Luku 5

Modulit

5.1. Modulien teoria

Tämä on kurssin viimeinen osio, joka tutustuttaa lukijaa modulien teorian alkeisiin.

Moduli on vektoriavaruuden käsitteen luonnollinen yleistys, jossa skalaarien oletetaan kunnan sijasta muodostavan vain renkaan.

Vektoriavaruuksien teorian voidaan katsoa syntyneen analyyttisestä geometriasta. Ensin huomattiin, että tuttuja klassisen geometrian objekteja kuten tason tai kolmiulotteisen avaruuden pisteitä voidaan ajatella reaalilukupareina (x, y) tai vastaavasti kolmikkoina (x, y, z). Tämä aikoinaan matematiikkaa mullistunut oivallus liitetään yleensä Rene Descarten nimeen. Tämän tulkinnan kautta keksittiin luonollisena yleistyksenä tapa puhua n-ulotteisesta avaruudesta $\mathbb{R}^n$, joka koostuu n-pituisista jonoista $(x_1, \ldots, x_n)$ (ja jolla ei ole enää selkeätä intuitiivista geometrista tulkintaa). Erityisen tärkeiksi osoittautuivat tällöin tämän "koordinaatisto-avaruuden" sellaiset osajoukot, jotka ovat suljettuja vektorien yhteenlaskun ja reaaliluvulla kertomisen suhteen, toisin sanoen $\mathbb{R}^n$:n *aliavaruudet*. Juuri avaruuden $\mathbb{R}^n$ aliavaruuksien keskeiset ominaisuudet otettiin vektoriavaruuden määritelmän lähtökohdaksi. Vektoriavaruuksien tärkeämpi tarkastelu osoitti, että juuri reaalilukujen joukon sellaiset ominaisuudet, jotka tekevät siitä *kunnan* ovat oleellisia teorian kannalta. Tämä johti yleisen K-vektoriavaruuden käsitteen syntyyn.

Toisaalta myös huomattiin, että monissa yhteyksissä esille nousevat sellaiset tilanteet, jossa luonnollinen "skalaarien" joukko ei olekaan kunta, vaan ainoastaan rengas. Esimerkiksi jokaisessa Abelin ryhmässä $(G, \cdot)$ voidaan puhua alkion x "monikerrasta" nx, mielivaltaisella kokonaisluvulla $n \in \mathbb{Z}$. Voidaan muodostaa kokonaislukukertoimisia "lineaarisia kombinaatioita"

$$n_1 x_1 + \ldots + n_k x_k,$$

missä $n_1, \ldots, n_k \in G$, $x_1, \ldots, x_k \in G$. Soveltamalla näihin vektoriavaruuksien teoriasta tuttuja "lineaarisia menetelmiä" tai niiden analogioita, saadaan uutta tietoa ryhmän G rakenteesta. Toisen meidän kannalta tärkeän esimerkin muodostaa Luvusta 3 tuttu polynomialgebran $K[\mathbf{X}]$ luonnollinen "toiminta" K-vektoriavaruuden V operaattorien muodostamassa joukossa $L(V)$. Nimittäin, jos $L\colon V \to V$ on lineaarinen operaattori ja $\mathbf{p} = \sum_{i=0}^{n} a_i \mathbf{X}^i \in K[\mathbf{X}]$ on K-kertoiminen polynomi, voidaan muodostaa operaattori $p(L)\colon V \to V$, $p(L) = \sum_{i=0}^{n} a_i L^i$. Merkitsemällä $p(L) = \mathbf{p} \cdot L = \mathbf{p}L$, tämä voidaan ajatella jonkinlaisena skalaarikertolaskuna Abelin ryhmässä $L(V)$, jossa skaalareina toimivat

polynomit. Nämä skalaarit eivät muodostaa kuntaa, mutta ne muodostavat renkaan, polynomirenkaan $K[\mathbf{X}]$. Tällä skalaarikertolaskulla varustettuna joukko $L(V)$ voidaan ajatella niin sanottuna $K[\mathbf{X}]$-*modulina*. Itse asiassa tämän materiaalin Luvun 3 sisältöä voidaan aika pitkälti tulkita tämän modulin struktuurin tutkimisena.

Formaalisti moduli määritellään samalla tavalla kuin vektoriavaruus, paitsi, että skalaarien ei vaadita muodostavan kuntaa, ainoastaan renkaan.

Määritelmä 5.1. *Olkoon $R = (R, +, \cdot)$ rengas ja olkoon $(M, +)$ Abelin ryhmä. Olkoon $\cdot\colon R \times M \to M$ joukon R (vasemmanpuoleinen) ulkoinen laskutoimitus joukossa M, jota merkitään multiplikatiivisesti, $\cdot(r, \mathbf{m}) = r\mathbf{m}$. Tällöin kolmikko $(M, +, \cdot)$ on (vasemmanpuoleinen) R-moduli jos seuraavat ehdot ovat voimassa kaikilla $r, r' \in R$, $\mathbf{m}, \mathbf{m}' \in M$.*

(i) $r(r'\mathbf{m}) = (rr')\mathbf{m}$.

(ii) $(r + r')\mathbf{m} = r\mathbf{m} + r'\mathbf{m}$.

(iii) $r(\mathbf{m} + \mathbf{m}') = r\mathbf{m} + r\mathbf{m}'$.

(iv) $1_K\mathbf{m} = \mathbf{m}$.

R-modulia $(M, +, \cdot)$ merkitään yleensä lyhyesti symbolilla M. Vaikka moduli ei yleisesti ottaen ole vektoriavaruus, sen alkioita on kuitenkin tapana sanoa tämän modulin *vektoreiksi*. Modulin vektoreita merkitään tässä materiaalissa pääsääntöisesti lihavoidulla fontilla, erottaakseen niitä *skalaareista* (eli *kerroinrenkaan* R alkioista). Koska moduli on erityisesti Abelin ryhmä, sillä on nolla-alkio (yhteenlaskun neutraalialkio), jota merkitään $\mathbf{0}_M$.

Huomaa, että yllä esitetyssä modulin määritelmässä on tarkoituksella syyllistytty ”tuplanotaatioon”. Nimittäin symboli + tarkoittaa siinä sekä renkaan R yhteenlaskuoperaatiota, että Abelin ryhmän M yhteenlaskuoperaatiota. Samoin $\cdot$ viittaa sekä renkaan R kertolaskuun, että modulin M skalaarikertolaskuun. Koska tällainen käytäntö on kuitenkin enemmänkin sääntö kuin poikkeus tieteellisissä piireissä, tällaisissa tapauksissa on opittava ymmärtämään asiayhteydestä milloin on kyse mistäkin symbolin merkityksestä. Esimerkiksi kaavassa

$$(r + r')\mathbf{m} = r\mathbf{m} + r'\mathbf{m}$$

plus-merkki vasemalla puolella tarkoittaa renkaan yhteenlaskua kun taas oikealla puolella sillä tarkoitetaan modulin yhteenlaskua.

Modulissa pätevät monet tutut laskusäännöt, esimerkiksi $0_R\mathbf{m} = \mathbf{0}_M$, $r\mathbf{0}_M = \mathbf{0}_M$, $(-1)\mathbf{m} = -\mathbf{m}$ ja niin edelleen. Niitä todistetaan samalla tavalla kuin vektoriavaruuksissa (vrt. Lemma 2.5). Täytyy kuitenkin olla tarkka - esimerkiksi vektoriavaruuksien teoriassa pätevä ”nollasääntö” (Lemman 2.5. neljäs kohta) ei ole yleisesti voimassa moduleille, ehdosta $r\mathbf{m} = \mathbf{0}_M$ ei välttämättä seuraa, että $r = 0_R$ tai $\mathbf{m} = \mathbf{0}_M$ (kts. esimerkkejä alla).

Oikeanpuoleiset modulit

Jos ollaan tarkkoja, Määritelmä 5.1 antaa niin sanotun *vasemmanpuoleisen modulin* käsitteen määritelmän. On olemassa myös hyödyllinen *oikeanpuoleisen modulin* käsite, joka sekin tulee monissa yhteyksissä luonnollisella tavalla vastaan.

Olkoon R rengas. Oikeanpuoleinen R-moduli on kolmikko $(M, +, \cdot)$, missä $(M, +)$ on Abelin ryhmä ja $\cdot$ on joukon R **oikeanpuoleinen** laskutoimitus $\cdot\colon M \times R \to M$ joukossa M, jota merkitään multiplikatiivisesti $\mathbf{m}r$ eli modulin vektori $\mathbf{m} \in M$ kerrotaan skalaarilla $r \in R$ "oikealta puolelta". Lisäksi vaaditaan, että seuraavat ehdot ovat voimassa:

(i) $(\mathbf{m}r')r = \mathbf{m}(r'r)$.

(ii) $\mathbf{m}(r + r') = \mathbf{m}r + \mathbf{m}r'$.

(iii) $(\mathbf{m} + \mathbf{m}')r = \mathbf{m}r + \mathbf{m}'r$.

(iv) $\mathbf{m} = \mathbf{m}1_K$.

Oikeanpuoleisissa moduleissa kyse ei ole vain notaatiotempusta. Jos oikeanpuoleisen modulin skalaarikertolasku kirjoitetaan vasemmalta eli merkitään tulo $\mathbf{m}r$ muodossa $r\mathbf{m}$, ei välttämättä saada vasemmanpuoleista modulia määritelmän 5.1 mielessä, sillä ehdosta (i) tulee tällöin yhtälö

$$r(r'\mathbf{m}) = (r'r)\mathbf{m},$$

eikä yhtälöä $r(r'\mathbf{m}) = (rr')\mathbf{m}$, kuten vasemmanpuoleisen modulin määritelmän kohta (i) vaatii (huomaa skalaarien kertolaskun järjestys oikealla puolella). Jos skalaarirengas R on *vaihdannainen*, jokainen vasemmanpuoleinen R-moduli on tämän nojalla selvästi myös oikeanpuoleinen R-moduli, mutta jos renkaan R kertolaskuoperaatio ei ole vaihdannainen, molempia käsitteitä tarvitaan. Oikeanpuoleisten modulien tarpeellisuuteen vasemmanpuoleisten modulien teoriassa törmätään luonnollisella tavalla esimerkiksi duaalien teorian yhteydessä (kts. osio 5.1 alla). Teorian näkökulmasta yleensä riittää tarkastella vain vasemmanpuoleisia moduleita, sillä todistukset ja tulokset toimivat analogisesti samalla tavalla kummankin käsitteen kohdalla. Tästä syystä jatkossa vasemmanpuoleisia moduleita sanotaan pääsääntöisesti yksinkertaisesti moduleiksi. Vasemman- ja oikeanpuoleisista moduleista puhutaan vain silloin, kun se on tarpeellista.

Esimerkkejä 5.2. *(1) Kun K on kunta, K-vektoriavaruus on sama asia kuin K-moduli.*

(2) Jokaisessa Abelin ryhmässä $(M, +)$ voidaan määritellä $\mathbb{Z}$-modulin struktuuri, vieläkin yksikäsitteisellä tavalla. Tässä $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$ on kokonaislukujen rengas tavallisilla lukujen yhteen-ja kertolaskulla varustettuna. Tarkemmin sanottuna olkoon $(M, +)$ Abelin ryhmä. Tällöin on olemassa yksikäsitteinen kuvaus $\cdot\colon \mathbb{Z} \times M \to M$ siten, että kolmikko $(M, +, \cdot)$ on $\mathbb{Z}$-moduli. Osoitetaan tämä väite todeksi. Olkoon $(M, +)$ Abelin ryhmä. Oletetaan, että $\cdot\colon \mathbb{Z} \times M \to M$ on kuvaus, jolle kolmikko $(M, +, \cdot)$ on $\mathbb{Z}$-moduli. Osoitetaan, että $\cdot(n, \mathbf{m}) = n \cdot \mathbf{m}$ on tällöin alkion $\mathbf{m}$ n's monikerta $n\mathbf{m}$ Abelin ryhmässä $(M, +)$. Oletetaan ensin, että $n \geq 0$ ja osoitetaan tämä väite induktiolla n:n suhteen. Kun $n = 0$ modulin skalaarikertolaskun ominaisuuksien ja monikerran $0\mathbf{m}$ määritelmän nojalla pätee

$$n \cdot \mathbf{m} = 0 \cdot \mathbf{m} = \mathbf{0}_M = 0\mathbf{m}.$$

Oletetaan, että $n \cdot \mathbf{m} = n\mathbf{m}$, missä $n \cdot \mathbf{m}$ tarkoittaa oletetun skalaarikertolaskun $\cdot\colon \mathbb{Z} \times M \to M$ arvoa parissa $(n, \mathbf{m})$ ja $n\mathbf{m} = \underbrace{\mathbf{m} + \mathbf{m} + \ldots + \mathbf{m}}_{n \text{ kpl}}$ on taas alkion $\mathbf{m}$ n:s monikerta Abelin ryhmässä $(M, +)$. Osoitetaan, että sama pätee kun n korvataan

seuraavalla luvulla $(n+1)$. Käyttämällä modulin skalaarikertolaskun ominaisuuksia, induktio-oletusta sekä monikerran rekursiivista määritelmää, saadaan

$$(n+1)\cdot\mathbf{m} = n\cdot\mathbf{m} + 1\cdot\mathbf{m} = n\cdot\mathbf{m} + \mathbf{m} = n\mathbf{m} + \mathbf{m} = (n+1)\mathbf{m}.$$

Näin ollen, on osoitettu induktiolla, että kaikilla $n \geq 0$ pätee

$$n\cdot\mathbf{m} = n\mathbf{m}.$$

Siirtymällä vasta-alkioihin nähdään helposti, että sama yhtälö pätee kaikilla $\mathbf{m} \in M$ myös kun $n < 0$. Toisin sanoen $\mathbb{Z}$-skalaarikertolasku, joka tekee annetusta Abelin ryhmästä M $\mathbb{Z}$-modulin, määräytyy yksikäsitteisellä tavalla tämän ryhmästruktuurista ja se on annettu kaavalla

$$n\cdot\mathbf{m} = n\mathbf{m}, \text{ kaikilla } n \in \mathbb{Z}, \mathbf{m} \in M.$$

Kääntäen nähdään helposti , että tällä kaavalla annettu $\mathbb{Z}$-skalaarikertolasku toteuttaa kaikki modulin määritelmässä vaaditut ehdot, joten $(M,+,\cdot)$ on $\mathbb{Z}$-moduli. Esimerkiksi yhtälö

$$(n+n')\cdot\mathbf{m} = n\cdot\mathbf{m} + n'\cdot\mathbf{m}$$

on sama asia kuin monikerroille voimassa oleva sääntö $(n+n')\mathbf{m} = n\mathbf{m}+n'\mathbf{m}$. Muut modulin ehdot palautuvat samalla tavalla ennestään tuttuihin monikerran ominaisuuksiin.

Näin ollen jokaisessa Abelin ryhmässä $(M,+)$ voidaan määritellä $\mathbb{Z}$-modulin $(M,+,\cdot)$ struktuuri, vieläpä yksikäsitteisellä tavalla. Toisin sanoen Abelin ryhmä ja $\mathbb{Z}$-moduli ovat käytännössä sama asia. Koska jokaista Abelin ryhmää voidaan ajatella modulina tällä tavalla, Abelin ryhmien teoria on täysin ekvivalentti $\mathbb{Z}$-modulien teorian kanssa. Erityisesti Abelin ryhmien tutkimuksessa voidaan käyttää lineaarialgebrallisia menetelmiä, käsitteitä ja tuloksia.

(3) Esimerkissä 2.6 Luvussa 2 näytettiin, että Abelin ryhmässä $(A,+)$ voidaan määritellä $\mathbb{Z}_p$-vektoriavaruuden struktuuri (missä p on alkuluku) jos ja vain jos ryhmässä $(A,+)$ jokaiselle $\mathbf{a} \in A$ pätee $p\mathbf{a} = \mathbf{0}_A$. Ainoa mihin oletusta siitä, että p on alkuluku tarvittiin silloin, oli se tosiasia, että $\mathbb{Z}_n$ on kunta jos ja vain jos n on alkuluku. Ilman tätä oletusta se on kuitenkin joka tapauksessa rengas, joten voidaan puhua $\mathbb{Z}_n$-moduleista. Aivan samalla tavalla kuin esimerkissä 2.6 nähdään, että Abelin ryhmässä $(A,+)$ voidaan määritellä $\mathbb{Z}_n$-skalaarikertolasku siten, että siitä tulee $\mathbb{Z}_n$-moduli jos ja vain jos ryhmässä A jokaiselle $\mathbf{a} \in A$ pätee $n\mathbf{a} = \mathbf{0}_A$.

(4) Olkoon R rengas ja olkoon X joukko. Tällöin joukossa

$$R^X = \{f\colon X \to R\}$$

on olemassa luonnollinen (vasemmanpuoleisen) R-modulin struktuuri, jossa laskutoimitukset on määritelty pisteittäin. Tarkemmin sanottuna kun $f, g\colon X \to R$ ovat kuvauksia ja $r \in R$ asetetaan kuvaukseksi $f+g$ ja rf kuvauksia, joille jokaisella $x \in X$ pätee

$$(f+g)(x) = f(x) + g(x),$$

$$(rf)(x) = rf(x).$$

Näiden yhtälöiden vasemmalla puolella käytetään renkaan R laskutoimituksia. Sen tarkistaminen, että näillä varustettuna R^X todellakin on R-moduli on suoraviivainen laskuharjoitus, joka jätetään lukijalle. Esimerkiksi kaikilla $r, r' \in R$, $f \in \mathbb{R}^X$ ja $x \in X$ pätee (skalaarikertolaskun määritelmän sekä renkaan kertolaskun liitännäisyyden nojalla)

$$(r(r'f))(x) = r((r'f)(x)) = r(r'f(x)) = (rr')f(x) = ((rr')f)(x).$$

Koska tämä pätee kaikilla $x \in X$, päätellään, että

$$r(r'f) = (rr')f.$$

(5) Edellisen esimerkin joukossa R^X voidaan määritellä luonnollisella tavalla myös oikeanpuoleisen R-modulin struktuuri. Määritellään yhteenlaskuoperaatio $+$ joukossa R^X samalla tavalla kuin edellisessä esimerkissä, eli kaavalla

$$(f + g)(x) = f(x) + g(x).$$

Lisäksi määritellään oikeanpuoleinen skalaarikertolasku $\cdot R^X \times R \to R^X$ kaavalla

$$(fr)(x) = f(x)r, \ x \in X.$$

Laskutoimitukset tässä modulissa ovat siis myös määriteltyjä pisteittäin, mutta skalaarikertolaskussa kerrotaan skalaarilla oikealta (eikä vasemmalta kuten edellisessä esimerkissä). Jälleen kerran helpoilla laskuilla nähdään, että nämä laskutoimitukset määrittelevät joukossa R^X oikeanpuoleisen $\mathbb{R}$-modulin struktuurin. Esimerkiksi kaikilla $r, r' \in R$, $f \in \mathbb{R}^X$ ja $x \in X$ pätee

$$((fr')r)(x) = ((fr')(x))r = (f(x)r')r = f(x)(r'r) = (f(rr'))(x).$$

Koska tämä pätee kaikilla $x \in X$, päätellään, että

$$(fr')r = f(rr').$$

Tämän ja edellisen esimerkin perusteella nähdään, että joukossa R^X voidaan määritellä luonnollisella tavalla sekä vasemman-, että oikeanpuoleisen R-modulin struktuurit. Kun rengas R on vaihdannainen, näiden välillä ei selvästikään ole mitään eroa, sillä tällöin saadaan aina sama alkio riipumatta siitä lasketaanko $rf(x)$ vai $f(x)r$. Jos R ei kuitenkaan ole vaihdannainen, näillä moduleilla voi yleisesti ottaen olla erilaisia ominaisuuksia.

(6) Ottamalla esimerkeissä 4 ja 5 joukoksi X äärellinen joukko $[n] = \{1, \ldots, n\}$ saadaan erikoistapauksena vasemman- ja oikeanpuoleisen R-modulin struktuuri karteesisessa tulossa R^n. Joukkona R^n koostuu kaikista mahdollisista n-pituisista jonoisa $(r_1, \ldots, r_n)$. Tällainen jono voidaan tulkita funktioksi $f\colon [n] \to R$, jolle $f(i) = r_i$ (itse asiassa tämä on tarkka formaali joukko-opillinen määritelmä jonolle). Vasemmanpuoleisen R-modulin R^n laskutoimitukset ovat määriteltyjä koordinateittain, eli

$$(r_1, \ldots, r_n) + (r'_1, \ldots, r'_n) = (r_1 + r'_1, \ldots, r_n + r'_n),$$

$$r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n).$$

Oikeanpuoleisessa on sama yhteenlasku ja kaavalla

$$(r_1, \ldots, r_n)r = (r_1 r, \ldots, r_n r).$$

määritelty oikeanpuoleinen R-skalaarikertolasku.

Kuten vektoriavaruuksien teoriassa, moduli R^n edustaa "tyyppillistä" n-ulotteista R-modulia (tästä puhutaan tarkemmin alla vapaiden modulien yhteydessä).

(7) Olkoon $(V, +, \cdot)$ K-vektoriavaruus jonkun kunnan K yli. Vektoriavaruuksien teoriasta tiedetään, että sen operaattorien joukko $L(V)$ on itse asiassa (yleensä ei-vaihdannainen) rengas pisteittäisen yhteenlaskun ja kuvausten yhdistämisen suhteen. Näytetään, että V voidaan ajatella myös (vasemmanpuoleisena) $L(V)$-modulina. Jätetään joukkoon V sama yhteenlaskuoperaatio $+$, joka sillä on vektoriavaruutena. Skalaarikertolasku $.$ renkaan $L(V)$ yli määritellään kaavalla

$$L.\mathbf{v} = L(\mathbf{v})$$

kaikilla $L \in L(V)$ ja $\mathbf{v} \in V$. Tässä määritelmässä $L(V)$-skalaarikertolaskulle käytetään symbolia $.$ erottamaan se avaruuden V alkuperäisestä K-skalaarikertolaskusta $\cdot$, mutta käytännössä sitä merkitään tässä yhteydessä yksinkertaisesti $L.\mathbf{v} = L\mathbf{v}$ eli jätetään skalaarikertolasku-operaatio merkitsemättä, kuten yleensä modulien kohdalla on tapana.

Tarkistetaan, että näillä määritelmillä V todellakin on $L(V)$-moduli. On selvää, että $(V, +)$ on Abelin ryhmä. Olkoot $L, L' \in L(V), \mathbf{v}, \mathbf{v}' \in V$. Tällöin kuvausten yhdistämisen määritelmän nojalla pätee

$$L(L'\mathbf{v}) = L(L'(\mathbf{v})) = (L \circ L')(\mathbf{v}) = LL'(\mathbf{v}) = (LL')\mathbf{v}.$$

Kuvausten yhteenlaskuoperaation määritelmän nojalla pätee

$$(L + L')\mathbf{v} = L\mathbf{v} + L'\mathbf{v}.$$

Koska L on lineaarinen, pätee

$$L(\mathbf{v} + \mathbf{v}') = L\mathbf{v} + L\mathbf{v}'.$$

Lopuksi identtisen kuvauksen (joka on renkaan $L(V)$ kertolaskun neutraalialkio) määritelmän nojalla pätee

$$\mathrm{id}_V\, \mathbf{v} = \mathrm{id}_V(\mathbf{v}) = \mathbf{v}.$$

Kaikki modulin ehdot siis ovat voimassa.

(8) Olkoon V kuten edellisessä esimerkissä äärellisulotteinen K-vektoriavaruus, esimerkiksi avaruus K^n. Tällöin, jos avaruudessa V kiinnitetään jokin kanta, operaattoreita $L \in L(V)$ vastaavat $(n \times n)$-kokoiset neliömatriisit. Tämä vastaavuus lisäksi säilyttää kaikki algebralliset ominaisuudet. Näin ollen siirtymällä operaatio-tulkinnasta

matriisi-tulkintaan, nähdään heti, että V voidaan ajatella modulina matriisirenkaan $M(n \times n; K)$ yli.

Esimerkiksi otetaan $V = K^n$ ja sen kannaksi standardikanta. Olkoon $A = (a_{ij})$ $(n \times n)$-kertoiminen matriisi ja olkoon $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$. Tällöin skalaarikertolaskun $A\mathbf{x}$ tulos on jono $\mathbf{y} = (y_1, \ldots, y_n) \in K^n$, jolle pätee

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

Tässä siis skalaarikertolasku $A\mathbf{x}$ on sama asia kuin matriisien kertolasku, kun vektori $\mathbf{x} = (x_1, \ldots, x_n)$ tulkitaan pystyvektorina eli $(n \times 1)$-matriisina.

Jos jokainen avaruuden K^n alkio $\mathbf{x} = (x_1, \ldots, x_n)$ tulkitaan sen sijaan vakaavektorina eli $(1 \times n)$-matriisina, joukossa K^n voidaan määritellä oikeanpuoleinen skalaarikertolasku . matriisirenkaan $M(n \times n; K)$ yli, kaavalla $\mathbf{x}.A = \mathbf{x}A$. Tälle pätee $\mathbf{x}A = \mathbf{y} = (y_1, \ldots, y_n) \in K^n$, missä

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

Kun edellä määriteltyä vasemmanpuoleista skalaarikertolaskua verrataan tähän oikeanpuoleiseen skalaarikertolaskuun, nähdään, että pätee

$$A\mathbf{x} = \mathbf{x}A^T.$$

9 *Olkoon V äärellisulotteinen K-vektoriavaruus ja olkoon $L\colon V \to V$ jokin sen (kiinnitetty) operaattori. Tällöin avaruudessa V voidaan määritellä skalaarikertolasku polynomirenkaan $K[\mathbf{X}]$ yli kaavalla*

$$\mathbf{pv} = p(L)(\mathbf{v}), \ \mathbf{p} \in K[\mathbf{X}], \mathbf{v} \in V.$$

Helposti nähdään, että tällä skalaarikertolaskulla ja alkuperäisellä yhteenlaskullaan varustettuna V on $K[\mathbf{X}]$-moduli. Tämän modulin struktuuri riippuu tietysti operaattorin L valinnasta.

Voidaan sanoa, että huomattava osa Luvun 3 sisällöstä oli omistettu juuri tällaisen modulin rakenteen tutkimiseen. Tässä mielessä ollaan siis nähty jo modulien teoriaa Luvussa 3, ei vaan tiedetty silloin, että kyse oli siitä. Nilpottenttien operaattorien ja Jordanin normaalimuodon teorian yhteydessä ollaan nähty hyviä esimerkkejä tyyppillisistä moduliteoreettisista menetelmistä. Jos luvun 3 sisältö tuntui vaikealta ja epätriviaalilta, tähän on nyt paljastunut hyvä syy - oleellisesti tämä havainnollistaa sitä tosiasiaa, että modulien teoria on vaikeampaa kuin vektoriavaruuksien teoria eikä ole niin "suoraviivaista".

Alimodulit, tekijämodulit ja lineaariset kuvaukset

R-modulin M alimoduli on epätyhjä osajoukko $N \subset M$, joka on suljettu modulin yhteenlaskun sekä skalaarikertolaskun suhteen. Samalla tavalla kuin vektoriavaruuksien kohdalla, nähdään, että tällöin $(N, +)$ on itse asiassa Abelin ryhmä ja N on itse R-moduli, kun se

varustetaan modulin M laskutoimitusten rajoittumilla $+\colon N \times N \to N$ ja $\cdot\colon R \times N \to N$ (vrt. Lemman 2.9 todistukseen).

Kun N on modulin M alimoduli, merkitään $N \leq M$. Tällöin voidaan muodostaa myös *tekijämoduli* M/N tavalliseen tapaan. Tarkemmin sanottuna oletetaan, että $N \leq M$. Määritellään modulissa M ekvivalenssirelaatio $\sim_N$ ehdolla $x \sim_N y$ jos ja vain jos $x - y \in N$. Tällöin relaatio $\sim_N$ on yhteensopiva modulin M laskutoimitusten suhteen, joten tekijäjoukossa M/N voidaan määritellä luonnollinen R-modulin struktuuri kaavoilla

$$\overline{\mathbf{m}} + \overline{\mathbf{m}'} = \overline{\mathbf{m} + \mathbf{m}'},$$

$$r\overline{\mathbf{m}} = \overline{r\mathbf{m}}.$$

Kanoninen projektio $p\colon M \to M/N$ on tällöin surjektiivinen lineaarinen kuvaus R-modulien välillä. Lineaarisen kuvauksen käsite määritellään alla.

Kuten vektoriavaruuksien kohdalla, voidaan näyttää, että kääntäen mikä tahansa modulin M tekijämoduli $M/\sim$ (missä $\sim$ on *laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio*) on muotoa M/N jollakin $N \leq M$.

Kuvausta $L\colon M \to N$ kahden R-modulin välistä kuvausta sanotaan *lineaariseksi* jos se on yhteensopiva laskutoimitusten kanssa. Tarkemmin sanottuna L on lineaarinen jos kaikilla $\mathbf{m}, \mathbf{m}' \in M$, $r \in R$ pätee

$$L(\mathbf{m} + \mathbf{m}') = L(\mathbf{m}) + L(\mathbf{m}'),$$

$$L(r\mathbf{m}) = rL(\mathbf{m}).$$

Kuten yleensä algebrassa, lineaarinen kuvaus $L\colon M \to N$ kahden R-modulin välillä määrittelee kaksi tärkeätä alimodulia, nimittäin ytimen $\operatorname{Ker} L$ ja kuvamodulin $\operatorname{Im} L$. Näistä ydin on M:n alimoduli ja koostuu niistä $\mathbf{m} \in M$ joille $L(\mathbf{m}) = \mathbf{0}_N$. Kuvamoduli $\operatorname{Im} L$ on puolestaan modulin N alimoduli.

Hajotelma-ja isomorfialauseet pätevät modulien teoriassa samoilla todistuksilla kuin vektoriavaruuksien teoriassa (vrt. Lause 2.24 ja Seuraus 2.25 Luvussa 2). Bijektiivistä lineaarista kuvausta sanotaan ismorfismiksi. Isomorfismin käänteiskuvaus on myös isomorfismi. Kahden lineaarisen kuvauksen $L\colon M \to N$, $L'\colon N \to P$ yhdiste $L'L\colon M \to P$ on lineaarinen kuvaus.

Esimerkkejä 5.3. *(1) Olkoon V äärellisulotteinen vektoriavaruus ja olkoon L sen operaattori. Esimerkin 5.2, (9) nojalla V on $K[\mathbf{X}]$-moduli, jossa skalaarikertolasku on määritely kaavalla*

$$\mathbf{pv} = p(L)(\mathbf{v}),\ \mathbf{p} \in K[\mathbf{X}], \mathbf{v} \in V.$$

Olkoon $W \subset V$. Tutkitaan milloin W olisi tämän modulin almoduli. Joukon W täytyy tällöin olla Abelin ryhmän $(V, +)$ aliryhmä ja lisäksi sen täytyy olla suljettu $K[\mathbf{X}]$-skalaarikertolaskun suhteen. Jälkimmäinen ehto tarkoittaa sitä, että kaikilla $\mathbf{p} \in K[\mathbf{X}]$ ja kaikilla $\mathbf{w} \in W$ täytyy päteä $p(L)(\mathbf{w}) \in W$. Valitsemalla tässä polynomiksi $\mathbf{p}$ nolla-asteinen vakiopolynomi $\mathbf{p} = k \in K$, nähdään, että W:n täytyy olla suljettu K-vektoriavaruuden V alkuperäisen K-skalaarikertolaskun suhteen. Yhdessä edellisen havainnon kanssa tämä tarkoittaa sitä, että W on K-vektoriavaruuden

V aliavaruus. Valitsemalla taas polynomiksi $\mathbf{p}$ polynomi $\mathbf{X}$, nähdään, että kaikilla $\mathbf{w} \in W$ täytyy päteä $X(L)(\mathbf{w}) = L(\mathbf{w}) \in W$. Toisin sanoen aliavaruuden W täytyy olla lisäksi invariantti operaattorin L suhteen.

Kääntäen nähdään helposti, että L-invariantti aliavaruus W on $K[\mathbf{X}]$-modulin V alimoduli. Näin ollen tämän modulin alimodulit vastaavat tasan avaruuden V L-invariantteja (vektori)aliavaruuksia.

(2) Olkoon A Abelin ryhmä. Esimerkissä 5.2, (2) on näytetty, että A voidaan tällöin tulkita luonnollisella tavalla $\mathbb{Z}$-modulina. Tämän modulin alimoduli on sama asia kuin ryhmän A aliryhmä. Tämä johtuu siitä, että jokainen aliryhmä on automaattisesti myös suljettu monikertojen suhteen.

(3) Olkoon R rengas ja olkoon $I \subset R$ tämän renkaan ideaali. Tällöin I on (vasemmanpuoleisen) R-modulin R alimoduli. Tämä johtuu siitä, että I on suljettu yhteenlaskun sekä mielivaltaisella renkaan alkiolla (vasemmalta) kertomisen suhteen. Muodostamalla tekijämoduli nähdään, että tekijärenkaalla R/I on olemassa luonnollinen (vasemmanpuoleisen) R-modulin struktuuri. R-skalaarikertolasku tässä modulissa on määritelty kaavalla

$$r(r' + I) = rr' + I.$$

Koska jokainen ideaali on myös suljettu oikealta kertomisen suhteen, renkaan R ideaali on sen alimoduli myös silloin, kun R ajatellaan oikeanpuoleisena R-modulina. Erityisesti tekijäjoukossa R/I on olemassa myös luonnollinen oikeanpuoleisen R-modulin struktuuri. R-skalaarikertolasku tässä modulissa on määritelty kaavalla

$$(r' + I)r = r'r + I.$$

Virittäminen ja lineaarinen riippumattomuus

Aivan kuten vektoriavaruuksien kohdalla, modulin alimodulien muodostaman perheen leikkaus on alimoduli. Tästä seuraa erityisesti, että modulin M jokaiselle osajoukolle A on olemassa sisältyvyysrelaation suhteen pienin modulin M alimoduli, joka sisältää joukon A. Tätä alimodulia sanotaan osajoukon A virittämäksi alimoduliksi ja merkitään $\mathrm{Span}(A)$.

Kuten vektoriavaruuksien teoriassa, alimoduli $\mathrm{Span}(A)$ voidaan karakterisoida myös suoraan lineaaristen kombinaatioiden avulla. Lineaarinen kombinaatio R-modulissa M on lauseke muotoa

$$r_1\mathbf{m}_1 + \ldots + r_n\mathbf{m}_n,$$

missä $r_1, \ldots, r_n \in R$ ja $\mathbf{m}_1, \ldots, \mathbf{m}_n \in M$. Helposti nähdään, että seuraava Lemman 2.30 yleistys pätee modulien teoriassa (samalla todistuksella kuin vektoriavaruuksille).

Lemma 5.4. *Olkoon M R-moduli ja olkoon $A \subset M$. Tällöin*

$$\mathrm{Span}(A) = \{r_1\mathbf{m}_1 + r_2\mathbf{m}_2 + \ldots + r_n\mathbf{m}_n \mid r_1, \ldots, r_n \in R, \mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n \in A, n \geq 0\}.$$

Alimodulien summa
Modulin M alimodulien $N_1, \ldots, N_n$ *summa* määritellään kaavalla

$$N_1 + \ldots + N_m = \{\mathbf{m}_1 + \mathbf{m}_2 + \ldots + \mathbf{m}_n \mid \mathbf{m}_i \in N_i, i = 1, \ldots, n\}.$$

Helposti nähdään, että tämä joukko on tällöin alimoduli, itse asiassa se on yhdisteen $\bigcup_{i=1}^n N_i$ virittämä aliavaruus, $N_1 + \ldots + N_n = \mathrm{Span}(\bigcup_{i=1}^n N_i)$. Summaa $\sum_{i\in I} N_i$ sanotaan *suoraksi*, jos jokaisella sen alkiolla on yksikäsitteinen esitys muodossa $\mathbf{m}_1 + \mathbf{m}_2 + \ldots + \mathbf{m}_n$. Seuraava Lemman 2.155 versio moduleille on voimassa, samantyyppisellä todistuksella kuin vektoriavaruuksien kohdalla.

Lemma 5.5. *Olkoon M R-moduli ja olkoot $N_1, \ldots, N_n$ sen alimodulit. Tällöin seuraavat ehdot ovat yhtäpitäviä.*

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

(ii) Oletetaan, että joillakin $\mathbf{m}_i \in N_i$, $i = 1, \ldots, n$, pätee

$$\mathbf{m}_1 + \ldots + \mathbf{m}_n = \mathbf{0}_M$$

Tällöin $\mathbf{m}_i = \mathbf{0}_M$ kaikilla $i = 1, \ldots, n$. Toisin sanoen ainoa tapa esittää nollavektori summan $N_1 + N_2 \ldots + N_n$ alkiona on triviaali esitys.

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

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

Muistutus: merkintä $N_1 + \ldots + \hat{N}_i + \ldots + N_n$ tarkoittaa summaa $\sum_{j\neq i} N_j$. Edellisestä lemmasta erityisesti seuraa, että kahden alimodulin N_1, N_2 muodostama summa on suora jos ja vain jos niiden leikkaus on triviaali alimoduli, $N_1 \cap N_2 = \{\mathbf{0}_M\}$. Jos $M = N_1 \oplus N_2$, alimodulia N_2 sanotaan alimodulin N_1 *komplementiksi* modulissa M.

Esimerkki 5.6. *Olkoon L äärellisulotteisen K-vektoriavaruuden nilpotentti operaattori. Esimerkin 5.2, (9) nojalla V voidaan ajatella modulina polynomirenkaan $K[\mathbf{X}]$ yli, jossa skalaarikertolasku on määritely kaavalla*

$$\mathbf{pv} = p(L)(\mathbf{v}).$$

Proposition 3.95 nojalla vektoriavaruudessa V on olemassa sellaiset vektorit $\mathbf{v}_1, \ldots, \mathbf{v}_l \in V$ siten, että K-vektoriavaruutena V on suora summa $\oplus_{i=1}^l V_i$, missä V_i on vektorin $\mathbf{v}_i$ määräämä syklinen aliavaruus

$$V_i = K[\mathbf{X}](L)(\mathbf{v}_i), i = 1, \ldots, l.$$

Tästä yhtälöstä seuraa, että jokaisella $i = 1, \ldots, n$ osajoukko V_i on yhden alkion $\mathbf{v}_i$ virittämä $K[\mathbf{X}]$-modulin V alimoduli, $V_i = \mathrm{Span}(\mathbf{v}_i)$ (tässä Span otetaan $K[\mathbf{X}]$-modulin struktuurin suhteen). Helposti nähdään, että alimodulit V_i edelleenkin muodostavat suoran summan, kun niitä ajatellaan $K[\mathbf{X}]$-modulin V alimoduleina.

Olkoon n_i vektorin $\mathbf{v}_i$ aste nilpotentin operaattorin L suhteen. Palautetaan mieleen, että tällöin $L^{n_i}(\mathbf{v}_i) = \mathbf{0}_V$, mutta $L^m(\mathbf{v}_i) \neq \mathbf{0}_V$ kaikilla $m < n_i$. Olkoon

$$J_i = \{\mathbf{p} \in K[\mathbf{X}] \mid p(L)(\mathbf{v}_i) = \mathbf{0}_V\}.$$

Helposti nähdään, että J_i on renkaan $K[\mathbf{X}]$ ideaali, jonka virittää polynomi $\mathbf{X}^{n_i}$. Kuvaus $f\colon K[\mathbf{X}] \to V_i$, $f(\mathbf{p}) = p(L)(\mathbf{v}_i)$ on surjektiivinen kuvaus, joka on lisäksi $K[\mathbf{X}]$-lineaarinen, kun rengas $K[\mathbf{X}]$ ajatellaan $K[\mathbf{X}]$-modulina luonnollisella tavalla (tarkista!). Tämän kuvauksen ydin on täsmälleen ideaali J_i. Isomorfialauseesta seuraa, että moduli V_i on isomorfinen tekijämodulin $K[\mathbf{X}]/J_i$ kanssa.

Saadaan siis seuraava tulos - jos L on äärellisulotteisen vektoriavaruuden V nilpotentti operaattori, niin yllä määritelty $K[\mathbf{X}]$-moduli V on (isomorfiaa vaille) äärellinen suora summa moduleista muotoa $K[\mathbf{X}]/(\mathbf{X}^n)$, $n \in \mathbb{N}$. Tämä voidaan ajatella tapana muotoilla Proposition 3.95 tulos moduliteorian kielellä.

Vapaat modulit

Sellaisia käsitteitä kuten vapaa ja sidottu jono/joukko, lineaarinen riippumattomuus ja kanta määritellään samalla tavalla kuin vektoriavaruuksien teoriassa. Jono $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ on vapaa modulissa M, jos jokaisen alimodulin $N = \mathrm{Span}(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ alkio voidaan esittää vektorien $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n$ lineaarisena kombinaationa yksikäsitteisellä tavalla. Helposti nähdään, että jono $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ on vapaa jos ja vain jos nollavektorin esitys vektorien $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n$ lineaarisena kombinaationa on triviaali (vrt. Lemma 2.33). Osajoukkoa $A \subset M$ (joka ei ole välttämättä äärellinen) sanotaan vapaaksi jos jokainen sen alkioiden muodostama äärellinen jono (ilman toistoja) on vapaa. Joukko/jono, joka ei ole vapaa, on sidottu. Lineaarinen riippumattomuus on vapauden synonyymi. Kanta on sellainen modulin osajoukko/vektorien jono joka on vapaa ja virittää koko modulin. Modulia sanotaan *vapaaksi*, jos sillä on (mahdollisesti ääretön) kanta.

Modulia sanotaan *äärellisviritteiseksi*, jos se on äärellisen joukon virittämä. Modulia sanotaan *äärellisulotteiseksi* jos sillä on äärellinen kanta. Kuten vektoriavaruuksien kohdalla R-modulilla M on olemassa kanta $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ jos ja vain jos M on isomorfinen R-modulin R^n kanssa. Tällöin modulin M *dimensiosta* ei välttämättä kuitenkaan voida puhua, sillä se ei ole aina hyvinmääritelty (kts. esimerkki 5.8 alla).

Tähän mennessä modulien teoria on ollut täysin analoginen vektoriavaruuksien teorian kanssa. Vapauden kohdalla yleinen modulien teoria alkaa kuitenkin poiketa huomattavasti vektoriavaruuksien teoriasta.

Tiedetään, että moduleille kuntien yli, eli vektoriavaruuksille, pätevät seuraavat väitteet.

- Jokainen vektoriavaruus on vapaa. Tätä väitettä ollaan todistettu vain äärellisvirritteisen vektoriavaruuden kohdalla (Propositio 2.41), mutta se pätee yleisesti kaikille vektoriavaruuksille (tähän palataan myöhemmin).
- Äärellisulotteisen vektoriavaruuden dimensio on yksikäsitteisesti määrätty (Seuraus 2.46).

- Vektoriavaruuden aliavaruuden kanta voidaan laajentaa koko avaruuden kannaksi. Tämäkin ollaan todistettu vain äärellisulotteisessa tapauksessa Propositiossa 2.48, mutta väite pätee yleisesti myös ääretönulotteisille vektoriavaruuksille ja niiden aliavaruuksille.

- Äärellisulotteisen avaruuden V aidon aliavaruuden $W \neq V$ dimensio on aidosti pienempi kuin V:n dimensio (Propositiossa 2.48), $\dim W < \dim V$.

- Jokainen äärellisviritteinen vektoriavaruus on äärellisulotteinen, erityisesti vapaa (Propositio 2.41).

- Vektoriavaruuden V jokaisella aliavaruudella on olemassa komplementti avaruudessa V. Äärellisulotteisessa tapauksessa tämä todistettiin Lemmassa 2.159.

- Olkoon V äärellisulotteinen vektoriavaruus ja olkoon $L\colon V \to V$ lineaarinen kuvaus. Tällöin L on injektio jos ja vain jos se on surjektio (Seuraus 2.94).

Mikään näistä väitteessä ei ole enää voimassa yleisesti, kun vektoriavaruudet korvataan niissä moduleilla.

Esimerkkejä 5.7. *(1) Olkoon A epätriviaali äärellinen Abelin ryhmä, $|A| \geq 2$. Esimerkin 5.2, (2) perusteella A on $\mathbb{Z}$-moduli. Tämä moduli on triviaalisti äärellisviritteinen, sillä $A = \mathrm{Span}(A)$. Ryhmä A ei kuitenkaan ole vapaa $\mathbb{Z}$-modulina. Tämä nähdään esimerkiksi seuraavasti. Olkoon B jokin $\mathbb{Z}$-modulin A kanta. Tällöin B on selvästi epätyhjä, sillä tyhjä joukko virittää triviaalin ryhmän. Näin ollen on olemassa $b \in B$. Koska A on äärellinen ja kokonaislukuja on ääretön määrä, monikertojen nb joukossa, $n \in \mathbb{Z}$, täytyy olla toistoja. Täsmällisesti sanottuna on olemassa $n, m \in \mathbb{Z}$, $n \neq m$ siten, että $nb = mb$. Tämä on sama asia kuin $(n-m)b = 0$. Koska $n \neq m$ ja $b \neq 0$ (vapaa joukko ei voi sisältää nolla-alkiota), tämä on ristiriidassa joukon B vapauden kanssa. Itse asiassa tästä nähdään, että ainoa A:n vapaa osajoukko on tyhjä joukko. Erityisesti siis A ei voi olla vapaa. Näin ollen äärellisviritteisen modulin ei tarvitse olla äärellisulotteinen.*

(2) Edellisessä esimerkissä syy modulin kannan olemattomuuteen on oleellisesti niin sanottujen epätriviaalien torsioalkioiden olemassaolo modulissa. R-modulin alkiota $\mathbf{m} \in M$ sanotaan torsioalkioksi jos on olemassa sellainen skalaari $r \in R$, $r \neq 0_R$, jolle pätee $r\mathbf{m} = \mathbf{0}_M$. Nolla-vektori on triviaalisti torsioalkio, mutta modulissa voi olla myös epätriviaaleja torsioalkioita. Helposti nähdään (HT), että vapaassa $\mathbb{Z}$-modulissa ei ole epätriviaaleja torsioalkioita (huom, tämä ei välttämättä päde jos $\mathbb{Z}$ korvataan tässä yhteydessä mielivaltaisella renkaalla R). Tällaisia moduleita sanotaan yleisemmin torsiovapaiksi.

On kuitenkin myös olemassa torsiovapaita $\mathbb{Z}$-moduleita, jotka eivät ole vapaita. Esimerkki tällaisesta modulista on rationaalilukujen muodostama Abelin ryhmä $(\mathbb{Q}, +)$ $\mathbb{Z}$-modulina ajateltuna. On melko selvä, että $\mathbb{Q}$ on torsiovapaa $\mathbb{Z}$:n suhteen. Kuitenkin $\mathbb{Q}$ ei ole vapaa $\mathbb{Z}$-moduli. Tämän väitteen tarkka todistus jätetään harjoitustehtäväksi.

(3) Parillisten lukujen muodostama joukko $2\mathbb{Z}$ on $\mathbb{Z}$-modulin $\mathbb{Z}$ alimoduli (tässä Abelin ryhmä $(\mathbb{Z},+)$ ajatellaan $\mathbb{Z}$-modulina). Kumpikin moduli $\mathbb{Z}$ ja $2\mathbb{Z}$ on vapaa, itse asiassa 1-ulotteinen. Esimerkiksi jono (1) on $\mathbb{Z}$-modulin $\mathbb{Z}$ kanta, sillä jokainen kokonaisluku $n \in \mathbb{Z}$ voidaan esittää yksikäsitteisellä tavalla ykkösen monikertana, $n = n \cdot 1$. Toinen modulin $\mathbb{Z}$ kanta on jono (-1) ja muita kantoja ei ole (mieti miksi!).

Samalla tavalla nähdään, että $\mathbb{Z}$-modulin $2\mathbb{Z}$ ainoat kannat ovat (2) ja (-2). Edellisestä seuraa, että kumpaakaan näistä kannoista ei voida laajentaa koko avaruuden kannaksi.Lisäksi tässä esimerkissä aidon alimodulin dimensio on sama kuin koko modulin dimensio (mikä on mahdotonta vektoriavaruuksille).

(4) Kuvaus $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$ kaikilla $n \in \mathbb{Z}$, on lineaarinen kuvaus, kun $\mathbb{Z}$ ajatellaan $\mathbb{Z}$-modulina. Tämä kuvaus on injektio, mutta ei ole surjektio.

(5) Abelin ryhmä $(\mathbb{Z}_4,+)$ voidaan ajatella $\mathbb{Z}_4$-modulina, jossa skalaarikertolaskuna käytetään renkaan $(\mathbb{Z}_4,+,\cdot)$ kertolaskua. Tällöin $\mathbb{Z}_4$ on $\mathbb{Z}_4$-modulina vapaa, itse asiassa yksiulotteinen. Kannaksi kelpaa esimerkiksi (1_4).

Osajoukko $N = \{0_4, 2_4\}$ on renkaan $(\mathbb{Z}_4,+,\cdot)$ ideaali (tarkista!). Esimerkin 5.2,(3) nojalla N on $\mathbb{Z}_4$-modulin $\mathbb{Z}_4$ alimoduli. N ei kuitenkaan ole vapaa $\mathbb{Z}_4$-moduli. Tämä nähdään esimerkiksi siitä, että sen kahdesta alkiosta vain 2_4 voi kuulua sen kantaan (kanta ei voi sisältää nolla-vektoria). Mutta $2_4 \cdot 2_4 = 0_4$, mistä nähdään, että jono (2_4) ei ole vapaa.

Näin ollen vapaan modulin alimodulin ei tarvitse olla vapaa.

Esimerkki 5.8. *Konstruoidaan esimerkki epätriviaalista renkaasta R joka on R-modulina n-ulotteinen jokaisella $n \in \mathbb{N}$. Tästä seuraa, että äärellisulotteisen vapaan modulin dimensio ei ole välttämättä hyvin määritelty.*

Riittää löytää sellainen rengas R joka on R-modulina isomorfinen R-modulin R^2 kanssa. Tällöin induktiolla saadaan yleisesti, että $R^n \cong R$ kaikilla $n \in \mathbb{N}$.

Olkoon K jokin kunta ja olkoon $V = K^{(\mathbb{N})}$ ääretönulotteinen vektoriavaruus, jolla on numeroituva kanta $\{\mathbf{e}_n \mid n \in \mathbb{N}\}$. Konkreettinen esimerkki tällaisesta avaruudesta on polynomialgebra $K[\mathbf{X}]$. Olkoon $R = L(V)$ avaruuden V operaattorien muodostama K-algebra. Tällöin R on erityisesti rengas. Olkoot $L_1, L_2 \in R$ sellaiset yksikäsitteiset lineaariset kuvaukset, joille pätee

$$L_1(\mathbf{e}_n) = \begin{cases} \mathbf{e}_k, \ \textit{jos } n = 2k, k \in \mathbb{N} \\ \mathbf{0}, \textit{muuten} \end{cases}$$

$$L_2(\mathbf{e}_n) = \begin{cases} e_k, \ \textit{jos } n = 2k+1, k \in \mathbb{N} \\ \mathbf{0}, \textit{muuten} \end{cases} .$$

Tällöin jokainen operaattori $L \in R = L(V)$ voidaan kirjoittaa yksikäsitteisellä tavalla muodossa

$$L = AL_1 + BL_2, \tag{5.9}$$

missä $A, B \in R$. Nimittäin, jos tämä yhtälö on voimassa, täytyy jokaisella $k \in \mathbb{N}$ päteä

$$A(\mathbf{e}_k) = L(\mathbf{e}_{2k}) \text{ ja } B(\mathbf{e}_k) = L(\mathbf{e}_{2k+1}).$$

Kääntäen, jos A ja B määritellään näillä ehdoilla, yhtälö 5.9 on voimassa. Lisäksi Proposition 2.57 nojalla tällaiset A ja B ovat olemassa ja yksikäsitteiset. Tästä tarkastelusta seuraa, että pari (L_1, L_2) on R-modulin R-kanta. Erityisesti R on isomorfinen R-modulin R^2 kanssa.

Ei ole vaikeaa näyttää, että R-modulilla R on itse asiassa olemassa myös ääretön, tarkemmin sanotuna numeroituva kanta. Tämän väitteen osoitamiseksi pitää avaruuden V kannan $\{\mathbf{e}_n \mid n \in \mathbb{N}\}$ indeksijoukko $\mathbb{N}$ jakaa äärettömään moneen erilliseen äärettömään osaan. Yllä annetussa konstruktiossa $\mathbb{N}$ jaettiin vain kahteen äärettömään osaan (parilliset ja parittomat luvut).

Edellisen esimerkin valossa nähdään, että äärellisulotteisella R-modulilla ei välttämättä ole hyvinmääriteltyä dimensiota. Kun R on kunta, tai yleisemmin, niin sanottu *vinokunta* (eli epätriviaali rengas, jossa jokaisella alkiolla on käänteisalkio), R-modulin äärellisen kannan koko ei riipu kannan valinnasta. Kunnan tapauksessa tämä oli osoitettu Propositiossa 2.42. Todistuksessa ei tarvittu kunnan kertolaskun vaihdannaisuutta, joten se pätee sellaisenaan myös vinokunnan tapauksessa.

Voidaan osoittaa, että kannan koko on invariantti, kun kerroinrengas on vaihdannainen. Tähän kuitenkin tarvitaan Zornin Lemman kaltaisia abstrakteja joukko-opillisia työkaluja, joten asiaan palataan myöhemmin Zornin Lemman sovellusten kohdalla. Osoitetaan tässä vaiheessa seuraava tekninen aputulos.

Propositio 5.10. *Oletetaan, että renkaalla R on olemassa sellainen ideaali I, jolle tekijärengas R/I on vinokunta. Tällöin äärellisulotteisen R-modulin kannan koko ei riipu kannan valinnasta.*

Todistus. Esitetään todistuksen idea, teknisten välivaiheiden läpikäynti jätetään lukijalle harjoitustehtäväksi. Olkoon M äärellisulotteinen R-moduli ja olkoon $(\mathbf{m}_1, \ldots, \mathbf{m}_n)$ sen kanta. Määritellään

$$N = \{\sum_{i=1}^{n} r_i \mathbf{m}_i \mid r_i \in I \text{ kaikilla } i = 1, \ldots, n\}.$$

Tällöin N on modulin M alimoduli (tarkista!), joten voidaan puhua tekijämodulista $P = M/N$. Tämä on tällöin R-moduli, mutta P:ssä voidaan määritellä myös R/I-modulin struktuuri. Nimittäin varustetaan P sen tavallisella yhteenlaskulla ja määritellään R/I-skalaarikertolasku kaavalla

$$(r + I)(\mathbf{m} + N) = r\mathbf{m} + N.$$

Tämä on hyvin määritelty (tarkista!), joten P on R/I-moduli. Suoralla laskulla nähdään, että jono $(\mathbf{m}_1 + N, \ldots, \mathbf{m}_n + N)$ on R/I-modulin P kanta. Koska R/I on vinokunta, äärellisulotteisilla moduleilla sen yli on hyvin määritelty dimensio (joka on kannan pituus), joka ei riipu kannan valinnasta. Näin ollen sama pätee myös alkuperäiselle R-modulille M. □

Kokonaislukujen renkaan $\mathbb{Z}$ ja polynomirenkaan $K[\mathbf{X}]$ kohdalla edellisen proposition oletus on voimassa. Nimittäin renkaassa $\mathbb{Z}$ voidaan valita $I = p\mathbb{Z}$, missä p on mikä tahansa alkuluku, tällöin tekijärengas $\mathbb{Z}/I = \mathbb{Z}_p$ on kunta. Samoin polynomirenkaan $K[\mathbf{X}]$ mikä tahansa jaoton polynomi $\mathbf{p}$ virittää polynomin $I = (\mathbf{p})$, jonka suhteen tekijärengas $K[\mathbf{X}]/(\mathbf{p})$ on kunta (Propositio 3.63). Näin ollen jokaisen äärellisulotteisen Abelin ryhmän (eli $\mathbb{Z}$-modulin) tai jokaisen äärellisulotteisen $K[\mathbf{X}]$-modulin dimensio on hyvin määritelty. Aliluvussa 5.3 osoitetaan, että edellisen proposition oletukset ovat voimassa jokaisessa *vaihdannaisessa* renkaassa.

Lineaariset kuvaukset

Olkoot M, N (vasemmanpuoleisia) R-moduleita. Kaikkien R-lineaaristen kuvausten $L\colon M \to N$ joukkoa merkitään $L(M, N)$. Jos kerroinrengasta halutaan korostaa, tätä joukkoa voidaan merkitä myös $L_R(M, N)$. Kun $M = N$, joukkoa $L(M, M)$ merkitään myös lyhyemmin symbolilla $L(M)$.

Lineaarisia kuvauksia $L, L'\colon M \to N$ voidaan laskea yhteen pisteittäin. Summakuvauksen $L + L'\colon M \to N$,

$$(L + L')(\mathbf{m}) = L(\mathbf{m}) + L'(\mathbf{m}), \mathbf{m} \in M,$$

helposti nähdään olevan R-lineaarinen. Lisäksi pari $(L(M, N), +)$ on tällöin Abelin ryhmä. 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 $(-L)(m) = -L(m)$.

Skalaarikertolaskun kanssa asia ei ole niin yksinkertainen. Luonnollinen kandidaatti alkioksi rL, missä $r \in R$ ja $L \in L(M, N)$, on kuvaus joka on määritelty pisteittäin ehdolla $(rL)(\mathbf{m}) = r \cdot L(\mathbf{m})$. Tällainen kuvaus ei välttämättä kuitenkaan ole R-lineaarinen, joten tällä tavalla määritelty R-skalaarikertolasku ei yleisesti ottaen pysy joukossa $L(M, N)$, joten jälkimmäinen ei ole R-moduli millään "luonnollisella tavalla".

Suoralla laskulla nähdään, että rL ON kyllä R-lineaarinen, mikäli kerroinrengas R on *vaihdannainen*. Tämän verifiointi menee samalla tavalla kuin erikoistapauksessa, missä $R = K$ on kunta.

Bimodulit

Edellä nähtiin, että kun kerroinrengas R ei ole vaihdannainen, lineaaristen kuvausten muodostama joukko $L(M, N)$ ei välttämättä ole R-moduli pisteittäisen skalaarikertolaskun suhteen. On olemassa käytännön sovellusten kannalta hyödyllinen erikoistapaus, jossa tästä joukosta saadaan moduli - kuitenkin jonkun toisen renkaan R' suhteen.

Olkoot R, R' renkaita. $R - R'$-*bimoduli* N on algebrallinen struktuuri, jossa joukolla N on sekä *vasemmanpuoleisen* R-modulin, että *oikeanpuoleisen* R'-modulin struktuuri. Lisäksi oletetaan, että näillä struktuureilla on yhteinen (eli sama) yhteenlasku-operaatio ja kaikilla $r \in R$, $r' \in R'$, $\mathbf{m} \in N$ pätee

$$(r\mathbf{m})r' = r(\mathbf{m}r').$$

Bimodulissa siis vasen-ja oikeanpuoleiset skalaarikertolaskut ovat ”yhteensopivia” (”kommutoivat”).

Oletetaan, että M on R-moduli ja N on $R-R'$ bimoduli. Tällöin N on erityisesti R-moduli, joten voidaan puhua R-lineaarisista kuvauksista $L\colon M \to N$. Nämä muodostavat joukon $L_R(M,N)$, joka on Abelin ryhmä kuvausten pisteittäisen yhteenlaskun suhteen. Koska N on myös oikeanpuoleinen R'-moduli, tässä joukossa voidaan määritellä *oikeanpuoleisen* R'-modulin struktuuri luonnollisella tavalla. Nimittäin jokaisella $L \in L_R(M,N)$ ja jokaisella $r' \in R$ määritellään kuvaus Lr' ”pisteittäin”,

$$(Lr')(\mathbf{m}) = L(\mathbf{m})r', \mathbf{m} \in M.$$

Tällöin bimodulin määritelmän avulla voidaan helposti tarkistaa, että Lr' on R-lineaarinen kaikilla $L \in L_R(M,N)$ ja kaikilla $r' \in R$. Joukossa $L_R(M,N)$ voidaan siis määritellä R'-skalaarikertolasku. Lisäksi $L_R(M,N)$ on tällöin *oikeanpuoleinen* R'-moduli.

Duaalimodulit

Olkoon M (vasemmanpuoleinen) R-moduli. Edellä esitetty erään oikeanpuoleisen skalaarikertolaskun konstruktio on erittäin käyttökelpoinen kun tarkastellaan R-lineaarisia kuvauksia $L\colon M \to R$, missä R ajatellaan *vasemmanpuoleisena* R-modulina luonnollisella tavalla (kertolasku vasemmalta). Nämä kuvaukset muodostavat joukon $L_R(M,R)$, jota merkitään myös M^* ja sanotaan modulin M *duaalimoduliksi*.

Jos R on vaihdannainen rengas, duaalimoduli M^* on myös vasemmanpuoleinen R-moduli luonnollisten pisteittäisten laskutoimitusten suhteen. Jos R ei ole vaihdannainen, tämä ei enää pidä paikkaansa, mutta tällöin R on $R-R$-*bimoduuli* luonnollisella tavalla, sillä R:ssä voidaan kertoa R:n alkioilla sekä vasemmalta, että oikealta. Edellisen nojalla biduaalissa M^* on tällöin olemassa luonnollinen *oikeanpuoleisen* R-modulin struktuuri. Näin ollen oikeanpuoleisten modulien käsite tulee luonnollisella tavalla eteen vasemmanpuoleisten modulien teoriassa duaalimodulien kohdalla.

Kuten vektoriavaruuksien teoriassa, jokaiseen lineaarisen kuvaukseen $L\colon M \to N$ vasemmanpuoleisten R-modulien M, N välillä voidaan liittää kanonisella tavalla sen duaali $L^*\colon N^* \to M^*$, joka on tällöin oikeanpuoleisten R-modulien N^*, M^* välinen lineaarinen kuvaus.

Biduaali ja refleksiivisyys

Edelliset tarkastelut toimivat samalla tavalla oikeanpuoleisille moduleille. Erityisesti, jos M on oikeanpuoleinen R-moduli, sen duaali M^* on vasemmanpuoleinen R-moduli luonnollisella tavalla. Tästä seuraa, että jos lähdetään liikkeelle vasemmanpuoleisesta R-modulista M, niin sen duaali M^* on oikeanpuoleinen R-moduli, joten tämän duaali $(M^*)^* = M^{**}$, eli modulin M *biduaali*, on taas *vasemmanpuoleinen* R-moduli. Toisin sanoen jokaisella vasemmanpuoleisella R-modulilla M on olemassa sen biduaali M^{**}, joka on myös vasemmanpuoleinen R-moduli, eli ”kuuluu samaan algebralliseen maailmaan” kuin M. Erityisesti voidaan verrata moduleita M ja M^{**}, muodostaa niiden välisiä R-lineaarisia kuvauksia ja niin edelleen (tämä ei yleisesti ottaen ole mahdollista M:lle ja sen duaalille M^*, sillä ei voida puhua lineaarisestä kuvauksesta vasemmanpuoleisen ja oikeanpuoleisen modulin välillä). Kuten vektoriavaruuksien teoriassa voidaan konstruoida

kanoninen kuvaus $\Phi\colon M \to M^{**}$ kaavalla $\Phi(\mathbf{m})(L) = L(\mathbf{m})$. Propositioiden 2.119 ja 2.121 analogiat moduleille ovat voimassa. Viimeksi mainittu sanoo tällöin sen, että vapaan modulin M kohdalla kanoninen isomorfismi Φ on injektio. Lisäksi se on isomorfismi, jos M on äärellisulotteinen. Modulien tapauksessa jälkimmäistä väitettä ei kuitenkaan voida enää päätellä käyttämällä "dimensioanalyysiä", joka on standardi tekniikka vektoriavaruuksien teoriassa, eli vetoamalla siihen, että äärellisulotteisessa tapauksessa lineaarinen injektio samaa ulottuvuutta olevien avaruusten välillä on automaattisesti myös surjektio. Tämä periaate ei nimittäin päde modulien teoriassa, kts. esimerkki 5.7, (4). Näin ollen Proposition 2.121 vastine moduleille pitää todistaa toisella tavalla.

Yleisesti ottaen kanonisen kuvauksen $\Phi\colon M \to M^{**}$ ei tarvitse olla injektio, jos moduli M ei ole vapaa. Esimerkiksi olkoot $R = \mathbb{Z}$, $M = \mathbb{Z}_3$. Tällöin mikä tahansa ryhmähomomorfismi (eli $\mathbb{Z}$-lineaarinen kuvaus) $L\colon \mathbb{Z}_3 \to \mathbb{Z}$ on nolla-kuvaus. Tämä nähdään seuraavasti. Olkoon $x \in \mathbb{Z}_3$, tällöin $3x = 0$, joten

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

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

Matriisit renkkaiden yli

Olkoon R rengas. $(n \times m)$-kokoinen R-kertoiminen matriisi määritellään ilmeisellä tavalla, eli $(n \times m)$ taulukkona

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

jonka jokainen alkio kuuluu renkaaseen R. Samankokoisia matriiseja voidaan laskea yhteen ja kertoa skalaareilla, eli renkaan R alkioilla "koordinaatteittain". Lisäksi skalaarilla kertominen voidaan suorittaa sekä *vasemmalta*, että *oikealta*. Näin ollen $(n \times m)$-kokoisten R-kertoimisten matriisien joukkoa $M(n \times m; R)$ voidaan ajatella sekä vasemmanpuoleisena, että oikeanpuoleisena R-modulina luonnollisella tavalla.

Olkoot M, N *äärellisulotteisia* (vasemmanpuoleisia) R-moduleita. Oletetaan, että $E = (\mathbf{m}_1, \dots, \mathbf{m}_m)$ on modulin M kanta ja $F = (\mathbf{n}_1, \dots, \mathbf{n}_n)$ on modulin N kanta. Tällöin poimimalla lineaarisista kombinaatioista

$$L(\mathbf{m}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{n}_i$$

kertoimia (a_{ij}) voidaan muodostaa kuvauksen L matriisi $[L]_{F,E}$ kantojen E ja F suhteen, aivan samalla tavalla kuin vektoriavaruuksien teoriassa. Vastaavuus $L \mapsto [L]_{F,E}$ on tällöin bijektiivinen kuvaus, joka on Abelin ryhmien $L(M, N)$ ja $M(n \times m; R)$ välinen

homomorfismi. Jos R on vaihdannainen, tämä vastaavuus säilyttää myös skalaarikertolaskun, mutta yleisesti ottaen sen lineaarisuudesta ei voida puhua, sillä $L(M,N)$ ei yleisesti ottaen ole välttämättä edes R-moduli.

R-kertoimisten matriisien kertolasku voidaan määritellä samalla tavalla kuin yleensäkin, eli säännöllä "rivi kertaa sarake", mutta voidaan määritellä myös säännöllä "sarake kertaa rivi". Tarkemmin sanottuna olkoon A $(n \times m)$-kokoinen R-kertoiminen matriisi ja olkoon B $(m \times l)$-kokoinen R-kertoiminen matriisi. Tällöin $AB = C = (c_{ij})$ voidaan määritellä $(n \times l)$-kokoisena matriisina, jolle pätee

$$c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}. \tag{5.11}$$

Yhtä hyvin tulo $AB = C = (c_{ij})$ voidaan määritellä myös kaavana

$$c_{ij} = \sum_{k=1}^{m} b_{kj} a_{ik}. \tag{5.12}$$

Jos kerroinrengas R on vaihdannainen, kumpikin määritelmä antaa saman tuloksen, mutta yleisesti kyseessä on eri operaatiot. Osoittautuu, että vasemmanpuoleisten modulien tapauksessa tällöin nimenomaan määritelmä 5.12 antaa "oikean määritelmän" siinä mielessä, että kertolasku vastaa *lineaaristen kuvausten yhdistämistä*, eli kaava

$$[L' \circ L]_{G,E} = [L']_{G,F}[L]_{F,E}$$

pätee, kun $L \in L(M,N), L' \in L(N,P)$ sekä E, F, G ovat äärellisulotteisten modulien M, N ja P kannat. Jos taas ollaan oikeanpuoleisten modulien maailmassa, kuvausten yhdistämistä vastaa tuttu "rivi kerrotaan sarakkeella" sääntö 5.11.

Determinantit

Neliömatriisin $A \in M(n \times n; R)$ determinantti voidaan määritellä multilineaaristen kuvausten teorian avulla samalla tavalla kuin kuntien yli, *jos kerroinrengas R on vaihdannainen.* Tällöin aliluvun 2.5 määritelmät ja determinanttien ominaisuudet pätevät sellaisinaan, esim. determinantti voidaan kehittää minkä tahansa rivin tai sarakkeen suhteen, pätee kaava

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

ja niin edelleen. Tämän kaavan avulla voidaan näyttää, että similaaristen matriisien determinantti on sama, jolloin voidaan puhua äärellisulotteisen modulin operaattorin determinantista. Proposition 2.145 vastine R-moduleille sanoo, että matriisi on kääntyvä matriisirenkaassa $M(n \times n; R)$ jos ja vain jos sen determinantti on kääntyvä alkio renkaassa R.

Jos rengas R ei ole vaihdannainen, matriisin determinanttien teoria ei toimi samalla tavalla kuin vaihdannaisessa tapauksessa eikä determinanteista tällöin ole niin paljon hyötyä. Esimerkiksi kaavan $\det(AB) = \det(A)\det(B)$ ei tarvitse päteä (riippumatta sitä, millä tavalla matriisien kertolaksu määritellään). Tästä syystä determinantteja yleensä määritellään ja tutkitaan vain vaihdannaisen kerroinrenkaan tapauksessa.

5.2. Äärellisviritteiset Abelin ryhmät

Tässä aliluvussa tutkitaan äärellisviritteisten Abelin ryhmien, eli äärellisviritteisten $\mathbb{Z}$-modulien rakennetta.

Palautetaan mieleen, että R-moduli M on äärellisviritteinen, jos on olemassa sellaiset alkiot $\mathbf{m}_1, \ldots, \mathbf{m}_k \in M$, joille pätee $M = \mathrm{Span}(\mathbf{m}_1, \ldots, \mathbf{m}_k)$. Kun $R = K$ on kunta, äärellisviritteiset R-modulit (eli äärellisviritteiset K-vektoriavaruudet) on helppo luokitella isomorfiaa vaille: kuten tiedetään Luvun 2 sisällön perusteella ne ovat äärellisulotteiset. Lisäksi jokaisella äärelliviritteisellä K-vektoriavaruudella on hyvinmääritelty dimensio $\dim K \in \mathbb{N}$. Kaksi äärellisviritteistä vektoriavaruutta ovat isomorfisia jos ja vain jos niillä on sama dimensio. Dimensio on siis *invariantti* joka *luokittelee* äärellisviritteiset vektoriavaruudet isomorfiaa vaille täydellisesti.

Kun R ei ole kunta, asia on monimutkaisempi. Kuntien jälkeen "yksinkertaisimpana" renkaana voidaan pitää kokonaislukujen rengasta $\mathbb{Z}$. Tästä syystä tässä osiossa tutkitaan äärellisviritteisiä $\mathbb{Z}$-moduleita, toisin sanoen *äärellisviritteisiä Abelin ryhmiä*. Kaikki tulokset, jotka saavutetaan tässä aliluvussa ovat (ainakin sopivasti yleistettynä ja tulkittuna) voimassa itse asiassa myös kun R on *pääideaalirengas* eli sellainen vaihdannainen rengas, jonka jokainen ideaali on yhden alkion virittämä. Kokonaislukujen rengas $\mathbb{Z}$ on pääideaalirengas. Meidän kannalta toinen tuttu ja tärkeä esimerkki pääideaalirenkaasta, joka ei ole kunta, on polynomirengas $K[\mathbf{X}]$ (missä K on kunta). Esimerkissä 5.2, (9) näytettiin, kuinka äärellisulotteisten vektoriavaruuksien lineaaristen operaattorien teoria voidaan tulkita myös eräiden äärellisviritteisten $K[\mathbf{X}]$-modulien teorian osaksi. Näin ollen tämän aliluvun tulosten luonnolliset yleistykset äärellisviritteisten $K[\mathbf{X}]$-modulien tapaukseen ovat hyödyllisiä myös "perinteisen" lineaarialgebran eli vektoriavaruuksien teorian kannalta.

Tässä aliluvussa Abelin ryhmien alkiota merkitään tavallisella, ei lihavoidulla fontilla (vaikka kyseessä ovatkin eräiden modulien vektorit).

Yksinkertaisin epätyhjä virittäjäjoukko sisältää yhden alkion, joten aloitetaan tarkastelu yhden alkion virittämistä Abelin ryhmistä. Tällaisia ryhmiä sanotaan *syklisiksi*.

Olkoon $(A, +)$ syklinen ryhmä ja olkoon $x \in A$ sen virittäjä. Määritellään kuvaus $f\colon (\mathbb{Z}, +) \to (A, +)$ kaavalla $f(n) = nx$. Helposti nähdään, että tämä kuvaus on ryhmien välinen homomorfismi. Lisäksi, koska x virittää ryhmän A, f on tässä tapauksessa surjektiivinen. Kuvauksen f ydin on jokin ryhmän $(\mathbb{Z}, +)$ aliryhmä, eli muotoa $m\mathbb{Z}$ jollakin $m \in \mathbb{N}$. Ryhmien isomorfialauseesta seuraa nyt, että $A \cong \mathbb{Z}/mZ = \mathbb{Z}_m$. Näin ollen jokainen syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}_m$ kanssa jollakin $m \in \mathbb{N}$. Kun $m = 0$, A on ääretön ja isomorfinen ryhmän $\mathbb{Z} = \mathbb{Z}_0$ kanssa. Kun $m > 0$, ryhmässä A on tasan m alkiota.

Yleisemmin olkoon A mielivaltainen Abelin ryhmä ja olkoon $a \in A$ jokin sen alkio. Tällöin alkion a virittämä aliryhmä $A' = \mathrm{Span}(a)$ on syklinen ja pätee

$$A' = \{na \mid n \in \mathbb{Z}\}.$$

Käytetään myös merkintää $A' = \mathrm{Span}(a) = \mathbb{Z}[a]$.

Jos syklinen ryhmä A' on ääretön, se on isomorfinen ryhmän $\mathbb{Z}$ kanssa. Tällöin kaikilla $n \in \mathbb{Z}, n \neq 0$, myös $na \neq 0$, ja sanotaan, että ryhmän A alkion a *kertaluku* on ääretön.

Toinen mahdollisuus on, että A' on äärellinen, jolloin se on isomorfinen ryhmän $\mathbb{Z}_m$ kanssa jollakin $m > 0$. Täsmällisesti sanottuna tällöin on olemassa sellainen isomorfismi $f\colon \mathbb{Z}_m \to A'$, jolle pätee $f(1_m) = a$. Silloin ryhmässä A pätee $ma = 0$, mutta alkiot $a, 2a, \ldots, (m-1)a$ eroavat nolla-alkiosta. Tässä tapauksessa sanotaan, että alkion a *kertaluku* on kokonaisluku m. Kertaluku on siis *pienin* positiivinen kokonaisluku n, jolle pätee $na = 0$, jos sellainen on olemassa, muuten kertaluku on ääretön. On selvää, että *äärellisessä* Abelin ryhmässä jokaisen alkion kertaluku on äärellinen.

Lemma 5.13. *Olkoon $b \neq 0$ syklisen äärellisen ryhmän $\mathbb{Z}_m$ alkio, $m \geq 1$. Olkoon n sen kertaluku. Tällöin: (i) Luku n on äärellinen ja se on luvun m tekijä.*
(ii) Olkoon $k \in \mathbb{N}$. Tällöin $kb = 0$ jos ja vain jos $k = qn$ jollakin $q \in \mathbb{Z}$, eli jos ja vain jos k on jaollinen n:llä.

Todistus. (i) Olkoon $b \neq 0$ syklisen äärellisen ryhmän $\mathbb{Z}_m$ alkio. Tällöin $mb = 0$. Olkoon n luvun b kertaluku Abelin ryhmässä $\mathbb{Z}_m$. Osoitetaan, että n on luvun m tekijä. Kokonaislukujen jakoyhtälön nojalla pätee $m = qn + r$, missä $0 \leq r < n$. Näin ollen

$$rb = (m - qn)b = mb - q(nb) = 0 - 0 = 0.$$

Koska n on pienin positiivinen kokonaisluku, jolle pätee $nb = 0$ ja $0 \leq r < n$, tästä seuraa, että täytyy olla $r = 0$. Näin ollen $m = qn$, toisin sanoen luku n on luvun m tekijä.

(ii) Kuvaus $\mathbb{Z}_n \to \mathbb{Z}[b]$, $\bar{k} \to kb$ on isomorfismi. Koska yhtälö $k = k_n = 0$ pätee ryhmässä $\mathbb{Z}_n$ jos ja vain jos k on jaollinen luvulla n, (ii) seuraa. □

Jokainen syklinen ryhmä on erityisesti äärellisviritteinen. Äärellinen suora summa äärellisviritteisistä ryhmistä on selvästi äärellisviritteinen, joten jokainen muotoa

$$\mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k} \tag{5.14}$$

oleva ryhmä, missä $n, k \in \mathbb{N}, m_1, \ldots, m_k \geq 1$, on äärellisviritteinen. Osoittautuu, että myös käänteinen väite pätee, nimittäin jokainen äärellisviritteinen Abelin ryhmä on isomorfiaa vaille muotoa 5.14 eli äärellinen suora summa syklisistä ryhmistä.

Abelin ryhmän esitys tässä muodossa ei ole yksikäsitteinen, jopa tekijöiden järjestystä vaille. Esimerkiksi voidaan näyttää, että

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_{30} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{10}.$$

Tämä seuraa itse asiassa suoraan Lemmasta 5.19, joka todistetaan myöhemmin.

Jos esityksessä 5.14 kuitenkin vaaditaan, että $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$, niin siitä tulee yksikäsitteinen. Tässä merkintä $p \mid q$ tarkoittaa, että p on luvun q tekijä eli q on jaollinen p:llä. Voimassa on siis seuraava **äärellisviritteisten Abelin ryhmien struktuurilause**.

Lause 5.15. *Olkoon A äärellisviritteinen Abelin ryhmä. Tällöin on olemassa yksikäsitteiset $n, k \in \mathbb{N}$, $m_1, \ldots, m_k \geq 2$, siten että $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$ ja*

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}. \tag{5.16}$$

Lauseen 5.15 todistus on suhteellisen pitkä ja sisältää lukuisia yksityiskohtia. Aloitetaan sen todistaminen tarkastelemalla ensin *äärellisulotteisia* eli vapaita äärellisviritteisiä Abelin ryhmiä. Abelin ryhmä A on äärellisulotteinen jos ja vain jos se on isomorfinen ryhmän $\mathbb{Z}^m$ kanssa jollakin $m \in \mathbb{N}$. Lisäksi tällöin ryhmän dimensio $m = \dim A$ on hyvin määritelty Proposition 5.10 nojalla.

Proposition 2.48 nojalla tiedetään, että äärellisulotteisen vektoriavaruuden aliavaruus on myös äärellisulotteinen. Lisäksi aliavaruuden jokainen kanta voidaan laajentaa koko avaruuden kannaksi. Modulien kohdalla vastaava tulos ei päde. Seuraava tulos on Proposition 2.48 paras mahdollinen vastine $\mathbb{Z}$-modulien teoriassa.

Propositio 5.17. *Olkoon $A \cong \mathbb{Z}^n$ n-ulotteinen vapaa Abelin ryhmä ja olkoon $B \subset A$ aliryhmä. Tällöin on olemassa ryhmän A kanta $(a_1, \ldots, a_n)$, luku $k = 0, \ldots, n$ ja positiiviset kokonaisluvut $m_1, \ldots, m_k$ siten, että jono $(m_1 a_1, m_2 a_2, \ldots, m_k a_k)$ on ryhmän B kanta. Lisäksi voidaan olettaa $m_i \mid m_{i+1}$ jokaisella $i = 1, \ldots, k-1$.*

Erityisesti jokaisen vapaan äärellisulotteisen Abelin ryhmän aliryhmä on myös vapaa.

Todistus. Väite osoitetaan induktiolla luvun $n = \dim A$ suhteen. Tapauksessa $n = 0$ väite on triviaalisti selvä, tällöin $A = \{0\}$ on triviaali ryhmä. Tapauksessa $n = 1$ väite seuraa siitä, että ryhmän $\mathbb{Z}$ jokainen aliryhmä on muotoa $m\mathbb{Z}$ jollakin (yksikäsitteisellä) $m \in \mathbb{N}$.

Oletetaan, että väite on tosi ryhmille, joiden dimensio on $n-1$ ja oletetaan, että $\dim A = n$.

Jos $B = \{0\}$ on triviaali aliryhmä, väite on selvä. Muuten aliryhmässä B löytyy nollasta eroava alkio $b \neq 0$. Valitaan ryhmälle A jokin kanta $(v_1, \ldots, v_n)$ ja esitetään b tässä kannassa eli lineaarisena kombinaationa

$$b = m_1 v_1 + \ldots + m_n v_n.$$

Koska $b \neq 0$, ainakin yksi kerroin m_i eroaa nollasta. Järjestelemällä kannan alkiot uudelleen tarvittaessa, voidaan olettaa, että $m_1 \neq 0$.

Positiivisten luonnollisten lukujen joukko on ”hyvinjärjestetty”. Tämä tarkoittaa sitä, että jokaisella sen epätyhjällä osajoukolla on pienin alkio. Voidaan siis valita sellainen ryhmän A kanta $(v_1, \ldots, v_n)$, että B sisältää alkion

$$b_1 = m_1 v_1 + \ldots + m_n v_n,$$

missä $m = m_1 \neq 0$ on pienin positiivinen kokonaisluku jolla on tällainen ominaisuus. Toisin sanoen jos $b \in B$, $(v_1', \ldots, v_n')$ on mikä tahansa ryhmän A kanta ja pätee

$$b = k_1' v_1' + \ldots + m_n' v_n',$$

niin joko $m_1' = 0$ tai $|m_1'| \geq m$. Koska kannan alkioita voidaan aina permutoida, tässä tilanteessa pätee $m_i' = 0$ tai $|m_1'| \geq m$.

Yhtälössä

$$b_1 = m_1 v_1 + \ldots + m_n v_n,$$

kirjoitetaan jokainen kerroin m_i, $i \geq 2$, muodossa $m_i = qm + r_i$, missä $0 \leq r_i < m$ on jakojäännös ja $q_i \in \mathbb{Z}$ (jakoyhtälö). Tällöin pätee

$$b_1 = ma_1 + r_2 v_2 + \ldots + r_n v_n,$$

missä $a_1 = v_1 + q_2 v_2 + \ldots + q_n v_n$. Helposti nähdään, että jono $(a_1, v_2, \ldots, v_n)$ on ryhmän A kanta (tässä siis alkuperäisen kannan ensimmäinen jäsen v_1 korvataan alkiolla a_1). Luvun m valinnasta ja siitä, että $0 \leq r_i < m$, seuraa tällöin, että $r_2 = \ldots = r_n = 0$. Näin ollen $b_1 = ma_1$.

Toistaiseksi on osoitettu, että ryhmällä A on sellainen kanta $(a_1, v_2, \ldots, v_n)$ jolle pätee $b_1 = m_1 a_1 \in B$, $b_1 \neq 0$ jollakin $m_1 \in \mathbb{Z}$. Koska $(a_1, v_2, \ldots, v_n)$ on kanta, on voimassa hajotelma

$$A = \mathbb{Z}[a_1] \oplus A',$$

missä $\mathbb{Z}[a_1] = \{ma_1 \mid m \in \mathbb{Z}\}$ on alkion a_1 virittämä syklinen aliryhmä ja A' on jonon $(v_2, \ldots, v_n)$ virittämä aliryhmä, $A_2 = \mathrm{Span}(v_2, \ldots, v_n)$.

Seuraavaksi näytetään, että

$$B = \mathbb{Z}[b_1] \oplus B',$$

missä $B' = A' \cap B$. Tässä $\mathbb{Z}[b_1] = \{mb_1 \mid m \in \mathbb{Z}\}$ on alkion b_1 virittämä syklinen aliryhmä (joka on myös ryhmän B aliryhmä). Olkoon $b \in B$. Esitetään se kannassa $(a_1, v_2, \ldots, v_n)$ eli lineaarisena kombinaationa

$$b = m_1' a_1 + m_2' v_2 + \ldots + m_n' v_n.$$

Jakoyhtälön nojalla $m_1' = qm_1 + r$, missä $0 \leq r < m_1$. Tästä seuraa, että

$$b = ra_1 + m_2' v_2 + \ldots + m_n' v_n + qm_1 a_1 = ra_1 + m_2' v_2 + \ldots + m_n' v_n + qb_1,$$

mikä voidaan kirjoittaa myös yhtälönä

$$ra_1 + m_2' v_2 + \ldots + m_n' v_n = b - qb_1 \in B.$$

Luvun m valinnan nojalla tästä seuraa, että $r = 0$. Näin ollen $b - qb_1 \in A' \cap B = B'$. On osoitettu, että $B = \mathbb{Z}[b_1] + B'$. Koska $\mathbb{Z}[b_1] \subset \mathbb{Z}[a_1]$, $B' \subset A'$ ja $\mathbb{Z}[a_1] \cap A' = \{0\}$, nähdään, että $\mathbb{Z}[b_1] \cap B' = \{0\}$. Näin ollen summa $\mathbb{Z}[b_1] + B'$ on suora.

Ryhmä $A' = \mathrm{Span}(v_2, \ldots, v_n)$ on vapaa ja $(n-1)$-ulotteinen. Induktio-oletuksen nojalla sillä on kanta $(a_2, \ldots, a_n)$ siten, että $(b_2, \ldots, b_k) = (m_2 a_2, \ldots, m_k a_k)$ on sen aliryhmän B' kanta jollakin $k \leq n$ ja positiivisilla kokonaisluvuilla $m_2, \ldots, m_k$. Lisäksi viimeksi mainitut voidaan valita niin, että $m_2 \mid m_3 \mid \ldots \mid m_{k-1} \mid m_k$.

Todistus on valmis kunhan vielä näytetään, että $m_1 \mid m_2$. Olkoon $m_2 = qm_1 + r$ (jakoyhtälö), missä $q, r \in \mathbb{Z}$ ja $0 \leq r < m_1$. Tällöin

$$b_1 + b_2 = m_1 a_1 + m_2 a_2 = m_1(a_1 + qa_2) + ra_2 = m_1 a' + ra_2.$$

Tässä $a' = a_1 + qa_2$. Helposti nähdään, että $(a', a_2, \ldots, a_n)$ on ryhmän A kanta. Luvun $m = m_1$ valinnasta seuraa, että $r = 0$. Väite on todistettu. □

Struktuurilauseen 5.15 olemassoloväite on nyt suhteellisen helppo seuraus edellisestä tuloksesta.

Lemma 5.18. Lauseen 5.15 olemassaoloväite
Olkoon A äärellisviritteinen Abelin ryhmä. Tällöin on olemassa $n, k \in \mathbb{N}$, $m_1, \ldots, m_k \geq 1$, siten että $m_1 \mid m_2 \mid \ldots | m_{k-1} \mid m_k$ ja

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Todistus. Olkoon $(v_1, \ldots, v_n)$ jokin ryhmän A virittäjäjoukko, $A = \mathrm{Span}(v_1, \ldots, v_n)$. Proposition 2.57 yleistyksestä moduleille seuraa, että on olemassa tasan yksi $\mathbb{Z}$-lineaarinen (eli ryhmähomomorfismi) kuvaus $f\colon \mathbb{Z}^n \to A$, jolle pätee $f(e_i) = v_i$ jokaisella $i = 1, \ldots, n$. Tässä $(e_1, \ldots, e_n)$ on vapaan $\mathbb{Z}$-modulin $\mathbb{Z}^n$ standardikanta (määritellään samalla tavalla kuin vektoriavaruuksien teoriassa).

Konstuktion perusteella kuvaus f on surjektio, joten se määrittelee isomorfismin

$$(\mathbb{Z}^n)/\operatorname{Ker} f \cong A.$$

Koska $\mathbb{Z}^n$ on vapaa äärellisulotteinen ryhmä, edellisen proposition nojalla sillä on kanta $(a_1, \ldots, a_n)$, siten, että joillakin positiivisilla kokonaisluvuilla $m_1, \ldots, m_k$ jono $(m_1 a_1, m_2 a_2, \ldots, m_k a_k)$ on aliryhmän $B = \operatorname{Ker} f$ kanta. Lisäksi voidaan olettaa, että $m_i \mid m_{i+1}$, $i = 1, \ldots, k-1$. Helposti nähdään, että tällöin

$$\mathbb{Z}^n/B = (\oplus\mathbb{Z}[a_i])/(\oplus\mathbb{Z}[m_i a_i]) = \oplus(\mathbb{Z}[a_i]/\mathbb{Z}[m_i a_i]) \cong$$

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m-2} \oplus \ldots \oplus \mathbb{Z}_{m_k} \oplus \mathbb{Z}_{m_{k+1}} \oplus \ldots \oplus \mathbb{Z}_{m_n}.$$

Tässä $m_{k+1} = \ldots = m_n = 0$, joten vastaaville tekijäryhmille pätee $\mathbb{Z}_{m_i} = \mathbb{Z}$. Hajotelman (5.16) olemassaolo on näytetty.

□

Seuraavaksi pyritään osoittamaan hajotelman 5.16 yksikäsitteisyys.
Olkoon A mielivaltainen Abelin ryhmä. Määritellään

$$\operatorname{Tor} A = \{x \in A \mid \textit{ on olemassa } n \in \mathbb{N}, n > 0 \textit{ siten, että } nx = 0\}.$$

Helposti nähdään, että $\operatorname{Tor} A$ on tällöin ryhmän A aliryhmä. Tätä aliryhmä sanotaan ryhmän A *torsioaliryhmäksi*. Jokainen aliryhmän $\operatorname{Tor} A$ sanotaan ryhmän A *torsioalkioksi*.

Oletetaan, että äärellisviritteinen Abelin ryhmä A on esitetty suorana summana muodossa

$$A = \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Tällöin helposti nähdään, että

$$\operatorname{Tor} A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Tästä puolestaan seuraa, että $A/\operatorname{Tor}(A) \cong \mathbb{Z}^n$. Koska vapaan äärellisulotteisen Abelin ryhmän dimensio on yksikäsitteinen, tästä nähdään heti, että $n = \dim(A/\operatorname{Tor} A)$ on yksikäsitteisesti määrätty.

Koska

$$\operatorname{Tor} A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}$$

riippuu vain ryhmästä A, riittää näyttää, että *äärellisen* Abelin ryhmän esitys muodossa

$$\mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k},$$

missä $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$, on yksikäsitteinen.

Lemma 5.19. *Olkoot nja m positiivisia kokonaislukuja. Tällöin seuraavat ehdot ovat yhtäpitäviä.*
(1) Ryhmä $\mathbb{Z}_n \oplus \mathbb{Z}_m$ on syklinen.
(2) $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.
(3) Luvut n ja m ovat keskenään jaottomat.

Todistus. Harjoitustehtävä. □

Olkoon A äärellinen ryhmä, joka on esitetty suorana summana

$$A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Oletetaan lisäksi, että $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$. Kirjoitetaan suurin indeksi m_k muodossa

$$m_k = p_1^{l_{1,k}} p_2^{l_{2,k}} \ldots p_s^{l_{s,k}},$$

missä $p_1, \ldots, p_s$ ovat (eri) alkulukuja ja $l_{i,k} > 0$, $i = 1, \ldots, s$. Tämä on mahdollista, sillä jokainen luonnollinen luku voidaan tunnetusti kirjoittaa (yksikäsitteisellä tavalla) alkulukujen tulona.

Koska $m_i \mid m_{i+1}$, $i = 1, \ldots, k-1$, luvun m_i jokainen alkulukutekijä on myös luvun m_k alkulukutekijä. Tästä seuraa, että kaikilla $i = 1, \ldots, k$

$$m_i = p_1^{l_{1,i}} p_2^{l_{2,i}} \ldots p_s^{l_{s,i}},$$

missä $0 \leq l_{r,1} \leq l_{r,2} \leq \ldots \leq l_{r,k}$ jokaisella $r = 1, \ldots, s$.

Koska eri alkuluvut (ja yleisemmin niiden potenssit) ovat keskenään jaottomia, Lemman (5.19) nojalla jokainen suoran summan tekijä $\mathbb{Z}_{m_i}$ voidaan esittää muodossa

$$\mathbb{Z}_{m_i} = \oplus_r \mathbb{Z}_{p_j}^{l_{i,r}}, \tag{5.20}$$

missä oikealla puolella riittää ottaa suora summa niistä termeistä joille $l_{i,r} > 0$. Jos oletetaan, että näin on tehty, jokainen tässä suorassa summassa oikealla puolella esiintyvä syklinen ryhmä on epätriviaali.

Jokaisella $r = 1, \ldots, s$ olkoon

$$A_r = \{a \in A \mid p_r^k a = 0 \text{ jollakin } k \in \mathbb{N}, k > 0\}.$$

Toisin sanoen A_r koostuu alkioista, joiden kertaluku on alkuluvun p_r potenssi. Määritelmänsä mukaan joukko A_r riippuu vain ryhmästä A, ei hajotelmasta (5.16). Helposti nähdään, että A_r on aliryhmä. Ryhmänä se on esimerkki niin sanotusta äärellisestä *p_r-ryhmästä.*

Määritelmä 5.21. *Olkoon A Abelin ryhmä ja oletetaan, että $p \in \mathbb{N}$ on alkuluku. Ryhmää A sanotaan äärelliseksi p-ryhmäksi, jos jokaisen sen alkion kertaluku on luvun p jokin potenssi, toisin sanoen jos kaikilla $x \in A$ on olemassa $k \in \mathbb{N}$ siten, että $p^k x = 0$.*

Aliryhmän $\mathbb{Z}_{m_i}$ hajotelmasta (5.20) nähdään, että

$$A_r \cap \mathbb{Z}_{m_i} = \mathbb{Z}_{p_r}^{l_{i,r}}.$$

Nimittäin, unohdetaan turhat indeksit hetkeksi ja tarkastellaan äärellisen syklisen ryhmän $\mathbb{Z}_m$ esitystä muodossa

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_l^{k_l}},$$

missä $p_1, \ldots, p_l$ ovat alkulukuja. Tämän yhtälön oikealla puolella esiintyvät ryhmät ovat kaikki syklisiä p_i-ryhmiä. Lisäksi jokainen ryhmän $\mathbb{Z}_m$ alkio x voidaan esittää (yksikäsitteisellä tavalla) muodossa $x_1 + \ldots + x_l$, missä $x_i \in \mathbb{Z}_{p_i^{k_i}}$. Oletetaan, että lisäksi $x \in A_r$. Tällöin sopivalla $k \in \mathbb{N}$ pätee

$$0 = p_r^k x = p_r^k x_1 + \ldots + p_r^k x_l,$$

missä $p_r^k x_i \in \mathbb{Z}_{p_i^{k_i}}$ kaikilla $i = 1, \ldots, l$. Koska summa $\oplus \mathbb{Z}_{p_i^{k_i}}$ on suora, tästä seuraa, että $p_r k x_i = 0 \in \mathbb{Z}_{p_i^{k_i}}$. Olkoon $r \neq i$. Soveltamalla tähän Lemmaa5.13 saadaan, että alkion x_i kertaluku on luvun p_r potenssi. Toisaalta saman lemman mukaan luvun x_i kertaluvun täytyy olla luvun $p_i^{k_i}$ tekijä. Koska p_i ja p_r ovat eri alkulukuja, ne ovat keskenään jaotomia, joten kertaluvun täytyy olla yksi, jolloin $x_i = 0$. Näin ollen $x_i = 0$ kaikilla $i \neq r$. On näytetty, että

$$A_r \cap \mathbb{Z}_{m_i} \subset \mathbb{Z}_{p_r}^{k_r}.$$

Sisältyvyys toiseen suuntaan seuraa helposti aliryhmän A_r määritelmästä.

Näin ollen, kun palataan alkuperäisin merkintöihin, edellisen nojalla saadaan, että $A_r \cap \mathbb{Z}_{m_i} = \mathbb{Z}_{p_r}^{l_{i,r}}$ jokaisella r, i. Koska aliryhmien $\mathbb{Z}_{m_i}$ summa on suora, nähdään, että ryhmä A_r on suora summa p_r-ryhmistä $\mathbb{Z}_{p_r}^{l_{i,r}}$, missä i käy läpi kaikki sellaiset indeksit $1, \ldots, k$, joille pätee $l_{i,r} > 0$. Aliryhmät A_r riippuvat vain ryhmästä A, eivätkä hajotelmasta (5.16). Lisäksi indeksit m_i saadaan takaisin tuloina

$$m_i = p_1^{l_{1,i}} p_2^{l_{2,i}} \ldots p_s^{l_{s,i}},$$

$i = 1, \ldots, k$. Tässä ne termit, joilla vastaavalle potenssille pätee $l_{i,r} = 0$, ovat ykkösiä, joten ne eivät vaikuta tuloon arvoon. Jos pystytään vielä osoittamaan, että p_r-ryhmän A_r esitys syklisten p-ryhmien suorana summana

$$A_r = \oplus \mathbb{Z}_{p_r}^{l^{i,r}}$$

on yksikäsitteinen, tulee samalla todistettua myös sen, että kertoimet $m_1, \ldots, m_k$ ovat yksikäsitteisiä, jolloin Äärellisviritteisten Abelin Ryhmien Struktuurilauseen 5.15 todistus on valmis.

Lemma 5.22. *Oletetaan, että A_i ja B_j ovat äärellisiä epätriviaaleja syklisiä p-ryhmiä (missä p on alkuluku), $i = 1, \ldots, r$, $j = 1, \ldots, s$. Oletetaan, että*

$$A_1 \oplus A_2 \oplus \ldots \oplus A_r \cong B_1 \oplus B_2 \oplus \ldots \oplus B_s.$$

Tällöin $r = s$ ja järjestystä vailla $A_i \cong B_i$ kaikilla $i = 1, \ldots, r$.

Todistus. Esitetään kaikki lemman muotoilussa esiintyvät sykliset ryhmät muodossa $A_i = \mathbb{Z}_{p^{k_i}}, B_j = \mathbb{Z}_{p^{l_j}}$. Järjestämällä suoran summat jäsenet uudelleen tarvittaessa, voidaan olettaa, että

$$k_1 \geq k_2 \geq \ldots \geq k_{n-1} > k_n = k_{n+1} = \ldots = k_r = 1,$$

$$l_1 \geq l_2 \geq \ldots \geq l_{m-1} > l_m = l_{m+1} = \ldots = l_s = 1.$$

Samaistamalla isomorfiset ryhmät samoiksi ryhmiksi voidaan lisäksi olettaa, että

$$A_1 \oplus A_2 \oplus \ldots \oplus A_r = A = B_1 \oplus B_2 \oplus \ldots \oplus B_s. \tag{5.23}$$

Pitää osoittaa, että $r = s$ ja $k_i = l_i$ kaikilla $i = 1, \ldots, r$. Tehdään tämä induktiolla ryhmän A koon $|A|$ suhteen.

Jos $|A| = 1$, väite on triviaali. Siirytään induktio-askelleeseen. Tarkastellaan osajoukkoa $pA = \{pa \mid a \in A\} \subset A$. Helposti nähdään, että tämä on ryhmän A aliryhmä. Itse asiassa kuvaus $f\colon A \to A$, $f(a) = pa$, on ryhmähomorfismi (tarkista!), joten $pA = \operatorname{Im} f$, ja isomorfialauseen nojalla pätee $pA \cong A/\operatorname{Ker} f$. Lisäksi kaikilla $i = 1, \ldots, r$ pätee $f(A_i) = pA_i \subset A_i$ ja vastaavasti kaikilla $j = 1, \ldots, s$ pätee $f(B_j) = pB_j \subset B_j$. Tästä seuraa, että ryhmä pA on p-ryhmä, jolle pätee

$$pA_1 \oplus pA_2 \oplus \ldots \oplus pA_r = pA = pB_1 \oplus pB_2 \oplus \ldots \oplus pB_s. \tag{5.24}$$

Tarkastellaan erikseen miltä ryhmä pA näyttää syklisellä p-ryhmällä $A = \mathbb{Z}_{p^k}$ (jokainen A_i ja B_j on tätä muotoa). Kuvaus $f\colon A \to pA$ on surjektiivinen homomorfismi. Lasketaan mikä on sen ydin. A:n alkiot ovat muotoa $0, 1, \ldots, p, \ldots, p^{k-1}, \ldots, p^k - 1$, missä merkintöjen yksinkertaistamiseksi kokonaisluvun r luokkaa $\overline{r} \in \mathbb{Z}_n$ merkitään yksinkertaisesti r. Luokka r kuuluu ytimeen $\operatorname{Ker} f$ jos kokonaislukujen tasolla luku pr on jaollinen luvulla p^k. Tämä on mahdollista jos ja vain jos r on jaollinen luvulla p^{k-1}. Näin ollen $\operatorname{Ker} f$ on syklinen aliryhmä, jonka virittää luvun p^{k-1} luokka. Tarkastelemalla tämän alkion virittämän ryhmän alkiota, nähdään, että niitä on tasan p kappaletta, sillä ne ovat $0, p^{k-1}, 2p_{k-1}, \ldots, (p-1)p^{k-1}$ (seuraava potenssi $pp^{k-1} = p^k$ on jo nolla ryhmässä A). Erityisesti, koska isomorfialauseen nojalla pätee $pA \cong A/\operatorname{Ker} f$, saadaan näiden ryhmien koolle

$$|pA| = |A/\operatorname{Ker} f| = |A|/|\operatorname{Ker} f| = p^k/p = p^{k-1}.$$

Tämä on erikoistapaus äärellisten ryhmien teoriaan kuuluvasta Langrange'n Lauseesta, joka sanoo, että jos H on äärellisen ryhmän G aliryhmä, niin $|G/H| = |G|/|H|$. Soveltamalla saatua tulosta hajotelman (5.24) vasempaan puoleen, nähdään, että

$$p^{k_1-1}p^{k_2-1}\ldots p^{k_{n-1}-1} = |pA| < |A|.$$

Näin ollen pA on p-ryhmä, jonka koko on pienempi kuin ryhmän A koko, joten siihen voidaan soveltaa induktio-oletusta. Koska pätee

$$pA_1 \oplus pA_2 \oplus \ldots \oplus pA_{k_{n-1}} = pA = pB_1 \oplus pB_2 \oplus \ldots \oplus pB_{m-1}, \tag{5.25}$$

induktio-oletuksesta seuraa, että $n = m$ ja $k_i - 1 = l_i - 1$ kaikilla $i = 1, \ldots, k_{n-1}$. Tässä ryhmiä $pA_{k_n}, pA_{k_{n+1}}, \ldots$ ja niiden vastineita ryhmän B puoleella ei merkitä näkyviin, sillä ne ovat kaikki ovat triviaaleja, yhden alkion ryhmiä. Edellisestä seuraa, että $k_i = l_i$ kun $i < n$.

Toisaalta, koska $n = m$ ja $k_i = 1 = l_i$ kaikilla $i \geq n$, riittää vielä näyttää, että $r = s$. Mutta kaikkien aliryhmien A_i, B_j, $i, j \geq n$ koot ovat tasan p, joten, vertaamalla taas A:n erilaisten esitysten kokoja hajotelmassa (5.23) saadaan yhtälö

$$p^{k_1+\ldots+k_{n-1}}p^{r-n} = p^{k_1+\ldots+k_{n-1}}p^{s-n}.$$

Tästä seuraa, että $r = s$. Todistus on valmis. □

Äärellisviritteisten Abelin ryhmien struktuurilauseen 5.14 yksikäsitteisyys-väite (ja samalla koko lause) tuli nyt todistetuksi.

Jokaisen äärellisviritteiseen Abelin ryhmään A voidaan siis liittää jono $(n; m_1, \ldots, m_k)$ sen invariantteja, jotka määräytyvät esityksestä

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}$$

sekä ehdosta $1 < m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$. Lukua n sanotaan ryhmän A *asteeksi* (engl. rank). Aste voidaan ajatella dimension yleistyksenä. Jos ryhmä A on äärellinen, sen aste on nolla. Jos taas äärellisviritteinen Abelin ryhmä A on *torsiovapaa* eli sille pätee $\operatorname{Tor} A = \{0\}$, niin yllä välttämättä $k = 0$ ja $A \cong \mathbb{Z}_n$. Jokainen äärellisviritteinen torsiovapaa Abelin ryhmä on siis erityisesti vapaa.

Ei-äärellisviritteisille ryhmille tämä ei päde, esimerkiksi rationaalilukujen ryhmä $\mathbb{Q}$ on torsiovapaa, mutta se ei kuitenkaan ole vapaa.

Abelin ryhmän eksponentti.
Olkoon A äärellinen Abelin ryhmä. Tällöin jokaisen $a \in A$ kertaluku on varmasti äärellinen, joten on olemassa $n_a \in \mathbb{N}, n_a > 0$, jolle $n_a a = 0$. Luvulle

$$n = \prod_{a \in A} n_a$$

tällöin pätee $na = 0$ kaikilla $a \in A$. Pienintä luonnollista lukua, jolla on tämä ominaisuus sanotaan ryhmän A *eksponentiksi*. Eksponentti on siis pienin positiivinen kokonaisluku m jolle pätee $ma = 0$ kaikilla $a \in A$.
Eksponentin avulla voidaan karakterisoida syklisiä ryhmiä.

Lemma 5.26. *Olkoon A äärellinen Abelin ryhmä ja olkoon m sen eksponentti. Tällöin A on syklinen jos ja vain jos $m = |A|$. Muuten $m < |A|$.*

Todistus. Struktuurilauseen 5.14 nojalla on olemassa esitys muotoa $A \cong \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}$, missä
$1 < m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$. Koska tällainen esitys on lisäksi yksikäsitteinen, A on syklinen jos ja vain jos $k = 1$, mikä puolestaan toteutuu jos ja vain jos pätee yhtälö $m_k = |A| = m_1 \ldots m_k$. Toisaalta helposti nähdään, että $m_k a = 0$ kaikilla $a \in A$ ja $m_k - 1 \neq 0 \in \mathbb{Z}_{m_k} \subset A$, joten m_k on äärellisen ryhmän A eksponentti. Väite seuraa. □

Seuraus 5.27. *Olkoon K äärellinen kunta. Tällöin sen kääntyvien alkioiden multiplikaativinen ryhmä $K^* = K \setminus \{0\}$ on syklinen.*

Todistus. Olkoon m ryhmän $A = K^*$ eksponentti. Edellisen lemman nojalla riittää osoittaa, että $m = |A|$. Tehdään vasta-oletus - $m < |A|$. Esponentin määritelmän mukaan jokaisella $x \in A$ pätee $x^m = 1$. Tämä on m-asteinen polynomiyhtälö, jolla on $|A| > m$ ratkaisua kunnassa K. Tämä on kuitenkin mahdotonta Proposition 3.54 nojalla. □

Äärellisviritteiset modulit pääideaalirenkkaiden yli
Kuten tämän aliluvun alussa on mainittu, Lause 5.15 yleistyy luonnollisella tavalla äärellisviritteisiin R-moduleihin, kun kerroinrengas R on *pääideaalirengas*. Täsmällisemmin sanottuna seuraava tulos pätee.

Lause 5.28. *Olkoon R pääideaalirengas ja olkoon M äärellisviritteinen R-moduli. Tällöin on olemassa yksikäsitteinen $n \in \mathbb{N}$ ja yksikäsitteiset renkaan R aidot ideaalit $I_1, I_2, \ldots, I_n$ siten, että*

$$I_1 \subset I_2 \subset \ldots \subset I_n \text{ ja}$$
$$M \cong R/I_1 \oplus R/I_2 \ldots \oplus R/I_n.$$

Koska jokainen pääideaalirenkaan R ideaali I on yhden alkion virittämä, edellisen lauseen tulos voidaan kirjoittaa myös muodossa

$$M \cong R/(d_1) \oplus R/(d_2) \ldots \oplus R/(d_n),$$

missä $d_1, \ldots, d_n \in R$ ovat sellaisia, että $d_n \mid d_{n-1} \mid \ldots \mid d_2 \mid d_1$. Alkiot d_i eivät tällöin ole välttämättä yksikäsitteisiä, sillä eri alkiot saattavat virittää saman ideaalin. Lisäksi mikään niistä ei ole kääntyvä, sillä kääntyvä alkio virittää ideaalin $I = R$. Jos taas $d_i = 0$, niin vastaavalle suoran summan tekijälle pätee $R/(d_i) = R$. Näin ollen tulos voidaan kirjoittaa myös muodossa

$$M \cong R^m \oplus R/(d_j) \ldots \oplus R/(d_n),$$

missä $d_n \mid d_{n-1} \mid \ldots \mid d_2 \mid d_j$ ja $d_k \neq 0_R$ kaikilla $k = j, \ldots, n$. Tässä tulkinnassa Lauseen 5.28 väite on lähempänä Lauseen 5.15 muotoilua. Lause 5.15 on puolestaan Lauseen 5.28 erikoistapaus kun $R = \mathbb{Z}$.

Lauseen 5.28 todistus tapauksessa $R = K[\mathbf{X}]$, tai yleisemmin kun R on niin sanottu *Eukleideen rengas*, etenee samalla tavalla kuin yllä esitetty todistus tapauksessa $R = \mathbb{Z}$. Eukleideen rengas on rengas, jossa on voimassa "jakoyhtälön" kaltainen tulos. Esimerkiksi kun $R = K[\mathbf{X}]$ Lause 5.28 voidaan todistaa samalla tavalla kuin yllä esitetty Lause 5.15, kunhan korvataan todistuksessa kokonaislukujen jakoyhtälö polynomien jakoyhtälöllä ja kokonaisluvun itseisarvo polynomin asteella.

Esimerkki 5.29. *Olkoon V äärellisulotteinen K-vektoriavaruus ja olkoon $L\colon V \to V$ jokin sen operaattori. Tällöin avaruudessa V voidaan määritellä $K[\mathbf{X}]$-modulin struktuuri, jossa skalaarikertolasku on määritelty kaavalla*

$$\mathbf{pv} = p(L)(\mathbf{v}),\ \mathbf{p} \in K[\mathbf{X}], \mathbf{v} \in V$$

(kts. esim. 5.2, (9)).

Koska V on äärellisulotteinen K-vektoriavaruutena, on selvä, että se on myös äärellisviritteinen $K[\mathbf{X}]$-modulina. Koska renkaan $K[\mathbf{X}]$ jokainen ideaali on pääideaalimuotoa $(\mathbf{p})$, missä $\mathbf{p}$ on pääpolynomi, Lauseen 5.28 nojalla nähdään, että $K[\mathbf{X}]$-moduli V on isomorfinen tulomodulin

$$M = K[\mathbf{X}]/(\mathbf{p}_1) \oplus K[\mathbf{X}]/(\mathbf{p}_2) \oplus K[\mathbf{X}]/(\mathbf{p}_n)$$

kanssa. Olkoon $f\colon M \to V$ isomorfismi. Tällöin f kuvaa alimodulin $K[\mathbf{X}]/(\mathbf{p}_1)$ erääksi yhden alkion $\mathbf{v}_i \in V$ virittämäksi $K[\mathbf{X}]$-alimoduliksi V_i. Tällainen alimoduli on vektoriavaruuden V aliavaruus, joka on lisäksi invariantti operaattorin L suhteen. Analysoimalla tätä tulosta tarkemmin, nähdään, että V_i on tällöin itse asiassa niin sanottu syklinen aliavaruus*, eli sen virittää jono muotoa*

$$(\mathbf{v}_i, L(\mathbf{v}_i), L^2(\mathbf{v}_i), \ldots, L^{n_i-1}(\mathbf{v}_i)).$$

Lisäksi tässä $n_i = \deg \mathbf{p}_i$ *ja* $\mathbf{p}_i$ *paljastuu alkion* $\mathbf{v}_i$ *minimipolynomiksi* $\mathbf{m}_{\mathbf{v}_i,L}$ *operaattorin* L *suhteen.*

Näin ollen, kääntämällä Lauseen 5.28 tulos tässä tilanteessa takaisin vektoriavaruuden kielelle, nähdään, että V *voidaan esittää suorana summana syklisiä* L*-invariantteja aliavaruuksia*

$$V_i = \mathrm{Span}(\mathbf{v}_i, L(\mathbf{v}_i), L^2(\mathbf{v}_i), \ldots, L^{n_i-1}(\mathbf{v}_i)).$$

Tämä tulos (joka oli mainittu Luvussa 3 ilman todistusta Propositiossa 3.118) on yleistys Proposition 3.95 tuloksesta, jossa vastaava väite osoitettiin siinä erikoistapauksessa, kun operaattori L *on nilpotentti. Proposition 3.95 avulla puolestaan johdettiin Seuraus 3.108, joka kertoo milloin operaattori voidaan esittää Jordanin normaalissa muodossa. Lisäksi Propositiossa 3.110 osoitettiin, että operaattorin Jordanin normaali muoto on oleellisesti yksikäsitteinen. Tämäkin tulos olisi mahdollista johtaa nyt yksinkertaisemmin Lauseen 5.28 yksikäsitteisyys-väitteen seurauksena.*

Syklisessä kannassa $(L^{n_i-1}(\mathbf{v}_i), \ldots, L^2(\mathbf{v}_i), L(\mathbf{v}_i), \mathbf{v}_i)$ *operaattorin* $L|V_i$ *matriisi on muotoa*

$$\begin{bmatrix} -a_{n-1} & 1 & 0 & \ldots & 0 \\ -a_{n-2} & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \\ -a_1 & 0 & 0 & \ldots & 1 \\ -a_0 & 0 & 0 & \ldots & 0 \end{bmatrix}, \tag{5.30}$$

missä luvut a_i *ovat minimipolynomin* $\mathbf{p}_i = \mathbf{X}^n + a_{n-1}\mathbf{X}^{n-1} + \ldots + a_1\mathbf{X} + a_0$ *kertoimet. Edellisestä seuraa, että jokainen äärellisulotteisen* K*-vektoriavaruuden* V *operaattori* L *voidaan esittää jossakin kannassa lohkomatriisina, jossa jokainen lohko on muotoa 5.30.*

5.3. Zornin Lemman sovelluksia lineaarialgebrassa

Matemaattisissa todistuksissa ja konstruktioissa joudutaan usein tekemään ”samanaikaisia valintoja” tai ”täydentämään haluttuja ominaisuuksia omaava olio maksimaaliseksi”. Vaikka ensi näkemältä nämä näyttävät erilaisilta menetelmiltä, kyse on itse asiassa samasta periaatteesta.

”Epäkonstruktiivistisesta” valinnasta on kyse silloin, kun tiedätään, että tietynlainen olio on olemassa, vaikka siitä ei konstruoida eksplisiittistä esimerkkiä. Usein tällaista eksplisiittista konstruktiota ei edes pystytä tekemään, vaan on ainoastaan mahdollista osoittaa (esimerkiksi vasta-väitteen avulla), että olion on pakko olla olemassa. Jos lisäksi tällainen olio ei ole välttämättä yksikäsitteinen, se joudutaan ”valitsemaan” samankaltaisten otusten joukosta. Esimerkiksi tarkastelemalla joukkojen ”mahtavuuksia” on helppoa näyttää, että algebrallisten reaalilukujen joukko on numeroituva. Koska toisaalta tiedetään, että reaalilukuja on ylinumeroituva määrä, tästä voidaan päätellä suoraan, että transkendentteja (eli ei-algebrallisia) lukuja on pakko olla olemassa, vaikka ei osattaisikaan antaa yhtään konkreettista esimerkkejä tällaisesta luvusta. Teoreettisesta tarkastelusta voidaan siis jossakin huoletta sanoa ”olkoon x transkendentti reaaliluku” ja käyttää x:ää, vain sen perusteella, että tiedetään sellaisen olevan olemassa. Teknisellä tasolla tämä tarkoittaa sitä, että transkendenttien lukujen joukosta *poimitaan* eli *valitaan* yksi alkio. Tähän ei

tarvita mitään erikoisia joukko-opillisia työkaluja, riittää vaan tietää, että transkendenttien lukujen joukko on epätyhjä. Epätyhjästä joukosta voidaan aina poimia tarvittaessa yksi alkio kertomatta eksplisiittisesti sen enempää mikä tämä alkio on, koska tämä on käytännössä epätyhjän joukon määritelmä.

Epätyhjästä joukosta siis voidaan aina valita tarvittaessa yksi alkio. Teknisiä ongelmia, tai pikemminkin epätriviaalin joukko-opillisen työkalun tarve syntyy, kun alkioita pitää valita samanaikaisesti enemmän kuin yksi. Mitä jos tarvitaan kaksi (eri) transkendenttia alkiota? No, valitaan yksi ja sen jäkeen valitaan toinen. Kolme? Valitaan yksi, sitten toinen, sitten kolmas. Alkiot eivät loppu kesken, sillä transkendettien lukujen joukko on ääretön. Yleisesti *äärellisen monen alkion* valinta voidaan suorittaa induktiolla. Mutta entä jos tarvitaankin samanaikaisesti *äärettömän* monta alkiota? Tällöin, jos näitä alkioita ei pystytä konstruoimaan eksplisiittisesti, joutaan turvautumaan niin sanottuun *valinta-aksioomaan*.

Valinta-aksiooma sanoo seuraavan. Oletetaan, että $(A_i)_{i\in I}$ on (indeksoitu) kokoelma joukkoja, joista jokainen on epätyhjä, $A_i \neq \emptyset$ kaikilla $i \in I$. Tällöin jokaisella $i \in I$ voidaan valita jokin alkio $a_i \in A_i$. Täsmällisesti sanottuna on olemassa kokoelma $(a_i)_{i\in I}$, siten, että $a_i \in A_i$ kaikilla $i \in I$. Vaikka tämä tuntuu intuitiivisesti ehkä itsestään selvältä, osoittautuu, että valinta-aksiooman väitettä ei voida johtaa muista joukko-opin aksioomista, joten, jos sitä haluaa käyttää, se on hyväksyttävä aksioomana.

Valinta-aksiooma voidaan muotoilla myös käyttämällä mielivaltaisen karteesisen tulon käsitettä. Nimittäin kokoelma $(a_i)_{i\in I}$, jossa $a_i \in A_i$ kaikilla $i \in I$, on määritelmän mukaan sama asia kuin karteesisen tulon $\prod_{i\in I} A_i$ alkio. Näin ollen valinta-aksiooma väittää, että epätyhjien joukkojen mielivaltainen karteesinen tulo on epätyhjä.

Edellä tarkasteltiin "samanaikaista valintaa". Toinen todistuksissa usein esiintyvä välivaihe on erään olion laajentaminen "maksimaaliseksi". Esimerkiksi olkoon R epätriviaali vaihdannainen rengas ja olkoon $I \neq R$ sen aito ideaali. Tällöin voidaan todistaa, että tekijärengas R/I on *kunta* jos ja vain jos I on *maksimaalinen* aito ideaali (sisältyvyysrelaation suhteen). Täsmällisesti tämä tarkoittaa sitä, että ei ole olemassa ideaalia J jolle pätisi $I \subsetneq J \subsetneq R$. Koska kunnilla on hyviä ominaisuuksia, olisi hyödyllistä tietää, milloin tekijärengas R/I on kunta. Edellisen nojalla tämä tarkoittaa sitä, että on löydettävä renkaassa R maksimaalinen ideaali I.

Miten maksimaalisen ideaalin olemassaolo voidaan todistaa? Intuitiivisesti ajatellen sellainen ideaali voitaisiin yrittää löytää seuraavasti. Lähdetään liikkelle jostakin aidosta ideaalista $I \subset R$ (esimerkiksi triviaalista ideaalista $I = \{0\}$, joka on jokaisella renkaalla). Jos tämä ideaali ei ole maksimaalinen, (ehkä) voidaan konstruoida suurempi aito ideaali J_1, eli sellainen, jolle pätee $I \subsetneq J_1 \subsetneq R$. Jos ei tämäkään ideaali ole maksimaalinen, löydetään vielä isompi aito ideaali J_2, $J_1 \subsetneq J_2 \subsetneq R$. Näin voidaan jatkaa jotenkin "induktiivisesti". Ongelma on siinä, että ei ole mitään varmuutta siitä, että tämä prosessi loppuisi äärellisen monen askeleen jälkeen tai edes koskaan, vaikka meillä olisikin tapa jatkaa induktiota äärettömyyteen saakka ja sen ylikin.

Miten tämä liittyy valinta-aksioomaan? Asiaa voidaan ajatella seuraavasti. Kuvitellaan, että halutaan osoittaa valinta-aksiooma todeksi ainakin jossakin konkreettisessa tapauksessa. Tällöin siis perhe epätyhjiä joukkoja $(A_i)_{i\in I}$ on annettu ja on konstruoituva jokin perhe $(a_i)_{i\in I}$, missä $a_i \in A_i$ kaikilla $i \in I$. Tämä konstruktio voidaan ajatella

”prosessina”, jossa aloitetaan valitsemalla $a_{i_0} \in I_{i_0}$ jollakin indeksillä $i_0 \in I$, ja sitten lisäämällä siihen $a_{i_1} \in I_{i_1}$ jollakin toisella indeksillä $i_1 \in I$. Yleisesti oletetaan, että on löydetty ”osittainen ratkaisu ” $(a_i)_{i \in J}$, missä $J \subset I$, ja siihen halutaan lisätä yksi alkio kerrallaan, eli *laajentaa* tämä osittainen ratkaisu isomaksi, kunnes koko indeksijoukko I ”tyhjentyy”. Jos I on äärellinen, tämä voidaan tehdä helpolla induktiolla. Mutta jos I on ääretön, ei ole ollenkaan selvää, miten tämä saadaan aikaan. Tarvitaan siis jonkinlainen yleinen ”konstruktion loppuun viemisen periaate”, joka antaisi aina tarvittaessa *maksimaalisen* ratkaisun annettuun ongelmaan. Kuuluisa **Zornin lemma** antaa juuri tällaisen periaateen.

Zornin Lemman muotoilua varten tarvitaan järjestysrelaation käsitettä. Joukon X relaatiota $\leq$ sanotaan *(osittaiseksi) järjestykseksi* jos se on transitiivinen ja refleksiivinen eli jos kaikilla $x, y, z \in X$ pätevät seuraavat ominaisuudet:

- $x \leq x$.
- Jos $x \leq y, y \leq z$ niin myös $x \leq z$.

Järjestysrelaatiolla varustettua joukkoa X (tarkemmin paria $(X, \leq)$) sanotaan (osittain) järjetetyksi joukoksi. Tyypillinen esimerkki osittain järjestetystä joukosta on joukon X osajoukkojen joukko $\mathcal{P}(X)$, joka varustetaan osajoukkojen sisältyvyysrelaatiolla $\subset$. Juuri tähän järjestettyyn joukkoon Zornin Lemmaa hyvin usein käytännössä sovelletaankin.

Järjestetyn joukon X osajoukkoa A sanotaan *ketjuksi* jos sen alkiot ovat *verrattavissa toisiinsa* eli jos kaikilla $x, y \in A$ aina joko $x \leq y$ tai $y \leq x$. Induktiolla nähdään, että jokainen ketjun äärellinen osajoukko $\{x_1, \ldots, x_n\}$ sisältää *suurimman alkion* eli sellaisen x_j jolle $x_i \leq x_j$ pätee kaikilla $i = 1, \ldots, n$.

Alkiota $z \in X$ kutsutaan järjestetyn joukon X osajoukon A *ylärajaksi* jos kaikilla $a \in A$ pätee $a \leq z$. Alkio $z \in X$ on *maksimaalinen* jos jokaisella $x \in X$ ehto $z \leq x$ implikoi, että myös $x \leq z$. Huomaa, että tämä ei välttämättä yleisesti tarkoitta sitä, että $x = z$, sillä oletuksemme mukaan osittaisen järjestyksen ei tarvitse olla *anti-symmetrinen.*

Lemma 5.31. Zornin Lemma.
Olkoon X epätyhjä osittain järjestetty joukko. Oletetaan, että jokaisella X:n ketjulla A on yläraja. Tällöin X sisältää maksimaalisen alkion.

Tässä materiaalissa ei anneta todistusta Zornin Lemmalle. Tietyssä mielessä sitä ”ei edes voi” todistaa. Nimittäin osoittautuu, että Zornin Lemma on täysin ekvivalentti valinta-aksiooman kanssa, toisin sanoen valinta-aksiooman avulla voidaan todistaa Zornin Lemma, mutta yhtä hyvin voidaan hyväksyä Zornin Lemman väite todeksi aksioomana, jolloin valinta-aksioma voidaan osoittaa sen avulla. Zornin Lemman todistus valinta-aksioomasta löytyy helposti matemaattisesta kirjallisuudesta, esimerkiksi J. Väisälän kirjasta ”Topologia II”.

Zornin Lemman sovelluksia lineaarialgebrassa
Propositiossa 2.41 ollaan osoitettu, että jokaisella äärellisviritteisellä vektoriavaruudella on kanta. Zornin Lemman avulla on mahdollista osoittaa, että jokaisella vektoriavaruudella on kanta.

Propositio 5.32. *Olkoon V vektoriavaruus kunnan K yli. Olkoon C jokin avaruuden V virittäjäjoukko ja olkoon A jokin avaruuden V vapaa osajoukko. Oletetaan, että $A \subset C$. Tällöin avaruudella V on olemassa kanta B siten, että $A \subset B \subset C$.*

Erityisesti jokaisella vektoriavaruudella V on kanta.

Todistus. Proposition jälkimmäinen väite seuraa edellisestä, kun valitaan siinä $A = \emptyset$ ja $B = V$. Riittää siis todistaa ensimmäinen väite.

Olkoon X joukko, jonka alkiot ovat kaikki avaruuden V vapaat osajoukot B', joille pätee $A \subset B' \subset C$. Kun tämä joukko varustetaan tavallisella osajoukkojen sisältyvyysrelaatiolla $\subset$, siitä tulee järjestetty joukko. Osoitetaan, että tämä joukko toteuttaa Zornin Lemman 5.3 oletukset.

Joukko X on epätyhjä, sillä ainakin $A \in X$. Olkoon $Y \subset X$ *ketju*. Jokainen osajoukon Y alkio on joukon X alkio, eli joukon Y eräs osajoukko. Osoitetaan, että joukon Y alkioiden *yhdiste*

$$D = \bigcup_{B' \in Y} B'$$

on ketjun Y yläraja. Selvästi $B' \subset D$ kaikilla $B' \in Y$. Tästä ei kuitenkaan voi heti päätellä, että D olisi ketjun Y yläraja joukossa X, sillä ei ole itsestään selvää, että D on joukon X alkio. Osoitetaan, että $D \in X$, toisin sanoen osoitetaan, että D on vapaa. On selvä, että yleensä vapaiden osajoukkojen yhdisteen ei tarvitse olla vapaa, joten tässä on todellakin käytettävää hyväksi sitä lisäoletusta, että Y on ketju.

Olkoon

$$k_1\mathbf{a}_1 + k_2\mathbf{a}_2 + \ldots + k_n\mathbf{a}_n = 0,$$

missä $k_1, \ldots, k_n \in K$ ja $\mathbf{a}_i \in D$ ovat eri alkioita. Tällöin jokaisella $i = 1, \ldots, n$ on olemassa $B'_i \in Y$ siten, että $\mathbf{a}_i \in B'_i$. Koska Y on ketju ja $\{B'_1, \ldots, B'_n\}$ on sen *äärellinen* osajoukko, tässä osajoukko on olemassa *suurin alkio*. Toisin sanoen on olemassa $j \in \{1, \ldots, n\}$ siten, että $B'_i \subset B_j$ kaikilla $i = 1, \ldots, n$. Tästä seuraa, että

$$r_1\mathbf{a}_1 + r_2\mathbf{a}_2 + \ldots + r_n\mathbf{a}_n = 0$$

on lineaarinen kombinaatio, jossa esiintyvät alkiot $\mathbf{a}_1, \ldots, \mathbf{a}_n$ kuuluvat erääseen vapaan osajoukoon B_j. Vapauden nojalla tämä kombinaatio on triviaali, $r_1 = \ldots = r_n = 0$. On osoitettu, että D on vapaa eli $D \in X$. Lisäksi se on ketjun Y yläraja joukossa X.

Järjestetty joukko X siis toteuttaa Zornin Lemman 5.3 oletukset, joten se sisältää maksimaalisen alkion B. Osoitetaan, että B on avaruuden V kanta. B on vapaa, sillä se on joukon X alkio, joten riittää osoittaa, että B virittää avaruuden V. Olkoon $\mathbf{v} \in C$. Osoitetaan että $\mathbf{v} \in \mathrm{Span}(B)$. Jos $v \in B$ asia on selvä. Muuten osajoukko $B' = B \cup \{\mathbf{v}\}$ sisältyy joukkoon C ja B on sen aito osajoukko. Koska B on maksimaalinen C:n vapaa osajoukko, joukko B' ei voi olla vapaa. Näin ollen on olemassa epätriviaali lineaarinen kombinaatio muotoa

$$r_1\mathbf{a}_1 + r_2\mathbf{a}_2 + \ldots + r_n\mathbf{a}_n + r_{n+1}\mathbf{v} = 0, \tag{5.33}$$

missä $\mathbf{a}_1, \ldots, \mathbf{a}_n \in B$. Jos tässä pätee $r_{n+1} = 0$, saadaan epätriviaali nollavektorin esitys vapaan joukon B alkioilla, mikä on mahdotonta. Näin ollen $r_{n+1} \neq 0$, joten r_{n+1}^{-1} on olemassa (tämä on todistuksen ainoa välivaihe, jossa tarvitaan kunnan K ominaisuuksia

ja joka ei menisi läpi yleisen renkaan tapauksessa). Tämän nojalla saadaan yhtälöstä 5.33 yhtälö

$$\mathbf{v} = r_1'\mathbf{a}_1 + r_2'\mathbf{a}_2 + \ldots + r_n'\mathbf{a}_n,$$

missä $r_i' = -r_i/r_{n+1}$. Näin ollen $\mathbf{v} \in \mathrm{Span}(B)$.

On osoitettu, että $C \subset \mathrm{Span}(B)$. Koska joukko C virittää avaruuden V, tästä helposti nähdään, että itse asiassa $V = \mathrm{Span}(B)$. Näin ollen B virittää avaruuden V. □

Seuraavaksi Zornin Lemman avulla todistetaan, että äärellisulotteisen R-modulin dimensio on hyvin määritelty kun $R \neq 0$ on *vaihdannainen* rengas.

Propositio 5.34. *Olkoon R vaihdannainen epätriviaali rengas ja olkoot $n, m \in \mathbb{N}$. Oletetaan, että $R^n \cong R^m$. Tällöin $n = m$. Erityisesti äärellisulotteisen R-modulin dimensio on hyvin määritelty*

Todistus. Proposition 5.10 nojalla riittää osoittaa, että epätriviaalilla vaihdannaisella renkaalla on olemassa ideaali J siten, että tekijärengas R/J on *kunta*.

Osoitetaan, että jokaisella epätriviaalilla vaihdannaisella renkaalla R on olemassa *maksimaalinen* aito ideaali I. Tämä riittää, sillä voidaan osoittaa, että tällöin tekijärengas R/I on kunta (harjoitustehtävä, huom., tämä tulos pätee vain vaihdannaiselle renkaalle).

Osoitetaan siis, että renkaalla R on niin sanottu *maksimaalinen* ideaali $I \subsetneq R$. Maksimaalisuus tarkoittaa sitä, että $I \neq R$ eikä ole olemassa sellaista ideaalia J, joille pätisi $I \subsetneq J \subsetneq R$. Olkoon X kaikkien renkaan R *aitojen* ideaalien $J \neq R$ muodostama joukko. Tämä joukko on (osittain) järjestetty joukkojen sisältyvyysrelaatiolla. Olkoon $Y \subset X$ ketju. Tällöin voidaan osoittaa (yksityiskohdat harjoitustehtävänä), että

$$J' = \bigcup_{J \in Y} I$$

on ketjun Y yläraja joukossa X. Järjestetty joukko X siis toteuttaa Zornin Lemman oletuksia, joten se sisältää maksimaalisen alkion. Edellisen nojalla tämä riittää. □

Voidaan osoittaa, että vastaava tulos pätee myös ääretönulotteisille R-moduleille (vaihdannaisen renkaan R yli). Toisin sanoen, jos R on vaihdannainen rengas ja A, B ovat kumpikin vapaan R-modulin M kannat, niin A ja B ovat aina "samankokoisia". Äärettömien joukkojen kohdalla samankokoisuus tarkoittaa sitä, että joukkojen A ja B välillä on olemassa bijektio. Tällöin myös sanotaan, että joukoilla A ja B on "sama mahtavuus" tai että ne ovat "yhtä mahtavia".