7. Modulit

Vektoriavaruudet ovat vaihdannaisia ryhmiä, joissa on määritelty jonkin kunnan skalaaritoiminta. Hyväksymällä kerroinrakenteeksi rengas kunnan sijaan 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, ja siksi 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 toiminta, nimitetään *moduliksi*. Renkaan 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*.

Aksioomat (M1) ja (M2) määrittelevät kertolaskumonoidin toiminnan, ja loput aksioomat määrittävät, miten renkaan ja modulin yhteenlaskut suhtautuvat tuohon toimintaan. 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.

Tässä määritelty renkaan toiminta on oikeastaan 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 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 $\mathbb{Z}$ on additiivisena ryhmänä alkion 1 virittämä, jolloin toiminta määräytyy 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 $|M| = n$. Toisaalta 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 vektoriavaruus.

- Olkoon K kunta. 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.
- Renkaan R ideaalit ovat R-moduleja, kun kertolaskuna on renkaan oma kertolasku. Ideaalit ovat samalla rengasmodulin R alimoduleja (määritelmä seuraa).

Olkoot M ja N jotain R-moduleja. Kuvausta $f : M \to N$ 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.

Kaikkien R-modulihomomorfismien $M \to N$ joukko on itse R-moduli, jos 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 $\mathrm{Hom}(M, N)$.

7.2. Ali- ja tekijämodulit. R-modulin M *alimoduli* N on ryhmän M aliryhmä, joka on vakaa kertolaskutoiminnan suhteen. Kaikilla $x, y \in N$ ja $a \in R$ täytyy siis päteä

(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 $0 = 0.x \in N$ jollain $x \in N$.

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. Koska modulit ovat vaihdannaisia ryhmiä, alimodulien summa on aina aliryhmä. Se on samalla pienin aliryhmä, joka sisältää summattavansa, eli $A + B = \langle A \cup B \rangle$. Lisäksi alimodulien summa on itse alimoduli, koska $r(a + b) = ra + rb \in A + B$ kaikilla $a \in A$ ja $b \in B$.

Summaa voidaan yleistää äärettömän monelle alimodulille edellä mainitun viritysominaisuuden avulla. Olkoon $(M_i)_{i\in I}$ perhe[13] 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, jotka sisältyvät johonkin alimoduleista M_i. Sen alkiot ovat siis muotoa $\sum_{i\in I} x_i$, missä $x_i \in M_i$ kaikilla i, ja $x_i = 0$ lukuunottamatta äärellistä määrää indeksejä i. Alimodulien yleinen summa on aina alimoduli.

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

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

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 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 7.2. 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 liittyvät *kanoniset projektiokuvaukset* $\pi_j : \prod_{i\in I} M_i \to M_j$, joille pätee $\pi_j(x) = x_j$. Projektiokuvaukset ovat modulihomomorfismeja.

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

---

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

Määritelmä 7.3. 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 liittyvät *kanoniset injektiot* $\iota_j : M_j \to \bigoplus_{i\in I} M_i$, missä $\iota_j(y) = (x_i)_{i\in I}$ ja

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

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. 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 7.4. *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 $\theta : \bigoplus_i M_i \to N$, jolle pätee*

$$\varphi_i = \theta \circ \iota_i \tag{7.5}$$

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 toteuttaa ehdon (7.5), 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 yksikäsitteisesti.

Osoitetaan sitten, että yllä 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

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

eli kuvaus θ toteuttaa ehdon (7.5). $\square$

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.

LAUSE 7.6. *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 $\theta : M \to \prod_i N_i$, 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. □

Ryhmiä tutkittaessa oli hyödyllistä tietää, milloin tietty ryhmä sattui olemaan isomorfinen jonkin tuloryhmän kanssa. Koska modulit ovat vaihdannaisia ryhmiä, myös moduleille saadaan vastaava tulos.

LAUSE 7.7. *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 $\varphi_i : M_i \to M$, missä $\varphi_i(x) = x$. Suoran summan universaalisuusominaisuuden perusteella löytyy R-lineaarinen kuvaus $\theta : \bigoplus_i M_i \to M$, jolle pätee $\theta(\iota_i(x)) = \varphi_i(x) = x$ kaikilla i ja $x \in M_i$. 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. $\square$

Huomautus. Ryhmäteoriassa vaihdannaisten ryhmien $(G_i, +)$ suora summa konstruoidaan samalla tavoin kuin modulien suora summa. Suoraksi tuloksi kuitenkin nimitetään täsmälleen samaa konstruktiota siinä tapauksessa, että ryhmän laskutoimitusta merkitään multiplikatiivisesti. Kummassakin rakenteessa siis alkioina ovat perheet (g_i), joissa $g_i = 0$ lukuunottamatta äärellistä määrää indeksejä. Jos viimeksi mainittu rajoitus jätetään pois (kuten modulien suorassa tulossa), ryhmien tuloa tai summaa kutsutaan *rajoittamattomaksi* suoraksi tuloksi tai summaksi.