaan kaikki *äärelliset* summat, jotka on muotoa

$$x_1 + \ldots + x_n,$$

missä jokainen x_i on poimittu jostakin modulista N_α. Tämä olisi itse asiassa oikea määritelmä, mutta tällainen esitystapa on hieman kömpelö. Siksi esitämme toisen tavan määritellä sama asia.
Ongelma on siis siinä, että emme yleensä voi laskea yhteen äärettömän monta modulin alkiota. Mutta jos äärettömän monesta alkiosta vain äärellisen monta eroaa nollasta, voimme määritellä niiden summan hyvin luonnollisella tavalla.

Tämän johdosta teemme seuraavan määritelmän. Olkoon M moduli ja $(x_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen indeksoitu perhe sen alkioita. Määritelemme tämän perheen *kantajan* $\mathcal{B}\subset\mathcal{A}$ seuraavaksi,

$$\mathcal{B} = \{\alpha\in\mathcal{A} \mid x_\alpha \neq 0\}.$$

Sanomme, että perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on *äärelliskantajainen* jos sen kantaja $\mathcal{B}$ on äärellinen joukko. Toisin sanoen perhe on äärelliskantajainen jos ja vain jos vain ainoastaan äärellisen monta perheen jäsentä eroavat nollasta.
Kun perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on äärelliskantajainen voimme muodostaa sen alkioiden summan, jota merkitään $\sum_{\alpha\in\mathcal{A}} x_\alpha$ - lasketaan vain kaikki nollasta eroavat alkiot yhteen. Täsmällisemmin sanottuna asetetaan

$$\sum_{\alpha\in\mathcal{A}} x_\alpha = \sum_{\alpha\in\mathcal{B}} x_\alpha,$$

missä $\mathcal{B}$ on perheen kantaja.
Nyt voimme määritellä perheen $(N_\alpha)_{\alpha\in\mathcal{A}}$ *summan*,

$$\sum_{\alpha\in\mathcal{A}} N_\alpha = \{\sum_{\alpha\in\mathcal{A}} x_\alpha \mid x_\alpha\in M_\alpha \text{ kaikilla } \alpha\in\mathcal{A} \text{ ja perhe } (x_\alpha)_{\alpha\in\mathcal{A}} \text{ on äärelliskantajainen}\}.$$

Helposti nähdään, että tällöin $\sum_{\alpha\in\mathcal{A}} N_\alpha$ on M:n alimoduli, itse asiassa *pienin alimoduli* joka sisältää kaikki alimodulit $M_\alpha, \alpha\in\mathcal{A}$ (harjoitustehtävä).

Jokainen summan $\sum_{\alpha\in\mathcal{A}} N_\alpha$ alkio voidaan esittää muodossa

$$\sum_{\alpha\in\mathcal{A}} x_\alpha,$$

missä $x_\alpha \in M_\alpha$ kaikilla $\alpha \in \mathcal{A}$ ja perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on äärelliskantajainen. Yleensä tämä esitys ei ole yksikäsitteinen. Jos se on, niin sanotaan summa $\sum_{\alpha\in\mathcal{A}} N_\alpha$ *suoraksi* ja merkitään se symbolilla

$$\oplus_{\alpha\in\mathcal{A}} N_\alpha.$$

Kuten äärellisessä tapauksessa voidaan osoittaa seuraava (todistus sivutetaan, sillä se on samanlainen kuin äärellisessä tapauksessa).

Lemma 2.70. *Olkoon M R-moduli ja $(N_\alpha)_{\alpha\in\mathcal{A}}$ sen alimodulien muodostama perhe. Tällöin seuraavat ehdot ovat yhtäpitäviä.*

1. *Summa $\sum_{\alpha\in\mathcal{A}} N_\alpha$ on suora.*
2. *Jos $\sum_{\alpha\in\mathcal{A}} x_\alpha = 0$ jollakin äärelliskantajaisella perheella $(x_\alpha)_{\alpha\in\mathcal{A}}$, missä $x_\alpha \in \mathcal{A}$ jokaisella $\alpha \in \mathcal{A}$, niin $x_\alpha = 0$ kaikilla $\alpha \in \mathcal{A}$.*
3. *Jokaisella $\beta \in \mathcal{A}$ pätee*

$$(\sum_{\alpha\in\mathcal{A},\alpha\neq\beta} N_\alpha) \cap N_\beta = \{0\}.$$

Esimerkki 2.71. *Nyt kun käytettävissämme on äärelliskantajaisen perheen summan käsite, voimme kirjoittaa vapaan perheen määritelmän uudella tavalla. Olkoon M R-moduli ja $(e_\alpha)_{\alpha\in\mathcal{A}}$ perhe sen alkioita. Tällöin se on vapaa jos ja vain jos jokaisella äärelliskantajaisella R:n osaperheella $(r_\alpha)_{\alpha\in\mathcal{A}}$ pätee*

$$\sum_{\alpha\in\mathcal{A}} r_\alpha e_\alpha = 0$$

jos ja vain jos $r_\alpha = 0$ kaikilla $\alpha \in \mathcal{A}$.
Tällainen määritelmä on paljon eleganttimpi kuin aikaisempi kömpelö lähestymistavamme, jossa jouduimme selittämään mitkä esitykset ovat "oleellisesti samat" ja mitkä taas "oleellisesti erilaiset".

Oletetaan, että modulin M alimodulit $N_1, \ldots, N_n$ muodostavat suoran summan. Tällöin suoran summan $N = N_1 \oplus \ldots \oplus N_n$ moduli-struktuuri on täysin ja yksikäsitteisesti määrätty, kun alimodulien N_i moduli-struktuurit tunnetaan. Esimerkiksi jos $x = l_1 + \ldots + l_n, y = l'_1 + \ldots + l'_n \in N$, niin summa

alkion $x + y$ samantyyppinen esitys on $x + y = (l_1 + l'_1) + \ldots + (l_n + l'_n)$.
Samanlainen huomatus koskee mielivaltaisia, ei vältämättä äärellisiä, suoria summia. Voimme siis "rekonstruoida" koko modulin algebrallinen struktuuri, kun tunnetaan sen suoran tekijöiden algebralliset struktuurit.
Tämä havainto motivoi toisen, "ulkoisen" näkökulman suoran summan käsitteeseen, jossa ei tarvitse etukäteen olettaa, että summattavat modulit ovat saman modulit alimodulit.

Palautetaan mieleen, miten karteesinen tulo yleisesti määritellään. Olkoon $(X_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe joukkoja, missä indeksijoukko $\mathcal{A}$ on mikä tahansa joukko (mahdollisesti ääretön). Pomitaan jokaisesta joukosta X_α tasan yksi alkio x_α, näin saadaan jokin perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$. *Karteesinen tulo* $\prod_{\alpha\in\mathcal{A}} X_\alpha$ on määritelmän mukaan kaikkien tällaisten perheiden muodostama joukko.
Olkoon $\beta \in \mathcal{A}$ indeksijoukon alkion. Perheen $(x_\alpha)_{\alpha\in\mathcal{A}}$ (eli tulon $\prod_{\alpha\in\mathcal{A}} X_\alpha$ alkion) *β-komponentti* on alkio $x_\beta \in X_\beta$. Tulon alkion komponentit määräävät sen yksikäsitteisesti. Komponentin ottaminen määrittelee jokaisella $\beta \in \mathcal{A}$ niin sanotun *projektiokuvauksen* $\mathrm{pr}_\beta\colon \prod_{\alpha\in\mathcal{A}} X_\alpha \to X_\beta$, $\mathrm{pr}_\beta((x_\alpha)_{\alpha\in\mathcal{A}}) = x_\beta$.
Karteesisen tulon tärkeys piilee sen "universaaliominaisuudessa", joka sanoo seuraavan. Kuvitellaan, että meillä on jokin joukko Y ja haluamme konstruoida kuvauksen $f\colon Y \to \prod_{\alpha\in\mathcal{A}} X_\alpha$. Tällöin jokaisella $y \in Y$ kuvalkio $f(y)$ on tulojoukon alkio, eli perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$, missä $x_\alpha = \mathrm{pr}_\alpha(f(y)) = (\mathrm{pr}_\alpha \circ f)(y)$. Näin ollen määritäksemme kuvauksen f, meidän on tunnettava kaikki sen "komponentit" $\mathrm{pr}_\alpha \circ f = f_\alpha$. Jokainen tällainen komponentti sinänsä on kuvaus $Y \to X_\alpha$. Kääntäen, kuvitellaan, että meille on annettu perhe kuvauksia $(f_\alpha\colon Y \to X_\alpha)_{\alpha\in\mathcal{A}}$, jotka ovat kaikki siis määriteltyjä samassa lähtöjoukossa Y, kun taas maalijoukko X_α saa vaihdella. Tällöin voimme "laittaa nämä kuvaukset yhteen" kuvauksena $f\colon Y \to \prod_{\alpha\in\mathcal{A}} X_\alpha$, jonka komponentit ovat tasan kuvaukset f_α. Karteesinen tulo antaa siis mahdollisuuden "koodata" kuvausten perhe yhdeksi kuvaukseksi, kunhan näillä kuvauksilla on sama lähtöjoukko. Lisäksi tämä "koodaus" ei menetä mitään informaatiota eli vastaavuus on bijektiivinen - jokaista koodia eli kuvausta $f\colon Y \to \prod_{\alpha\in\mathcal{A}} X_\alpha$ vastaa täsmälleen yksi perhe $(f_\alpha\colon Y \to X_\alpha)_{\alpha\in\mathcal{A}}$. Juuri tätä ominaisuutta sanotaan tulon "universaaliseksi ominaisuudeksi".

Edellisessä keskustelussa tarkastelttiin joukkoopillinen tilanne, joissa joukoissa ei ollut mitään algebrallista struktuuria eikä kuvauksiltakaan vaadittu mitään. Katsotaan nyt miltä samanlainen tilanne näyttää lineaarialgebrassa.

Olkoon $(M_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe R-moduleita, missä R on jokin rengas. Perheen $(M_\alpha)_{\alpha\in\mathcal{A}}$ *karteesinen tulo* $M = \prod_{\alpha\in\mathcal{A}} M_\alpha$ varustetaan R-

modulin struktuurilla luonnollisella tavalla, eli jos $m = (m_\alpha)_{\alpha\in\mathcal{A}}$ ja $m' = (m'_\alpha)_{\alpha\in\mathcal{A}}$ asetetaan

$$m + m' = (m_\alpha + m'_\alpha)_{\alpha\in\mathcal{A}}$$

ja jos $r \in R$ asetetaan

$$rm = (rm_\alpha)_{\alpha\in\mathcal{A}}.$$

Toisin sanoen tulomodulissa M R-modulioperaatiot sovelletaan komponenteittain.

Tälla tavalla konstruoitu moduli M sanotaan perheen $(M_\alpha)_{\alpha\in\mathcal{A}}$ *tulomoduliksi* tai yksinkertaisemmin *tuloksi*. Jätetään lukijalle harjoitustehtäväksi tarkistaa, että M on tosiaankin moduli näillä operaatioilla vasrustettuna.

Jokaisella $\beta \in \mathcal{A}$ voidaan määritellä tärkeät kanoniset kuvaukset $i_\beta\colon M_\beta \to M$ ja $p_\beta\colon M \to M_\beta$ seuraavasti. Kuvaus p_β on yksinkertaisesti karteesiseen tuloon liityvä projektiokuvaus, joka poimii alkiosta $m = (m_\alpha)_{\alpha\in\mathcal{A}}$ sen β-komponentin m_β. Kuvausta p_β sanotaankin kanoniseksi projektioksi.
Kuvaus i_β määritellään seuraavalla tavalla. Olkoon $m_\beta \in M_\beta$ mielivaltainen. Asetetaan $i_\beta(m)$'ksi sellainen tulomodulin alkio $m = (m_\alpha)_{\alpha\in\mathcal{A}}$, jonka β-komponentti on tasan m_β ja muut komponentit ovat vastavien modulien nolla-alkiot 0. Kuvausta i_α sanotaan *kanoniseksi injektioksi*. Kuten tästä terminologian valinnasta voi arvata, tämä kuvaus on aina injektio. Tämä todistetaan seuraavassa lemmassa. Isomorfialauseesta seuraa tällöin, että M:n alimoduli $i_\beta(M_\beta)$ on isomorfinen modulin M_β kanssa. Yleensä identifioidaan modulit M_β ja $i_\beta(M_\beta)$, minkä johdosta voimme ajatella, että jokainen perhessa $(M_\alpha)_{\alpha\in\mathcal{A}}$ esiintyvä moduli M_β on tulomodulin alimoduli.

Lemma 2.72. *Yllä määritellyille kuvauksille i_β, p_β pätee:*

(1) jokaisella $\beta \in \mathcal{A}$

$$p_\beta i_\beta = \mathrm{id},$$

(2) kaikilla $\beta, \gamma \in \mathcal{A}$, $\beta \neq \gamma$

$$p_\gamma i_\beta = 0,$$

(3) jokaisella $\beta \in \mathcal{A}$ kuvaus i_β on injektio ja kuvaus p_β on surjektio.

Todistus. Olkoot $\beta, \gamma \in \mathcal{A}$, $\beta \neq \gamma$. Olkoon $x \in M_\beta$. Tällöin $i_\beta(x)$:n β-komponentti on i_β:n määritelmän nojalla x. Toisaalta tämä komponentti on tasan $p_\beta(i_\beta(x))$. Näin ollen

$$p_\beta(i_\beta(x)) = x$$

kaikilla $x \in M_\beta$. Väite (1) on todistettu.
Alkion $i_\beta(x)$:n γ-komponentti on taas i_β:n määritelmän nojalla $0 \in M_\gamma$. Näin ollen

$$p_\gamma(i_\beta(x)) = 0.$$

Väite (2) on todistettu.

Osoitetaan, että i_β on injektio. Olkoot $x, y \in M_\beta$ sellaiset, että $i_\beta(x) = i_\beta(y)$. Tällöin (1):stä seuraa, että

$$x = p_\beta(i_\beta(x)) = p_\beta(i_\beta(y)) = y.$$

Osoitetaan, että p_β on surjektio. Olkoon $y \in M_\beta$. Tällöin

$$y = p_\beta(i_\beta(y)) = p_\beta(x),$$

missä $x = i_\beta(y) \in M$.

□

Olemme nyt valmiit määritelemään "ulkoisen" suoran summan. Olkoon $(M_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe R-moduleita kuten yllä. Tulomodulin $\prod_{\alpha\in\mathcal{A}} M_\alpha$ alkion $m = (m_\alpha)_{\alpha\in\mathcal{A}}$ *kantaja* $\mathcal{B}$ määritellään joukkona

$$\mathcal{B} = \{\alpha \in \mathcal{A} \mid x_\alpha \neq 0\}.$$

Alkio m on *äärelliskantajainen* jos sen kantaja on äärellinen joukko. Toisin sanoen alkio on äärelliskantajainen jos sen komponenteista vain äärellisen monta eroavat nollasta.
Kaikkien äärelliskantajaisten alkioiden muodostamaa tulomodulin osajoukkoa sanotaan perheen $(M_\alpha)_{\alpha\in\mathcal{A}}$ *(ulkoiseksi) suoraksi summaksi* ja merkitään

$$\oplus_{\alpha\in\mathcal{A}} M_a.$$

Tämä joukko on tulomodulin alimoduli (harjoitustehtävä).

Koska $\oplus_{\alpha\in\mathcal{A}} M_a$ on tulomodulin $\prod_{\alpha\in\mathcal{A}} M_\alpha$ alimoduli, voimme määritellä projektiokuvaus $p_\beta\colon \oplus_{\alpha\in\mathcal{A}} M_a \to M_\beta$ jokaisella $\beta \in \mathcal{A}$ yksinkertaisesti rajoittamalla kanoninen projektio p_β osajoukkoon. Lisäksi jokaisella $\beta \in \mathcal{A}$ ja jokaisella $m_\beta \in M_\beta$ alkio $i_\beta(m_\beta)$ on äärelliskantajainen (sillä on itse asiassa korkeintaan yksi nollasta eroava komponentti), joten voimme määritellä myös kuvauksen $i_\beta\colon M_\beta \to \oplus_{\alpha\in\mathcal{A}} M_\alpha$ samalla kaavalla kuin ennen.

Kuvaukset i_β ja p_β sanotaan suoran summan tapauksessa myös kanoniseksi injektioksi ja kanoniseksi projektioksi. Näillä kuvauksilla on samantyyppiset ominaisuudet kuin vastaavilla kuvauksilla tulomodulin tapauksessa, kuten seuraava lemma sanoo. Erityisesti, koska jokainen kuvaus i_β on injektio, voimme identifioida M_β ja sen kuva $i_\beta(M_\beta)$ ja ajatella M_β suoran summan $\oplus_{\alpha\in\mathcal{A}} M_\alpha$ alimodulina.

Lemma 2.73. *Yllä määritellyille kuvauksille i_β, p_β pätee:*

(1) jokaisella $\beta \in \mathcal{A}$

$$p_\beta i_\beta = \mathrm{id},$$

(2) kaikilla $\beta, \gamma \in \mathcal{A}$, $\beta \neq \gamma$

$$p_\beta i_\beta = 0,$$

(3) jokaisella $\beta \in \mathcal{A}$ kuvaus i_β on injektio ja kuvaus p_β on surjektio.

Lisäksi jokainen $x \in \oplus_{\alpha\in\mathcal{A}} M_\alpha$ voidaan esittää yksikäsitteisellä tavalla muodossa

$$x = \sum_{\alpha\in\mathcal{A}} x_\alpha,$$

missä perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on äärelliskantajainen ja $x_\alpha \in M_\alpha (= i_\alpha(M_\alpha))$ jokaisella $\alpha \in \mathcal{A}$. Tässä itse asiassa

$$x_\alpha = i_\alpha(p_\alpha(x))$$

jokaisella $\alpha \in \mathcal{A}$.

Todistus. (1) (2) ja (3) todistetaan täsmälleen samalla tavalla kuin tulomodulin tapauksessa, kts. Lemma 2.72.

Oletetaan, että $x \in \oplus_{\alpha\in\mathcal{A}} M_\alpha$ on esitetty muodossa

$$x = \sum_{\alpha\in\mathcal{A}} x_\alpha, \tag{2.74}$$

missä perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on äärelliskantajainen ja $x_\alpha \in M_\alpha (= i_\alpha(M_\alpha))$ jokaisella $\alpha \in \mathcal{A}$. Tällöin jokaisella $\beta \in \mathcal{A}$ saadaan kohtien (1) ja (2) avulla, että

$$p_\beta(x) = \sum_{\alpha\in\mathcal{A}} p_\beta(i_\alpha(x_\alpha)) = x_\beta.$$

Ottaen huomioon samaistus $M_\beta = i_\beta(M_\beta)$, nähdään, että

$$x_\beta = i_\beta(p_\beta(x)),$$

joten esitys (2.74) on yksikäsitteinen.

Kääntäen, jos $x = (x_\alpha) \in \oplus_{\alpha\in\mathcal{A}} M_\alpha$, niin perhe $(x_\alpha)_{\alpha\in\mathcal{A}}$ on määritelmän mukaan äärelliskantajainen. Lisäksi selvästi

$$x = \sum_{\alpha\in\mathcal{A}} i_\alpha(x_\alpha) = \sum_{\alpha\in\mathcal{A}} x_\alpha.$$

□

Edellisesta lemmasta seuraa suoraan, että modulien ulkoinen suora summa voidaan aina tulkita myös niiden sisäisenä suorana summana, joka oli määritelty tämän luvun alussa. Näin ollen luvun alussa määritelty "sisäinen" suora summa ja myöhemmin konstruoitu "ulkoinen" suora summa ovat olennaisesti sama asia. Muotoillaan tämä tulos viralliseksi lemmaksi.

Lemma 2.75. *Olkoon $(M_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe R-moduleita. Tällöin niiden ulkoinen suora summa $\oplus_{\alpha\in\mathcal{A}} M_\alpha$ on alimoduliensa $(M_\alpha)_{\alpha\in\mathcal{A}}$ suora summa. Tässä identifioimme $M_\alpha = i_\alpha(M_\alpha)$, kuten yleensä.*

Modulien tulo ja suora summa toteuttavat tärkeitä *universaalia ominaisuuksia*, jotka määrävät niitä yksikäsitteisesti isomorfiaa vaille.
Mainitsemme ensin tulomodulin universaalin ominaisuuden ilman todistusta, sillä emme tarvitse sitä jatkossa, ja koska se seuraa hyvin helposti (joukkooppilisen) karteesisen tulon samanlaisesta universaalisesta ominaisuudesta.

Propositio 2.76. *Olkoon M R-moduli ja $(M_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe R-moduleita. Oletetaan, että jokaisella $\alpha \in \mathcal{A}$ on olemassa R-lineaarinen kuvaus $L_\alpha\colon M \to M_\alpha$. Tällöin on olemassa täsmälleen yksi R-lineaarinen kuvaus $L\colon M \to \prod_{\alpha\in\mathcal{A}} M_\alpha$ siten, että*

$$p_\alpha \circ L = L_\alpha$$

jokaisella $\alpha \in \mathcal{A}$.

Tämä ominaisuus karakterisoi tulomodulin ja kuvaukset $(p_\alpha)_{\alpha\in\mathcal{A}}$ yksikäsitteisesti isomorfiaa vaille. Täsmällisemmin olkoon N jokin R-moduli ja $(p'_\alpha)_{\alpha\in\mathcal{A}}$ kokoelma R-lineaarisia kuvauksia $N \to M_\alpha$, $\alpha \in \mathcal{A}$. Oletetaan, että N toteuttaa saman universaalin ominaisuuden, eli jos M on mikä tahansa R-moduli ja jokaisella $\alpha \in \mathcal{A}$ on annettu R-lineaarinen kuvaus $L_\alpha\colon M \to M_\alpha$, niin on olemassa täsmälleen yksi R-lineaarinen kuvaus $L\colon M \to N$ siten, että

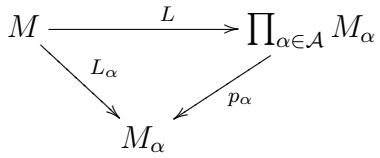
$$p'_\alpha \circ L = L_\alpha$$

jokaisella $\alpha \in \mathcal{A}$. Tällöin N on isomorfinen tulomodulin $\prod_{\alpha\in\mathcal{A}}$ kanssa. Tarkemmin on olemassa isomorfismi $\Phi\colon N \to \prod_{\alpha\in\mathcal{A}}$ siten, että

$$p_\alpha \circ \Phi = p'_\alpha$$

jokaisella $\alpha \in \mathcal{A}$. Tällainen isomorfismi on yksikäsitteinen.

Edellisen proposition muotoilu saattaa näyttää pelottavammalta ja vaikeammalta kuin se oikeasti on. Valaistaan sen sisältö diagrammien avulla. Tulon universaalisuus siis sanoo, että jokaisella $\alpha \in \mathcal{A}$ kolmionmuotoinen digrammi

(2.77)


voidaan aina *täydentää* samalla kuvausella L ja lisäksi tämä L on *ainoa* kuvaus, joka täydentää kaikki nämä kolmiot. Voimme ajatella asia myös toisesta näkökulmasta - molemmat perheet $(L_\alpha)_{\alpha\in\mathcal{A}}$ ja $(p_\alpha)_{\alpha\in\mathcal{A}}$ ovat esimerkkejä perheestä lineaarisia kuvauksia $M \to M_\alpha$, missä lähtömoduli on kaikilla kuvauksilla sama ja maalimoduli on M_α, joka riippuu indeksista α. Perhe $(p_\alpha)_{\alpha\in\mathcal{A}}$ on *universaalinen* kaikkien muiden tällaisten perheiden suhteen, siinä mielessä, että mielivaltaisen perheen kuvaukset voidaan **hajota** kuvausten p_α suhteen samanaikaisesti. Lisäksi tämä ominaisuus kuvailee perheen $(p_\alpha)_{\alpha\in\mathcal{A}}$ yksikäsitteisesti - mikä tahansa muu perhe, jolla on sama universaaliominaisuus, on oleellisesti sama perhe isomorfiaa vaille.

Yksi (kategoriateorettisesta näkökulmasta parempi) tapa määritellä tulomoduli onkin universaaliominaisuuden kautta - sanomme, että systeemi $(N, (p_\alpha)_{\alpha\in\mathcal{A}})$, missä $p_\alpha\colon N \to M_\alpha$ R-lineaarinen jokaisella $\alpha \in \mathcal{A}$, on moduliperheen $(M_\alpha)_{\alpha\in\mathcal{A}}$ *tulo* jos se toteuttaa tulon universaaliominaisuuden (määritelty yllä).
Tällöin tulo ei ole määritelty yksikäsitteisesti, vaan ainoastaan isomorfiaa vaille ja mikä tahansa tulomodulin kanssa isomorfinen moduli toteuttaa saman määritelmän. Mutta sillä ei ole mitään merkitystä, sillä kaikki mistä olemme kiinnostuneet on universaaliominaisuus. Kaikki tulomodulin ominaisuudet voidaan johtaa tästä abstraktista määritelmästä. Ainoa mihin konkrettinen konstruuktio (kuten se, mikä me annettiin tulomodulille alunperin) tarvitaan, on että voimme vakuuttua siitä, että kyseistä määritelmää toteuttava olio **on olemassa**. Sitten, kun olemme varmoja siitä, että se on olemassa, voimme operoida sillä käyttämällä vain sen universaaliominaisuutta. Meidän ei tarvitse tiedä miten tämä olio on konkrettisesti konstruoitu ja

mitä sen ” sisällä ” on.
Tietojenkäsittelyyn perehtyneelle tilanne on tuttu olio-ohjelmoinnista, jonka idea perustuu samaan periaatteseen - ei ole mitään väliä sillä, miten olio on konkrettisesti ”tehty” eli toteuttuu, ainoastaan sen ominaisuuksilla on merkistystä.

Suora summa voidaan myöskin karakterisoida sen universaaliominaisuuden kautta. Tämä on seuraavan proposition sisältö.

Propositio 2.78. *Olkoon M R-moduli ja $(M_\alpha)_{\alpha\in\mathcal{A}}$ mielivaltainen perhe R-moduleita. Oletetaan, että jokaisella $\alpha \in \mathcal{A}$ on olemassa R-lineaarinen kuvaus $L_\alpha\colon M_\alpha \to M$. Tällöin on olemassa täsmälleen yksi R-lineaarinen kuvaus $L\colon \oplus_{\alpha\in\mathcal{A}} M_\alpha \to M$ siten, että*

$$L \circ i_\alpha = L_\alpha$$

jokaisella $\alpha \in \mathcal{A}$.

Tämä ominaisuus karakterisoi suoran summan ja kuvaukset $(i_\alpha)_{\alpha\in\mathcal{A}}$ yksikäsitteisesti isomorfiaa vaille. Täsmällisemmin olkoon N jokin R-moduli ja $(i'_\alpha)_{\alpha\in\mathcal{A}}$ kokoelma R-lineaarisia kuvauksia $M_\alpha \to N$, $\alpha \in \mathcal{A}$. Oletetaan, että N toteuttaa saman universaalin ominaisuuden, eli jos M on mikä tahansa R-moduli ja jokaisella $\alpha \in \mathcal{A}$ on annettu R-lineaarinen kuvaus $L_\alpha\colon M_\alpha \to M$, niin on olemassa täsmälleen yksi R-lineaarinen kuvaus $L\colon N \to M$ siten, että

$$L \circ i'_\alpha = L_\alpha$$

jokaisella $\alpha \in \mathcal{A}$. Tällöin N on isomorfinen suoran summan $\oplus_{\alpha\in\mathcal{A}} M_\alpha$ kanssa. Tarkemmin on olemassa isomorfismi $\Phi\colon \oplus_{\alpha\in\mathcal{A}} \to N$ siten, että

$$\Phi \circ i_\alpha = i'_\alpha$$

jokaisella $\alpha \in \mathcal{A}$. Tällainen isomorfismi on yksikäsitteinen.

Todistus. Osoitetaan ensin, että suoran summan konstruktio, joka on annettu yllä, toteuttaa tämän universaaliominaisuuden. Olkoon $L_\alpha\colon M_\alpha \to M$ R-lineaarinen kuvaus jokaisella $\alpha \in \mathcal{A}$. Lemman 2.73 nojalla jokainen $x \in \oplus_{\alpha\in\mathcal{A}}(M_\alpha)$ voidaan kirjoittaa täsmälleen yhdellä tavalla muodossa

$$x = \sum_{\alpha\in\mathcal{A}} i_\alpha(x_\alpha),$$

missä perhe

$$\{i_\alpha(x_\alpha)\}$$

on ain äärelliskantajainen. Jos $L\colon (M_\alpha)_{\alpha\in\mathcal{A}} \to M$ on R-lineaarinen kuvaus, jolle $L \circ i_\alpha = L_\alpha$, niin

$$L(x) = \sum_{\alpha\in\mathcal{A}} L(i_\alpha(x_\alpha)) = \sum_{\alpha\in\mathcal{A}} L_\alpha(x_\alpha).$$

Tämä osoittaa sen, että tällainen kuvaus L on yksikäsitteinen. Kääntäen, määritellään L kaavalla

$$L(x) = \sum_{\alpha\in\mathcal{A}} L_\alpha(x_\alpha),$$

missä $x = \sum_{\alpha\in\mathcal{A}} i_\alpha(x_\alpha)$. Koska tällainen esitys on yksikäsitteinen ja summa on itse asiassa äärellinen, L on hyvin määritelty kuvaus $\oplus_{\alpha\in\mathcal{A}} M_\alpha \to M$. Helposti nähdään, että se on R-lineaarinen ja toteuttaa vaaditun ehdon (tarkista).

Oletetaan kääntäen, että N on mikä tahansa R-moduli, joka toteuttaa suoran summan universaalin ominaisuuden. Koska suora summa toteuttaa sen ominaisuuden (mikä juuri todistetiin), on olemassa yksikäsitteinen R-lineaarinen kuvaus $L\colon \oplus_{\alpha\in\mathcal{A}} M_\alpha \to N$ jolle

$$L \circ i_\alpha = i'_\alpha$$

jokaisella $\alpha \in \mathcal{N}$. Toisaalta koska N ja kuvaukset i'_α puolestaan toteuttavat saman ominaisuuden, on olemassa R-lineaarinen kuvaus $L'\colon N \to \oplus_{\alpha\in\mathcal{A}} M_\alpha$ jolle

$$L' \circ i'_\alpha = i_\alpha$$

jokaisella $\alpha \in \mathcal{N}$.
Tarkastellaan kuvausta $\Phi = L \circ L'\colon N \to N$. Tällöin Φ on sellainen R-lineaarinen kuvaus, jolle

$$\Phi \circ i'_\alpha = L \circ L' \circ i'_\alpha = L \circ i_\alpha = i'_\alpha = \mathrm{id}_N \circ i'_\alpha.$$

Nyt id_N ja Φ ovat molemmat R-lineaariset kuvaukset, joille $\Phi \circ i'_\alpha = \mathrm{id}_N \circ i'_\alpha$ jokaisella $\alpha \in \mathcal{A}$. Oletuksen, eli universaaliominaisuuden, nojalla tällainen kuvaus on kuitenkin yksikäsitteinen. Näin ollen $\Phi = \mathrm{id}_N$, eli $L \circ L' = \mathrm{id}_N$.
Vaihtamalla N:n ja suoran summan $\oplus_{\alpha\in\mathcal{A}} M_\alpha$ roolit yllä olevassa tarkastelussa, saadaan samalla tavalla näytettyä, että $L' \circ L$ on identtinen kuvaus.
Näin ollen L (ja L') on erityisesti bijektio, eli isomorfismi. □

Huomaa, että suoran summan universaaliominaisuus saadaan tulon universaaliominaisuudesta vaihtamalla kaikkien siinä esiintyvien kuvausten suunnat. Koska diagrammeissa kuvaukset on tapana esittää nuolina tämä periaate tunnetaan myös nimellä ”nuolten suuntien vaihto”. Tilanne joka saadaan

toisesta tilannesta vaihtamalla ”nuolten suunnat” sanotaan matematiikassa alkuperäisen tilanteen *duaaliksi*. Suora summa ja tulo ovat siis toistensa *duaaleja*.
Palautetaan mieleen, että olemme jo törmäneet aikaisemmin ”duaali”-termin, itse asiassa viimeisessä luvussa, jossa olemme kutsuneet modulia $L(M, R)$ modulin M duaaliksi. Olemme myös näyttäneet, että jokaista lineaarikuvausta $L\colon M \to N$ vastaa duaalikuvaus $L^*\colon N^* \to M^*$ joka ikäänkuin *vaihtaa suuntaa*. Tästä duaaliavaruuden nimitys tuleekin.

Suoran summan universaaliominaisuutta sovelletaan käytännössä kun konstruoidaan lineaariset kuvaukset $L\colon \oplus_{\alpha\in\mathcal{A}} M_\alpha \to N$. Nimittäin universaaliominaisuushan sanoo, että jos haluamme konstruoida sellainen kuvaus riittää antaa sen arvot alimoduleilla M_α eli antaa jokaisella $\alpha \in \mathcal{A}$ lineaarinen kuvaus $L_\alpha\colon M_\alpha \to N$. Tällöin L on määritelty kaavalla

$$L(\sum_{\alpha\in\mathcal{A}} x_\alpha) = \sum_{\alpha\in\mathcal{A}} L_\alpha(x_\alpha).$$

Tämän luvun lopuksi huomautetaan, että kun indeksijoukko $\mathcal{A} = \{1, \ldots, n\}$ on äärellinen, jokainen tulomodulin $\prod_{i=1}^n M_i$ alkio on äärelliskantajainen, joten tässä tapauksessa suora summa $\oplus_{i=1}^n M_i$ ja tulo $\prod_{i=1}^n M_i$ ovatkin isomorfiset. Kun $\mathcal{A}$ on ääretön tämä ei yleensä pidä paikkansa.

Edellä olemme osoittaneet, että kun R on ykkösellinen rengas, jokaisella $n \in \mathbb{N}$ on olemassa ainakin yksi (itse asiassa isomorfiaa vaille tasan yksi) n-ulotteinen R-moduli, nimittäin R^n.
Käytämällä suoran summan käsitteen voimme nyt konstruoida mielivaltaisella, myös äärettömällä, kannalla varustetun vapaan modulin.
Nimittäin olkoon $\mathcal{A}$ mielivaltainen indeksijoukko. Jokaisella $\alpha \in \mathcal{A}$ olkoon R_α kopio renkaasta R. Ajatelemme jokaisen R_α:n 1-ulotteisena R-modulina, kuten yleensä. Muodostetaan suora summa

$$R^{(\mathcal{A})} = \oplus_{\alpha\in\mathcal{A}} R_\alpha.$$

Jokaisella $\alpha \in \mathcal{A}$ olkoon $e_\alpha \in R^{(\mathcal{A})}$ sellainen alkio, jonka α-komponentti on $1 \in R$ ja muut komponentit ovat nollia. Selvästi e_α on äärelliskantajainen, joten se on hyvin määritelty $R^{(\mathcal{A})}$:n alkio.
Näin konstruoitu joukko $\{e_\alpha \mid \alpha \in \mathcal{A}\}$ on modulin $R^{(\mathcal{A})}$ kanta. Tämän todistaminen jätetään lukijalle harjoitustehtäväksi. Identifioimalla $\alpha \in \mathcal{A}$ ja e_α saadaan todistettua seuraava tulos.

Propositio 2.79. *Olkoon R ykkösellinen rengas ja $\mathcal{A}$ mielivaltainen joukko. Tällöin on olemassa vapaa R-moduli, jonka kanta on joukko $\mathcal{A}$, esimerkiksi moduli $R^{(\mathcal{A})}$.*

Kun $\mathcal{A}$ on äärellinen ja siinä on n alkiota, $R^{(\mathcal{A})}$ on siis n-ulotteinen, eli oleellisesti R^n.

2.6 Multilineaariset kuvaukset ja determinaantti

Olkoot $M_1, \ldots, M_n$ ja N R-modulit (missä edellenkin oletamme, että rengas R on vaihdannainen ja ykkösellinen). Olkoon $F\colon M_1 \times M_2 \times \ldots \times M_n \to N$ kuvaus. F on siis määritelty joukkojen M_i, $i = 1, \ldots, n$ *karteesisessa tulossa*, jonka alkiot ovat järjestyt jonot $(m_1, m_2, \ldots, m_n)$, missä $m_i \in M_i$ kaikilla $i = 1, \ldots, n$.
Kiinnitetään $i \in \{1, \ldots, n\}$ ja alkiot $m_1 \in M_1, m_2 \in M_2, \ldots, m_{i_1} \in M_{i-1}, m_{i+1} \in M_{i+1}, \ldots, m_n \in M_n$. Määritelemme kuvaus $F^i = F^i_{m_1,m_2,\ldots,m_{i-1},m_{i+1},\ldots,m_n}\colon M_i \to N$ kaavalla

$$F^i(m) = F(m_1, m_2, \ldots, m_{i-1}, m, m_{i+1}, \ldots, m_n).$$

Toisin sanoen annetaan kaikille muuttujille, paitsi i:nnelle, vakioarvot ja tarkastellaan syntyvää F:n rajottumaa, joka riippuu siis vain muuttujasta modulista M_i. Jos tämä rajoittuma on aina R-lineaarinen kuvaus $M_i \to N$, sanomme F *n-lineaariseksi*. Toisin sanoen kuvaus $F\colon M_1 \times M_2 \times \ldots \times M_n \to N$ on *n-lineaariseksi* jos ja vain jos kaikilla $i = 1, \ldots, n$, kaikilla $m_1, m_2, \ldots, m_{i-1}, m_i, m_i', m_{i+1}, \ldots, m_n$ ja kaikilla $r \in R$ pätee

$$F(m_1, m_2, \ldots, m_{i-1}, m_i + m_i', m_{i+1}, \ldots, m_n) =$$

$$= F(m_1, m_2, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n) + F(m_1, m_2, \ldots, m_{i-1}, m_i', m_{i+1}, \ldots, m_n),$$

ja

$$F(m_1, m_2, \ldots, m_{i-1}, rm_i, m_{i+1}, \ldots, m_n) = rF(m_1, m_2, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n).$$

Kuvaus, joka on n-multilineaarinen jollakin $n \in \mathbb{N}$, sanotaan yleisesti *multilineaariseksi*. 1-lineaarinen kuvaus on tietenkin sama asia kuin lineaarinen kuvaus $L\colon M \to N$. 2-lineaariset kuvaukset sanotaan *bilineaarisiksi*.

Huomautus: Emme ajatelee tässä karteesista tuloa $M_1 \times M_2 \times \ldots \times M_n$ tulomodulina, vaan tavallisena karteesisina tulona ilman erityista algebrallista struktuuria. Multilineaarinen kuvaus on yleensä ihan eri asia kuin tulomodulilla määritelty lineaarikuvaus!

Olkoon $n \in \mathbb{N}$, $M_1, \ldots, M_n$ ja N R-modulit. Kaikkien n-lineaaristen kuvausten $F\colon M_1 \times M_2 \times \ldots \times M_n \to N$ joukkoa merkitään $L(M_1, M_2, \ldots, M_n; N)$. Aivan kuten erikoistapauksessa $n = 1$, tällä joukolla on luonnollinen R-modulin struktuuri, joka on määritelty pisteittäin ehdoilla

$$(F + F')(m_1, m_2, \ldots, m_n) = F(m_1, m_2, \ldots, m_n) + F'(m_1, m_2, \ldots, m_n),$$

$$(rF)(m_1, m_2, \ldots, m_n) = r \cdot F(m_1, m_2, \ldots, m_n).$$

Myös seuraava Proposition 2.22 yleistys pätee samantyyppisellä todistuksella.

Propositio 2.80. *Olkoon $n \in \mathbb{N}$, $M_1, \ldots, M_n$ ja N R-modulit. Oletetaan, että jokainen moduli M_i on vapaa kannalla $(e^i)_\alpha$, $\alpha \in \mathcal{A}_i$.*
Olkoon $(b_{j_1,\ldots,j_n})_{j_i \in \mathcal{A}_i}$ perhe N:n alkioita, joka on indeksoitu karteesisilla tulolla $\mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{A}_n$. Tällöin on olemassa yksikäsitteinen n-lineaarinen kuvaus $F\colon M_1 \times M_2 \times \ldots \times M_n \to N$ jolle

$$F(e^1_{j_1}, e^2_{j_2}, \ldots, e^n_{j_n}) = b_{j_1,\ldots,j_n}.$$

Todistus. Harjotustehtävä. □

Seuraus 2.81. *Olkoot $M_1, \ldots, M_n$ ja N R-modulit äärellisulotteiset R-modulit. Tällöin $L(M_1, M_2, \ldots, M_n; N)$ on myös äärellisulotteinen ja*

$$\dim L(M_1, M_2, \ldots, M_n; N) = \dim M_1 \cdot \dim M_2 \cdot \ldots \cdot \dim M_n \cdot \dim N.$$

Tärkeä erikoistapaus multilineaarisista kuvauksista on tapaus jossa $M_1 = M_2 = \ldots = M_n = M$ ovat sama moduli ja $N = R$. Multilineaarinen kuvaus $F\colon M^n = M \times M \times \ldots \times M \to R$ sanotaan myös *lineaariseksi n-muodoksi*. Kaikkien lineaaristen n-muotojen joukkoa merkitsemme symbolilla $L^n(M)$. Tämä on R-moduli.

-Permutaatiot.
Palautetaan mieleen sellaisia käsitteitä, kuten äärellisen joukon permutaatio ja sen merkki. Joukon $[n] = \{1, \ldots, n\}$ *permutaatio* on mikä tahansa bijektio $\sigma\colon [n] \to [n]$. Kaikki permutaatiot $[n] \to [n]$ muodostavat ryhmän $\mathrm{Perm}([n]) = \mathrm{Perm}(n)$ (kts. esimerkki 1.3) kuvausten yhdistämisen suhteen. Tämä ryhmä sanotaan myös *symmetriseksi ryhmäksi* kertalukua n ja merkitään lyheämmin symbolilla S_n.
Joukon S_n alkio siis *permutoi* luvut $1, \ldots, n$ eli laittaa ne uuteen järjestykseen. Tätä mielikuvaa vastaa tapa esittää kuvaus $\sigma \in S_n$ muodossa $(i_1, i_2, \ldots, i_n)$ eli jonona jossa $i_1 = \sigma(1), i_2 = \sigma(2)$ ja niin edelleen. Esimerkiksi $(2, 3, 1)$ on

sellainen joukon $\{1,2,3\}$ permutaatio σ jolle pätee $\sigma(1)=2, \sigma(2)=3, \sigma(3)=1$. Koska jokainen permutaatio on bijektio, jono $(i_1, i_2, \ldots, i_n)$ esittää joukon $[n]$ permutaatiota jos ja vain jos siinä ei ole toistoja, eli jonossa esiintyvät alkiot ovat kaikki eri alkioita.
Permutaatio $\sigma \in S_n$ sanotaan *vaihdoksi* jos se vaihtaa kaksi alkiota keskenään, jäättäen muut paikalleen. Täsmällisemmin sanottuna $\sigma \in S_n$ on vaihdos jos on olemassa $i, j \in [n], i \neq j$ niin, että

$$\sigma(k) = \begin{cases} j, \text{ jos } k = i, \\ i, \text{ jos } k = j, \\ k, \text{ muuten .} \end{cases}$$

Vaihdos joka vaihtaa keskenään alkiot i ja j merkitään symbolilla $(i\ j)$. Esimerkiksi joukon $[3]$ vaihdos $(1\ 2)$ on sellainen kuvaus $\sigma\colon [3] \to [3]$ jolle $\sigma(1)=2, \sigma(2)=1, \sigma(3)=3$.

Kurssilla "Lineaarialgebra ja matriisilaskenta" on osoitettu seuraava.

Lemma 2.82. *Olkoon $n \in \mathbb{N}$.*
Jokainen joukon S_n alkio σ voidaan esittää vaihdosten äärellisenä yhdisteenä, toisin sanoen vaihdokset virittävät S_n ryhmänä.
Esitys muodossa $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_i$, missä jokainen τ_k on vaihdos, ei ole yksikäsitteinen, mutta jos $\sigma = \tau_1' \circ \tau_2' \circ \ldots \circ \tau_j'$ on toinen tällainen esitys, joko molemmat i ja j ovat parilliset, tai molemmat parittomat. Näin ollen voidaan määritellä kuvaus sgn: $S_n \to \{1,-1\}$, $sgn(\sigma) = (-1)^i$, missä $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_i$ kuten yllä.
Kuvaus sgn on ryhmähomomorfismi (missä joukossa $\{1,-1\}$ laskutoimitus on tavallinen kertolasku).

Riippuen siitä onko $\operatorname{sgn}(\sigma) = 1$ tai $\operatorname{sgn}(\sigma) = -1$, sanomme permutaatio σ *parilliseksi* tai *parittomaksi.*

Olkoon M R-moduli. Lineaarinen n-muoto $F\colon M^n \to R$ sanotaan *symmetriseksi* jos lähtöjoukon jonon permutaatio ei muuta sen arvoa F:n suhteen. Toisin sanoen F on symmetrinen jos ja vain jos kaikilla $(x_1, \ldots, x_n) \in M^n$ ja jokaisella $\sigma \in S_n$ pätee

$$F(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = F(x_1, \ldots, x_n).$$

F on *antisymmetrinen*, jos kaikilla $(x_1, \ldots, x_n) \in M^n$ ja jokaisella $\sigma \in S_n$ pätee

$$F(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \operatorname{sgn}(\sigma) F(x_1, \ldots, x_n).$$

Koska jokainen permutaatio voidaan kirjoittaa vaihdosten perusteella, nähdään helposti, että pätee seuraava (tarkka todistus harjoitustehtävänä).

Lemma 2.83. *Olkoon $F\colon M^n \to R$ lineaarinen n-muoto. Tällöin F on symmetrinen jos ja vain jos kaikilla $(x_1, \ldots, x_n) \in M^n$ ja $i, j \in [n], i < j$ pätee*

$$F(x_1, \ldots, x_i, \ldots, x_j, x_n) = F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Vastaavasti F on antisymmetrinen jos ja vain jos kaikilla $(x_1, \ldots, x_n) \in M^n$ ja $i, j \in [n], i < j$ pätee

$$F(x_1, \ldots, x_i, \ldots, x_j, x_n) = -F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Toisin sanoen multilineaarinen kuvaus on symmetrinen, jos kahden muuttujan vaihto keskenään ei vaikuta arvoon ja antisymmetrinen, jos kahden muuttujan vaihto muuttaa arvon merkkiä.

Esimerkki 2.84. *Olkoon $n \in \mathbb{N}$ ja tarkastellaan äärellisulotteinen R-moduli R^n. Määritellään niin sanottu "pistetulo" R^n:ssä bilineaarisena muotona $\cdot\colon R^n \times R^n \to R$, joka on määritelty kaavalla*

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i.$$

Helposti nähdään, että tämä kuvaus todellakin on bilineaarinen. Lisäksi se on symmetrinen (koska oletamme, että R on vaihdannainen rengas).
Pistetulon avulla voimme kirjoittaa matriisitulon määritelmä kompaktissa muodossa. Nimittäin olkoot $A \in M(m \times n; R), B \in M(n \times k; R)$ matriisit ja olkoon $C = (c_{ij})$ tulo AB. Tällöin määritelmän nojalla

$$c_{ij} = A_i \cdot B^j,$$

missä tulkitsemme matriisien rivit ja sarakkeet R^n:n alkioina.

Antisymmetriset kuvaukset yleensä nimetetään myös termillä *alternoiva*, paitsi eräässä erikoistapauksessa, jossa osoittautuu, että yllä annettu määritelmä antisymmetriselle kuvaukselle ei ole sitä, mitä halutaan. Syy tähän selviää seuraavasta lemmasta.

Lemma 2.85. *Olkoon $F\colon M^n \to R$ lineaarinen n-muoto. Tarkastellaan seuraavat ehdot.*

1) $F(x_1, \ldots, x, \ldots, x, \ldots, x_n) = 0$ eli jos kaksi argumenttia saavat saman arvon, muodon arvo on 0.

2) F on antisymmetrinen.

Tällöin 1)⇒ 2). Jos lisäksi renkaan R jokaiselle nollasta eroavalle alkiolle pätee $a \neq -a$, niin ehdot 1) ja 2) ovat yhtäpitäviä.
Edellinen ehto on tosi kunnassa K jos ja vain jos K:ssä pätee $2 \neq 0$ (eli kunnan K niin sanottu karakteristiikka *ei ole 2).*

Todistus. Oletetaan, että ehto 1) on voimassa. Olkoot $x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n \in M$, $i < j$. Ehdon 1) nojalla

$$F(x_1, \ldots, x_i + x_j, \ldots, x_i + x_j, \ldots, x_n) = 0.$$

Mutta toisaalta multilineaarisuuden nojalla

$$F(x_1, \ldots, x_i + x_j, \ldots, x_i + x_j, \ldots, x_n) =$$

$$F(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n) + F(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) +$$
$$+F(x_1, \ldots, x_j + x_i, \ldots, x_i + x_j, \ldots, x_n) + F(x_1, \ldots, x_j, \ldots, x_j, \ldots, x_n) =$$
$$= F(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) + F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n),$$

sillä kaksi muuta termiä ovatkin arvoltaan nolla taas ehdon 1) nojalla. Näin olleen

$$F(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) + F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = 0$$

eli

$$F(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = -F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Toisin sanoen F on antisymmetrinen.

Oletetaan, että F on antisymmetrinen. Olkoot $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in M$ ja $x \in M$ mielivaltaiset. Antisymmetrisuudesta seuraa, että

$$F(x_1, \ldots, x, \ldots, x, \ldots, x_n) = -F(x_1, \ldots, x, \ldots, x, \ldots, x_n).$$

Merkitään $a = F(x_1, \ldots, x, \ldots, x, \ldots, x_n) \in R$. Olemme osoittaneet, että R:ssä pätee $a = -a$. Jos renkaassa R tämä tapahtuu jos ja vain jos $a = 0$, tästä seuraa, että

$$F(x_1, \ldots, x, \ldots, x, \ldots, x_n) = 0,$$

eli ehto 1).
Jos tarkasteltava rengas onkin kunta, niin siinä on voimassa supistussääntö, eli ehdosta $1 \cdot a = -a = (-1) \cdot a$ seuraa $1 = -1$ (eli $2 = 0$) tai $a = 0$. □

Edellinen tulos motivoi seuraavan määritelmän.

Määritelmä 2.86. *Olkoon $F\colon M^n \to R$ lineaarinen n-muoto. Sanomme, että F* on alternoiva *n-muoto jos $F(x_1, \ldots, x, \ldots, x, \ldots, x_n) = 0$ eli aina jos kaksi muodon argumenttia saavat saman arvon, muodon arvo on* 0.

Lemma 2.85 sanoo, että alternoiva muoto on aina antisymmetrinen, mutta kääntäinen väite ei vältämättä päde. Esimerkiksi jos $R = \mathbb{Z}_2$, siinä pätee $2 = 1 + 1 = 0$ eli $1 = -1$ Näin ollen tässä tapauksessa muoto $F\colon M^n \to R$ on antisymmetrinen jos ja vain jos se on symmetrinen.
Esimerkiksi olkoot $R = M = \mathbb{Z}_2$ ja määritellään M:ssä 2-muoto F ehdolla

$$F(x, y) = xy.$$

Helposti nähdään, että tämä on symmetrinen lineaarinen 2-muoto, joten se on myös antisymmetrinen. Kuitenkin tämä muoto ei ole alternoiva, sillä

$$F(1, 1) = 1 \cdot 1 = 1 \neq 0 \in \mathbb{Z}_2.$$

Huomaa, että $\mathbb{Z}_2$ on kunta, joten havaittu "ongelma" ei postu, jos rajoitamme tarkastelun vektoriavaruuksiin.

Olkoon M R-moduli. Kaikkien alternoivien muotojen joukkoa merkitään $\mathrm{Alt}^n(M)$. Helposti verifioidaan, että $\mathrm{Alt}^n(M)$ on R-modulin $L^n(M)$ alimoduli, eli R-moduli itse.

Olkoon M äärellisulotteinen R-moduli. Proposition 2.80 nojalla voimme konstruoida multilineaarinen muoto $F\colon M^n \to R$ yksinkertaisesti asettamalla sen arvot mielivaltaisella tavalla kannan alkioista muodostetuista jonoilla. Jos haluamme, että näin saatu kuvaus toteuttaa joitakin lisäominaisuuksia, nämä arvot ei enää voi valita mielivaltaisesti. Tutkitaan, mitä lisäehtoja pitää asettaa, jos haluamme konstruoida alternoivia kuvauksia tällä tavalla.

Lemma 2.87. *Olkoon $F\colon M^n \to R$ multilineaarinen n-muoto, missä M on vapaa R-moduli. Olkoon $(e_\alpha)_{\alpha \in \mathcal{A}}$ sen kanta. Tällöin F on alternoiva jos ja vain jos seuraavat ehdot toteuttuvat.*
Olkoon $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{A}^n$ mielivaltainen n-pituinen jono indeksejä joukosta $\mathcal{A}$. Tällöin
1) jos $\alpha_i = \alpha_j$ joillakin $i < j$, niin

$$F(e_{\alpha_1}, e_{\alpha_2}, \ldots, e_{\alpha_n}) = 0,$$

2) jos $\sigma \in S_n$ on permutaatio, niin

$$F(e_{\alpha_{\sigma(1)}}, e_{\alpha_{\sigma(2)}}, \ldots, e_{\alpha_{\sigma(n)}}) = \operatorname{sgn}\sigma F(e_{\alpha_1}, e_{\alpha_2}, \ldots, e_{\alpha_n}).$$

Toisin sanoen F on alternoiva jos ja vain jos se toteuttaa sekä antisymmetrisen, että alternoivan kuvauksen määritelmän, kun ne sovelletaan kanta-alkioista muodostetuihin jonoihin.

Todistus. Alternoiva kuvaus on myös antisymmetrinen (Lemma 2.85), joten jos F on alternoiva, ehto toteutuu.

Oletetaan kääntäen, että F toteuttaa ehdon. Olkoot $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j_1}, x_{j+1}, \ldots, x_n \in M$ mielivaltaiset ja $x_i = x_j = x$. Meidän on todistettavaa, että

$$F(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_n) = 0.$$

Ensin esitetään jokainen alkio, paitsi x, kanta-alkioiden lineaarisena kombinaationa, eli

$$x_k = \sum_{i_k=1}^{m_k} a_{i_k} e_{\alpha_{i_k}},$$

$k \in [n], k \neq i, j$. Tällöin multilineaarisuudesta seuraa, että

$$F(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_n)$$

voidaan esittää lineaarisena kombinaationa alkioista, jotka ovat muotoa

$$F(e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_{j-1}, x, e_{j+1}, \ldots, e_n),$$

missä $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_{j-1}e_{j+1}, \ldots, e_n$ ovat joitakin kanta-alkioita. Näin ollen riittää osoittaa, että

$$F(e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_{j-1}, x, e_{j+1}, \ldots, e_n) = 0$$

kun $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_{j-1}e_{j+1}, \ldots, e_n$ ovat (mielivaltaisia) kanta-alkioita. Esitetään x lineaarisena kombinaationa

$$x = \sum_{p=1}^{m} a_p f_p,$$

missä f_p, $p = 1, \ldots, m$ ovat (eri)kanta-alkiot. Multilineaarisuuden nojalla

$$F(e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_{j-1}, x, e_{j+1}, \ldots, e_n) =$$

$$= \sum_{p,q} a_p a_q F(e_1, \ldots, e_{i-1}, f_p, e_{i+1}, \ldots, e_{j-1}, f_q, e_{j+1}, \ldots, e_n)$$

Tässä summassa kaikki termit, joissa $p = q$ ovat nolla oletuksen nojalla. Jokaista termiä $F(e_1, \ldots, e_{i-1}, f_p, e_{i+1}, \ldots, e_{j-1}, f_q, e_{j+1}, \ldots, e_n)$, jossa $p < q$, taas vastaa termi $F(e_1, \ldots, e_{i-1}, f_q, e_{i+1}, \ldots, e_{j-1}, f_p, e_{j+1}, \ldots, e_n)$, jonka arvo on tasan $-F(e_1, \ldots, e_{i-1}, f_p, e_{i+1}, \ldots, e_{j-1}, f_q, e_{j+1}, \ldots, e_n)$ oletuksen nojalla. Näin ollen kaikki nämä termit kumoaa toisiaan ja lopputulokseksi tulee nolla. Väite on todistettu. □

Edellisen tuloksen nojalla voimme konstruoida multilineaariset kuvaukset. Rajoitutaan äärellisulotteisen modulin tapaukseen.

Esimerkki 2.88. *Olkoon M n-ulotteinen R-moduli ja olkoon $m \in \mathbb{N}$. Tutkitaan modulia* $\mathrm{Alt}^m(M)$.
Olkoon $(e_1, \ldots, e_n)$ M:n kanta. Tarkastellaan ensin tapausta $m > n$. Olkoon $F\colon M^m \to R$ alternoiva. Nyt jos $(e_{i_1}, \ldots, e_{i_m})$ on mielivaltainen m-pituinen jono M:n kanta-alkioita, niin siinä on pakko olla toistoja (sillä $m > n$). Näin ollen

$$F(e_{i_1}, \ldots, e_{i_m}) = 0$$

Koska tämä pätee kaikille kanta-alkioista muodostetuille jonoille, F:n on oltava nolla-kuvaus. Näin ollen $\mathrm{Alt}^m(M) = \{0\}$ *kun $m > n$.*
Olkoon seuraavaksi $m \leq n$. Olkoon I joukon $[n] = \{1, \ldots, n\}$ osajoukko, jossa on m alkiota. Kirjoitetaan I muodossa

$$I = \{i_1, \ldots, i_m\},$$

siten, että $i_1 < i_2 < \ldots < i_m$. Määritellään multilineaarinen kuvaus $\varepsilon_I\colon M^m \to R$ seuraavasti. Olkoon $(e_{j_1}, \ldots, e_{j_m})$ mielivaltainen m-pituinen kanta-alkioista muodostettu jono. Jos $\{j_1, \ldots, j_m\} \neq \{i_1, \ldots, i_m\}$ asetetaan $\varepsilon_I(e_{j_1}, \ldots, e_{j_m}) = 0$. Huomaa, että erityisesti näin käy kun jonossa $(e_{j_1}, \ldots, e_{j_m})$ on toistoja. Kun taas $\{j_1, \ldots, j_m\} = \{i_1, \ldots, i_m\}$, niin on olemassa tasan yksi permutaatio $\sigma \in S_n$ siten, että $j_k = i_{\sigma(k)}$ jokaisella $k = 1, \ldots, m$. Asetetaan

$$\varepsilon_I(e_{j_1}, \ldots, e_{j_m}) = \operatorname{sgn}\sigma.$$

Edellisen lemman mukaan ε_I on alternoiva m-muoto (tarkista yksitysikohdat).

Lause 2.89. *Olkoon M äärellisulotteinen R-moduli ja olkoon $(e_1, \ldots, e_n)$ sen kanta. Tällöin* $\mathrm{Alt}^m(M)$ *on vapaa äärellisulotteinen R-moduli jokaisella $m \in \mathbb{N}$. Lisäksi*

1) *jos $m > n$ moduli* $\mathrm{Alt}^m(M)$ *on triviaali eli ei ole olemassa nollasta eroavia m-alternovia muotoja,*

2) *jos $m \leq n$ modulin* $\mathrm{Alt}^m(M)$ *dimensio on*

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

ja joukko

$$\{\varepsilon_I \mid I \subset [n], |I| = m\}$$

on sen kanta.

Erityisesti $\mathrm{Alt}^m(M)$ *on* 1*-ulotteinen ja eräs sen viritävää alkio on multilineaarinen alternoiva muoto* $\varepsilon_{[n]}$ *jolle pätee*

$$\varepsilon_{[n]}(e_1, \ldots, e_n) = 1.$$

Todistus. 1) on osoitettu jo edellisessä esimerkissä. Siinäkin on konstruoitu joukko aternoivia muotoja $\{\varepsilon_I \mid I \subset [n], |I| = m\}$. Huomaa, että tämän joukon koko on tasan $\binom{n}{m} = \frac{n!}{m!(n-m)!}$.
Osoitetaan, että tämä joukko on kanta kun $m = n$. Yleinen tapaus jätetään harjoitustehtäväksi.
Olkoon $F\colon M^n \to R$ alternoiva n-muoto. Olkoon $a = F(e_1, \ldots, e_n)$. Osoitetaan, että $F = a\varepsilon_{[n]}$. Olkoon $(e_{i_1}, \ldots, e_{i_n})$ n-pituinen jono, joka on muodostettu kanta-alkioista. Jos siinä on toistoja, sekä F, että $\varepsilon_{[n]}$ antavat molemmilla arvokseen 0. Jos taas siinä ei ole toistoja, niin $(i_1, \ldots, i_n)$ on $\{1, \ldots, n\}$:n permutaatio, eli on olemassa $\sigma \in S_n$ siten, että $i_j = \sigma(j)$, $j = 1, \ldots, n$. Koska F ja ε_I ovat molemmat alternoivia,

$$F(e_{i_1}, \ldots, e_{i_n}) = \operatorname{sgn}\sigma F(e_1, \ldots, e_n) = \operatorname{sgn}\sigma a = a\varepsilon_{[n]}(e_{i_1}, \ldots, e_{i_n}).$$

Näin ollen $\varepsilon_{[n]}$ virittää avaruuden $\mathrm{Alt}^n(M)$. Jos

$$a\varepsilon_{[n]} = 0,$$

niin $a = a\varepsilon_{[n]}(e_1, \ldots, e_n) = 0$. Näin ollen $\{\varepsilon_{[n]}\}$ on vapaa.
Väite on todistettu. □

Matriisin determinantti.
Sovellamme seuraavaksi alternoivien muotojen teoriaa määritääksemme matriisin ja lineaarisen kuvauksen determinantin. Aloitetaan matriiseista. Olkoon $A \in M(n \times n; R)$ *neliö*-matriisi, jonka kertoimet ovat vaihdannaisen renkaan R alkiot. Palautetana mieleen, että A:n i:s $(a_{1i}, a_{2i}, \ldots, _{ni})$ sarake merkitään symbolilla A^i ja ajatellaan vapaan modulin R^n alkiona. Tällöin voimme määritellä kuvaus $M(n \times n; R) \to (R^n)^n$,

$$A \mapsto (A^1, A^2, \ldots, A^n).$$

Helposti nähdään, että tämä kuvaus on R-modulien *isomorfismi*, toisin sanoen voimme identifioida matriisi A ja sen sarakkeitten muodostama jono keskenään.

Olkoon $(e_1, \ldots, e_n)$ R^n:n standardi kanta, jossa $e_i = (0, \ldots, 1, \ldots, 0)$. Lauseen 2.89 mukaan n-alternoivien muotojen moduli $\mathrm{Alt}^n(R^n)$ on 1-ulotteinen ja jokainen alternoiva n-muoto $F\colon (R^n)^n \to R$ voidaan kirjoittaa muodossa

$$F = a\ \varepsilon^{[n]}$$

yksikäsiteisellä $a \in R$. Huomaa, että määritelmän mukaan pätee

$$\varepsilon^{[n]}(e_1, \ldots, e_n) = 1,$$

joten jos $F = a\ \varepsilon^{[n]}$, niin

$$a = F(e_1, \ldots, e_n).$$

Saamme siis seuraavan tuloksen.

Lemma 2.90. *On olemassa tasan yksi alternoiva n-muoto $F \in \mathrm{Alt}^n(R^n)$, jolle*

$$F(e_1, \ldots, e_n) = 1,$$

nimittäin muoto $\varepsilon^{[n]}$.

Jos tämä tulos käännetään $(n \times n)$-matriisien kielelle, saadaan osoitettua niin sanottu *determinantin* olemassaolo ja yksikäsiteisyys.

Lause 2.91. *Olkoon R vaihdannainen ykkösellinen rengas ja olkoon $n \in \mathbb{N}$. Tällöin on olemassa tasan yksi kuvaus* $\det\colon M(n \times n; R) \to R$ *jolla on seuraavat ominaisuudet,*

(1) $\det(A)$ *on multilineaarinen kuvaus matriisin A sarakkeiden suhteen,*

(2) jos matriisilla A on kaksi täysin samanlaista saraketta, niin $\det A = 0$ *(toisin sanoen sarakkeiden suhteen* det *on alternoiva n-muoto),*

(3) $\det(I_n) = 1$*, missä I_n on $(n \times n)$-kokoinen yksikkömatriisi.*

Tämä kuvaus sanotaan determinantti *kuvaukseksi. Jos A on neliömatriisi,* $\det(A)$ *on* matriisin A determinantti.

Kuten lukija on varmasti oppinut aikaisemmalla lineaarialgebran kurssilla, determinanttien käyttö helpottaa lineaarikuvausten tutkimista. Näemme tästä paljon esimerkkejä jatkossa. Palautetaan vielä mieleen determinantin perusominaisuuksia.
Jotta determinantistä olisi hyötyä käytännössä, on osatava laskea determinantin arvo annetulle matriisille. Suoraan määritelmästä saamme determinantille konkrettisen kaavan seuraavasti. Olkoon $A = (a_{ij})_{i,j=1,\ldots,n}$ neliömatriisi. Tulkitaan se, kuten yllä, $(R^n)^n$:n alkiona $(A^1, \ldots, A^n)$, missä

$A^j = \sum_{i=1}^n a_{ij} e_i$ (lineaarinen esitys R^n:n standardikannan $(e_1, \ldots, e_n)$ suhteen). Koska $\det A$ on tällöin sama asia kuin $\varepsilon^{[n]}(A^1, A^2, \ldots, A^n)$ saamme

$$\det(A) = (\varepsilon^{[n]})(A^1, A^2, \ldots, A^n) = \sum_{i_1,\ldots,i_n} a_{i_1 1} a_{i_2 2} \ldots a_{i_n n} \varepsilon^{[n]}(e_{i_1}, e_{i_2}, \ldots, e_{i_n}).$$

Tässä summataan siis kaikkien mahdollisten jonojen $(i_1, \ldots, i_n) \in [n]^n$ yli. Mutta jos tällaisessa jonossa on toistoja, $\varepsilon^{[n]}(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) = 0$ alternoivan muodon määritelmän nojalla. Jos taas siinä ei ole toistoja, on olemassa permutaatio $\sigma \in S_n$ siten, että $i_j = \sigma(j)$ kaikilla $j = 1, \ldots, n$, jolloin

$$\varepsilon^{[n]}(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) = (\operatorname{sgn} \sigma)\varepsilon(e_1, \ldots, e_n) = \operatorname{sgn} \sigma.$$

Näin ollen

$$\det(A) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma(1)1} a_{\sigma(2)2} \ldots a_{\sigma(n)n}. \tag{2.92}$$

Tämä kaava on käyttökelpoinen esimerkiksi kun lasketaan (2×2)-matriisin determinantin, sillä tällöin summassa on vain kaksi termiä ja saadaan

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

(3×3)-matriisin determinantin laskeminen yllä annetun kaavan mukaan myös onnistuu periaattessa ihan hyvin, silloin summassa on 6 termiä, mutta jo seuraavassa dimensiossa, eli (4×4)-matriisin tapauksessa, kaavassa on 24 yhteenlaskettavaa termiä, eikä kaava (2.92) ole enää kovin käyttökelpoinen. (5×5)-matriisin tapauksessa summassa on jo 120 termiä, eikä sillä enää kannattaa laskea mitään ollenkaan (paitsi jos olet tietokone, mutta silloinkin parempi säästää aikaa käyttämällä muita menetelmiä). Kaavalla (2.92) onkin lähinnä teorettisia sovelluksia, kuten esimerkiksi seuraavan lemman todistuksessa.

Lemma 2.93. *Olkoon A $(n \times n)$-matriisi. Tällöin*

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

Todistus. Kaavan 2.92 nojalla

$$\det(A^T) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}.$$

Olkoon $\sigma \in S_n$. Merkitään $\sigma(i) = k_i$, tällöin $\sigma^{-1}(k_i) = i$. Näillä mekinnäillä voimme siis jokainen termi $a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)}$ yhtä hyvin kirjoittaa muodossa

$$a_{\sigma^{-1}(k_i)k_i}a_{\sigma^{-1}(k_2)k_2} \dots a_{\sigma^{-1}(k_n)k_n}.$$

Koska σ on bijektio, jono $(k_1, k_2, \dots, k_n)$ sisältää jokaisen luvun joukosta $\{1, \dots, n\}$ täsmälleen kerran. Koska oletamme, että kerroinrengas R on vaihdannainen, voimme permutoimalla termit kirjoittaa $a_{\sigma^{-1}(k_i)k_i}a_{\sigma^{-1}(k_2)k_2} \dots a_{\sigma^{-1}(k_n)k_n}$ muodossa

$$a_{\sigma^{-1}(1)1}a_{\sigma^{-1}(2)2} \dots a_{\sigma^{-1}(n)n}.$$

Näin ollen

$$\det(A^T) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma^{-1}(1)1}a_{\sigma^{-1}(2)2} \dots a_{\sigma^{-1}(n)n}.$$

Koska σ^{-1} käy läpi täsmälleen samat arvot kuin σ, kun viimeiksi mainittu käy läpi kaikki permutaatiot joukosta S_n (eli vastaavuus $\sigma \mapsto \sigma^{-1}$ on bijektio, mieti miksi), ja $\operatorname{sgn} \sigma^{-1} = \operatorname{sgn} \sigma$ (tarkista!), summa oikealla puoleella on sama kuin

$$\sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma(1)1}a_{\sigma(2)2} \dots a_{\sigma(n)n}$$

eli $\det A$. □

Kuten olemme jo huomauttaneet, kaavaa (2.92) on yleensä mahdotonta käytää sellaisina konkrettisissa laskuissa, joten meidän on keksittävää parempia menetelmiä determinantin laskemiseksi. Suosittu menetelmä on niin sanottu ”kehittäminen rivin/sarakkeen mukaan”, joka on varmasti tuttu lukijalle. Palautetaan mieleen miten se menee. Määritellään ensin matriisin alimatriisin käsitteen.

Olkoon $A = (a_{ij})_{i=1,\dots,m,j=1,\dots,n}$ matriisi (ei vältämättä neliömatriisi). Mikä tahansa matriisi joka saadaan poistamalla A:sta mielivaltainen (mahdollisesti tyhjä) määrä riveja ja sarakkeita sanotaan A:n *alimatriisiksi* tai *minoriksi*. Jos alimatriisin koko on $(k \times l)$, puhutaan $(k \times l)$-minorista.
Täsmällisemmin voimme määritellä alimatriisin käsitettä seuraavasti. Valitaan jonosta $1, \dots, m$ osajono $i_1 < i_2 < \dots < i_k$ ja jonosta $1, \dots, n$ osajono $j_1 < i_2 < \dots < i_l$. Tällöin $B = (a_{i_p j_q})_{p=1,\dots,k,q=1,\dots,l}$ on A:n $(k \times l)$-alimatriisi. Olkoon A $(n \times n)$-matriisi ja $i, j \in \{1, \dots, n\}$. Tällöin merkitsemme symbolilla A_{ij} sellainen A:n $(n-1) \times (n-1)$-alimatriisi, joka on saatu A:sta poistamalla siitä i'nnes rivi ja j'nnes sarake.

Propositio 2.94. *Olkoon A $(n \times n)$-matriisi, missä $n > 1$.*
*1) Kiinnitetään $i = 1, \ldots, n$. Tällöin (*kehittäminen rivin i mukaan*)*

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

*2) Kiinnitetään $j = 1, \ldots, n$. Tällöin (*kehittäminen sarakkeen j mukaan*)*

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

Todistus. 1) Riittää osoittaa, että kaava

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

määrittelee kuvauksen, joka on multilineaarisen matriisin A sarakkeiden suhteen, alternoiva ja antaa arvokseen 1, kun $A = I_n$ on yksikkömatriisi. Tämä on helppo lasku, joka jätetään lukijalle harjoitustehtäväksi.
2) Sovelletaan 1) A:n transpoosiin A^T ja käytetään sitä tietoa, että $\det A^T = \det A$ jokaiselle matriisille A (Lemma 2.93). □

Determinantti on yhteensopiva matriisien kertolaskun ja renkaan kertolaskun suhteen.

Propositio 2.95. *Olkoot A, B $(n \times n)$-matriisit. Tällöin*

$$\det(AB) = \det A \cdot \det B.$$

Todistus. Kiinnitetään matriisi A ja osoitetaan, että kuvaus $B \mapsto \det(AB)$ on multilineaarinen ja alternoiva B:n sarakkeiden suhteen. Merkitään, kuten ennen, A:n rivit $A_1, \ldots, A_n$ ja B:n sarakkeet $B^1, \ldots, B^n$. Olkoon B' matriisi, jolla on samat sarakkeet kuin B:llä, paitsi sarake B'^k on erilainen. Merkitään B'':llä matriisi,jolla on samat sarakkeet kuin B:llä (ja B':llä), paitsi $B''^k = B_k + B'^k$. Merkitään $C = AB, C' = AB', C'' = AB''$. Meidän on osoitettavaa, että

$$\det(C'') = \det(C) + \det(C').$$

Käytämällä pistetuloa (kts. esim. 2.84), näemme, että $c_{ij} = A_i \cdot B^j$, joten C:n j'nnes sarake C^j on jono $(A_1 \cdot B^j, A_2 \cdot B^j, \ldots, A_n \cdot B^j)$. Tästä seuraa, että C':n kaikki sarakkeet ovat samat kuin C:n sarakkeet, paitsi, että sarake C'^k on jono $(A_1 \cdot B'^k, A_2 \cdot B'^k_k, \ldots, A_n \cdot B'^k_k)$. Samoin C'':n kaikki sarakkeet ovat samat kuin C:n sarakkeet, paitsi, että C''^k_k on jono $(A_1 \cdot (B^k + B'^k), A_2 \cdot (B^k +$

$B'^k), \ldots, A_n \cdot (B^k + B'^k))$. Koska pistetulo on bilineaarinen, pätee $A_i \cdot (B^k + B'^k) = A_i \cdot B^k + A_i \cdot B'^k$, eli

$$C''^k = C^k + C'^k.$$

Koska det on multilineaarinen, pätee $\det(C'') = \det(C) + \det(C')$, mitä pitikin todistaa.
Samalla tavalla todistetaan, että toinen multilineaarisuus-ehdoista on voimassa.
Osoitetaan, että kuvaus on alternoiva. Olkoon B:n sarakkeet B^i ja B^j samat, $i \neq j$. Tällöin kuten yllä nähdään, että matriisin $C = AB$ vastaavat sarakkeet C^i ja C^j ovat samat. Koska det on alternoiva, $\det(AB) = \det C = 0$. Näin ollen kuvaus $B \mapsto \det(AB)$ on alternoiva n-muoto (sarakkeiden suhteen). Koska det virittää avaruuden $\mathrm{Alt}^n(R^n)$, on olemassa vakio $a \in R$ siten, että

$$\det(AB) = a \det(B)$$

kaikilla $B \in M(n \times n; R)$. Laskemalla yhtälön molempien puolten arvo kun $B = I_n$ on yksikkömatriisi, saadaan $a = \det(A)$. Näin ollen

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

□

Determinaantin avulla voi tarkistaa onko matriisi kääntyvä vai singulaarinen. Tämä on itse asiassa yksi tärkeimmistä determinaantin sovelluksista.

Propositio 2.96. *(***Cramerin sääntö***)Olkoon A R-kertoiminen $n \times n$-matriisi. Tällöin A on kääntyvä jos ja vain jos* $\det A$ *on kääntyvä R:ssä. Jos* $\det A$ *on kääntyvä, käänteismatriisin A^{-1} alkiot saadaan kaavasta*

$$(A^{-1})_{ij} = (\det A)^{-1}(-1)^{i+j} \det(A_{ji}).$$

Lisäksi tässä tapauksessa

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

Todistus. Olkoon A kääntyvä. Tällöin edellisen proposition nojalla

$$\det A \det(A^{-1}) = \det AA^{-1} = \det I_n = 1 = \det A^{-1}A = \det A^{-1} \det A.$$

Näin ollen $\det A$ on kääntyvä renkaassa R ja lisäksi

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

Oletetaan kääntäen, että $\det A = a$ on kääntyväc renkaassa R. Muodostetaan matriisi $B = (b_{ij}) \in M(n \times n, R)$ ehdolla

$$b_{ij} = a^{-1}(-1)^{i+j} \det(A_{ji}).$$

Lasketaan AB. Olkoot $i, j \in [n]$. Tällöin

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a^{-1}(\sum_{k=1}^{n} (-1)^{k+j} a_{ik} \det(A_{jk})).$$

Oletetaan ensin, että $i \neq j$. Olkoon A' sellainen matriisi, joka on muuten kuin A, paitsi, että rivi A'_i on sama kuin rivi A_j. Jos tällaisen matriisin determinaantti lasketaan kehittelemällä sen j:n rivin mukaan, saadaan juuri yllä esintyvä lauseke $\sum_{k=1}^{n} (-1)^{k+j} a_{ik} \det(A_{jk})$. Toisaalta A' on sellainen matriisi, jolla on kaksi samaa riviä, joten A'^T on matriisi, jolla on kaksi sama saraketta, mistä seuraa, että

$$\sum_{k=1}^{n} (-1)^{k+j} a_{ik} \det(A_{jk}) = \det A' = \det A'^T = 0.$$

Näin ollen $(AB)_{ij} = 0$.
Seuraavaksi oletetaan, että $i = j$. Saadaan

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} = a^{-1}(\sum_{k=1}^{n} (-1)^{k+i} a_{ik} \det(A_{ik})).$$

Oikealla puoleella suluissa esiintyvä lauseke $\sum_{k=1}^{n} (-1)^{k+i} a_{ik} \det(A_{ik})$ on tasan $\det A = a$ (kehitetään rivin i mukaan). Näin ollen $(AB)_{ii} = 1$.
Olemme näyttäneet, että $AB = I_n$. Samalla tavalla voidaan osoittaa, että $BA = I_n$. Näin ollen A on kääntyvä ja sen käänteismatriisi on B. □

Erityisesti kääntyvän 2×2-matriisin käänteismatriisille saada helppo kaava

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Esimerkki 2.97. *Palataan kompleksilukujen konstruktioon (kts. luku 1.1) ja näytetään, miten voidaan helposti osoittaa, että kompleksilukujen joukko $\mathbb{C}$ on kunta lineaarialgebran avulla. Samalla johdetaan lauseke kompleksiluvun käänteisalkiolle.*
Olkoon $z = (a, b) \in \mathbb{R}^2 = \mathbb{C}$ mielivaltainen kompleksiluku. Tarkastellaan kuvaus $\phi_z \colon \mathbb{C} \to \mathbb{C}$, $\phi_z(w) = zw$. Kuvaus ϕ_z on siis z:lla kertominen $\mathbb{C}$:ssä. Jos

ϕ_z ajatellaan kuvauksena $\mathbb{R}^2 \to \mathbb{R}^2$, sille saadaan kompleksilukujen kertolaskun määritelmän nojalla kaavan

$$\phi_z(x, y) = (ax - by, ay + bx).$$

Tämä on selvästi $\mathbb{R}$-lineaarinen kuvaus, jos tarkastellaan $\mathbb{R}^2$ $\mathbb{R}$-vektoriavaruutena. Tämä avaruus on 2-ulotteinen ja sillä on kanoninen kanta $\mathbf{e} = \{e_1, e_2\}$, missä $e_1 = (1, 0)$ ja $e_2 = (0, 1)$. Tämän kannan suhteen kuvauksella ϕ_z on matriisiesitys

$$\Phi_z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Näin saadaan kuvaus $\Phi\mathbb{C} \to M(2 \times 2; \mathbb{R})$, $z \mapsto \Phi(z)$.
Helposti verifioidaan, että tämä kuvaus on yhteensopiva sekä yhteenlaskun-, että kertolaskun suhteen, missä vasemmalla puoleella ovat $\mathbb{C}$:n laskutoimitukset, ja oikealla puolella matriisien yhteen-ja kertolasku (harjoitustehtävä). Lisäksi kuvaus Φ on injektio, sillä z:n komponentit a ja b saadaan takaisin matriisin Φ_z ensimmäisestä sarakkesta. Näin ollen algebrallisena struktuurina $(\mathbb{C}, +, \cdot)$ on täysin isomorfinen erään struktuurin $(M(2 \times 2; \mathbb{R}), +, \cdot)$ alistruktuurin

$$\mathbb{C}' = \{\Phi_z \mid z \in \mathbb{C}\}$$

kanssa. Erityisesti sillä on kaikki samat ominaisuudet, mitä matriisien yhteen- ja kertolaskulla on. Esimerkiksi nähdään heti, että kompleksilukujen kertolasku on assosiatiivinen ja osittelee yhteenlaskun suhteen. Koska tiedämme sen lisäksi, että kompleksiluvulla (a, b) on olemassa yhteenlaskun suhteen vastaalkio $(-a, -b)$, olemme näyttäneet, että $(\mathbb{C}, +, \cdot)$ on ykkösellinen rengas. Kertolaskun kommutatiivisuus on helppo lasku.
Jäljelle jää sen osoittameinen, että $\mathbb{C}$:ssä jokaisella nollasta eroavalla alkiolla on kertolaskun suhteen käänteisalkio. Koska $\mathbb{C}$ on isomofinen $\mathbb{C}'$:n kanssa, riittää osoittaa sama $\mathbb{C}'$:lle. Mutta $\mathbb{C}'$:n alkiot ovat 2×2-matriiseja ja meillä on helppo tapa tarkistaa, onko matriisi kääntyvä - laskemalla sen determinantti. Koska

$$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2,$$

nähdään, että Φ_z on kääntyvä täsmälleen silloin kun $z = (a, b) \neq 0$ eli täsmälleen silloin, kun Φ_z ei ole nolla-matriisi. Lisäksi Cramerin sääntö antaa suoraan kaavan matriisille Φ_z^{-1},

$$(\Phi_z)^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \Phi_{z'},$$

missä $z' = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$*. Näin ollen* $zz' = z'z = 1$*, joten osoitettiin, että* $\mathbb{C}$ *todellakin on kunta. Samalla johdettiin kaavaa käänteisluvulle.*

Sen lisäksi, että olemme näyttäneet $\mathbb{C}$ *kunnaksi, olemme myös samalla keksineet uuden tavan konstruoida ja tulkita kompleksilukuja. Nimittäin kompleksiluku voi ajatella muotoa*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \mathbb{R}$$

olevana matriisina tai ekvivalentisti vastavaana lineaarisena kuvauksena (standardikantojen suhteen). Algebralliset operaatiot ovat tällöin tuttuja matriisien (tai lineaarikuvausten) laskutoimituksia.

Jos $a^2 + b^2 = 1$*, eli kompleksiluku* (a, b) *sijaitsee tason yksikköympyrällä, vastaava lineaarikuvaus on tason* **kierto** *origon ympärillä (vastapäivään) pisteen* (a, b) *määrämän kulman verran. Tästä puhutaan tarkemmin myöhemmin, kun käsitellään sisätuloavaruuksia.*

Jos taas $z = (a, 0)$ *on reaaliluku, sitä vastaava lineaarinen kuvaus* Φ_z *on yksinkertaisesti sama kuin skalaarikertoiminen a:llä* $\mathbb{R}$*-modulissa* $\mathbb{R}^2$*. Geometrisesti tämä kuvaus säilyttää kaikkien pisteiden suunnan, mutta venyttää niiden etäisyys origosta luvulla a (jos a on negatiivinen ensin peilataan piste* (x, y) *origon suhteen vasta-alkioksi* $(-x, -y)$*). Tällainen venetys kutsutaan myös* dilataatioksi
Yleinen ϕ_z *on näiden kahden tapauksen kombinaatio - se on kierron ja dilaataation yhdistelmä.*

Olemme ennen näyttäneet, että kompleksiluvut ja niiden algebralliset operaatiot pulpahtavat auttomaattisesti näkyviin, jos yritetään keksiä luonnollinen laajennus reaaliluvuille, jossa yhtälöllä

$$x^2 = -1$$

olisi ratkaisu. Tämä on puhtaasti "algebrallinen" tapa päästää kompleksilukujen käsiksi. Se saattaa näyttää huijakselta - vaikka tiedämme, että yllämainitulla yhtälöllä "oikeasti" ole ratkaisuja, keksitään sellaiset väkisin "tyhjästä"

Tässä esimerkissä olemme törmänneet luonnolliseen kompleksilukujen "geometriseen" tulkintaan, jonka mukaan niitä voi ajatella tason yksinkertaisina ja hyvin konkrettisina liikkeinä - kiertoina, peilauksina ja dilaatatioina. Ehto $i^2 = 1$ *tässä tulkinnassa tarkoittaa yksinkertaisesti sitä, että kun suoritetaan*

90 *asteen kierto kahdesti, ollaan tehty kaiken kaikkiaan* 180 *asteen kierron, mikä on triviaalisti selvää. Tämä osoittaa sen, että vaikka kompleksilukuja ajateltiinkin aikoinaan "kuvittelisina oliona "(mistä englanninkielinen "imaginary number" termi tulee), joita " ei ole olemassa", ei kompleksiluvuissa ole mitään kuvittelistä ja epätodellista - niitä voi ajatella hyvin konkrettisina ja luonnollisina geometerisina liikkeinä, joita sekä matemaatikot, että esimerkiksi fyysikot ovat tutkineet jo vuosisatoja.*

- **Lineaarisen kuvauksen determinantti.** Olkoon M äärellisulotteinen R-moduli ja olkoon $L\colon M \to M$ lineaarinen kuvaus (tällaisia lineaarisia kuvauksia, joilla lähtö ja maali ovat sama moduli sanotaan myös *endomorfismiksi*). Haluamme määritellä kuvauksen L determinantti. Koska M on äärellisulotteinen, sillä on kanta $\bar{e} = (e_1, \ldots, e_n)$. Määritelemme

$$\det L = \det[L]_{\bar{e},\bar{e}}. \tag{2.98}$$

Toisin sanoen esitetaan L matriisina kannassa $\bar{e}$ (sama kanta lähtö- ja maalipuoleella!) ja otetaan determinantti tästä matriisista.
Mutta onko kaava 2.98 hyvin määritelty? Voimmehan löytää M:lle toinen kanta $\bar{f} = (f_1, \ldots, f_n)$, jolloin saadaan toinen matriisiesitys $[L]_{\bar{f},\bar{f}}$. Onko tällä matrisilla sama determinantti kuin matriisilla $[L]_{\bar{e},\bar{e}}$ (jos ei ole, määritelmässämme ei ole mitään järkeä)?

Osoitauttu, että näillä matriiseilla on sama determinaantti, joten kaava 2.98 on hyvin määritelty. Nimittäin on olemassa kannanvaihtomatriisit $A = [\mathrm{id}]_{\mathbf{e},\mathbf{f}}$ ja $B = [\mathrm{id}]_{\mathbf{f},\mathbf{e}}$. Lisäksi A on kääntyvä ja $A^{-1} = B$. Pätee

$$[L]_{\mathbf{e},\mathbf{e}} = A[L]_{\mathbf{f},\mathbf{f}}A^{-1},$$

joten Propositioista 2.95, 2.96 ja siitä, että R on kommutatiivinen rengas, saadaan

$$\det[L]_{\mathbf{e},\mathbf{e}} = \det A \det[L]_{\mathbf{f},\mathbf{f}} \det A^{-1} = \det A \det A^{-1} \det[L]_{\mathbf{f},\mathbf{f}} = \det[L]_{\mathbf{f},\mathbf{f}}.$$

Näin ollen endomorfismin determinantti kaavassa 2.98 on hyvin määritelty.

Koska lineaarinen kuvaus on isomorfismi jos ja vain jos sen matriisi on kääntyvä, Propositiosta 2.96 seuraa heti seuraava tulos.

Seuraus 2.99. *Olkoon M äärellisulotteinen R-moduli ja $L\colon M \to M$ lineaarinen endomorfismi. Tällöin L on isomorfismi jos ja vain jos* $\det L$ *on kääntyvä renkaassa R.*
Erityisesti jos K on kunta ja V K-vektoriavaruus, niin lineaarinen kuvaus $L\colon V \to V$ on isomorfismi jos ja vain jos $\det L \neq 0$.

Vaikka determinaantit sellaisenaan ovat määriteltyjä vain neliömatriiseille ja endomorfismeille, niitä voi soveltaa myös yleisempien lineaaristen kuvausten tutkimiseen. Tarkastelemme vain vektoriavaruuksien tapaus. Vaikka seuraavan proposition olisimme voineet muotoilla ja todistaa aikaisemminkin, se kuuluu hengeltään tähän osioon.

Olkoon $L\colon M \to N$ R-lineaarinen kuvaus äärellisulotteisten R-modulien välillä. Olkoon $A = [L]_{\mathbf{f},\mathbf{e}}$ L:n matriisi joidenkin M:n ja N:n kantojen suhteen.
Tällöin pätee

$$\dim \operatorname{Im} L = \dim \operatorname{Col}(A).$$

Propositio 2.100. *Olkoon $L\colon V \to W$ K-lineaarinen kuvaus äärellisulotteisten K-vektoriavaruuksien välillä. Olkoon $A = [L]_{\mathbf{f},\mathbf{e}}$ L:n matriisi joidenkin V:n ja W:n kantojen suhteen. Tällöin* $\dim \operatorname{Im} L = k$ *on suurin sellainen luku k, jolle matriisilla A on olemassa kääntyvä $(k \times k)$-alimatriisi.*

Todistus. Olkoon k suurin luonnollinen luku siten, että A:lla on olemassa kääntyvä $(k \times k)$-alimatriisi B. Tulkitsemme (0×0)-matriisi eli tyhjä matriisi kääntyväksi matriisiksi, joten k on olemassa joka tapauksessa.
Osoitetaan, että $k \leq \dim \operatorname{Im} L$. Koska alimatriisi B on kääntyvä, sen sarakkeet $B^1, \ldots, B^k$ muodostavat avaruuden K^k kannan, erityisesti vapaan jonon. Tarkastellaan vastavien A:n sarakkeiden $A^{i_1}, \ldots, A^{i_k}$ muodostamaa jonoa. Oletetaan, että se on sidottu ja olkoon

$$r_1 A^{i_1} + \ldots + r_k A^{i_k} = 0$$

epätriviaali kombinaatio. Rajoittumalla B:n riveihin saadaan vastaava B:n sarakkeista muodostettu epätriviaali kombinaatio. Tämä on ristiriidassa sen kanssa, että $B^1, \ldots, B^k$ on vapaa jono. Näin ollen myös jono $A^{i_1}, \ldots, A^{i_k}$ on vapaa. Tämä on avaruuden $\operatorname{Col}(A)$ vapaa osajono, joten $\dim \operatorname{Col}(A) \geq k$ (tässä kohdassa tarvitaan oletus "K on kunta"). Mutta $\operatorname{Col}(A)$ ja $\operatorname{Im}(L)$ ovat isomorfiset, joten erityisesti $\dim \operatorname{Im} L \geq k$.

Seuraavaksi osoitetaan, että $\operatorname{Im} L \leq k$. Olkoon $\operatorname{Im} L = l$. Riittää löytää A:n $(l \times l)$-alimatriisi B, joka on kääntyvä. Koska $\dim \operatorname{Col} A = \dim \operatorname{Im} L = l$, voidaan löytää l kappaletta A:n sarakkeita $A^{i_1}, \ldots, A^{i_l}$, jotka muodostavat $\operatorname{Col}(A)$:n kannan (Lemma 2.13). Muodostetaan A:n $(m \times l)$-alimatriisi C, johon otetaan mukaan täsmälleen sarakkeet $A^{i_1}, \ldots, A^{i_l}$. Tällöin $\dim \operatorname{Col}(C) = l$. Toisaalta $\dim \operatorname{Row}(C) = \dim \operatorname{Col}(C) = l$ (Propositio 2.59), joten voimme C:n riveistä valita täsmälleen l riviä $C_{j_1}, \ldots, C_{j_l}$, jotka muodostavat avaruuden $\operatorname{Row}(C)$ kannan. Muodostetaan näistä riveistä C:n $(l \times l)$-alimatriisi B. Tällöin B on myös A:n alimatriisi ja $\dim \operatorname{Row} B = \dim \operatorname{Col} B = l$. Tästä seuraa, että B on kääntyvä. □

Seuraus 2.101. *Olkoot $L\colon V \to W$ K-lineaarinen kuvaus äärellisulotteisten K-vektoriavaruuksien välillä. Olkoon $A = [M]_{\mathbf{f},\mathbf{e}}$ L:n matriisi joidenkin V:n ja W:n kantojen suhteen ja oletetaan, että A on $n \times m$-kokoinen. Tällöin*
1) L on surjektio jos ja vain jos $m \geq n$ ja A:llä on $(n \times n)$-alimatriisi B jolle $\det B \neq 0$.
2) L on injektio jos ja vain jos $m \leq n$ ja A:llä on $(m \times m)$-alimatriisi C jolle $\det C \neq 0$.

Todistus. 1) Jos L on surjektio, niin pakko olla $m \geq n$ ja $\dim \mathrm{Col}(A) = \dim \mathrm{Im}\, L = n$. Väite seuraa tästä ja edellisestä tulokesta. Kohta 2) osoitetaan samalla tavalla. □

Esimerkki 2.102. *Esitetään edellisen tuloksen sovellus, jossa mennään hieman topologian puoleelle. Olkoon $A = (a_{ij}) \in M(n \times m; \mathbb{R})$ reaaliarvoinen matriisi, jota vastaava lineaarinen kuvaus L_A on surjektio. Tällöin erityisesti $m \geq n$. Osoitetaan, että jokainen matriisi $B = (b_{ij})$, joka on "tarpeeksi lähellä " A:ta on myös surjektio lineaarisena kuvauksena (eli L_B on surjektio). "Tarpeeksi lähellä" tarkoittaa tässä yhteydessä täsmälleen sitä, että on olemassa $\varepsilon > 0$ siten, että aina kun $|b_{ij} - a_{ij}| < \varepsilon$, matriisi B on surjektio (lineaarisena kuvauksena).*

Väite seuraa edellisestä korolaarista. Nimittäin A:llä on olemassa $(n \times n)$-alimatriisi A' jonka determinaantti eroaa nollasta. Koska determinaantti on matriisin alkioden "jatkuva kuvaus", on olemassa pieni $\varepsilon > 0$, siten, että kun A':n alkiot muutetaan korkeintaan ε:n verran, uuden matriisin determinantti on edelleenkin nollasta eroava. Näin ollen, kun B:n alkiot ovat tarpeeksi lähellä A:n alkioita, B:llä on $(n \times n)$-alimatriisi, jonka determinantti ei ole nolla. Edellisen korollaarin nojalla B on surjektio.
Lukija, joka on tutustunut topologian alkeisiin huomanee, että todistettu väite voidaan muotoilla muotoon "$M(n \times m; R)$:n osajoukko $\{A \mid L_A$ on surjektio$\}$ on **avoin** *$M(n \times m; R)$:ssä".*
Samalla tavalla voidaan todistaa, että injektiivisten matriisien joukko on avoin vastaavassa matriisiavaruudessa.