7. Modulit

Vektoriavaruudet ovat vaihdannaisia ryhmiä, joissa on määritelty jonkin kunnan skalaaritoiminta. Hyväksymällä kerroinrakenteeksi kunnan sijaan rengas saadaan rakenne nimeltä *moduli*. Modulin käsite on siis vektoriavaruuden yleistys, mutta modulien teoria poikkeaa melko paljon vektoriavaruuksien teoriasta. Yleisellä modulilla ei esimerkiksi välttämättä ole kantaa, ja vaikka olisikin, kannan pituus ei ole välttämättä yksikäsitteinen, jolloin dimensiota käsitettä ei voida määritellä. Toisaalta jokaiselle vaihdannaiselle ryhmälle voidaan määritellä luonnollinen modulirakenne, missä alkioita kerrotaan kokonaisluvuilla, mistä johtuen modulien teoria on myös suurelta osin vaihdannaisten ryhmien teoriaa.

7.1. Modulit ja lineaarikuvaukset.

Määritelmä 7.1. Olkoon R rengas. Vaihdannaista ryhmää $(M, +)$, jossa on määritelty renkaan R lineaarinen toiminta, nimitetään *moduliksi*. Renkaan lineaarinen toiminta on renkaan kertolaskumonoidin $(R, \cdot)$ toiminta, joka toteuttaa seuraavat ehdot kaikilla $a, b \in R$ ja $x, y \in M$:

(M1) $1.x = x$
(M2) $(ab).x = a.(b.x)$
(M3) $(a + b).x = a.x + b.x$
(M4) $a.(x + y) = a.x + a.y$.

Rengasta R kutsutaan modulin *kerroinrenkaaksi*, ja sen toimintaa *skalaarikertolaskuksi*.

Modulia, jossa kerroinrenkaana on R, voidaan nimittää R-moduliksi. Aksioomat (M1) ja (M2) määrittelevät renkaan kertolaskumonoidin toiminnan, aksiooma (M3) kertoo, miten renkaan yhteenlasku suhtautuu tähän toimintaan, ja aksiooma (M4) varmistaa, että toiminta on lineaarista (vrt. lineaarikuvauksiin). Modulin aksioomista voidaan helposti johtaa tuttuja laskusääntöjä, kuten $0.x = 0$, $(-1).x = -x$ jne. Yleensä toimintaa merkitään yksinkertaisesti kertolaskuna jättämällä alkioiden välistä piste pois.

Huomaa, että renkaan toiminnan olemassaolo pitää sisällään sen oletuksen, että $a.x \in M$ kaikilla $a \in R$ ja $x \in M$. Tämä voidaan myös ilmaista sanomalla, että modulin täytyy olla *suljettu skalaarikertolaskun suhteen.*

Tässä määritelty renkaan toiminta on tarkasti ottaen renkaan *vasen* toiminta, ja siksi tällaista modulia nimitetään joskus *vasemmaksi* R-moduliksi. Vastaavasti voitaisiin määritellä oikeat modulit renkaan oikean toiminnan avulla.

Esimerkkejä moduleista:

- Jos K on kunta, jokainen K-vektoriavaruus on samalla K-moduli, sillä modulin aksioomat ovat tällöin täsmälleen samat kuin vektoriavaruuden aksioomat.
- Rengas R on itse R-moduli, kun skalaarikertolaskuksi otetaan renkaan oma kertolasku.

- Jokainen vaihdannainen ryhmä on $\mathbb{Z}$-moduli, kun skalaarikertolaskuksi määritellään monikerran ottaminen: $n.x = nx = x + \cdots + x$ (n kertaa). Tämä on itse asiassa ainoa tapa, jolla $\mathbb{Z}$ voi toimia vaihdannaisessa ryhmässä, sillä renkaan $\mathbb{Z}$ additiivinen ryhmä on alkion 1 virittämä, ja toiminta määräytyy tällöin täysin aksioomista (M1) ja (M3).
- Jäännösluokkarenkaiden $\mathbb{Z}_n$ toiminta ryhmässä M on myös yksikäsitteisesti määrätty: $[k]_n.x = kx$ (monikerta). Jotta tällainen toiminta olisi hyvin määritelty, täytyy ryhmässä M päteä $nx = 0$, eli jokaisen alkion kertaluvun täytyy jakaa luku n. Tämä toteutuu muun muassa silloin kun $|M| = n$. Kuitenkin esimerkiksi Kleinin neliryhmä on $\mathbb{Z}_2$-moduli. Kun p on alkuluku, rengas $\mathbb{Z}_p$ on kunta, ja jokainen $\mathbb{Z}_p$-moduli on siis vektoriavaruus.
- Olkoon K kunta. Kaikki K-kertoimiset $n \times n$-matriisit muodostavat renkaan $M_n(K)$, joka ei ole vaihdannainen. Tämä rengas toimii matriisikertolaskulla vasemmalta sarakevektorien avaruudessa K^n ja oikealta vastaavassa rivivektorien avaruudessa. Vektoriavaruutta K^n voidaan siis tarkastella joko vasempana tai oikeana $M_n(K)$-modulina. Nämä kaksi struktuuria ovat lisäksi täysin samanlaiset.
- Renkaan R ideaalit ovat R-moduleja, kun kertolaskuna on renkaan oma kertolasku. Ideaalit ovat samalla rengasmodulin R alimoduleja (määritelmä seuraa). Alirenkaat sen sijaan eivät yleensä ole alimoduleja, koska ne eivät ole vakaita renkaan kertolaskutoiminnassa.

Olkoot M ja N joitain R-moduleja. Kuvausta $f\colon M \to N$ kutsutaan *R-modulihomomorfismiksi* tai *R-lineaarikuvaukseksi*, jos se on skalaarikertolaskun säilyttävä ryhmähomomorfismi, eli seuraavat ehdot pätevät kaikilla $x, y \in M$ ja $a \in R$:

(L1) $f(x + y) = f(x) + f(y)$
(L2) $f(a.x) = a.f(x)$.

Bijektiivistä lineaarikuvausta nimitetään *lineaariseksi isomorfismiksi*. Lineaarikuvauksen ydin on sama kuin vastaavan ryhmähomorfismin ydin, eli nollan alkukuva.

Lineaarisuusehdot voidaan myös yhdistää yhdeksi *lineaarisuuskriteeriksi*, joka on toisinaan kätevämpi tarkistaa:

(LK) $f(a.x + y) = a.f(x) + f(y)$ kaikilla $x, y \in M$ ja $a \in R$.

Esimerkki 7.2. Voidaan osoittaa, että jos rengas R on vaihdannainen, kaikkien R-modulihomomorfismien $M \to N$ joukko on itse R-moduli, kun laskutoimitukset määritellään pisteittäin:

$$(f + g)(x) = f(x) + g(x) \qquad \text{ja} \qquad (a.f)(x) = a.f(x).$$

Tätä modulia merkitään $\mathrm{Hom}_R(M, N)$, tai jos kerroinrengas on selvä asiayhteydestä, yksinkertaisemmin $\mathrm{Hom}(M, N)$. Tarkka todistus jätetään harjoitustehtäväksi. Huomaa, että ei ole edes itsestään selvää, että lineaarikuvausten $M \to N$ joukko on suljettu annettujen laskutoimitusten suhteen.

7.2. Ali- ja tekijämodulit. Modulin M *alimoduli* N on ryhmän M aliryhmä, joka on vakaa kertolaskutoiminnan suhteen. Kaikilla $x, y \in N$ ja $a \in R$ (kerroinrengas) täytyy siis päteä seuraavat ehdot:

(AM1) $N \neq \emptyset$
(AM2) $x - y \in N$
(AM3) $a.x \in N$.

Ehdot (AM1) ja (AM2) tulevat aliryhmäkriteeristä. Ehdoista (AM1) ja (AM3) seuraa, että $0_M \in N$.

Mielivaltaisten alimodulien leikkaus on aina alimoduli. Lineaarikuvausten kuvat ja ytimet ovat myös alimoduleja.

Olkoot A ja B kaksi modulin M alimodulia. Niiden *summa* on

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Tämä määritelmä on additiivinen versio aliryhmien tulon määritelmästä (katso luku 4.1). Koska modulit ovat vaihdannaisia ryhmiä, alimodulien summa on aina aliryhmä. Se on samalla pienin aliryhmä, joka sisältää summattavansa, mikä voidaan ilmaista kaavalla $A + B = \langle A \cup B \rangle$. Lisäksi alimodulien summa on suljettu skalaarikertolaskun suhteen, koska $r(a+b) = ra+rb \in A+B$ pätee kaikilla $a \in A$ ja $b \in B$.

Summaa voidaan yleistää äärettömän monelle alimodulille yllä mainitun viritysominaisuuden avulla. Olkoon $(M_i)_{i \in I}$ perhe[15] modulin M alimoduleita. Määritellään näiden alimodulien summa seuraavasti:

$$\sum_{i \in I} M_i = \left\langle \bigcup_{i \in I} M_i \right\rangle.$$

Toisin sanoen summa on sellaisten alkioiden x virittämä aliryhmä, joista kukin sisältyy johonkin alimoduleista M_i. Summan alkiot ovat siis muotoa

$$x_{i_1} + x_{i_2} + \cdots + x_{i_n},$$

missä jokainen x_{i_k} sisältyy johonkin alimoduliin M_{i_k}. Tämä voidaan ilmaista myös sanomalla, että alkiot ovat summia $\sum_{i \in I} x_i$, missä $x_i \in M_i$ kaikilla i, ja $x_i = 0$ lukuunottamatta äärellistä määrää indeksejä i. Alimodulien yleinen summa on aina alimoduli.

Esimerkki 7.3. Tarkastellaan reaalilukujen yhteenlaskuryhmää $\mathbb{Z}$-modulina. Määritellään kullakin alkuluvulla p joukko

$$M_p = \{n/p^k \mid n \in \mathbb{Z}, k \in \mathbb{N}\}.$$

Joukot M_p ovat $\mathbb{Z}$-modulin $\mathbb{R}$ alimoduleja. Määritetään näiden alimodulien summa $S = \sum_p M_p$. Selvästikin jokaisella p pätee $M_p \subset \mathbb{Q}$, ja $\mathbb{Q}$ on modulin $\mathbb{R}$ alimoduli. Täten $S \subset \mathbb{Q}$, koska S on pienin alimoduli, joka sisältää kaikki modulin M_p. Toisaalta jokainen rationaaliluku voidaan ilmaista summana $\sum_{i=0}^{n} m_i/p_i^{k_i}$, missä osoittajat ovat kokonaislukuja ja nimittäjät alkulukujen potensseja. Siispä $S = \mathbb{Q}$.

Modulin M mikä tahansa alimoduli N on normaali aliryhmä, koska M on vaihdannainen ryhmä. Aliryhmän N suhteen voidaan siis muodostaa tekijäryhmä. Tästä tekijäryhmästä tulee samalla *tekijämoduli*, sillä sivuluokkien skalaarikertolasku

$$a(x + N) = ax + N$$

[15] Perheellä tarkoitetaan kuvausta $i \mapsto M_i$ indeksijoukolta I johonkin alimodulien joukkoon. Jos $I = \mathbb{N}$, tämä on sama kuin jono $(M_0, M_1, M_2, \dots)$.

on automaattisesti hyvin määritelty. Jos nimittäin $x = y + n$ jollain $n \in N$, niin $ax = ay + an \in ay + N$, sillä $an \in N$. Tekijämodulia merkitään tavalliseen tapaan symbolilla M/N.

Tekijämoduleille pätee samanlainen homomorfialause kuin ryhmille ja renkaille. Lisäksi Noetherin isomorfialauseet pätevät myös modulien tapauksessa.

7.3. Modulien suorat summat ja tulot. Useimpien algebrallisten rakenteiden tapauksessa kahden rakenteen karteesinen tulo on myös samantyyppinen rakenne (kunnat ovat poikkeus tästä). Kahden R-modulin karteesista tuloa nimitetään *suoraksi summaksi* ja merkitään $M \oplus N$. Se on R-moduli, joka koostuu pareista (m, n), missä $m \in M$ ja $n \in N$. Useamman modulin tapauksessa summaa voidaan merkitä

$$\bigoplus_{i=1}^{n} M_i,$$

ja sen alkioiksi tulevat n-jonot $(m_1, m_2, \ldots, m_n)$, missä $m_i \in M_i$ kaikilla i. Äärettömän indeksijoukon tapauksessa suoran summan määritelmä poikkeaa karteesisen tulon määritelmästä. Molemmat ovat kuitenkin R-moduleja, ja jälkimmäistä nimitetään *suoraksi tuloksi*.

MÄÄRITELMÄ 7.4. Olkoon $(M_i)_{i \in I}$ jokin perhe R-moduleita. Modulien M_i *suora tulo* koostuu alkioperheistä $x = (x_i)_{i \in I}$, missä $x_i \in M_i$ kaikilla i. Suora tulo on R-moduli, kun laskutoimitukset määritellään pisteittäin:

$$(x + y)_i = x_i + y_i \qquad \text{ja} \qquad (ax)_i = ax_i.$$

Suoraa tuloa merkitään $\prod_{i \in I} M_i$.

Suoraan tuloon liitetään *kanoniset projektiokuvaukset* $\pi_j \colon \prod_{i \in I} M_i \to M_j$, joille pätee $\pi_j(x) = x_j$. Projektiokuvaukset ovat modulihomomorfismeja.

Modulien suora summa on nyt suoran tulon eräs osajoukko. Oletetaan jälleen, että $(M_i)_{i \in I}$ on jokin perhe R-moduleita.

MÄÄRITELMÄ 7.5. Modulien M_i *suora summa* koostuu alkioperheistä $(x_i)_{i \in I}$, missä $x_i \in M_i$ kaikilla i ja lisäksi $x_i \neq 0$ vain äärellisellä määrällä indeksejä. Suora summa on R-moduli, kun laskutoimitukset määritellään pisteittäin kuten suorassa tulossa. Suoraa summaa merkitään $\bigoplus_{i \in I} M_i$.

Suoran summan alkiot ovat siis perheitä, joissa vain äärellisen moni jäsen on nollasta poikkeava. Tällaista perhettä sanotaan *äärelliskantajaiseksi*.

Suoraan summaan liitetään *kanoniset injektiot* $\iota_j \colon M_j \to \bigoplus_{i \in I} M_i$, joille pätee $\iota_j(y) = (x_i)_{i \in I}$, missä

$$x_i = \begin{cases} y, & \text{kun } i = j \\ 0 & \text{muuten.} \end{cases}$$

Esimerkiksi jos indeksijoukko on $I = \{1, 2, 3, 4\}$ ja $a \in M_2$, voidaan kirjoittaa $\iota_2(a) = (0, a, 0, 0)$. Kanoniset injektiot ovat modulihomomorfismeja. Lisäksi voidaan nähdä, että jokainen suoran summan alkio (x_i) voidaan kirjoittaa muodossa $\sum_i \iota_i(x_i)$. Tämä summa on äärellinen (oikeammin äärelliskantajainen), koska $x_i = 0$ äärellistä indeksijoukkoa lukuunottamatta.

Kanonisille injektioille pätee seuraava lause, jota nimitetään suoran summan *universaaliominaisuudeksi.*

LAUSE 7.6. *Olkoon (M_i) perhe R-moduleja. Oletetaan lisäksi, että N on R-moduli ja φ_i on R-lineaarinen kuvaus $M_i \to N$ jokaisella i. Tällöin löytyy yksikäsitteinen R-lineaarinen kuvaus $\theta\colon \bigoplus_i M_i \to N$, jolle pätee*

$$\varphi_i = \theta \circ \iota_i \tag{7.7}$$

kaikilla i, eli seuraava kaavio kommutoi:

$$\begin{tikzcd} M_i \arrow[rr, "\varphi_i"] \arrow[dr, "\iota_i"'] & & N \\ & \bigoplus_i M_i \arrow[ur, dashed, "\theta"'] & \end{tikzcd}$$

TODISTUS. Jokainen suoran summan alkio $x = (x_i)$ voidaan kirjoittaa muodossa $x = \sum_i \iota_i(x_i)$. Näin ollen, mikäli θ on lineaarinen ja toteuttaa ehdon (7.7), täytyy kaikilla $x \in \bigoplus_i M_i$ päteä

$$\theta(x) = \theta\left(\sum_i \iota_i(x_i)\right) = \sum_i (\theta \circ \iota_i)(x_i) = \sum_i \varphi_i(x_i).$$

Tämä kaava määrittelee kuvauksen θ arvot yksikäsitteisesti.

Osoitetaan sitten, että yllä olevan kaavan avulla määritelty θ toteuttaa lauseessa mainitut ehdot. On helppo nähdä, että θ on R-lineaarinen. Lisäksi, jos $y \in M_j$, niin $(\iota_j(y))_i = 0$ kaikilla $i \neq j$. Täten kaikilla j pätee

$$\theta(\iota_j(y)) = \sum_i \varphi_i((\iota_j(y))_i) = \varphi_j(y),$$

eli kuvaus θ toteuttaa ehdon (7.7). $\square$

Universaalisuudella tarkoitetaan sitä, että aina kun käsillä on perhe lineaarikuvauksia johonkin tiettyyn moduliin, tämä perhe voidaan korvata yhdellä kuvauksella suorasta summasta kyseiseen moduliin. Modulien suora summa on ikäänkuin "universaali" lineaarikuvausperhe (ι_i), joka voidaan täydentää lineaarikuvauksella θ vastaamaan mitä tahansa lineaarikuvausperhettä (φ_i). Vastaavanlainen tulos pätee myös suoralle tulolle ja kanonisille projektioille.

LAUSE 7.8. *Olkoon (N_i) perhe R-moduleja. Oletetaan lisäksi, että M on R-moduli, ja φ_i on R-lineaarinen kuvaus $M \to N_i$ jokaisella i. Tällöin löytyy yksikäsitteinen R-lineaarinen kuvaus $\theta\colon M \to \prod_i N_i$, jolle pätee $\varphi_i = \pi_i \circ \theta$ kaikilla i, eli oheinen kaavio kommutoi.*

$$\begin{tikzcd} M \arrow[rr, "\varphi_i"] \arrow[dr, dashed, "\theta"'] & & N_i \\ & \prod_i N_i \arrow[ur, "\pi_i"'] & \end{tikzcd}$$

TODISTUS. Sivuutetaan. $\square$

Ryhmiä tutkittaessa oli hyödyllistä tietää, milloin tietty ryhmä sattui olemaan isomorfinen jonkin tuloryhmän kanssa. Myös moduleille saadaan vastaava tulos.

Lause 7.9. *Olkoon* $(M_i)_{i\in I}$ *perhe* R*-modulin* M *alimoduleja. Jos* $\sum_i M_i = M$ *ja* $M_i \cap \sum_{j\neq i} M_j = \{0\}$ *kaikilla* i*, niin* M *on isomorfinen suoran summan* $\bigoplus_i M_i$ *kanssa.*

Todistus. Jokaisella i voidaan määritellä inkluusiokuvaus $\varphi_i \colon M_i \to M$, missä $\varphi_i(x) = x$. Suoran summan universaaliominaisuuden perusteella löytyy eräs R-lineaarinen kuvaus $\theta \colon \bigoplus_i M_i \to M$, jolle pätee $\theta(\iota_i(x)) = \varphi_i(x) = x$ kaikilla i ja kaikilla $x \in M_i$. Osoitetaan, että θ on bijektio.

$$\begin{tikzcd} M_i \arrow[rr, "\varphi_i"] \arrow[dr, "\iota_i"'] & & \sum_i M_i \\ & \bigoplus_i M_i \arrow[ur, "\theta"'] & \end{tikzcd}$$

Todetaan ensin, että jos $x = (x_i) \in \bigoplus_i M_i$, niin

$$\theta(x) = \theta\left(\sum_i \iota_i(x_i)\right) = \sum_i \varphi_i(x_i) = \sum_i x_i.$$

Surjektiivisuuden osoittamiseksi oletetaan, että $y \in M$ on mielivaltainen. Koska $M = \sum_i M_i$, alkio y voidaan kirjoittaa äärellisenä summana $y = \sum_i x_i$, missä $x_i \in M_i$ kaikilla i. Nyt $x = \sum_i \iota_i(x_i)$ on suoran summan $\bigoplus_i M_i$ alkio, ja yllä todetun perusteella $\theta(x) = \sum_i x_i = y$.

Oletetaan sitten, että $\theta(x) = \theta(y)$ joillain $x, y \in \bigoplus_i M_i$. Tämä tarkoittaa sitä, että $\sum_i x_i = \sum_i y_i$, eli toisin sanoen $\sum_i (x_i - y_i) = 0$. Edelleen, jokaisella i pätee

$$(x_i - y_i) = -\sum_{i\neq j} (x_j - y_j).$$

Yhtälön vasen puoli on alimodulin M_i alkio, ja oikea puoli taas kuuluu summamoduliin $\sum_{i\neq j} M_j$. Oletuksen mukaan näiden leikkaus on triviaali, joten erityisesti $x_i - y_i = 0$. Koska tämä pätee kaikilla i, saadaan $x_i = y_i$ kaikilla i, joten $x = y$. Tämä todistaa injektiivisyyden. □

Edellinen lause antaa perustelun sille, miksi modulien suorat summat ovat yleensä algebrassa tärkeämpiä kuin suorat tulot. Ajatellaan esimerkiksi suoraa tulomodulia $\prod_{i\in I} \mathbb{R}$. Jos indeksijoukko on äärellinen, kyseessä on tavallinen vektoriavaruus $\mathbb{R}^n$. Tässä avaruudessa jokainen koordinaattiakseli on alimoduli, joka koostuu muotoa $\iota_i(x) = (0, \ldots, 0, x, 0, \ldots, 0)$ olevista jonoista. Avaruuden kaikki pisteet puolestaan saadaan summaamalla koordinaattiakselien vektoreita. Koordinaattiakselit ovat isomorfisia modulin $\mathbb{R}$ kanssa, ja edellinen lause ilmaisee vastaavuuden $\bigoplus_i \iota_i(\mathbb{R}) \cong \mathbb{R}^n$.

Jos indeksijoukko kuitenkin on ääretön, avaruudessa $\prod_{i\in I} \mathbb{R} = \mathbb{R}^I$ on pisteitä, joita *ei saada* summaamalla koordinaattiakselien vektoreita yhteen. Alimodulien summa $\sum_i \iota_i(\mathbb{R})$ on tällöin aito alimoduli, mikä lauseen mukaan vastaa sitä, että $\bigoplus_i \mathbb{R}$ on aidosti pienempi kuin suora tulo $\mathbb{R}^I$.

Huomautus. Ryhmäteoriassa vaihdannaisten ryhmien $(G_i, +)$ suora summa konstruoidaan samalla tavoin kuin modulien suora summa. Suoraksi tuloksi nimitetään kuitenkin täsmälleen samaa konstruktiota siinä tapauksessa, että ryhmän laskutoimitusta merkitään kertolaskuna. Kummassakin rakenteessa siis alkioina ovat perheet (g_i), joissa g_i on 0 lukuunottamatta äärellistä määrää indeksejä. Jos tämä äärellisyysrajoitus jätetään pois, saadaan modulien suoraa tuloa vastaava rakenne, jota ryhmien tapauksessa kutsutaan *rajoittamattomaksi* suoraksi tuloksi tai summaksi, laskutoimituksesta riippuen.