Pääideaalialueen moduulien päälause

Vilppu Lehtikangas

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2021

Tiivistelmä: Vilppu Lehtikangas, *Pääideaalialueiden moduulien päälause* (engl. *The Fundamental Theorem of Modules Over Principal Ideal Domains*), Matematiikan Pro Gradu -tutkielma, 69s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, Kevät 2021.

Tämän tutkielman tarkoituksena on rakentaa moduulien teoria ryhmä- ja rengasteorian alkeista lähtien, sekä osoittaa pääideaalialueiden moduulien päälause.

Moduuli on joukko G varustettuna yhteenlaskutoimituksella, joka tekee siitä abelin ryhmän, sekä toiminnaksi kutsutulla kuvauksella joka liittää jokaiseen G:n kertoimien renkaan alkioon ja G:n alkioon jonkin G:n alkion. Toiminnan määritellään myös toteuttavan vektoriavaruuksien tunnetut distributiivisuusominaisuudet, jolloin se yleistää vektoriavaruuden skalaaritulon käsitteen yleiselle renkaalle. Näin ollen vektoriavaruuden yleisen määritelmän nojalla vektoriavaruudet ovat täsmälleen kuntakertoimisia moduuleja. Osoittautuu, että myös abelin ryhmät ja renkaat ovat moduuleja, joiden kerroinrenkaina ovat vastaavasti kokonaislukujen rengas $\mathbb{Z}$, sekä rengas itse. Tulemme huomaamaan, että monet ryhmä- ja rengasteorian tuloksista yleistyvät myös moduuleille.

Tutkimme, kuinka moduulin kerroinrenkaan rakenne vaikuttaa itse moduulin ominaisuuksiin. Tulemme osoittamaan, että pääideaalialueitten tapauksessa jokainen pääideaalialueen moduuli voidaan esittää yksikäsitteisesti suorana summana vapaasta moduulista, eli moduulista jolla on vektoriavaruuden tavoin kanta, sekä äärellisen monesta syklisestä tekijämoduulista. Tarkastelemme lopuksi lyhyesti joitain tämän pääideaalimoduulien päälauseeksi kutsutun tuloksen sovelluksia, kuten äärellisesti viritettyjen abelin ryhmien päälausetta, sekä neliömatriisin Jordanin kanonista muotoa.

Sisällys

LUKU 1

Johdanto

Tämän tutkielman tarkoituksena on rakentaa moduulit ryhmä- ja rengasteorian alkeista lähtien ja osoittaa pääideaalialueen moduulien päälause käyttäen läpikäytyä teoriaa.

Ryhmät ovat eräs abstraktin algebran perusrakenteista, joiden voidaan ajatella yleistävän kokonaislukujen yhteenlaskun mielivaltaiselle joukolle ja laskutoimitukselle, joka muistuttaa yhteenlaskua. Täten kokonaislukuja mukaillen määritellään, että ryhmä on joukko varustettuna kuvauksella, joka kuvaa jokaiset kaksi sen alkiota joksikin kyseisen joukon alkioksi siten, että tämä kuvaus muistuttaa vahvasti kokonaislukujen yhteenlaskua. Vastaavasti määritellään, että *rengas* on ryhmä, joka on varustettu myös toisella kokonaislukujen kertolaskua muistuttavalla laskutoimituksella.

Vektoriavaruudet ovat taas tunnetusti reaalilukujen n-uloitteista avaruutta $\mathbb{R}^n$ muistuttavia joukkoja varustettuna vektoreiden yhteenlaskutoimituksella, sekä skalaaritulolla, jossa vektoreita kerrotaan jollain kerroinkunnan alkiolla. Osoittautuu, että vektoriavaruuksien rakenne voidaan itse asiassa yleistää tietyille ryhmille siten, että kyseisen ryhmän kerrointen joukkona on jokin rengas, kunhan kerroinrenkaan ja ryhmän alkioiden skalaarituloa vastaava kuvaus yhdessä ryhmän yhteenlaskutoimituksen kanssa muistuttaa riittävästi vektoreiden yhteenlaskua ja skalaarituloa. Tällaista konstruktiota kutsutaan *moduuliksi*. Osoittautuu, että vektoriavaruuksien lisäksi, myös renkaat ja ryhmät ovat itse moduuleja. Tulemme myös osoittamaan, että jos rajoittaudumme tarkastelemaan tarpeeksi hyvin käyttäytyvien renkaiden moduuleja – nimittäin *pääideaalialueiden* moduuleja, niin kyseisen pääideaalialueen rakenne antaa meille tietoa sen moduulien rakenteesta.

Renkaan *alirengas* on sen osajoukko, joka on itsessään rengas määriteltynä alkuperäisen renkaan laskutoimituksien rajoittumalla kyseiseen osajoukkoon. Samoin renkaan *ideaali* on alirengas, joka on erittäin vakaa renkaan kertolaskun suhteen, siten että tulo jokaisen ideaalin alkion ja minkä vain renkaan alkion kanssa kuuluun aina kyseiseen ideaaliin. Näin ollen määrittelemme, että renkaan *pääideaali* on sen ideaali, joka on yhden alkion virittämä, eli jossa jokainen pääideaalin alkio voidaan esittää sen virittävän alkion ja jonkin renkaan alkion tulona. Täten sanotaan, että *pääideaalialue* on kertolaskun suhteen tietyssä mielessä hyvin käyttäytyvä rengas, jonka jokainen ideaali on pääideaali.

Näin ollen sanotaan, että moduuli, jonka kerroinjoukko on pääideaali on *pääideaalialueen moduuli*. *Vapaa moduuli* on moduuli jolla on vektoriavaruuden tavoin *kanta*, eli lineaarisesti riippumaton osajoukko, joka virittää kyseisen moduulin. *Torsiomoduulit* ovat taas moduuleita, joilla ei ole tällaistä kantaa ja jotka ovat pääideaalialueiden tapauksessa yhden alkion virittämiä, eli *syklisiä*

moduuleja. *Pääideaalialueen moduulien päälause* kertoo, että jokainen pääideaalialueen äärellisesti viritetty moduuli voidaan esittää vapaan moduulin, sekä äärellisen monen torsiomoduulin avulla.

Pääideaalialueiden päälauseella on myös mielenkiintoisia sovelluksia. Voidaan osoittaa, että *abelin ryhmät*, eli ryhmät joiden alkioiden yhteenlaskutoimituksen järjestyksellä ei ole väliä, ovat itsessään pääideaalialueen moduuleja, jolloin päälause antaa niille vastaavan esityksen. Tätä tulosta kutsutaan *äärellisesti viritettyjen abelin ryhmien päälauseeksi*, jonka avulla voidaan esimerkiksi määrittää jokainen tietyn kokoinen äärellinen abelin ryhmä. Soveltamalla pääideaalialueiden moduulien päälausetta polynomikertoimiseen vektoriavaruuteen voidaan osoittaa, että jokaista neliömatriisia vastaa niin sanotussa *Jordanin kanonisessa muodossa* oleva samankokoinen diagonaali lohkomatriisi, jonka lohkot ovat diagonaalimatriiseja muistuttavia Jordanin lohkoja. Osoittautuu myös, että tällainen *Jordan-matriisi* saadaan alkuperäisestä matriisista vaihtamalla siihen liittyvän vektoriavaruuden kantaa.

LUKU 2

Ryhmät

Tässä luvussa käsittelemme ryhmäteorian perusteita. Tunnetusti kokonaislukujen välille voidaan määritellä yhteenlaskuksi kutsuttu kuvaus, joka liittää jokaiseen kahteen kokonaislukuun jonkin kokonaisluvun. Kokonaislukujen yhteenlasku on siis esimerkki joukon sisäisestä laskutoimituksesta. On luontevaa tarkastella, millaisia rakenteita saadaan aikaiseksi korvaamalla joko kokonaislukujen joukko jollain muulla joukolla tai kyseinen laskutoimitus jollain sitä muistuttavalla kuvauksella. Ryhmien voidaan näin ollen ajatella yleistävän kokonaislukujen yhteenlaskun mielivaltaiselle joukolle, sekä laskutoimitukselle, jolla on monet kokonaislukujen yhteenlaskun perusominaisuuksista. Luku perustuu lähteisiin [**1**], [**2**], [**3**], [**4**] ja [**5**].

2.1. Ryhmät ja aliryhmät

Määritellään ensiksi joitain ryhmäteoriassa tarvittavia peruskäsitteitä.

MÄÄRITELMÄ 2.1. Joukon A *laskutoimitus* on kuvaus $\star : A \times A \to A$, jolle käytetään merkitää $\star(a, b) = a \star b$. Laskutoimitus $\star$ on *liitännäinen* jos

$$a \star (b \star c) = (a \star b) \star c$$

kaikilla $a, b, c \in A$. Jos $a \star b = b \star a$ kaikilla $a, b \in A$, niin sanotaan, että laskutoimitus $\star$ on *kommutatiivinen* tai *vaihdannainen*.

MÄÄRITELMÄ 2.2. Laskutoimituksen $\star$ *neutraalialkio* on alkio $e \in A$, jolle pätee $a \star e = e \star a = a$ kaikilla $a \in A$. Jos laskutoimituksella $\star$ on neutraalialkio, niin alkion $a \in A$ käänteisalkio laskutoimituksen $\star$ suhteen on alkio $a^{-1} \in A$, jolle pätee $a \star a^{-1} = a^{-1} \star a = e$.

MÄÄRITELMÄ 2.3. Olkoon $\star$ joukon A laskutoimitus ja $B \subset A$. Jos $b \star b' \in B$ kaikilla $b, b' \in B$ niin joukko B on *vakaa* laskutoimituksen $\star$ suhteen. Tällöin sanotaan, että laskutoimituksen $\star$ rajoittuma osajoukkoon $B \times B$ on laskutoimituksen $\star$ *indusoima* laskutoimitus. Indusoidulle laskutoimitukselle käytetään myös merkintää $\star_{|B \times B} = \star$, jos tämä ei aiheuta sekaannusta.

MÄÄRITELMÄ 2.4. *Ryhmä* on järjestetty pari $(G, \star)$ jossa G on joukko ja $\star$ on joukon G laskutoimitus siten, että

(1) $\star$ on liitännäinen,
(2) laskutoimituksella $\star$ on neutraalialkio $e \in G$ ja
(3) jokaisella $a \in G$ on käänteisalkio $a^{-1} \in G$.

Jos ryhmän $(G, \star)$ laskutoimitus $\star$ on kontekstista selvä niin yleensä sanotaan vain, että G on ryhmä ja tällöin merkitään $a \star b = ab$, sekä $e = 1$. Jos $ab = ba$ kaikilla $a, b \in G$ niin sanotaan, että ryhmä G kommutoi, tai että G on abelin ryhmä. Abelin ryhmän G laskutoimitukselle $\star$, neutraalialkiolle e, sekä alkion $a \in G$ käänteisalkiolle a^{-1} käytetään usein vastaavasti merkintöjä

$+$, 0, sekä $-a$. Tällöin merkitään myös $x + (-y) = x - y$, kaikilla $x, y \in G$. Näin merkittyä ryhmää kutsutaan monesti *additiiviseksi* ryhmäksi. Additiivisen ryhmän alkioiden $a_1, a_2 \dots, a_n$ väliselle laskutoimitukselle käytetään myös usein merkintää

$$((\dots(a_1 + a_2) + a_3)\dots) + a_n = a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_n,$$

jossa yhden alkion summaa merkitään usein $\sum_{i=1}^{n} g = ng$, missä $n \in \mathbb{Z}^+$, $g \in G$.

Esimerkki 2.5. Kokonaislukujen joukko $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2 \dots\}$ varustettuna kokonaislukujen tunnetulla yhteenlaskulla $+$, eli pari $(\mathbb{Z}, +)$, on abelin ryhmä. Emme paneudu niin kokonaislukujen joukon, kuin niiden yhteenlaskun täsmälliseen konstruktioon, mutta aiheesta löytyy lisätietoa esimerkiksi teoksesta [**1**, s. 348]. Yhteenlasku on määritelmän mukaisesti liitännäinen ja kommutatiivinen joukon $\mathbb{Z}$ laskutoimitus. Yhteenlaskun neutraalialkio on luku 0 ja jokaisen luvun $x \in \mathbb{Z}$ käänteisalkio, jota joskus kutsutaan *vastaluvuksi* on luku $-x$. Näin ollen additiiviset ryhmät muistuttavat niin rakenteeltaan, kuin merkinnöiltään kokonaislukujen ryhmää $(\mathbb{Z}, +)$. Tulemme jatkossa merkitsemään niin sanottujen *luonnollisien lukujen* joukkoa $\mathbb{N} = \{0, 1, 2, \dots\}$, sekä *positiivisien kokonaislukujen* joukkoa $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$

Esimerkki 2.6. Ryhmien $(G_1, \star_1), (G_2, \star_2), \dots, (G_n, \star_n)$, $n \in \mathbb{Z}^+$ *suora tulo*, eli tulojoukko $G_1 \times G_2 \times \cdots \times G_n$ varustettuna komponenteittain määritellyllä tulojoukon laskutoimituksella $\star$, jolle pätee

$$(g_1, g_2, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots, g_n \star_n h_n)$$

on ryhmä. Suoran tulon neutraalialkio on alkio $(1_{G_1}, 1_{G_2}, \dots, 1_{G_n})$, jossa 1_{G_i} on ryhmän G_i neutraalialkio ja tuloryhmän alkion $(g_1, g_2, \dots, g_n)$ käänteisalkio on $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$, jossa $g_i \in G_i$ kaikilla $i \in \{1, \dots, n\}$.

Määritelmä 2.7. *Kunta* on kolmikko $(K, +, \cdot)$, jossa $+$ ja $\cdot$ ovat joukon K laskutoimituksia siten, että parit $(K, +)$ sekä $(K - \{0\}, \cdot)$ ovat abelin ryhmiä ja että laskutoimitus $\cdot$ on *distributiivinen* laskutoimituksen $+$ suhteen, eli

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{ja} \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c),$$

kaikilla $a, b, c \in K$.

Esimerkki 2.8. Olkoon K kunta ja $GL_n(V)$ kunnan K alkioista koostuvien kääntyvien $n \times n$ matriisien joukko, eli

$$GL_n(V) = \{M \mid M \text{ on kääntyvä } n \times n \text{ matriisi ja } M_{ij} \in K \text{ kaikilla } 1 \leqslant i, j \leqslant n\}.$$

Olkoon myös $\times$ joukon $GL_n(V)$ laskutoimitus siten, että $\times$ on kokoa $n \times n$ olevien matriisien kertolasku jossa kahden matriisin tulon [**1**, s. 3] $A \times B = AB$ komponentit $(AB)_{ij}$, saadaan yhtälöstä

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

kaikilla $A, B \in GL_n(V)$, $1 \leqslant i, j \leqslant n$. Tällöin *yleinen lineaarinen ryhmä* $GL_n(V) = (GL_n(V), \times)$ on ryhmä, jonka neutraalialkio on identiteettimatriisi I ja jossa jokaisen matriisin $A \in GL_n(V)$ käänteisalkio on sen käänteismatriisi A^{-1}.

ESIMERKKI 2.9. Olkoon $A \neq \varnothing$ joukko. Tällöin joukon A *symmetriaryhmä* $S_A = \{\sigma : A \to A \mid \sigma \text{ on bijektio}\}$ on ryhmä varustettuna kuvausten $\sigma_i \in S_A$ yhdistämisellä $\circ : S_A \to S_A$, $\circ(\sigma_1, \sigma_2) = \sigma_1 \circ \sigma_2$. Koska kahden bijektion $A \to A$ yhdiste on bijektio $A \to A$, niin $\circ$ on joukon S_A laskutoimitus. Kuvausten yhdistäminen on myös tunnetusti liitännäinen operaatio. Ryhmän $(S_A, \circ)$ neutraalialkio on identtinen kuvaus Id ja jokaisen $\sigma \in S_A$ käänteisalkio on bijektion σ käänteiskuvaus σ^{-1}. Symmetriaryhmän S_A alkioita kutsutaan usein joukon A *permutaatioiksi*.

Tarkastellaan seuraavaksi ryhmien perusominaisuuksia.

LAUSE 2.10. *Olkoon $(G, \star)$ ryhmä. Tällöin*

(1) sen neutraalialkio e on yksikäsitteinen,
(2) jokaisen $a \in G$ käänteisalkio a^{-1} on yksikäsitteinen,
(3) $(a^{-1})^{-1} = a$, sekä
(4) $(ab)^{-1} = b^{-1}a^{-1}$ kaikilla $a, b \in G$.

TODISTUS. Olkoon $a, b \in G$. (1) Jos $e, e' \in G$ ovat ryhmän G neutraalialkioita, niin määritelmän mukaan $e = ee' = e'$.

(2) Olkoon $a \in G$. Tällöin jos $a^{-1}, b \in G$ ovat alkion a käänteisalkioita, niin määritelmän mukaan $ab = e = a^{-1}a$, jolloin $b = eb = a^{-1}ab = a^{-1}e = a^{-1}$.

(3)Koska määritelmän mukaan $(a^{-1})^{-1}$ on alkion $a \in G$ käänteisalkion a^{-1} käänteisalkio, niin $a^{-1}(a^{-1})^{-1} = e$. Tällöin

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$

(4) Koska $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, niin $b^{-1}a^{-1}$ on alkion ab vasen käänteisalkio. Vastaavalla päättelyllä saadaan, että $b^{-1}a^{-1}$ on myös alkion ab oikea käänteisalkio, joten $(ab^{-1}) = b^{-1}a^{-1}$. □

MÄÄRITELMÄ 2.11. Olkoon $(G, \star)$ ryhmä ja $H \subset G$. Tällöin $(H, \star)$ on ryhmän G *aliryhmä* indusoidulla laskutoimituksella $\star$ ja merkitään $H \leqslant G$, jos

(1) $H \neq \varnothing$ ja
(2) $x^{-1} \in H$ ja $x \star y \in H$ kaikilla $x, y \in H$.

Koska ryhmän G määritelmän 2.4 ominaisuudet pätevät jokaiselle joukon G alkiolle, niin ne pätevät myös jokaiselle osajoukon $H \subset G$ alkiolle. Koska $H \neq \varnothing$, niin on olemassa jokin $x \in H$, jolloin kohdan (2) mukaan myös $x^{-1} \in H$ ja täten $1 = xx^{-1} \in H$. Näin ollen voitaisiin yhtäpitävästi määritellä, että ryhmän aliryhmä on sen epätyhjä laskutoimituksen suhteen vakaa osajoukko, joka on itsessään ryhmä varustettuna indusoidulla laskutoimituksella.

LAUSE 2.12. *Jos $(G, \star)$ on abelin ryhmä ja $H \leqslant G$, niin $(H, \star)$ on abelin ryhmä.*

TODISTUS. Koska $H \leqslant G$, niin erityisesti $H \subset G$. Nyt, koska $\star_{|H \times H} = \star$ joukossa $H \times H$, niin $a \star_{|H \times H} b = a \star b = b \star a = b \star_{|H \times H} a$ kaikilla $a, b \in H$, eli $(H, \star)$ on abelin ryhmä. □

Jatkossa käytämme aliryhmien laskutoimituksille, sekä neutraali ja käänteisalkioille samoja merkintöjä kuin ryhmille.

LAUSE 2.13 (Aliryhmätesti). *Olkoon G ryhmä ja $H \subset G$. Tällöin $H \leqslant G$ jos ja vain jos*

(1) $H \neq \varnothing$ *ja*
(2) $xy^{-1} \in H$ *kaikilla* $x, y \in H$.

TODISTUS. Olkoon $H \leqslant G$. Tällöin $1 \in H$, joten $H \neq \varnothing$. Koska H on aliryhmä, niin määritelmän 2.11 mukaan $y^{-1} \in H$ ja $xy \in H$, joten erityisesti $y^{-1}x \in H$ kaikilla $x, y \in H$.

Oletetaan, että ominaisuudet (1) ja (2) pätevät ryhmän G osajoukolle H. Tällöin kohdan (1) perusteella on jokin $x \in H$, jolloin kohta (2) sovellettuna alkioon x antaa $1 = xx^{-1} \in H$. Näin ollen myös $x^{-1} = 1x^{-1} \in H$, eli jokaisella $x \in H$ on käänteisalkio $x^{-1} \in H$. Tällöin, koska lauseen 2.10 mukaan $y = (y^{-1})^{-1}$ kaikilla $y \in H$, niin kohdan (2) mukaan $xy = x(y^{-1})^{-1} \in H$. Näin ollen H on ryhmän G aliryhmä. □

MÄÄRITELMÄ 2.14. Olkoon G ryhmä ja $A \subset G$. Joukon A *virittämä aliryhmä* $\langle A \rangle$ koostuu kaikista joukon A *sanoista*, eli joukon A alkioiden ja niiden käänteisalkioiden äärellisistä tuloista. Täsmällisesti

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} \mid n \in \mathbb{Z},\, a_i \in A,\, \alpha_i = \pm 1\}$$

ja $\langle A \rangle = \{1\}$ jos $A \neq \varnothing$. Jos ryhmä G on äärellisen joukon $\{g_1, g_2, \dots, g_k\} \subset G$ virittämä, niin merkitään $G = \langle g_1, g_2, \dots, g_k \rangle$. Jos ryhmä G on yhden alkion virittämä ryhmä, eli $G = \langle g \rangle$ jollain $g \in G$ niin sanotaan, että G on *syklinen*.

ESIMERKKI 2.15. Jokainen kokonaisluku $x \in \mathbb{Z} - \{0\}$ voidaan kirjoittaa muodossa $x = \sum_{i=1}^{|x|} \pm 1$, jossa summan termien etumerkit $\pm$ ovat $+$, jos x on positiivinen ja $-$ jos x on negatiivinen. Täten, koska myös $0 = 1 - 1$, niin luku 1 virittää ryhmän $(\mathbb{Z}, +)$, eli $\mathbb{Z} = \langle 1 \rangle$. Näin ollen kokonaislukujen ryhmä $\mathbb{Z}$ on syklinen.

ESIMERKKI 2.16. Olkoon $n \in \mathbb{Z}^+$. Tällöin n-alkioista syklistä ryhmää merkitään $\mathbb{Z}_n = \langle x \rangle$, missä $nx = 1$. Ryhmä $\mathbb{Z}_n$ koostuu täten alkioista mx, missä $m \in \{0, \dots, n-1\}$.

MÄÄRITELMÄ 2.17. Ryhmän G aliryhmä N on *normaali aliryhmä*, jos

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} = N$$

kaikilla $g \in G$. Tällöin merkitään $N \trianglelefteq G$.

ESIMERKKI 2.18. Olkoon G ryhmä. Tällöin $\{1\} \trianglelefteq G$ ja $G \trianglelefteq G$, sillä jos $g, g' \in G$, niin tällöin $g1g^{-1} = gg^{-1} = 1 \in \{1\}$, eli $\{1\} \trianglelefteq G$ ja ryhmän määritelmän mukaan $gg'g^{-1} \in G$, eli $G \trianglelefteq G$.

LAUSE 2.19. *Abelin ryhmän jokainen aliryhmä on normaali.*

TODISTUS. Olkoon G ryhmä ja $N \leqslant G$. Lauseen 2.12 mukaan abelin ryhmän G jokainen aliryhmä on abelin ryhmä. Nyt, koska normaali aliryhmä N on ryhmän G aliryhmä, niin jokaisella $g \in G$, $n \in N$ pätee $gng^{-1} = gg^{-1}n = n$. Näin ollen $gNg^{-1} = N$. □

2.2. Ryhmien morfismit

Tarkastelemme seuraavaksi ryhmien välisiä homo- sekä isomorfismeja ja niiden ominaisuuksia. Ryhmähomomorfismi on kahden ryhmän välinen kuvaus, joka säilyttää ryhmien rakenteen laskutoimituksiensa suhteen.

MÄÄRITELMÄ 2.20. Olkoot $(G, \star), (H, \circ)$ ryhmiä. Kuvaus $\varphi : G \to H$ on *ryhmähomomorfismi*, jos

$$\varphi(x \star y) = \varphi(x) \circ \varphi(y)$$

kaikilla $x, y \in G$. Bijektiivinen ryhmähomomorfismi on *ryhmäisomorfismi*. Jos on olemassa ryhmäisomorfismi $\varphi : G \to H$ niin sanotaan, että ryhmät G ja H ovat ryhmäisomorfiset ja merkitään $G \cong H$. Ryhmähomomorfismin φ *ydin* $\ker \varphi$ on joukko $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$. Jos on selvää, että kuvaus on ryhmien välinen homo- tai isomorfismi, niin sitä kutsutaan usein vain homo- tai isomorfismiksi.

Voimme osoittaa suoraan määritelmää käyttämällä, että ryhmähomomorfismi säilyttää ryhmien rakenteen seuraavan lauseen tavoin.

LAUSE 2.21. *Olkoon G ja H ryhmiä ja $\varphi : G \to H$ homomorfismi. Tällöin kaikilla $g \in G$ ja $n \in \mathbb{Z}$ pätee*

(1) $\varphi(1_G) = 1_H$,
(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$,
(3) $\varphi(g^n) = \varphi(g)^n$.

TODISTUS. Olkoon $g \in G$, $n \in \mathbb{Z}$. (1) Ryhmän neutraalialkion ja ryhmähomomorfismien ominaisuuksien perusteella pätee

$$\begin{aligned}\varphi(1_G) &= 1_H\varphi(1_G)\\ &= \varphi(g)^{-1}\varphi(g)\varphi(1_G)\\ &= \varphi(g)^{-1}\varphi(g1_G)\\ &= \varphi(g)^{-1}\varphi(g) = 1_H.\end{aligned}$$

(2) Edellisen kohdan perusteella saadaan

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H,$$

jolloin kertomalla saatua yhtälöä puolittain vasemmalta alkion g käänteisalkiolla $\varphi(g)^{-1} \in G$ saadaan

$$\varphi(g^{-1}) = \varphi(g)^{-1}\varphi(g)\varphi(g^{-1}) = \varphi(g)^{-1}1_H = \varphi(g)^{-1}.$$

(3) Koska φ on homomorfismi, niin $\varphi(xy) = \varphi(x)\varphi(y)$ kaikilla $x, y \in G$. Erityisesti $\varphi(g^2) = \varphi(gg) = \varphi(g)\varphi(g) = \varphi(g)^2$. Oletetaan, että $\varphi(g^k) = \varphi(g)^k$, jollain $k \in \mathbb{N}$. Tällöin

$$\varphi(g^{k+1}) = \varphi(g^k g) = \varphi(g^k)\varphi(g) = \varphi(g)^k\varphi(g) = \varphi(g)^{k+1}.$$

Näin ollen väite pätee kaikille $n \in \mathbb{N}$. Soveltamalla vastaavaa päättelyä kohdan (2) tulokseen nähdään, että väite pätee myös kaikille $-n$, jossa $n \in \mathbb{N}$, joten väite pätee kaikilla $n \in \mathbb{Z}$. □

SEURAUS 2.22. *Olkoon $\varphi : G \to H$ ryhmähomomorfismi ja G', sekä H' vastaavasti ryhmien G ja H aliryhmiä. Tällöin homomorfismi φ säilyttää aliryhmien rakenteen siten, että*

(1) $\varphi(G') \leqslant \varphi(G)$, *sekä*
(2) $\varphi^{-1}(H') \leqslant G$.

TODISTUS. (1) Olkoon $\varphi : G \to H$ ryhmähomomorfismi. (1) Koska $G' \leqslant G$, niin erityisesti $1_G \in G'$ jolloin edellisen lauseen mukaan $\varphi(1_G) = 1_H \in \varphi(G')$, eli $\varphi(G') \neq \varnothing$. Olkoon $x, y \in \varphi(G')$ siten, että $x = \varphi(x')$ ja $y = \varphi(y')$, joillain $x', y' \in G'$. Tällöin, koska $G' \leqslant G$, niin aliryhmätestin 2.13 mukaan $x'y'^{-1} \in G'$, jolloin edellisen lauseen mukaan

$$\begin{aligned} xy^{-1} &= \varphi(x')\varphi(y')^{-1} \\ &= \varphi(x')\varphi(y'^{-1}) \\ &= \varphi(x'y'^{-1}) \in \varphi(G'). \end{aligned}$$

Näin ollen aliryhmätestin mukaan $\varphi(G') \leqslant \varphi(G)$.

(2) Koska $H' \leqslant H$, niin $1_H \in H'$, jolloin $1_G \in \varphi^{-1}(H')$. Tällöin erityisesti $\varphi^{-1}(H') \neq \varnothing$. Olkoon nyt $x, y \in \varphi^{-1}(H')$. Tällöin, koska $H' \leqslant H$, niin aliryhmätestin mukaan

$$\begin{aligned} \varphi(xy^{-1}) &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(x)\varphi(y)^{-1} \in H'. \end{aligned}$$

Näin ollen $xy^{-1} \in \varphi^{-1}(H)$, jolloin aliryhmätestin mukaan $\varphi^{-1}(H') \leqslant G$. □

SEURAUS 2.23. *Olkoon $\varphi : G \to H$ ryhmähomomorfismi ja G', sekä H' vastaavasti ryhmien G ja H aliryhmiä. Tällöin homomorfismi φ säilyttää normaalien aliryhmien rakenteen, eli*

(1) $\varphi(G') \trianglelefteq \varphi(G)$, sekä
(2) $\varphi^{-1}(H') \trianglelefteq G$.

TODISTUS. Olkoon $\varphi : G \to H$ ryhmähomomorfismi. (1) Koska $G' \trianglelefteq G$, niin $gG'g^{-1} = G'$ kaikilla $g \in G$. Olkoon $h \in \varphi(G)$ siten, että $\varphi(g) = h$. Tällöin

$$\begin{aligned} h\varphi(G')h^{-1} &= \varphi(g)\varphi(G')\varphi(g^{-1}) \\ &= \varphi(gG'g^{-1}) \\ &= \varphi(G'). \end{aligned}$$

Nyt, koska edellisen lauseen nojalla pätee $\varphi(G') \leqslant \varphi(G)$, niin $\varphi(G') \trianglelefteq \varphi(G')$.

(2) Olkoon $g \in G$. Tällöin, koska $H' \trianglelefteq H$, niin $hH'h^{-1} = H'$ kaikilla $h \in H$. Nyt, jos $\varphi(g) = h$, niin

$$\begin{aligned} \varphi(g\varphi^{-1}(H')g^{-1}) &= \varphi(g)\varphi(\varphi^{-1}(H'))\varphi(g^{-1}) \\ &= \varphi(g)H'\varphi(g)^{-1} \\ &= hH'h^{-1} \\ &= H'. \end{aligned}$$

Näin ollen $g\varphi^{-1}(H')g^{-1} = \varphi^{-1}(H')$ kaikilla $g \in G$. Nyt, koska edellisen lauseen nojalla $\varphi^{-1}(H) \leqslant G$, niin $\varphi^{-1}(H') \trianglelefteq G$. □

Näin ollen edellisen lauseen nojalla erityisesti $\ker\varphi \trianglelefteq G$ ja $\varphi(G) \trianglelefteq H$ jokaiselle homomorfismille $\varphi : G \to H$. Seuraavaksi määrittelemme ryhmien sivuluokat ja tekijäryhmät, sekä tarkastelemme niiden yhteyttä ryhmien morfismeihin.

MÄÄRITELMÄ 2.24. Olkoon G ryhmä ja $N \leqslant G$. Tällöin joukot

$$gN = \{gn \mid n \in N\} \quad \text{ja} \quad Ng = \{ng \mid n \in N\}$$

kaikilla $g \in G$ ovat aliryhmän N *vasen sivuluokka*, sekä *oikea sivuluokka* ryhmässä G. Kyseisen sivuluokan alkiota kutsutaan sen *edustajaksi*. Jos G on abelin ryhmä, niin sen vasemmat sekä oikeat sivuluokat ovat täsmälleen samat. Tällöin puhutaan usein vain aliryhmän N sivuluokasta ryhmässä G. Ryhmän G kaikkien vasenten sivuluokkien joukolle käytetään merkintää $GN = \{gN \mid g \in N\}$.

LAUSE 2.25. *Olkoon G ryhmä ja $N \leqslant G$. Tällöin $gN = Ng$ kaikilla $g \in G$ jos ja vain jos N on ryhmän G normaali aliryhmä.*

TODISTUS. Olkoon $gN = Ng$ kaikilla $g \in G$. Tällöin pätee

$$gNg^{-1} = Ngg^{-1} = N1 = N,$$

eli $N \trianglelefteq G$. Jos taas N on normaali aliryhmä, niin $gNg^{-1} = N$ kaikilla $g \in G$, jolloin

$$Ng = gNg^{-1}g = gN1 = gN,$$

eli N on ryhmän G normaali aliryhmä. □

Näin ollen voimme normaalien aliryhmien tapauksissa puhua oikeiden- sekä vasempien sivuluokkien sijasta vain sivuluokista vaikka kyseinen ryhmä ei olisikaan kommutatiivinen.

MÄÄRITELMÄ 2.26. Joukon A *ositus* on kokoelma $\{A_i \neq \varnothing \mid A_i \subset A,\ i \in I\}$, jollain indeksijoukolla I, jos

(1) $A = \bigcup_{i \in I} A_i$ ja
(2) $A_i \cap A_j = \varnothing$, jos $i \neq j$ kaikilla $i, j \in I$.

Tällöin sanotaan, että A on osajoukkojen A_i *erillinen yhdiste*.

LAUSE 2.27. *Olkoon G ryhmä ja $N \leqslant G$. Tällöin aliryhmän N vasempien sivuluokkien joukko ryhmässä G muodostaa ryhmän G osituksen.*

TODISTUS. Koska $N \leqslant G$, niin $1 \in N$, jolloin erityisesti $g = g1 \in gN$ kaikilla $g \in G$. Näin ollen ryhmä G voidaan esittää yhdisteenä vasemmista sivuluokista gN, eli

$$G = \bigcup_{g \in G} gN.$$

Oletetaan, että eri sivuluokat eivät ole erillisiä. Tällöin on $g, g' \in G$, $g \neq g'$ siten, että $gN \cap g'N \neq \varnothing$. Olkoon nyt $x \in gN \cap g'N$. Tällöin $x = gn = g'm$, joillain $n, m \in N$. Nyt, koska N on ryhmä, niin

$$g = gnn^{-1} = g'mn^{-1} = g'(mn^{-1}) = g'm',$$

jossa $m' = mn^{-1} \in N$. Näin ollen jokaiselle $gn' \in gN$ pätee

$$gn' = (g'm')n' = g'(m'n'),$$

jossa $m'n' \in N$. Täten $gn' \in g'N$, eli $gN \subseteq g'N$. Vastaavalla päättelyllä saadaan myös $g'N \subseteq gN$, joten $gN = g'N$. Tämä on ristiriidassa oletuksen kanssa, jolloin välttämättä pätee $gN \cap g'N = \varnothing$ kaikilla $g \neq g'$. Näin ollen sivuluokat gN muodostavat ryhmän G osituksen. □

SEURAUS 2.28. *Kaikilla $x, y \in G$ pätee $xN = yN$ jos ja vain jos $y^{-1}x \in N$.*

TODISTUS. Edellisen lauseen mukaan $xN = yN$ jos ja vain jos $x = x1 \in yN$. Tällöin $x = yn$ jollain $n \in N$, joten $y^{-1}x = n$. Näin ollen $y^{-1}x \in N$. Koska $x \in yN$ ja erityisesti $y \in yN$, niin $xN = yN$ jos ja vain jos $x, y \in xN = yN$. □

Soveltamalla edellistä seurausta tapaukseen $y = 1 \in G$ nähdään erityisesti, että $xN = 1N = N$ jos ja vain jos $x \in N$. Tämä erityistapaus antaa tavan nähdä, milloin jokin ryhmän alkio kuuluu tarkasteltavaan normaaliin aliryhmään. Määritellään seuraavaksi ryhmän normaalia aliryhmää vastaava tekijäryhmä.

MÄÄRITELMÄ 2.29. Ryhmän G normaalia aliryhmää N vastaava *tekijäryhmä* modulo N on pari $G/N = (GN, \star)$, jossa GN on ryhmän G kaikkien aliryhmää N vastaavien sivuluokkien joukko, sekä $\star$ on joukon GN laskutoimitus siten, että kaikilla $x, y \in G$ pätee

$$xN \star yN = (xy)N.$$

Osoitetaan seuraavaksi, että ryhmän normaalia aliryhmää vastaava tekijäryhmä on todellakin itsessään ryhmä.

LAUSE 2.30. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin tekijäryhmä G/N on ryhmä, jonka neutraalialkio on $1N = N$ ja jossa jokaisen alkion xN käänteisalkio on $x^{-1}N$.*

TODISTUS. Olkoon $x, x' \in xN$ ja $y, y' \in yN$. Osoitetaan ensiksi, että laskutoimitus $\star$ on hyvin määritelty, eli että jos $x' \in xN$ ja $y' \in yN$, niin $x'y' \in (xy)N$. Koska $x' = xn$ ja $y' = ym$ joillain $n, m \in N$, niin

$$\begin{aligned} x'y' &= (xn)(ym) = x1nym = x(yy^{-1})nym \\ &= (xy)(y^{-1}ny)m = (xy)(y^{-1}n(y^{-1})^{-1})m. \end{aligned}$$

Nyt, koska $N \trianglelefteq G$, niin $y^{-1}n(y^{-1})^{-1} \in N$, jolloin $x'y' = (xy)(n'm)$, jossa $xy \in G$ ja $n'm \in N$. Täten $x'y' \in (xy)N$ eli laskutoimitus on hyvin määritelty.

Osoitetaan seuraavaksi, että laskutoimitus $\star$ on liitännäinen. Jos $x, y, z \in G$, niin ryhmän G liitännäisyyden mukaan

$$\begin{aligned} (xN)(yNzN) &= (xN)(yzN) = x(yz)N \\ &= (xy)zN = (xyN)zN \\ &= (xNyN)(zN), \end{aligned}$$

eli laskutoimitus $\star$ on liitännäinen.

Osoitetaan vielä, että tekijäryhmässä G/N on laskutoimituksen $\star$ neutraalialkio, sekä jokaisen alkion käänteisalkio. Laskutoimituksen $\star$ määritelmän mukaan jokaisella $x \in G$ pätee

$$xN1N = (x1)N = xN = (1x)N = 1NxN,$$

joten $1N = N$ on laskutoimituksen $\star$ neutraalialkio. Jos $x \in G$, niin

$$xNx^{-1}N = (xx^{-1})N = 1N = (x^{-1}x)N = x^{-1}NxN,$$

joten $x^{-1}N$ on alkion xN käänteisalkio kaikilla $x \in G$. Näin ollen $(GN, \star)$ on ryhmä. □

ESIMERKKI 2.31. Olkoon $n \in \mathbb{Z}$. Tällöin joukko $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ varustettuna kokonaislukujen indusoidulla laskutoimituksella on aliryhmätestin 2.13 nojalla kokonaislukujen ryhmän $\mathbb{Z}$ aliryhmä, sillä $n1 = n \in \mathbb{Z}$ ja jos $nx, ny \in n\mathbb{Z}$, niin $nx - ny = n(x-y) \in n\mathbb{Z}$. Olkoon nyt $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, jossa $\varphi(z) = zx$, kun x on ryhmän $\mathbb{Z}_n$ virittävä alkio. Koska $\mathbb{Z}_n$ on syklinen, niin φ on selvästi surjektio. Tällöin, koska määritelmän mukaan $\varphi(z+z') = (z+z')x = zx+z'x = \varphi(z)\varphi(z')$, niin φ on surjektiivinen ryhmähomomorfismi.

Näin ollen, koska ryhmän $\mathbb{Z}_n$ määritelmän 2.16 mukaan $nx = 1$, niin homomorfismin φ ydin on aliryhmä $n\mathbb{Z}$. Tällöin lauseen 2.34 mukaan $n\mathbb{Z}$ on ryhmän $\mathbb{Z}$ normaali aliryhmä, jolloin tekijäryhmä $\mathbb{Z}/n\mathbb{Z}$ on hyvin määritelty. Tekijäryhmä $\mathbb{Z}/n\mathbb{Z}$ koostuu alkioista $z + n\mathbb{Z}$, jossa $z \in \mathbb{Z}$. Tällöin, koska $\mathbb{Z}$ on esimerkin 2.15 mukaan syklinen, niin tekijäryhmä $\mathbb{Z}/n\mathbb{Z}$ koostuu alkioista $z(1 + n\mathbb{Z})$. Näin ollen $\mathbb{Z}/n\mathbb{Z}$ on myös syklinen. Samoin, koska $nz \in n\mathbb{Z}$ kaikilla $z \in \mathbb{Z}$, niin $n(z + n\mathbb{Z}) = nz + n\mathbb{Z} = n\mathbb{Z} = 0_{\mathbb{Z}/n\mathbb{Z}}$. Näin ollen tekijäryhmä $\mathbb{Z}/n\mathbb{Z}$ koostuu alkioista $m + n\mathbb{Z}$, missä $m \in \{0, \ldots, n-1\}$, eli toisin sanottuna, $\mathbb{Z}/n\mathbb{Z}$ on n-alkioinen ryhmä.

MÄÄRITELMÄ 2.32. Olkoon $N \trianglelefteq G$. Ryhmän G *luonnollinen projektio* tekijäryhmälle G/N on kuvaus $\pi : G \to G/N$, jossa $\pi(g) = gN$.

Osoitamme seuraavaksi, että ryhmän luonnollinen projektio normaalille aliryhmälleen on itse asiassa surjektiivinen ryhmähomomorfismi.

LAUSE 2.33. *Olkoon $N \trianglelefteq G$ ja π luonnollinen projektio. Tällöin π on surjektiivinen ryhmähomomorfismi ja* $\ker \pi = N$.

TODISTUS. Olkoon $N \trianglelefteq G$ ja $x, y \in G$. Tällöin määritelmän mukaan

$$\pi(xy) = (xy)N = xNyN = \pi(x)\pi(y),$$

eli π on ryhmähomomorfismi. Koska jokaisella aliryhmän N sivuluokalla xN pätee $\pi(x) = xN$, niin π on selvästi surjektiivinen ryhmähomomorfismi. Koska lauseen 2.30 mukaan tekijäryhmän G/N neutraalialkio on normaali aliryhmä N, niin lauseen 2.28 mukaan

$$\begin{aligned}\ker \pi &= \{g \in G \mid \pi(g) = 1N\} \\ &= \{g \in G \mid gN = 1N\} \\ &= \{g \in G \mid g \in N\} \\ &= N,\end{aligned}$$

eli aliryhmä N on homomorfismin π ydin. □

Edellisestä lauseesta seuraa myös, että normaalit aliryhmät ovat täsmälleen ryhmähomomorfismien ytimiä.

SEURAUS 2.34. *Ryhmän G aliryhmä N on normaali jos ja vain jos se on jonkin homomorfismin ydin*

TODISTUS. Lauseen 2.23 mukaan homomorfismin ydin on aina lähtöjoukkonsa normaali aliryhmä. Normaalin aliryhmän N luonnollinen projektio on taas edellisen lauseen mukaan homomorfismi jonka ydin on N, joten normaalit aliryhmät ovat homomorfismien ytimiä. □

Näin ollen voimme korvata esimerkiksi tekijäryhmien määritelmässä esiintyvän ehdon aliryhmän normaaliudesta ehdolla, että kyseinen aliryhmä on jonkin ryhmähomomorfismin ydin. Seuraavaksi muotoilemme ryhmien ensimmäisen isomorfismilauseen.

LAUSE 2.35. *Olkoon $\varphi : G \to H$ ryhmähomomorfismi. Tällöin*

$$G/\ker \varphi \cong \varphi(G).$$

TODISTUS. Koska $\ker\varphi$ on homomorfismin φ ydin, niin tekijäryhmä $G/\ker\varphi$ on hyvin määritelty. Koska φ on homomorfismi, niin sen rajoittuma kuvajoukkoonsa $\varphi(G)$ on surjektiivinen homomorfismi. Osoitetaan, että tällöin kuvaus $\phi : G/\ker\varphi \to \varphi(G)$, $\phi(g\ker\varphi) = \varphi(g)$ on bijektiivinen homomorfismi.

Osoitetaan ensiksi, että ϕ todellakin on homomorfismi. Olkoot $x\ker\varphi$, sekä $y\ker\varphi$ tekijäryhmän $G/\ker\varphi$ alkioita. Tällöin pätee

$$\begin{aligned}\phi(x\ker\varphi y\ker\varphi) &= \phi((xy)\ker\varphi)\\ &= \varphi(xy)\\ &= \varphi(x)\varphi(y)\\ &= \phi(x\ker\varphi)\phi(y\ker\varphi),\end{aligned}$$

eli ϕ on todellakin homomorfismi. Koska jokaisella $g' \in \varphi(G)$ on $g \in G$ siten, että $\varphi(g) = g'$, niin $\phi(g\ker\varphi) = \varphi(g) = g'$, eli ϕ on surjektio. Olkoon taas $x\ker\varphi, y\ker\varphi \in G/\ker\varphi$. Nyt, jos $\phi(x\ker\varphi) = \phi(y\ker\varphi)$, niin määritelmän mukaan $\varphi(x) = \varphi(y)$, josta kertomalla puolittain termillä $\varphi(y)^{-1} \in H$ saadaan $\varphi(y)^{-1}\varphi(x) = \varphi(y)^{-1}\varphi(y) = 1_H$. Täten

$$1_H = \varphi(y)^{-1}\varphi(x) = \varphi(y^{-1})\varphi(x) = \varphi(y^{-1}x),$$

joka ytimen määritelmän 2.20 mukaan tarkoittaa, että $y^{-1}x \in \ker\varphi$. Näin ollen lauseen 2.28 perusteella pätee $x\ker\varphi = y\ker\varphi$, joten ϕ on injektio. Täten ϕ on haluttu isomorfismi $G/\ker\varphi \to \varphi(G)$, eli $G/\ker\varphi \cong \varphi(G)$. □

Näin ollen erityisesti surjektiiviselle ryhmähomomorfismille $\varphi : G \to H$ pätee $G/\ker\varphi \cong H$.

ESIMERKKI 2.36. Esimerkin 2.31 mukaan ryhmä $n\mathbb{Z}$ on surjektiivisen ryhmähomomofismin $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ ydin, jolloin ensimmäisen isomorfismilauseen mukaan $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Ensimmäisen isomorfismilauseen seuraus osoittaa, että surjektiivisien homomorfismien tapauksessa tekijäryhmät ovat isomorfiset luonnollisella tavalla.

SEURAUS 2.37. *Olkoon $\varphi : G \to H$ surjektiivinen ryhmähomomorfismi, sekä $H' \trianglelefteq H$. Tällöin $G/\varphi^{-1}(H') \cong H/H'$.*

TODISTUS. Olkoon π luonnollinen ryhmähomomorfismi $H \to H/H'$. Koska $H' \trianglelefteq H$, niin lauseen 2.23 mukaan $\varphi^{-1}(H') \trianglelefteq G$, jolloin tekijäryhmät $G/\varphi^{-1}(H')$ ja H/H' ovat hyvin määriteltyjä. Tällöin yhdistetty kuvaus $\pi\circ\varphi : G \to H/H'$ on surjektiivisten homomorfismien yhdisteenä surjektiivinen homomorfismi. Koska $\ker\pi = H'$ ja $\varphi(\varphi^{-1}(H')) = H'$, niin yhdistetyn kuvauksen $\pi \circ \varphi$ ytimeksi saadaan $\ker(\pi\circ\varphi) = \varphi^{-1}(H')$. Näin ollen ensimmäinen isomorfismilauseen 2.35 nojalla saadaan $G/\varphi^{-1}(H') \cong H/H'$. □

Päätämme ryhmäteorian käsittelyn tekijäryhmien vastaavuuslauseen todistukseen, jota kutsutaan myös ryhmien neljänneksi isomorfismilauseeksi.

LAUSE 2.38. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin on bijektiivinen kuvaus ryhmän G normaalin aliryhmän N sisältävien aliryhmien joukolta tekijäryhmän G/N aliryhmien joukolle. Erityisesti A on ryhmän G normaali aliryhmä jos ja vain jos A/N on tekijäryhmän G/N normaali aliryhmä.*

TODISTUS. Olkoot $\mathcal{A} = \{A \mid A \leqslant G, N \subseteq A\}$ normaalin aliryhmän $N \trianglelefteq G$ sisältävien ryhmän G aliryhmien joukko, $\mathcal{B} = \{B \mid B \leqslant G/N\}$ tekijäryhmän G/N aliryhmien joukko, sekä $\phi : \mathcal{A} \to \mathcal{B}$ kuvaus, joka kuvaa joukon $A \in \mathcal{A}$ sen luonnollisen projektiohomomorfismin kuvakseen, eli $\phi(A) = \pi(A) = A/N \in \mathcal{B}$, jossa $A/N = \{aN \mid a \in A\}$. Osoitetaan, että tällöin kuvaus ϕ on bijektio.

Osoitetaan, että ϕ on surjektio. Olkoon $B \in \mathcal{B}$ jokin tekijäryhmän G/N aliryhmä. Tällöin, koska luonnollinen projektiohomomorfismi $\pi : G \to G/N$, $\pi(g) = gN$ on lauseen 2.33 mukaan surjektiivinen ryhmähomomorfismi, niin jokaisella $bN \in B$ on $b \in G$ siten, että $\pi(b) = bN$. Näin ollen alkukuvalle $\pi^{-1}(B) = \{b \in G \mid bN \in B\} \subseteq G$ pätee $\pi(\pi^{-1}(B)) = B$. Täten kuvauksen ϕ määritelmän mukaan riittää osoittaa, että joukko $\pi^{-1}(B)$ on ryhmän G aliryhmä joka sisältää normaalin aliryhmän N eli, että $\pi^{-1}(B) \in \mathcal{A}$.

Koska B on tekijäryhmän G/N aliryhmä ja $\pi : G \to G/N$ on ryhmähomomorfismi, niin lauseen 2.22 mukaan $\pi^{-1}(B)$ on ryhmän G aliryhmä. Koska B on aliryhmä, niin $\{N\} = \{1N\} = \{1_{G/N}\} \subseteq B$, jolloin $N = \pi^{-1}(\{N\}) \subseteq \pi^{-1}(B)$. Näin ollen $\pi^{-1}(B)$ on ryhmän G aliryhmä, joka sisältää normaalin aliryhmän N, eli $\pi^{-1}(B) \in \mathcal{A}$. Täten $\phi(\pi^{-1}(B)) = \pi(\pi^{-1}(B)) = B$, eli kuvaus ϕ on surjektio. Lauseen 2.23 nojalla vastaava päättely normaalien aliryhmien tapauksessa antaa normaalien aliryhmien vastaavan tuloksen.

Osoitetaan, että ϕ on injektio. Olkoot A_1 ja A_2 ryhmän G aliryhmiä, jotka sisältävät aliryhmän N. Jos nyt $A_1 \neq A_2$, niin on $x \in A_1$ siten, että $x \notin A_2$, tai päinvastoin. Tällöin, jos $\phi(A_1) = \phi(A_2)$, niin erityisesti $\pi(x) = xN = yN$, jollain $y \in A_2$. Kuitenkin, lauseen 2.28 nojalla pätee $xN = yN$ jos ja vain jos $y^{-1}x \in N$. Nyt, koska $N \subseteq A_2$ ja A_2 on ryhmän G aliryhmä, niin $x = yy^{-1}x \in A_2$, joka on ristiriita. Näin ollen $\phi(A_1) \neq \phi(A_2)$, eli kuvaus ϕ on injektio. Koska normaalit aliryhmät ovat erityisesti aliryhmiä, niin tämä pätee myös normaalien aliryhmien tapauksessa. Näin ollen ϕ on haluttu bijektio. □

LUKU 3

Renkaat

Seuraavaksi käsittelemme *renkaiden* teoriaa ja käymme läpi joitain tarvittavia rengasteorian tuloksia. Siinä missä ryhmät yleistävät kokonaislukujen yhteenlaskun käsitteen mielivaltaisille joukoille ja laskutoimituksille, jotka muistuttavat yhteenlaskua, niin renkaat muistuttavat kokonaislukujen joukkoa varustettuna sen yhteen-, sekä kertolaskutoimituksellaan. Tulemme tarkastelemaan erilaisien renkaiden ja niiden alirenkaiden ominaisuuksia ja osoitamme joitain rengasteorian hyödyllisiä tuloksia, kuten niin sanotun *kiinalaisen jakojäännöslauseen*. Näytämme myös että, jos renkaan jokainen kertolaskun suhteen vakaa alirengas on yhden alkion virittämä, niin sen jokaisella alkiolla on kokonaislukuja muistuttava yksikäsitteinen alkulukujen tulo esitys. Tämä kappale perustuu teoksiin [**1**], [**2**], [**4**], sekä [**5**].

3.1. Renkaat ja alirenkaat

MÄÄRITELMÄ 3.1. *Rengas* on kolmikko $(R, +, \cdot)$, jossa R on joukko ja kuvaukset $+$, sekä $\cdot$ ovat joukon R laskutoimituksia siten, että

(1) $(R, +)$ on abelin ryhmä,
(2) laskutoimitus $\cdot$ on liitännäinen ja
(3) laskutoimitus $\cdot$ on *distributiivinen* laskutoimituksen $+$ suhteen, eli kaikilla $a, b, c \in R$ pätee

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{ja} \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Jos lisäksi laskutoimitus $\cdot$ on kommutatiivinen, niin R on *kommutatiivinen rengas*. Jos renkaan $(R, +, \cdot)$ laskutoimitukset $+$ ja $\cdot$ ovat selvät, niin sanotaan vain että R on rengas. Tällöin, kuten ryhmäteorian tapauksessa merkitään $a \cdot b = ab$, vaikkei $(R, \cdot)$ välttämättä olekaan ryhmä. Laskutoimituksia $+$ ja $\cdot$ kutsutaan yleensä yhteenlaskuksi ja kertolaskuksi.

Abelin ryhmän $(R, +)$ alkiolle ja laskutoimituksille käytetään ryhmäteoriasta tuttuja additiivisen ryhmän merkintöjä 2.4. Joukon R alkiolle kertolaskun suhteen käytetään taas ryhmäteorian normaaleja tuloja muistuttavia merkintöjä, jolloin esimerkiksi kertolaskun mahdollista neutraalialkiota merkitään symbolilla 1 ja alkion $a \in R$ mahdollista käänteisalkiota kertolaskun suhteen merkitään symbolilla a^{-1}. Jos rengas R sisältää laskutoimituksen $\cdot$ neutraalialkion 1, niin R on *yksiköllinen rengas*. Tulemme jatkossa olettamaan, että käsittelemämme renkaat ovat yksiköllisiä ja kutsumme niitä vain renkaiksi.

ESIMERKKI 3.2. *Nollarengas*, eli kolmikko $(\{0\}, +, \cdot)$, jossa $+, \cdot$ ovat *triviaalin joukon* $\{0\}$ laskutoimituksia on rengas. Tämä on selvää, sillä ainoa joukon $\{0\}$ laskutoimitus on $(0, 0) \mapsto 0$ ja näin ollen yhteen- ja kertolaskun neutraalialkiot ovat 0, eli $1 = 0$. Jos rengas R on nollarengas, niin usein merkitään vain $R = 0$.

Vaikka renkaan määritelmässä ei oleteta, että alkiot 1 ja 0 ovat eri alkiota, niin tulemme monissa rengasteorian sovelluksissa tarvitsemaan tietoa, että käsiteltävässä renkaassa pätee $1 \neq 0$. Seuraava lause osoittaa, että itse asiassa mielivaltaisessa renkaassa pätee $1 = 0$ jos ja vain jos kyseessä on nollarengas.

LAUSE 3.3. *Olkoon R rengas. Tällöin $1 = 0$ jos ja vain jos R on* nollarengas, *eli $R = \{0\}$.*

TODISTUS. Olkoon $1 = 0$ ja $r \in R$. Tällöin, koska $0r = 0$ ja $1r = r$, niin

$$r = 1r = 0r = 0,$$

eli $R = 0$. Jos taas R on nollarengas, niin selvästi $1 = 0$, sillä 0 on ainoa renkaan R alkio. □

ESIMERKKI 3.4. Renkaiden $(R_1, +_1, \cdot_1), (R_2, +_2, \cdot_2), \ldots, (R_n, +_n, \cdot_n)$, $n \in \mathbb{Z}^+$ *suora tulo*, eli abelin ryhmien $(R_i, +_i)$, $i \in \{1, \ldots, n\}$ esimerkin 2.6 mukainen suora tulo varustettuna tulojoukon $R_1 \times R_2 \times \cdots \times R_n$ laskutoimituksella $\cdot$, jolle pätee $(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \ldots, x_n \cdot_n y_n)$ on rengas.

ESIMERKKI 3.5. Kokonaislukujen joukko $\mathbb{Z}$ varustettuna kokonaislukujen tunnetulla yhteenlaskulla $+$ ja kertolaskulla $\cdot$, eli kolmikko $(\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas, jossa yhteenlaskun neutraalialkio on luku 0 ja kertolaskun neutraalialkio on luku 1. Samoin myös rationaalilukujen-, reaalilukujen- ja kompleksilukujen joukot $\mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$ varustettuna niiden yhteen, sekä kertolaskutoimituksillaan ovat renkaita ja erityisesti määritelmän 2.7 nojalla kuntia [**1**, s. 82].

ESIMERKKI 3.6. Kunnan määritelmän 2.7 mukaan jokainen kunta $(K, +, \cdot)$ on rengas. Koska kunnan määritelmässä vaadittiin, että kertolaskun neutraalialkio 1 sisältyy joukkoon $K - \{0\}$, niin erityisesti $1 \neq 0$ ja näin ollen kunnassa K on ainakin kaksi eri alkiota.

ESIMERKKI 3.7. Abelin ryhmän R *endomorfismien joukko*

$$\mathrm{End}(R) = \{\varphi : R \to R \mid \varphi \text{ on homomorfismi}\}$$

varustettuna laskutoimituksillaan $+'$ ja $\circ$, joilla $(\varphi_1 +' \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$, sekä, $\varphi_1 \circ \varphi_2(x) = \varphi_1(\varphi_2(x))$ on rengas $(\mathrm{End}(R), +', \circ)$. Kuvauksien yhteenlaskun $+'$ neutraalialkio on *nollakuvaus* $\varphi_0 : x \mapsto 0$ ja kuvauksien yhdistämisen $\circ$ neutraalialkio on *identtinen kuvaus* $\mathrm{Id} : x \mapsto x$, kaikilla $x \in R$.

MÄÄRITELMÄ 3.8. Rengaan R alirengas on additiivisen ryhmän $(R, +)$ aliryhmä, joka on vakaa renkaan R kertolaskun suhteen. Yhtäpitävästi renkaan R alirengas on sen osajoukko, joka on itsessään rengas varustettuna indusoiduilla laskutoimituksilla.

Osoitetaan seuraavaksi, että myös renkaille pätee ryhmäteorian aliryhmätestiä 2.13 muistuttava tulos.

LAUSE 3.9 (Alirengastesti). *Olkoon R rengas ja $R' \subset R$. Tällöin R' on renkaan R alirengas jos ja vain jos*

(1) $x - y \in R'$ ja
(2) $xy \in R'$ kaikilla $x, y \in R'$.

TODISTUS. Osajoukko R' on renkaan R alirengas jos ja vain jos R' varustettuna indusoiduilla laskutoimituksilla on rengas. Koska R on rengas, niin indusoidut laskutoimitukset toteuttavat renkaan liitännäisyys- ja distributiivisuus ehdot (2) ja (3). Näin ollen R' on renkaan R aliregas jos ja vain jos $(R', +) \leqslant (R, +)$ ja kertolasku on vakaa joukossa R'. Aliryhmätestin 2.13 mukaan $R' \leqslant R$ jos ja vain jos $x - y \in R'$ kaikilla $x, y \in R$, joka osoittaa kohdan (1). Kertolasku taas on määritelmän mukaan vakaa joukossa R' jos ja vain jos $xy \in R'$ kaikilla $x, y \in R'$, joka osoittaa kohdan (2). □

MÄÄRITELMÄ 3.10. Olkoon $R \neq \{0\}$ rengas. Alkio $u \in R$ on renkaan R *yksikkö*, jos sillä on kertolaskun käänteisalkio $u^{-1} \in R$. Renkaan R yksiköiden joukkoa merkitään symbolilla $R^\times$. Jos jokainen renkaan R nollasta poikkeava alkio on yksikkö, niin R on *jakorengas*.

Koska kommutatiivinen jakorengas R on nollasta poikkeava rengas, niin lauseen 3.3 mukaan $1 \neq 0$. Tällöin, koska jokaisella jakorenkaan nollasta poikkeavalla alkiolla on kertolaskun käänteisalkio, niin $(R - \{0\}, \cdot)$ on abelin ryhmä. Näin ollen kunnan määritelmän 2.7 mukaan kunnat ovat täsmälleen kommutatiivisia jakorenkaita. Tarkastellaan seuraavaksi joitain renkaiden perusominaisuuksia.

LAUSE 3.11. *Olkoon R rengas ja $a, b \in R$. Tällöin:*

(1) $0a = a0 = 0$,
(2) $(-a)b = a(-b) = -(ab)$,
(3) $(-a)(-b) = ab$ *ja*
(4) kertolaskun neutraalialkio $1 \in R$ *on yksikäsitteinen ja* $-a = (-1)a$.

TODISTUS. Olkoon R rengas ja $a, b \in R$. (1) Renkaan määritelmän 3.1 kohdan (3) mukaan $0a = (0 + 0)a = 0a + 0a$, jolloin lisäämällä puolittain alkio $-(0a) \in R$ saadaan $0a = 0$. Yhtälö $a0 = 0$ saadaan vastaavalla päättelyllä. Renkaan määritelmän kohdan (3) ja edellisen kohdan mukaan pätee

$$ab + (-a)b = (a + (-a))b = 0b = 0,$$

jolloin lisäämällä puolittain alkio $-(ab) \in R$ saadaan $(-a)b = -(ab)$. Vastaavalla päättelyllä saadaan myös yhtälö $a(-b) = -(ab)$.

(2) Edellisen kohdan mukaan saadaan vastaavasti

$$\begin{aligned} -(ab) + (-a)(-b) &= (-a)b + (-a)(-b) \\ &= (-a)(b + (-b)) \\ &= (-a)0 = 0, \end{aligned}$$

jolloin $(-a)(-b) = ab$ yhteenlaskun kommutatiivisuuden perusteella.

(3) Jos on olemassa $x \in R$ siten, että x on myös kertolaskun neutraalialkio, niin määritelmän mukaan $1 = 1x = x$. Lisäksi renkaan määritelmän kohdan (3) mukaan $a + (-1)a = 1a + (-1)a = (1 - 1)a = 0$, eli $-a = (-1)a$. □

MÄÄRITELMÄ 3.12. Olkoon $R \neq \{0\}$ rengas. Alkio $a \in R$, $a \neq 0$ on *nollanjakaja*, jos on $b \in R$, $b \neq 0$ siten, että joko $ab = 0$ tai $ba = 0$. Kommutatiivinen rengas R, jossa ei ole nollanjakajia on *kokonaisalue*.

Osoittautuu, että kokonaisalueissa pätee seuraava, niin sanottu kertolaskun supistussääntö.

LAUSE 3.13. *Olkoon R kokonaisalue ja $r \in R$, $r \neq 0$. Tällöin, jos $ra = rb$, niin $a = b$.*

TODISTUS. Jos $ra = rb$, niin renkaan laskutoimituksien mukaan $r(a-b) = 0$ jolloin, koska kokonaisalueessa R ei ole nollanjakajia ja $r \neq 0$, niin $a - b = 0$ eli $a = b$. □

LAUSE 3.14. *Kunta on kokonaisalue.*

TODISTUS. Jos R on kunta, niin se on kommutatiivinen jakorengas. Tällöin jokaisella $a \in R$, $a \neq 0$ on kertolaskun käänteisalkio a^{-1}. Nyt jos $ab = 0$, jollain $b \in R$, $b \neq 0$, kuitenkin $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$, joka on ristiriita. Täten R ei sisällä nollanjakajia eli se on kokonaisalue. □

3.2. Rengashomomorfismit ja ideaalit

Seuraavaksi yleistämme ryhmäteoriasta tutut morfismien käsitteet renkaille. Koska renkaat ovat erityisesti additiivisia abelin ryhmiä, joille on yhteenlaskun lisäksi määritelty myös kertolaskutoimitus, niin monet määritelmistä ja todistuksista ovat hyvin samanlaisia, kuin ryhmien tapauksessa.

MÄÄRITELMÄ 3.15. Olkoot R ja S renkaita. Tällöin kuvaus $\varphi : R \to S$ on *rengashomomorfismi*, jos kaikilla $a, b \in R$ pätee

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(2) $\varphi(ab) = \varphi(a)\varphi(b)$ ja
(3) $\varphi(1_R) = 1_S$

Rengashomomorfismin φ *ydin* on joukko $\ker \varphi = \{a \in R \mid \varphi(a) = 0\}$. Bijektiivinen rengashomomorfismi on *rengasisomorfismi*. Jos $\varphi : R \to S$ on rengasisomorfismi niin sanotaan, että renkaat R ja S ovat rengasisomorfiset ja merkitään $R \cong S$. Jos on selvää, että φ on renkaiden välinen homo- tai isomorfismi, niin sanotaan vain, että φ on homomorfismi tai isomorfismi.

Koska rengashomomorfismin määritelmän kohta (1) vastaa ryhmähomomorfismin määritelmää 2.20, niin rengashomomorfismi φ on erityisesti additiivisien ryhmien $(R, +_R)$ ja $(S, +_S)$ välinen ryhmähomomorfismi.

Tarkastellaan seuraavaksi rengashomomorfismien ytimiä ja niiden ominaisuuksia.

LAUSE 3.16. *Olkoot R ja S renkaita ja $\varphi : R \to S$ homomorfismi. Tällöin*

(1) kuvajoukko $\varphi(R)$ on renkaan S alirengas ja
(2) ydin $\ker \varphi$ on renkaan R alirengas ja erityisesti $xr, rx \in \ker \varphi$ kaikilla $x \in \ker \varphi$ ja $r \in R$.

TODISTUS. Olkoon $\varphi : R \to S$ rengashomomorfismi. (1) Koska homomorfismin φ rajoittuma joukkoon $\varphi(R)$ on surjektio, niin kaikilla $s, s' \in \varphi(R) \subseteq S$ on alkiot $r, r' \in R$ siten, että $\varphi(r) = s$ ja $\varphi(r') = s'$. Tällöin, koska R on rengas, niin alkioille $s, s' \in \varphi(R)$ pätee

$$s - s' = \varphi(r) - \varphi(r') = \varphi(r - r') \in \varphi(R),$$

sekä $ss' = \varphi(r)\varphi(r') = \varphi(rr') \in \varphi(R)$. Täten alirengastestin 3.9 mukaan $\varphi(R)$ on renkaan S alirengas.

(2) Olkoon $x, y \in \ker \varphi$. Tällöin $\varphi(x) = 0 = \varphi(y)$, jolloin pätee

$$\varphi(x - y) = \varphi(x) - \varphi(y) = 0,$$

sekä $\varphi(xy) = \varphi(x)\varphi(y) = 0$, eli $x - y \in \ker \varphi$ ja $xy \in \ker \varphi$. Täten alirengastestin mukaan $\ker \varphi$ on renkaan R alirengas. Nyt, jos $r \in R$, niin $\varphi(rx) = \varphi(r)\varphi(x) = 0$ ja $\varphi(xr) = \varphi(x)\varphi(r) = 0$, eli $xr, rx \in \ker \varphi$. □

Rengashomomorfismin ytimet ovat siis erittäin vakaita kertolaskun suhteen. Määritellään seuraavaksi ideaalit eli alirenkaat, jotka toteuttavat edellisen lauseen vakausominaisuuden, sekä tekijäryhmien regasvastikkeet eli tekijärenkaat.

MÄÄRITELMÄ 3.17. Renkaan R *ideaali* on alirengas $I \subseteq R$ jossa $ri \in I$ ja $ir \in I$ kaikilla $r \in R$, $i \in I$. Renkaan R *tekijärengas* ideaalin I suhteen R/I on tekijäryhmä R/I varustettuna renkaan R laskutoimituksilla $+$ ja $\cdot$ joille pätee

(1) $(r + I) + (s + I) = (r + s) + I$ ja
(2) $(r + I) \cdot (s + I) = (rs) + I$ kaikilla $r, s \in R$.

Jos renkaan R ideaalille I pätee $I \subsetneq R$, niin sanotaan, että I on renkaan R *aito ideaali*.

Koska ideaalit ovat määritelmän mukaisesti jonkin rengashomomorfismin ytimiä ja rengashomomorfismit ovat erityisesti renkaita vastaavien additiivisien abelin ryhmien välisiä ryhmähomomorfismeja, niin renkaan ideaalit ovat lauseen 2.34 nojalla erityisesti kyseistä rengasta vastaavan abelin ryhmän normaaleja aliryhmiä. Näin ollen edellinen tekijärenkaiden määritelmä sopii yhteen tekijäryhmien määritelmän 2.29 kanssa.

Osoitetaan seuraavaksi, että tekijärengas on todellakin rengas.

LAUSE 3.18. *Tekijärengas R/I on rengas, jonka neutraalialkiot yhteen- ja kertolaskun suhteen ovat vastaavasti joukon R/I alkiot $1 + I$, sekä I ja jossa jokaisen alkion $r + I \in R/I$ käänteisalkio yhteenlaskun suhteen on $-r + I \in R/I$.*

TODISTUS. Koska R on rengas, niin $(R, +)$ on abelin ryhmä jolloin lauseen 2.19 mukaan sen aliryhmä $(I, +)$ on normaali aliryhmä. Näin ollen lauseen 2.30 mukaan abelin tekijäryhmä $(R/I, +)$, jonka sivuluokat ovat $r+I$, missä $r \in R$ on hyvin määritelty laskutoimituksellaan $+$ jolle pätee $(r+I)+(s+I) = (r+s)+I$ kaikilla $r, s \in R$. Samoin lauseen 2.30 mukaan tekijäryhmän neutraalialkio yhteenlaskun suhteen on alkio $0+I = I \in R/I$ ja jokaisen $r+I \in R/I$ käänteisalkio yhteenlaskun suhteen on $-r + I$. Näin ollen riittää osoittaa, että tekijäryhmä R/I varustettuna laskutoimituksella $\cdot$, jossa $(r + I) \cdot (s + I) = (rs) + I$ kaikilla $r, s \in R$ on rengas.

Koska renkaan R kertolasku on liitännäinen ja distributiivinen yhteenlaskunsa suhteen ja tekijärenkaan R/I laskutoimitukset $+$ ja $\cdot$ ovat määritelty niiden avulla, niin tekijärenkaan laskutoimitukset toteuttavat renkaan määritelmän liitännäisyys- ja distributiivisuusvaatimukset, jos laskutoimitus $\cdot$ on hyvin määritelty sivuluokkien joukossa R/I. Olkoon $r' \in r + I$ ja $s' \in s + I$. Tällöin $r' = r+n$ ja $s' = s+m$, joillain $n, m \in I$. Näin ollen, koska renkaan määritelmän

mukaan $rm + ns + nm \in I$, niin saadaan

$$\begin{aligned}(r' + I)(s' + I) &= ((r + n) + I)((s + m) + I)\\ &= (r + n)(s + m) + I\\ &= (rs + rm + ns + nm) + I\\ &= rs + (rm + ns + nm) + I\\ &= rs + I.\end{aligned}$$

Täten laskutoimitus $\cdot$ on hyvin määritelty. Lisäksi $1 + I$ on kertolaskun neutraalialkio, sillä $(r+I)(1+I) = r1+I = r+I$ ja $(1+I)(r+I) = 1r+I = r+I$. Näin ollen tekijärengas R/I on rengas, joka toteuttaa halutut ominaisuudet. □

Koska rengashomomorfismit ovat erityisesti ryhmähomomorfismeja ja ideaalit ovat lauseen 3.16 mukaan rengashomomorfismien ytimiä, niin monet ryhmähomomorfismien ytimiä koskevat tulokset kääntyvät suoraan rengasteorian kielelle korvaamalla homomorfismien ytimet eli normaalit aliryhmät ideaaleilla.

Tarkastellaan seuraavaksi renkaiden isomorfismilauseita. Näytetään ensiksi, että ryhmien ensimmäisellä isomorfismilauseella on rengasteorian vastike, jota kutsutaan vastaavasti renkaiden ensimmäiseksi isomofismilauseeksi.

Lause 3.19 (Ensimmäinen rengasisomorfismilause). *Jos $\varphi : R \to S$ on rengashomomorfismi, niin $\ker\varphi$ on renkaan R ideaali ja*

$$R/\ker\varphi \cong \varphi(R).$$

Todistus. Koska lauseen 3.16 mukaan rengashomomorfismin φ ydin on ideaali, niin tekijärengas $R/\ker\varphi$ on hyvin määritelty ja lauseen 2.19 mukaan $\ker\varphi$ on ryhmän $(R, +)$ normaali aliryhmä. Koska rengashomomorfismi on erityisesti additiivisien ryhmien välinen ryhmähomomorfismi, niin ensimmäisen ryhmäisomorfismilauseen mukaan on olemassa ryhmäisomorfismi $\phi : R/\ker\varphi \to \varphi(R)$, $\phi(r + \ker\varphi) = \varphi(r)$. Nyt, koska φ on rengashomomorfismi, niin

$$\begin{aligned}\phi((r + \ker\varphi)(s + \ker\varphi)) &= \phi(rs + \ker\varphi)\\ &= \varphi(rs)\\ &= \varphi(r)\varphi(s)\\ &= \phi(r + \ker\varphi)\phi(s + \ker\varphi)\end{aligned}$$

ja $\phi(1_R + \ker\varphi) = \varphi(1_R) = 1_S$. Täten ϕ on renkaiden $R/\ker\varphi$ ja $\varphi(R)$ välinen rengasisomorfismi, eli $R/\ker\varphi \cong \varphi(R)$. □

Myös ryhmäteoriasta tutulla luonnollisella projektiohomomorfismilla 2.32 on rengasteorian vastike, joka on vastaavasti surjektiivinen rengashomomorfismi.

Lause 3.20. *Jos I on renkaan R ideaali, niin renkaan R luonnollinen projektio tekijärenkaalle $\varphi : R \to R/I$, $\varphi(r) = r + I$ on surjektiivinen rengashomomorfismi ja $\ker\varphi = I$.*

Todistus. Koska rengas $(R, +)$ on abelin ryhmä ja $I \subset R$ on renkaan R ideaalina sen normaali aliryhmä, niin lauseen 2.33 mukaan luonnollinen projektiokuvaus on surjektiivinen ryhmähomomorfismi jonka ydin on $\ker\pi = I$. Täten riittää osoittaa, että $\pi(rs) = \pi(r)\pi(s)$ kaikilla $r, s \in R$ ja $\pi(1_R) = 1_{R/I}$.

Olkoon $r, s \in R$. Tällöin pätee

$$\begin{aligned}\pi(rs) &= rs + I \\ &= (r + I)(s + I) \\ &= \pi(r)\pi(s),\end{aligned}$$

sekä $\pi(1_R) = 1_R + I = 1_{R/I}$. Näin ollen luonnollinen projektio on surjektiivinen rengashomomorfismi jonka ydin $\ker \pi = I$. □

Koska luonnollinen projektiohomomorfismi on rengashomomorfismi, niin myös renkaiden neljäs isomorfismilause 2.38 yleistyy renkaiden tapaukseen, kun normaalit aliryhmät korvataan ideaaleilla.

SEURAUS 3.21. *Olkoon I renkaan R ideaali. Tällöin on ideaalin I sisältävien renkaan R alirenkaiden A joukon ja tekijärenkaan R/I alirenkaiden välinen bijektiivinen kuvaus. Erityisesti A on renkaan R ideaali jos ja vain jos A/I on tekijärenkaan R/I ideaali.*

3.3. Ideaalien ominaisuudet

Aloitetaan laajentamalla ryhmäteoriassa käsitelty viritetyn ryhmän määritelmä 2.14 kommutatiivisille renkaille.

MÄÄRITELMÄ 3.22. Olkoon R kommutatiivinen rengas ja $A \subset R$. Joukon A virittämä ideaali on alirengas

$$(A) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R,\, a_i \in A,\, n \in \mathbb{N}\},$$

jossa $(A) = \{0\}$ jos $A = \varnothing$. Äärellisen joukon $A = \{a_1, \ldots, a_n\}$ virittämää ideaalia $(A) = (a_1, \ldots, a_n)$ kutsutaan *äärellisesti viritetyksi ideaaliksi* ja samoin yhden alkion virittämää ideaalia (a) kutsutaan renkaan R *pääideaaliksi*.

MÄÄRITELMÄ 3.23. *Pääideaalialue* on kokonaisalue, jonka jokainen ideaali on pääideaali.

ESIMERKKI 3.24. Koska esimerkin 2.15 mukaan kokonaislukujen rengas on alkion 1 virittämä, niin erityisesti $\mathbb{Z} = (1)$, eli kokonaislukujen rengas on pääideaalialue.

Tarkastellaan seuraavaksi joitain ideaalien ominaisuuksia. Osoitetaan ensiksi, että aidossa ideaalissa ei ole yksiköitä sekä, että kunnassa ei ole aitoja ideaaleja.

LAUSE 3.25. *Olkoon I renkaan R ideaali. Tällöin pätee:*

(1) $I = R$ jos ja vain jos ideaali I sisältää jonkin renkaan R yksikön.
(2) Jos R on kommutatiivinen rengas, niin R on kunta jos ja vain jos sen ainoat ideaalit ovat $\{0\}$ ja R.

TODISTUS. Olkoon R rengas. (1) Olkoon $I \subseteq R$ ideaali, joka sisältää jonkin renkaan R yksikön u. Koska jokaisella yksiköllä $u \in I$ on määritelmän 3.10 mukaan kertolaskun käänteisalkio $u^{-1} \in R$, niin tällöin ideaalin määritelmän 3.17 mukaan $uu^{-1} = 1 \in I$, jolloin myös $r = 1r \in I$ kaikilla $r \in R$. Näin ollen $R \subseteq I$. Koska ideaalin määritelmän mukaan myös $I \subseteq R$, niin $I = R$. Jos taas $I = R$, niin $1 \in R = I$, eli I sisältää jonkin renkaan R yksikön.

(2) Kommutatiivinen rengas R on määritelmän 2.7 mukaan kunta jos ja vain jos jokainen $r \in R$, $r \neq 0$ on yksikkö. Olkoon R on kunta. Jos ideaali $I \neq \{0\}$, niin se sisältää jonkin renkaan R alkion, joka on määritelmän mukaan yksikkö. Tällöin kohdan (1) mukaan $I = R$. Oletetaan, että kommutatiivisen renkaan R ainoat ideaalit ovat $\{0\}$ ja R, sekä $u \in R$, $u \neq 0$. Tällöin, koska $u \neq 0$, niin pätee $(u) \neq (0) = \{0\}$, jolloin oletuksen mukaan $(u) = R$. Koska $1 \in R$, niin $1 \in (u)$, jolloin pääideaalin määritelmän ja renkaan R kommutatiivisuuden mukaan on $u^{-1} \in R$ siten, että $uu^{-1} = u^{-1}u = 1$. Näin ollen jokainen renkaan R nollasta poikkeava alkio on yksikkö, eli R on kunta. □

Esimerkki 3.26. Jos K on kunta, niin edellisen lauseen mukaan sen ainoat ideaalit ovat 0 ja K. Tällöin, koska $\{0\} = (0)$, sekä jokaisella alkiolla $k \in K$ pätee $k = 1k \in (1)$, niin $K \subseteq (1)$. Näin ollen, koska myös $(1) \subseteq K$, niin $K = (1)$, eli kunta on pääideaalialue.

Siirrytään tarkastelemaan renkaan suurimpia aitoja ideaaleja, eli *maksimaalisia ideaaleja*.

Määritelmä 3.27. Renkaan R aito ideaali $M \subsetneq R$ on *maksimaalinen ideaali*, jos ainoat ideaalin M sisältävät ideaalit ovat M ja R. Toisin sanoen M on maksimaalinen ideaali, jos inkluusiosta $M \subseteq I$, missä I on renkaan R ideaali seuraa joko $I = M$ tai $I = R$.

Seuraava tulos osoittaa, että jokaisella nollarenkaasta poikkeavalla renkaalla on maksimaalinen ideaali. Tuloksen todistus nojaa osittain järjestettyjen joukkojen teoriaan ja erityisesti Zornin lemmaan, jota emme käsittele tarkasti tässä tutkielmassa. Aiheesta löytää lisätietoa esimerkiksi teoksista [**1**, s. 588], [**2**, s. 907], sekä [**4**, s. 12].

Lause 3.28. *Jokaisen renkaan aito ideaali sisältyy maksimaaliseen ideaaliin.*

Todistus. Olkoon R rengas ja I sen aito ideaali. Koska $I \neq R$, niin erityisesti rengas R ei ole nollarengas, sillä muuten inkluusiosta $I \subset R$ seuraisi $I = (0) = \{0\} = R$. Olkoon $\mathcal{I}$ ideaalin I sisältävien renkaan R aitojen ideaalien kokoelma. Tällöin, koska $I \in \mathcal{I}$, niin $\mathcal{I}$ on epätyhjä ja osittain järjestetty osajoukkojen inkluusion $\subseteq$ mukaan. Nyt, jos $\mathcal{K}$ on joukon $\mathcal{I}$ ketju, eli joukon $\mathcal{I}$ täysin järjestetty osajoukko, niin olkoon

$$\mathcal{M} = \bigcup_{A \in \mathcal{K}} A$$

ketjun $\mathcal{K}$ ideaalien A yhdiste. Osoitetaan seuraavaksi, että $\mathcal{M}$ on myös renkaan R ideaali.

Olkoon $a, b \in \mathcal{M}$. Tällöin joukon $\mathcal{M}$ määritelmän mukaan on jotkin ideaalit $A, B \in \mathcal{K}$ siten, että $a \in A$ ja $b \in B$. Koska $\mathcal{K}$ on ketju, niin joko $A \subseteq B$ tai $B \subseteq A$. Voidaan siis olettaa, että $A \subseteq B$. Tällöin, koska A ja B ovat renkaan R ideaaleja ja $a, b \in B$, niin alirengastestin 3.9 mukaan $a - b \in B \subseteq \mathcal{M}$, sekä $ab \in B \subseteq \mathcal{M}$. Näin ollen alirengastestin mukaan $\mathcal{M}$ on renkaan R alirengas. Olkoon nyt $r \in R$. Tällöin, koska B on renkaan R ideaali, niin $ra, ar \in B \subseteq \mathcal{M}$, jolloin $\mathcal{M}$ on renkaan R ideaali.

Nyt, jos $\mathcal{M} = R$, niin lauseen 3.25 mukaan $\mathcal{M}$ sisältää jonkin renkaan R yksikön u, jolloin ideaalin määritelmän mukaan $uu^{-1} = 1 \in \mathcal{M}$. Tällöin 1 sisältyy johonkin ideaaliin $A \in \mathcal{M}$, jolloin $A = R$. Kuitenkin ideaalin $\mathcal{M}$

määritelmän mukaan ideaalit $A \in \mathcal{M}$ ovat aitoja ideaaleja, joka on ristiriita. Täten $\mathcal{M}$ on myös renkaan R aito ideaali joka sisältää ideaalin I, eli toisin sanoen $\mathcal{M} \in \mathcal{I}$.

Nyt, koska jokainen ketjun $\mathcal{K}$ ideaali A sisältyy määritelmän mukaan ideaaliin $\mathcal{M}$, niin $\mathcal{M}$ on ketjun $\mathcal{K}$ yläraja. Tällöin Zornin lemman [**4**, s. 13] mukaan joukossa $\mathcal{I}$ on maksimaalinen alkio, eli renkaassa R on maksimaalinen ideaali, joka sisältää ideaalin I. □

Seuraavaksi osoitamme, että kommutatiivisen renkaan tekijärengas jonkin ideaalinsa suhteen on kunta jos ja vain jos kyseinen ideaali on maksimaalinen. Tämä tulos tulee antamaan meille keinon tehdä päättelyjä tarkasteltavan renkaan ominaisuuksista soveltamalla kuntien ominaisuuksia sen tekijärenkaaseen maksimaalisen ideaalin suhteen.

LAUSE 3.29. *Olkoon R kommutatiivinen rengas. Ideaali $\mathcal{M} \subset R$ on maksimaalinen ideaali jos ja vain jos tekijärengas $R/\mathcal{M}$ on kunta.*

TODISTUS. Renkaan R ideaali $\mathcal{M}$ on määritelmän mukaan maksimaalinen ideaali jos ja vain jos ei ole olemassa renkaan R ideaalia I siten, että $\mathcal{M} \subsetneq I \subsetneq R$. Tällöin, koska renkaiden neljännen isomorfismilauseen 3.21 mukaan renkaan R ideaalin $\mathcal{M}$ sisältävien ideaalien joukon ja tekijärenkaan $R/\mathcal{M}$ ideaalien välillä on bijektiivinen kuvaus $I \mapsto I/\mathcal{M}$, niin ideaali $\mathcal{M}$ on maksimaalinen jos ja vain jos jäännösrenkaassa ei ole ideaalia $I' \in R/I$, jolle pätee $\phi(\mathcal{M}) \subset I' \subset R/I$. Nyt, koska $\phi(\mathcal{M}) = \mathcal{M}/\mathcal{M} = 0$, niin $\mathcal{M}$ on maksimaalinen ideaali jos ja vain jos jäännösrenkaan $R/\mathcal{M}$ ideaalit ovat vain 0 ja $R/\mathcal{M}$, joka lauseen 3.25 mukaan pätee jos ja vain jos $R/\mathcal{M}$ on kunta. □

Tarkastellaan seuraavaksi ideaalien tuloja, sekä niiden yhteyttä rengashomomorfismeihin.

MÄÄRITELMÄ 3.30. Olkoon R kommutatiivinen rengas ja $I_1, I_2, \ldots I_n$ sen ideaaleja. Tällöin ideaalien tulo $I_1 I_2 \cdots I_n$ on joukko

$$I_1 I_2 \cdots I_n = \{x_1^1 x_1^2 \cdots x_1^n + \cdots + x_m^1 x_m^2 \cdots x_m^n \mid x_j^i \in I_i \text{ kaikilla } 1 \leqslant i, j \leqslant n, m\},$$

joka koostuu kaikista ideaalien $I_1, I_2, \ldots, I_n$ alkioiden äärellisien tulojen äärellisistä summista.

LAUSE 3.31. *Ideaalien tulo on ideaali*

TODISTUS. Olkoon $I_1, I_2, \ldots I_n$ renkaan R ideaaleja, sekä $x_i \in I_i$ kaikilla $i \in \{1, \ldots, n\}$. Tällöin, koska I_1 on ideaali, niin $r x_1 x_2 \ldots x_n = x_1' x_2 \ldots x_n$, jossa $x_1' = r x_1 \in I_1$ kaikilla $r \in R$. Tällöin renkaan R distributiivisuusominaisuuden perusteella jokainen alkioiden $x_1 x_2 \ldots x_n$ äärellinen summa kerrottuna renkaan alkiolla koostuu vieläkin ideaalien I_i alkioista, eli $r I_1 I_2 \ldots I_n = I_1 I_2 \ldots I_n$ kaikilla $r \in R$. Koska renkaan R kommutatiivisuuden perusteella pätee myös, että $I_1 I_2 \ldots I_n r = r I_1 I_2 \ldots I_n$, niin ideaalien tulo on todellakin ideaali. □

MÄÄRITELMÄ 3.32. Renkaan R ideaalit I ja J ovat *komaksimaaliset*, jos

$$I + J = \{x + y \mid x \in I, y \in J\} = R.$$

Todistetaan seuraavaksi niin sanottuna *kiinalaisena jakojäännöslauseena* tunnettu ideaalien tuloja käsittelevä tulos, joka on erään kongruenssiyhtälöiden ratkaisun yksikäsitteisyyttä käsittelevän lukuteorian tuloksen yleistys [**3**, s. 132].

LAUSE 3.33 (Kiinalainen jakojäännöslause). *Olkoon $R \neq \{0\}$ kommutatiivinen rengas ja olkoot $I_1, I_2, \ldots, I_k$ renkaan R ideaaleja, jollain $k \geqslant 2$. Tällöin kuvaus*

$$\varphi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_k, \qquad \varphi(r) = (r + I_1, r + I_2, \ldots, r + I_k)$$

on rengashomomorfismi, jonka ydin on $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_k$. *Jos ideaalit I_i, I_j ovat komaksimaaliset kaikilla $i, j \in \{1, \ldots, k\}$ ja $i \neq j$, niin kuvaus φ on surjektiivinen ja ideaaleille pätee $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \ldots I_k$, jolloin*

$$R/(I_1 I_2 \ldots I_k) = R/(I_1 \cap I_2 \cap \cdots \cap I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

TODISTUS. Todistetaan väite induktioperiaatteen avulla. Tarkastellaan ensiksi tapausta $k = 2$. Olkoon $\varphi : R \to R/I_1 \times R/I_2$, jossa $\varphi(r) = (r + I_1, r + I_2)$. Tällöin kuvauksen φ komponentit ovat luonnollisia projektioita tekijärenkaille R/I_1 ja R/I_2, joten φ on lauseen 3.20 mukaan homomorfismi, jonka ydin on $I_1 \cap I_2$. Oletetaan nyt, että ideaalit I_1 ja I_2 ovat komaksimaaliset. Näin ollen, koska $I_1 + I_2 = R$, niin on olemassa $x \in I_1$ ja $y \in I_2$ siten, että $x + y = 1$. Olkoon $(r_1 + I_1, r_2 + I_2) \in R/I_1 \times R/I_2$. Nyt, koska $x = 1 - y$, niin

$$\varphi(x) = (x + I_1, 1 - y + I_2) = (I_1, 1 + I_2) = (0, 1).$$

Vastaavalla päättelyllä saadaan myös $\varphi(y) = (1, 0)$, jolloin

$$\begin{aligned}
\varphi(r_2 x + r_1 y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\
&= (r_2 + I_1, r_2 + I_2)(0, 1) + (r_1 + I_1, r_1 + I_2)(1, 0) \\
&= (0, r_2 + I_2) + (r_1 + I_1, 0) \\
&= (r_1 + I_1, r_2 + I_2).
\end{aligned}$$

Näin ollen φ on surjektiivinen rengashomomorfismi. Osoitetaan seuraavaksi, että $I_1 \cap I_2 = I_1 I_2$. Koska joukko

$$I_1 I_2 = \{x_1 y_1 + \cdots + x_n y_n \mid x_i \in I_1, y_i \in I_2, \text{ kaikilla } i \in \{1, \ldots, n\}\}$$

koostuu kaikista alkioiden $x_i y_i$ äärellisistä summista ja koska I_1, I_2 ovat renkaan R ideaaleja, niin määritelmän mukaan $I_1 I_2 \subseteq I_1 \cap I_2$. Nyt, koska ideaalit I_1 ja I_2 ovat komaksimaaliset, niin jokaisella $z \in I_1 \cap I_2$ pätee

$$z = z1 = z(x + y) = zx + zy \in I_1 I_2.$$

Täten $I_1 \cap I_2 = I_1 I_2$, eli $\ker \varphi = I_1 I_2$. Näin ollen renkaiden ensimmäisen isomorfismilauseen 3.19 mukaan

$$R/(I_1 I_2) = R/(I_1 \cap I_2) \cong R/I_1 \times R/I_2.$$

Oletetaan nyt, että väite pätee jollain $k \geqslant 2$. Olkoot $I_1, \ldots, I_{k+1}$ renkaan R pareittain komaksimaalisia ideaaleja ja $i \in \{1, \ldots, k\}$. Tällöin erityisesti jokainen ideaali I_{k+1} on komaksimaalinen jokaisen ideaalin I_i kanssa, jolloin on alkiot $x_i \in I_i$ ja $y_i \in I_{k+1}$ siten, että $x_i + y_i = 1$. Täten renkaan R kommutatiivisuuden nojalla

$$\begin{aligned}
1 &= (x_1 + y_1)(x_2 + y_2) \cdots (x_k + y_k) \\
&= \Big(\sum_{i=1}^{n} x_1 x_i + \sum_{i=1}^{n} x_1 y_i + \sum_{i=1}^{n} y_1 x_i \Big) + \sum_{i=1}^{n} y_1 y_i,
\end{aligned}$$

jossa alkupään äärellinen summa kuuluu ideaalin määritelmän mukaan ideaalien tuloon $I = I_1 I_2 \dots I_k$ ja $\sum_{i=1}^{n} y_1 y_i \in I_{k+1}$. Täten $1 \in I + I_{k+1}$, eli on olemassa alkiot $x' \in I$ ja $y' \in I_{k+1}$ siten, että $1 = x' + y'$. Näin ollen jokaisella $r \in R$ pätee

$$r = r1 = r(x' + y') = rx' + ry' \in I + I_{k+1},$$

eli ideaalit I ja I_{k+1} ovat komaksimaaliset. Nyt, koska induktio-oletuksen mukaan väite pätee kaikilla $i \in \{1, \dots, k\}$, niin erityisesti se pätee komaksimaalisilla ideaaleilla I ja I_{k+1}. Täten $R/(II_{k+1}) \cong R/I \times R/I_{k+1}$. Nyt, koska induktio-oletuksen mukaan väite pätee myös ideaaleille $I_1, I_2, \dots, I_k$, niin

$$R/I = R/(I_1 I_2 \dots I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

Näin ollen

$$R/(I_1 I_2 \dots I_k I_{k+1}) = R/(II_{k+1}) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k \times R/I_{k+1},$$

jolloin väite pätee induktioperiaatteen mukaisesti kaikilla $k \geqslant 2$. □

3.4. Pääideaali- ja yksikäsitteisen tekijäjaon alueet

Käsittelemme seuraavaksi kommutatiivisien renkaiden jaollisuusominaisuuksia ja niiden yhteyttä pääideaalialueisiin. Aloitamme lukuteoriaa mukailevilla määritelmillä ja tuloksilla.

MÄÄRITELMÄ 3.34. Olkoon R kommutatiivinen rengas ja $a, b \in R$, $b \neq 0$.

(1) Alkio b *jakaa* alkion a, jos on $x \in R$ siten, että $a = bx$. Tällöin merkitään $b \mid a$ ja sanotaan, että a on alkion b *monikerta*.
(2) Alkioiden a ja b *suurin yhteinen tekijä* $\mathrm{syt}(a, b)$ on alkio $d \in R$, $d \neq 0$ jolle pätee
   (i) $d \mid a$ ja $d \mid b$ ja
   (ii) jos $d' \mid a$ ja $d' \mid b$, niin $d' \mid d$ kaikilla $d' \in R$.

Seuraava tulos osoittaa, että kommutatiivisen renkaan alkioiden suurin yhteinen tekijä voidaan yhtäpitävästi määritellä renkaan R ideaalien avulla.

LAUSE 3.35. *Olkoon R kommutatiivinen rengas ja I renkaan R alkioiden a ja $b \neq 0$ virittämä ideaali. Tällöin alkio $d \in R$ on renkaan R alkioiden a ja b suurin yhteinen tekijä, eli syt(a,b) = d jos ja vain jos*

(i) $I \subseteq (d)$ ja
(ii) jos $I \subseteq (d')$, niin $(d) \subseteq (d')$.

TODISTUS. Olkoon R kommutatiivinen rengas ja $a, b, d \in R$.

(i) Määritelmän mukaan $d \mid a$ jos ja vain jos $a = rd$, jollain $r \in R$, eli jos ja vain jos $a \in (d)$. Nyt, jos I on renkaan R alkioiden a ja b virittämä ideaali, niin jokaisella $x \in I$ pätee $x = r_1 a + r_2 b$. Tällöin $d \mid a$ ja $d \mid b$ jos ja vain jos $x = r_1(dr) + r_2(ds) = d(r_1 r + r_2 s)$ joillain $r, s \in R$, eli jos ja vain jos $x \in (d)$. Täten ehto (i) on yhtäpitävä suurimman yhteisen tekijän ehdon (i) kanssa.

(ii) Olkoon $d' \in R$ ja $I \subseteq (d')$. Koska I on alkioiden a ja b virittämä ideaali, niin jokaiselle $x \in I$ pätee $x = r_1 a + r_2 b$ joillain $r_1, r_2 \in R$. Täten, jos $I \subseteq (d')$, niin erityisesti $a, b \in (I) \subseteq (d')$, jolloin $d' \mid a$ ja $d' \mid b$. Jos taas $d' \mid a$ ja $d' \mid b$, niin $a = q_1 d'$ ja $b = q_2 d'$ joillain $q_1, q_2 \in R$, jolloin jokaisella $x \in I$ pätee $x = (r_1 q_1)d' + (r_2 q_2)d' \in (d')$, eli $I \subseteq (d')$. Koska $d' \mid d$ jos ja vain jos $d \in (d')$, eli $(d) \subseteq (d')$, niin lauseen ehto (ii) on yhtäpitävä suurimman yhteisen tekijän määritelmän ehdon (ii) kanssa. □

Seuraava esimerkki osoittaa, että mielivaltaisen kokonaisalueen alkioilla ei ole välttämättä suurinta yhteistä tekijää.

ESIMERKKI 3.36. Joukko $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ varustettuna kompleksilukujen tunnetuilla yhteen- ja kertolaskutoimituksilla on kokonaisalue. Koska luvulla $6 \in \mathbb{Z}[\sqrt{-5}]$ on esitykset $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ niin osoittautuu, että sen ainoat tekijät ovat luvut $1, 2, 3, 1 + \sqrt{-5}$ ja $1 - \sqrt{-5}$. Näin ollen lukujen 6 ja $2 \cdot (1 + \sqrt{-5})$ yhteiset tekijät ovat täsmälleen luvut $1, 2$ ja $1 + \sqrt{-5}$. Koska $2 \mid 1$ ja $1 + \sqrt{-5} \mid 1$, niin 1 ei voi olla suurin yhteinen tekijä. Voidaan osoittaa, että kumpikaan yhteisistä tekijöistä 2 ja $1 + \sqrt{-5}$ ei jaa toistaan, jolloin määritelmän 3.34 mukaan luvuilla 6 ja $2 \cdot (1 + \sqrt{-5})$ ei ole suurinta yhteistä tekijää. [**1**, s. 394]

Seuraava tulos antaa ehdon suurimman yhteisen tekijän olemassaololle, sekä liittää kommutatiivisen renkaan alkioiden suurimman yhteisen tekijän käsitteen pääideaalialueisiin.

SEURAUS 3.37. *Jos R on kommutatiivinen rengas ja $a, b \in R$, $b \neq 0$ siten, että alkioiden a ja b virittämä ideaali on pääideaali (d), niin $\text{syt}(a, b) = d$.*

TODISTUS. Koska pääideaali (d) on kommutatiivisen renkaan R alkioiden a ja $b \neq 0$ virittämä ideaali, niin sijoittamalla edelliseen lauseeseen $I = (d)$ selvästi $\text{syt}(a, b) = d$. □

Osoitetaan seuraavaksi, että kokonaisalueen alkioiden suurin yhteinen tekijä on yksikäsitteinen yksiköllä kertomista vaille.

LAUSE 3.38. *Olkoon R kokonaisalue. Jos $(d) = (d')$ joillain $d, d' \in R$, niin $d' = ud$ jollain $u \in R^\times$. Erityisesti, jos $a, b \in R$, $a, b \neq 0$ siten, että $\text{syt}(a, b) = d$ ja $\text{syt}(a, b) = d'$, niin $d' = ud$ jollain $u \in R^\times$.*

TODISTUS. Koska $(d) = (d')$, niin $d = r'd'$ ja $d' = rd$, joillain $r, r' \in R$. Tällöin, jos esimerkiksi $d = 0$, niin $0 = r'0 = 0 = u0$, missä $u \in R^\times$. Vastaavalla päättelyllä väite pätee myös, jos $d' = 0$. Oletetaan siis, että $d, d' \neq 0$. Tällöin $d = r'd' = r'(rd) = (r'r)d$, jolloin kokonaisalueen R supistussäännön 3.13 ja kommutatiivisuuden mukaan $r'r = rr' = 1$. Täten r' on renkaan R yksikkö, jolloin alkiolla d on haluttu esitys.

Lauseen 3.35 kohdan (ii) nojalla, jos $\text{syt}(a, b) = d$ ja $\text{syt}(a, b) = d'$, niin $(d) = (d')$, jolloin edellä olevan päättelyn mukaan $d = ud'$, jollain $u \in R^\times$. □

Voimme yhdistää edellä olevat lauseet seuraavaksi pääideaalialueiden suurimman yhteisen tekijän lauseeksi.

SEURAUS 3.39. *Olkoon R pääideaalialue ja $a, b \in R$, $a, b \neq 0$. Jos $I \subseteq R$ on alkioiden a ja b virittämä ideaali siten, että $I = (d)$, jollain $d \in R$, niin*

(1) $\text{syt}(a, b) = d$,
(2) on alkiot $x, y \in R$ siten, että $d = ax + by$ ja
(3) jos $d' = \text{syt}(a, b)$, niin $d' = ud$, jollain $u \in R^\times$.

SEURAUS 3.40. *Olkoon R pääideaalialue ja $a, b, c \in R - \{0\}$ siten, että $\text{syt}(a, b) = 1$. Tällöin, jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.*

TODISTUS. Koska $\text{syt}(a, b) = 1$, niin edellisen lauseen mukaan on alkiot $x, y \in R$ siten, että $1 = ax + by$. Tällöin kertomalla puolittain alkiolla c saadaan

$c = cax + cby$. Nyt, koska $a \mid c$ ja $b \mid c$, niin on alkiot $x', y' \in R$ siten, että $c = x'bax + y'aby = (x'x + y'y)ab$, eli $ab \mid c$. □

Yleistetään seuraavaksi kokonaislukujen renkaan tunnettu alkulukujen käsite mielivaltaisille kokonaisalueille. Tarkastellaan ensiksi kommutatiivisen renkaan alkuideaaleja ja niiden ominaisuuksia.

MÄÄRITELMÄ 3.41. Olkoon R kommutatiivinen rengas. Renkaan R aito ideaali P on *alkuideaali*, jos ehdosta $ab \in P$ joillain $a, b \in R$ seuraa, että $a \in P$ tai $b \in P$.

LAUSE 3.42. *Olkoon R kommutatiivinen rengas. Tällöin P on alkuideaali jos ja vain jos tekijärengas R/P on kokonaisalue.*

TODISTUS. Olkoon $r + P \in R/P$. Tällöin lauseen 2.28 nojalla $r \in P$ jos ja vain jos $r + P = 0 + P = P = 0_{R/P}$. Näin ollen P on alkuideaali jos ja vain jos $P \neq R$, eli $R/P \neq R/R = \{0\}$ ja jos ehdosta $(a + P)(b + P) = ab + P = 0_{R/P}$ seuraa $a + P = 0_{R/P}$ tai $b + P = 0_{R/P}$, joka on täsmälleen kokonaisalueen määritelmä 3.12. □

SEURAUS 3.43. *Kommutatiivisen renkaan maksimaalinen ideaali on alkuideaali.*

TODISTUS. Olkoon R kommutatiivinen rengas ja $\mathcal{M}$ sen maksimaalinen ideaali. Lauseen 3.29 mukaan tekijärengas $R/\mathcal{M}$ on kunta, jolloin se on lauseen 3.14 mukaan kokonaisalue. Tällöin edellisen lauseen mukaan $\mathcal{M}$ on alkuideaali. □

LAUSE 3.44. *Pääideaalialueen jokainen nollasta poikkeava alkuideaali on maksimaalinen ideaali.*

TODISTUS. Olkoon R pääideaalialue ja (p) sen alkuideaali, missä $p \neq 0$. Tällöin $(p) \subsetneq R$. Olkoon (m) pääideaali siten, että $(p) \subseteq (m)$. Tällöin erityisesti $p \in (m)$, eli $p = rm$ jollain $r \in R$. Näin ollen $rm = 1p \in (p)$. Nyt, koska (p) on alkuideaali, niin $r \in (p)$ tai $m \in (p)$.

Tällöin, jos $m \in (p)$, niin jokaisella $x \in (m)$ pätee $x = sm = s(qp) = (sq)p$, joillain $s, q \in R$. Näin ollen $(m) \subseteq (p)$, eli $(m) = (p)$. Jos taas $r \in (p)$, niin $r = sp$ jollain $s \in R$. Tällöin, koska $p \in (m)$, niin pätee $p = rm = (sp)m = p(sm)$. Näin ollen kokonaisalueen R supistussäännön 3.13 ja kommutatiivisuuden mukaan pätee $sm = ms = 1$, eli m on renkaan R yksikkö.

Nyt, koska pääideaali (m) sisältää renkaan R yksikön, niin lauseen 3.25 mukaan $(m) = R$. Koska $(p) \neq R$ ja ainoat ideaalit joka sisältävät alkuideaalin (p) ovat (p) ja R, niin (p) on maksimaalinen ideaali. □

Näin ollen pääideaalialueen alkuideaalit ovat täsmälleen maksimaalisia ideaaleja. Määritellään seuraavaksi kokonaisalueen *alkuluvut* ja *supistamattomat alkiot*.

MÄÄRITELMÄ 3.45. Olkoon R kokonaisalue.

(1) Olkoon $r \in R - \{0\}$ siten, että $r \notin R^\times$. Jos ehdosta $r = ab$, $a, b \in R$ seuraa $a \in R^\times$ tai $b \in R^\times$, niin sanotaan, että r on *supistamaton*. Jos alkio ei ole supistumaton, niin sanotaan, että se on *supistuva*.
(2) Jos $p \in R - \{0\}$ siten, että pääideaali (p) on alkuideaali niin sanotaan, että p on kokonaisalueen R *alkuluku*.

Tarkastellaan seuraavaksi joitain alkulukujen ja supistamattomien alkioiden ominaisuuksia. Aloitetaan osoittamalla, että alkuluvut voidaan määritellä yhtäpitävästi seuraavan lauseen tavoin.

LAUSE 3.46. *Olkoon R kokonaisalue ja $p \in R$. Tällöin p on kokonaisalueen R alkuluku jos ja vain jos se ei ole yksikkö ja jos ehdosta $p \mid ab$, joillain $a, b \in R$ seuraa $p \mid a$ tai $p \mid b$*

TODISTUS. Olkoot $p, a, b \in R$. Pääideaalin ja jaollisuuden määritelmien 3.17, 3.34 mukaan $ab \in (p)$ jos ja vain jos $ab = rp$, jollain $r \in R$, eli jos ja vain jos $p \mid ab$. Täten väite $a \in (p)$ tai $b \in (p)$ on yhtäpitävä väitteen $p \mid a$ tai $p \mid b$ kanssa jolloin alkuideaalin määritelmän 3.41 mukaan riittää osoittaa, että (p) on aito ideaali, jos ja vain jos p ei ole yksikkö.

Lauseen 3.25 mukaan renkaan R pääideaali (p) on sen aito ideaali jos ja vain jos (p) ei sisällä renkaan R yksikköä. Tällöin, jos (p) on alkuideaali, niin se on aito ideaali, jolloin pääideaali (p) ei sisällä renkaan R yksikköä. Täten erityisesti $p \in (p)$ ei ole yksikkö. Oletetaan siis, että p ei ole renkaan R yksikkö. Tällöin, jos $(p) = R$, niin erityisesti $1 \in R$, jolloin renkaan R kommutatiivisuuden nojalla $1 = rp = pr$ jollain $r \in R$. Täten p on yksikkö, joka on ristiriita. Näin ollen $(p) \neq R$, eli (p) on aito ideaali jos ja vain jos p ei ole yksikkö. □

LAUSE 3.47. *Pääideaalialueen alkio on alkuluku jos ja vain jos se on supistamaton.*

TODISTUS. Olkoon R pääideaalialue ja $p \in R - \{0\}$ sen alkuluku. Tällöin edellisen lauseen mukaan $p \notin R^\times$, sekä ehdosta $p \mid ab$ seuraa $p \mid a$ tai $p \mid b$. Jos $p \mid a$, niin $a = rp$ jollain $r \in R$, jolloin $p = rpb = (rb)p$. Nyt, koska R on kokonaisalue, niin supistussäännön 3.13 ja kokonaisalueen kommutatiivisuuden mukaan $rb = br = 1$, eli $b \in R^\times$. Vastaavasti, jos $p \mid b$, niin edellä olevan päättelyn nojalla pätee $a \in R^\times$, joten p on pääideaalialueen R supistamaton alkio.

Jos taas p on pääideaalialueen R supistamaton alkio, niin $p \notin R^\times$ ja ehdosta $p = ab$, missä $a, b \in R$ seuraa, että $a \in R^\times$ tai $b \in R^\times$. Koska lauseen 3.46 todistuksen mukaan ehdosta $(p) = R$ seuraa, että $p \in R^\times$, niin $(p) \neq R$. Tällöin, jos pääideaali (p) sisältyy johonkin pääideaalialueen R ideaaliin (q), missä $q \in R$, niin $p = rq$, jollain $r \in R$. Näin ollen, koska p on supistumaton, niin $r \in R^\times$ tai $q \in R^\times$. Jos $r \in R^\times$, niin rengas R sisältää alkion r käänteisalkion, jolloin $q = r^{-1}p$, eli $q \in (p)$. Näin ollen $(p) = (q)$. Jos taas $q \in R^\times$, niin lauseen 3.25 mukaan $(q) = R$, jolloin ainoat pääideaalin (p) sisältävät ideaalit ovat itse $(p) \neq R$, sekä R. Näin ollen (p) on maksimaalinen ideaali, jolloin lauseen 3.43 mukaan se on myös alkuideaali. □

Koska kokonaislukujen kokonaisalueen $\mathbb{Z}$ ainoa yksikkö on luku $1 \in \mathbb{Z}$, niin edellisen lauseen mukaan yleisen kokonaisalueen alkuluvun määritelmä sopii yhteen tunnetun kokonaislukujen alkuluvun määritelmän kanssa, jossa $p \in \mathbb{Z}$ on alkuluku jos ja vain jos sen ainoat tekijät ovat 1, sekä p [**4**, s. 11]

Tarkastellaan seuraavaksi *yksikäsitteisen tekijäjaon alueita* ja niiden yhteyttä pääideaalialueisiin. Yksikäsitteisen tekijäjaon alue on kokonaisalue, jonka jokainen alkio voidaan esittää yksikäsitteisesti alkulukujen tulona, kokonaislukujen renkaan tavoin. Tulemme osoittamaan, että itse asiassa pääideaalialueen alkioilla on aina kyseinen alkulukuesitys, eli että pääideaalialue on yksikäsitteisen tekijäjaon alue.

MÄÄRITELMÄ 3.48. *Yksikäsitteisen tekijäjaon alue* on kokonaisalue R, jossa jokaisella $r \in R - \{0\}$, $r \notin R^\times$ pätee seuraavat ehdot.

(1) Alkio r voidaan esittää kokonaisalueen R supistamattomien alkioiden äärellisenä tulona. Toisin sanoen $r = p_1 p_2 \dots p_n$, joillain $p_i \in R, n \in \mathbb{Z}$, missä alkiot $p_1, \dots, p_n$ ovat supistamattomia.
(2) Kohdan (1) esitys on yksikäsitteinen yksiköllä kertomista vaille. Toisin sanoen, jos $r = p_1 \dots p_n = q_1 \dots q_m$, joillain supistamattomilla alkioilla $r_i, q_i \in R$, niin $n = m$ ja alkiot $q_1, \dots, q_m$ voidaan järjestää siten, että $p_i = u_i q_i$, jossa $u_i \in R^\times$ kaikilla $i \in \{1, \dots, n\}$.

LEMMA 3.49. *Olkoon R pääideaalialue ja $(r_1), (r_2), (r_3) \dots$ sen pääideaaleja. Tällöin jokaisella kasvavalla ketjulla $(r_1) \subseteq (r_2) \subseteq (r_3) \subseteq \cdots$ on yläraja (r_n), jollain $n \in \mathbb{Z}^+$, jolloin $(r_i) = (r_n)$ kaikilla $i \geqslant n$.*

TODISTUS. Koska $I = \bigcup_{i=1}^{\infty}(r_i)$ on lauseen 3.28 todistuksen nojalla renkaan R ideaali ja koska R on pääideaalialue, niin I on pääideaali (a), jollain $a \in R$. Tällöin, koska erityisesti $a \in (a) = I$, niin $a \in (r_n)$, jollain $n \in \mathbb{Z}^+$. Täten ideaalin määritelmän mukaan $(r_i) \subseteq I \subseteq (r_n)$, kaikilla $i \in \mathbb{Z}^+$. Koska $(r_n) \subseteq (r_i)$ kaikilla $i \geqslant n$, niin $(r_i) = (r_n)$ kun $i \geqslant n$. □

LAUSE 3.50. *Pääideaalialue on yksikäsitteisen tekijäjaon alue.*

TODISTUS. Olkoon R pääideaalialue ja $r \in R - \{0\}$, joka ei ole yksikkö. Jos r on supistamaton, niin sillä on määritelmän 3.48 mukainen esitys, joten voimme olettaa, että r ei ole supistamaton. Tällöin supistamattoman alkion määritelmän 3.45 mukaan alkio r voidaan esittää tulona $r = r_1 q_1$, missä alkiot $r_1, q_1 \in R$ eivät ole yksiköitä. Näin ollen pääideaalin määritelmän mukaan $r \in (r_1)$, jolloin $(r) \subseteq (r_1)$. Jos $(r) = (r_1)$, niin $r_1 = r'r$, jollain $r' \in R$, jolloin $r = q_1 r_1 = q_1 r' r$. Tällöin kokonaisalueen supistussäännön 3.13 ja renkaan R kommutatiivisuuden mukaan $q_1 r = r q_1 = 1$, eli $q_1 \in R^\times$. Tämä on ristiriita, jolloin pätee $(r) \subset (r_1)$.

Nyt, jos alkiot r_1 ja q_1 ovat supistamattomia, niin alkiolla r on taas haluttu esitys. Oletetaan siis, että ainakin alkio r_1 ei ole supistumaton. Tällöin vastaavasti $r_1 = r_2 q_2$, joillain $r_2, q_2 \in R$, $r_2, q_2 \notin R^\times$, jolloin aikaisemman päättelyn mukaan pätee myös $(r_1) \subset (r_2)$, jolloin $(r) \subset (r_1) \subset (r_2)$. Näin jatkamalla jokainen askel jonka tuloalkiot ovat supistamattomia antaa pääideaalin, joka sisältää aikaisempien askelien ideaalit. Täten, jos alkion r edellä oleva tuloesityksen konstruktio ei pääty äärellisen monen askeleen jälkeen, niin saamme äärettömän aidosti kasvavan pääideaalien ketjun

$$(r) \subset (r_1) \subset (r_2) \subset \cdots .$$

Tällöin, koska lemman 3.49 mukaan kyseisellä kasvavalla pääideaalialueen ideaalien ketjulla on yläraja (r_n), jollain $n \in \mathbb{Z}^+$, niin edellä oleva päättelyketju loppuu äärellisen monen askeleen jälkeen, jolloin r voidaan esittää pääideaalialueen R supistumattomien alkioiden äärellisenä tulona.

Osoitetaan seuraavaksi, että kyseinen tuloesitys on yksikäsitteinen yksiköllä kertomista vaille. Olkoon $r = p_1p_2 \dots p_n = q_1q_2 \dots q_m$ alkion $r \in R$ renkaan R supistamattomien tekijöiden p_1 ja q_i muodostamat tuloesitykset jollain $n, m \in \mathbb{Z}^+$, missä $m \geqslant n$. Nyt, jos $n = 1$, niin $p_1 = q_1q_2 \dots q_m$, eli $p_1 \mid q_1q_2 \dots q_m$. Nyt, koska lauseen 3.47 mukaan pääideaalialueen supistumattomat tekijät ovat täsmälleen alkulukuja, niin 3.46 mukaan jakoyhtälöstä $p_1 \mid q_1q_2 \dots q_m$ seuraa, että $p_1 \mid q_i$, jollain $j \in \{1, \dots, m\}$. Järjestetään alkiot $q_1, q_2, \dots, q_m$ siten, että $p_1 \mid q_1$. Tällöin $q_1 = up_1$, jollain $u \in R$. Täten, koska alkio q_1 on supistamaton, niin u tai p_1 on renkaan R yksikkö. Koska p_1 ei voi olla supistamattomana alkiona yksikkö, niin u on renkaan R yksikkö. Tällöin

$$p_1 = q_1q_2 \dots q_m = up_1q_2 \dots q_m = p_1(uq_2 \dots q_m),$$

jolloin kokonaisalueen R supistussäännön 3.13 mukaan $uq_2 \dots q_m = 1$. Nyt, jos $m > n$, niin $1 = (uq_2 \dots q_{j-1}q_{j+1} \dots q_m)q_j$, jolloin $1 \in (q_j)$, eli $(q_j) = R$ kaikilla $j \in \{2, \dots, m\}$. Tämä on ristiriita, sillä määritelmän mukaan alkulukuja q_j vastaavat ideaalit (q_j) ovat alkuideaaleja kaikilla $j \in \{2, \dots, m\}$. Täten $m = 1$.

Oletetaan nyt, että väite pätee jollain $n > 1$ eli, että jos alkiolla r on supistamattomien alkioiden esitykset

$$r = p_1p_2 \dots p_n = q_1q_2 \dots q_m,$$

missä $m \geqslant n$, niin $n = m$, sekä alkiot q_i voidaan järjestää siten, että $p_i = u_iq_i$, jossa $u_i \in R^\times$ kaikilla $i \in \{1, \dots, n\}$. Tällöin, jos alkiolla $r \in R$ on supistamattomien alkioiden esitys $r = p_1p_2 \dots p_np_{n+1} = q_1q_2 \dots q_m$ jollain $m \geqslant n + 1$, niin vastaavan päättelyn nojalla on alkioiden $q_1q_2 \dots q_m$ järjestys siten, että $p_{n+1} \mid q_1q_2 \dots q_m$. Näin ollen $p_{n+1} = uq_m$, jollain yksiköllä $u \in R$, sekä

$$p_1p_2 \dots q_n = uq_1q_2 \dots q_{m-1}.$$

Tällöin induktio-oletuksen mukaan $n = m - 1$, eli $n + 1 = m$, sekä on alkioiden $q_1, \dots, q_m$ järjestys siten, että $p_i = u_iq_i$, missä u_i on renkaan R yksikkö kaikilla $i \in \{1, \dots, n\}$, jolloin kyseinen esitys on olemassa kaikilla $i \in \{1, \dots, n + 1\}$. Täten siis väite pätee kaikilla $n \in \mathbb{Z}^+$. □

Pääideaalialueen kommutatiivisuuden nojalla jokaisella pääideaalialueen R alkiolla $x \in R$ on yksikäsitteinen alkulukujen $p_1, \dots, p_n$ tuloesitys $x = up_1^{\alpha_1} \dots p_n^{\alpha_n}$, jossa $\alpha_1, \dots, \alpha_n \in \mathbb{Z}^+$ ovat alkulukujen p_i potenssit. Koska edellisen lauseen perusteella kokonaislukujen rengas $\mathbb{Z}$ on myös pääideaalialueena yksikäsitteisen tekijäjaon alue, niin edellisen lauseen seurauksena saadaan myös aritmetiikan peruslause [**2**, s. 289].

LUKU 4

Moduulit

Tässä kappaleessa käsittelemme moduuleja ja niiden perusominaisuuksia. Kuten ryhmien ja renkaiden voidaan ajatella olevan kokonaislukujen yhteenlaskun sekä kertolaskun yleistyksiä mielivaltaisille joukoille ja laskutoimituksille, niin moduulit pyrkivät yleistämään vektoriavaruuksien rakenteen yleisille kerroinrenkaille ja skalaarituloille. *Vektoriavaruudet* ovat tunnetusti joukkoja, joiden alkioiden, eli *vektoreiden*, välillä on määritelty kommutatiivinen yhteenlasku. Vektoreiden ja vektoriavaruuden *kerroinkunnan* alkioiden, joita kutsutaan monesti *kertoimiksi* tai *skalaareiksi*, välillä on myös määritelty *skalaarituloksi* kutsuttu kuvaus, joka liittää jokaiseen kertoimeen ja vektoriin jonkin vektorin. Moduulit pyrkivät yleistämään vastaavan rakenteen mielivaltaisille renkaille ja laskutoimituksille, jotka toteuttavat vektoreiden tunnetut laskusäännöt. Kappale perustuu lähteisiin [**1**], [**2**] ja [**4**].

4.1. Moduulit ja alimoduulit

Kuntakertoimiset vektoriavaruudet määritellään seuraavasti. [**1**, s. 86]

MÄÄRITELMÄ 4.1. Olkoon K kunta. Tällöin $(V, K, +, \cdot)$ on *K-kertoiminen vektoriavaruus*, jos $+$ on joukon V laskutoimitus ja $\cdot$ on *skalaarituloksi* kutsuttu kuvaus $K \times V \to V$, $(\lambda, v) \mapsto \lambda v$ siten, että $(V, +)$ on abelin ryhmä ja kaikille $v, w \in V$, sekä $a, b \in K$ pätee

(1) $(a + b)v = av + bv$,
(2) $a(v + w) = av + aw$,
(3) $(ab)v = a(bv)$, sekä
(4) $1_K v = v$.

Laajennetaan seuraavaksi kuntakertoimisen vektoriavaruuden määritelmä mielivaltaisille renkaille ja niiden skalaarituloja muistuttaville kuvauksille.

MÄÄRITELMÄ 4.2. Olkoon R rengas. *Vasen R-moduuli* on additiivinen abelin ryhmä $(M, +)$ varustettuna kuvauksella $R \times M \to M$, $(r, m) \mapsto rm$ siten, että kaikilla $r, s \in R$ ja $m, n \in M$ pätee

(1) $(r + s)m = rm + sm$,
(2) $r(m + n) = rm + rn$,
(3) $(rs)m = r(sm)$, sekä
(4) $1_R m = m$.

Jatkossa kutsumme vasempia R-moduuleja pelkästään R-moduuleiksi, moduuleiksi yli renkaan R tai pelkästään moduuleiksi, jos rengas R on konteksista selvää. Kuvausta $(r, m) \mapsto rm$ kutsutaan monesti renkaan R *toiminnaksi* joukossa M tai vain vektoriavaruuksia mukaillen *tuloksi*. Tarkastellaan seuraavaksi joitain moduulien perusominaisuuksia.

LAUSE 4.3. *Olkoon R rengas ja M R-moduuli. Tällöin kaikilla $r \in R$ ja $m \in M$ pätee*

(1) $0_R m = 0_M$,
(2) $r0_M = 0_M$,
(3) $(-1_R)m = -m$, *sekä*
(4) $r(-m) = -rm$.

TODISTUS. (1) R-moduulin M toiminnan määritelmän kohdan (1) ja renkaan R ominaisuuksien mukaan

$$\begin{aligned} 0_R m &= (0_R + 0_R)m \\ &= 0_R m + 0_R m. \end{aligned}$$

Nyt, koska määritelmän mukaan $0_R m \in M$ ja M on abelin ryhmä, niin vähentämällä puolittain $0_R m$ saadaan $0_R m = 0_M$.

(2) R-moduulin M toiminnan määritelmän kohdan (1) ja abelin ryhmän M ominaisuuksien mukaan

$$\begin{aligned} r0_M &= r(0_M + 0_M) \\ &= r0_M + r0_M. \end{aligned}$$

Nyt, koska $r0_M \in M$, niin vähentämällä puolittain 0_M saadaan $r0_M = 0$.

(3) Koska kohdan (1) mukaan $0_R m = 0_M$, kaikilla $r \in R$ ja $m \in M$, niin moduulin M toiminnan määritelmän kohtien (1) ja (4) mukaan

$$\begin{aligned} 0_M &= 0_R m \\ &= (1_R - 1_R)m \\ &= 1_R m + (-1_R)m \\ &= m + (-1_R)m, \end{aligned}$$

josta vähentämällä puolittain m saadaan $(-1_R)m = -m$.

(4) Edellisten kohtien mukaan pätee

$$\begin{aligned} 0_M &= r0_M \\ &= r(m - m) \\ &= rm + r(-m), \end{aligned}$$

josta vähentämällä puolittain saadaan $r(-m) = -rm$. □

MÄÄRITELMÄ 4.4. Olkoon M R-moduuli. Moduulin M R-alimoduuli on ryhmän M aliryhmä N, jolle $rn \in N$ kaikilla $r \in R$ ja $n \in N$.

LAUSE 4.5 (Alimoduulitesti). *Olkoon R rengas ja M R-moduuli. Tällöin osajoukko $N \subset M$ on moduulin M alimoduuli jos ja vain jos*

(1) $N \neq \varnothing$,
(2) $x + ry \in N$ *kaikilla* $r \in R$ *ja* $x, y \in N$.

TODISTUS. Olkoon $N \subset M$ alimoduuli. Tällöin, koska joukko N varustettuna indusoidulla laskutoimituksella on abelin ryhmän $(M, +)$ aliryhmä, niin erityisesti $0 \in N$, eli $N \neq \varnothing$. Olkoot $x, y \in N$ ja $r \in R$. Koska alimoduulin määritelmän mukaan $ry \in N$ ja N on aliryhmänä ryhmä, niin $x + ry \in N$.

Oletetaan, että ehdot (1) ja (2) pätevät. Olkoot $x, y \in N$ ja $r \in R$. Tällöin, koska $N \neq \varnothing$ niin on olemassa jokin $x \in N$, jolloin ehdon (2) ja lauseen 4.3

mukaan $0 = x-x = x+(-1)x \in N$. Tällöin alimoduulitestin kohdan (2) mukaan $ry = 0+ry \in N$. Koska $1 \in R$, niin renkaan määritelmän mukaan $-1 \in R$, jolloin lauseen 4.3 mukaan $x - y = x + (-1)y \in N$. Näin ollen aliryhmätestin 2.13 mukaan N on abelin ryhmän M aliryhmä. Koska N on ryhmän M aliryhmä, niin erityisesti $0 \in N$, jolloin ehdon (2) mukaan $ry = 0 + ry \in N$ kaikilla $y \in N$ ja $r \in R$. Täten N on moduulin M alimoduuli.

□

Esimerkki 4.6. Jos K on kunta, niin K kertoiminen vektoriavaruus V on yleisen määritelmän 4.1 mukaisesti täsmälleen K-moduuli. Täten myös vektoriavaruuden V aliavaruudet ovat täsmälleen vastaavan K-moduulin alimoduuleja.

Esimerkki 4.7. Renkaan määritelmän 3.1 mukaan rengas $(R, +, \cdot)$ on R-moduuli varustettuna kerto- ja yhteenlaskutoimituksillaan. Täten R-moduulin R alimoduulit ovat määritelmän mukaan täsmälleen ne renkaan R aliryhmät I joilla $rx \in I$ kaikilla $x \in R$, eli toisin sanoen renkaan R vasemmat ideaalit. Näin ollen kommutaatiivisen renkaan alimoduulit ovat täsmälleen sen ideaaleja.

Esimerkki 4.8. Olkoon A additiivinen abelin ryhmä. Tällöin $(A, +, \cdot)$ on $\mathbb{Z}$-moduuli, kun määritellään toiminta $\cdot : \mathbb{Z} \times A \to A$ siten, että kaikilla $n \in \mathbb{Z}$ ja $a \in A$ pätee

$$na = \begin{cases} \sum_{i=1}^{n} a & n > 0 \\ \sum_{i=1}^{n} (-a) & n < 0 \\ 0 & n = 0. \end{cases}$$

Tarkistetaan, että moduulin määritelmän 4.2 kohdat (1)–(4) pätevät kyseisellä toiminnalla. Olkoon $x, y \in \mathbb{Z}$ ja $a, b \in A$. Tällöin, jos $r, s > 0$, niin

(1) $(x + y)m = \sum_{i=1}^{x+y} m = \sum_{i=1}^{x} m + \sum_{i=1}^{y} m = xm + ym$,
(2) $(xy)m = \sum_{i=1}^{xy} m = \sum_{i=1}^{x} (\sum_{i=1}^{y} m) = \sum_{i=1}^{x} (ym) = x(ym)$,
(3) $x(a + b) = \sum_{i=1}^{x} (a + b) = \sum_{i=1}^{x} a + \sum_{i=1}^{x} b = xa + xb$ ja
(4) $1a = \sum_{i=1}^{1} a = a$.

Tapaus $n < 0$ saadaan kertomalla saatuja yhtälöitä luvulla -1 ja tapaus $n = 0$ on selvä lauseen 4.3 nojalla. Näin ollen jokainen abelin ryhmä on $\mathbb{Z}$ moduuli. Nyt, koska jokainen $\mathbb{Z}$ on määritelmän mukaan erityisesti abelin ryhmä, niin abelin ryhmät ovat täsmälleen $\mathbb{Z}$ moduuleja.

4.2. Moduulien isomorfisuus ja tekijämoduulit

Määritellään R-moduulien väliset morfismit ryhmä- ja rengasteorian määritelmiä mukaillen.

Määritelmä 4.9. Olkoon R rengas ja M sekä N R-moduuleja. Tällöin kuvaus $\varphi : M \to N$ on *R-moduulihomomorfismi*, jos

(1) $\varphi(x + y) = \varphi(x) + \varphi(y)$ ja
(2) $\varphi(rx) = r\varphi(x)$, kaikilla $x, y \in M$ ja $r \in R$.

Bijektiivinen R-moduulihomomorfismi on *R-moduuli isomorfismi*. Jos φ on R-moduuli isomorfismi, niin sanotaan, että moduulit M ja N ovat *isomorfiset* ja merkitään $M \cong N$. R-moduulihomomorfismin φ *ydin* on joukko

$$\ker \varphi = \{m \in M \mid \varphi(m) = 0\}.$$

Merkitään kaikkien R-moduulihomomorfismien $\varphi : M \to N$ joukkoa

$$\mathrm{Hom}_R(M, N) = \{\varphi : M \to N \mid \varphi \text{ on homomorfismi}\}.$$

Jos on selvää, että φ on R-moduulien välinen morfismi, niin sitä kutsutaan yleensä vain homo- tai isomorfismiksi.

Määritelmän mukaan R-moduulihomomorfismit ovat täsmälleen vastaavien abelin ryhmien välisiä ryhmähomomorfismeja jotka toteuttavat myös ehdon (2). Näin ollen monet ryhmähomomorfismien ominaisuuksista saadaan pätemään myös moduuleille, kunhan osoitetaan, että kyseessä oleva toiminta toteuttaa vaaditut ominaisuudet.

LAUSE 4.10. *Olkoon $\varphi : M \to N$ R-moduulihomomorfismi. Tällöin, jos M' ja N' ovat vastaavasti R-moduulien M ja N alimoduuleja, niin*

(1) kuvajoukko $\varphi(M') \subseteq N$ on moduulin N alimoduuli, sekä
(2) alkukuva $\varphi^{-1}(N') \subseteq M$ on moduulin M alimoduuli.

TODISTUS. Lauseen 2.22 mukaan väite pätee ryhmien tapauksessa. Nyt, koska alimoduulit ovat määritelmän mukaan abelin additiivisen ryhmän aliryhmiä, jotka ovat suljettuja moduulin toiminnan suhteen, niin riittää osoittaa, että kyseessä olevat aliryhmät ovat suljettuja toiminnan suhteen. Olkoon $x \in \varphi(M')$ ja $r \in R$. Tällöin on $y \in M'$ siten, että $\varphi(x) = y$, joten

$$\begin{aligned} rx &= r\varphi(y) \\ &= \varphi(ry) \in \varphi(M'), \end{aligned}$$

sillä M' on moduulin M alimoduuli. Vastaavalla päättelyllä nähdään myös, että $rx \in \varphi^{-1}(N')$ kaikilla $r \in R$, $x \in \varphi^{-1}(N')$, jolloin kyseiset aliryhmät ovat myös alimoduuleja. □

LAUSE 4.11. *Olkoon R rengas ja N R-moduulin M alimoduuli. Abelin tekijäryhmä M/N varustettuna yhteenlaskulla $+$ ja jäännösryhmän renkaan R toiminnalla tekijäryhmään M/N, jolle pätee*

$$r(x + N) = (rx) + N, \qquad \text{kaikille } r \in R,\ x + N \in M/N,$$

on R-moduuli. Lisäksi luonnollinen projektio $\pi : M \to M/N$, $\pi(x) = x + N$ on surjektiivinen R-moduulihomomorfismi, jonka ydin $\ker \pi$ on alimoduuli N.

TODISTUS. Koska M on R-moduulina abelin ryhmä ja alimoduulin määritelmän 4.4 mukaan alimoduuli N on sen aliryhmä, niin lauseen 2.12 mukaan N on myös abelin ryhmä. Tällöin lauseen 2.19 mukaan N on ryhmän M normaali aliryhmä, jolloin seurauksen 2.34 mukaan jäännösryhmä M/N on hyvin määritelty. Näin ollen tekijämoduuli M/N on myös hyvin määritelty, eli riittää osoittaa, että toiminta $r(x + N)$ on hyvin määritelty ja toteuttaa R-moduulin määritelmän ehdot (1)–(4).

Olkoon $x, y \in M$ ja $r \in R$. Koska rx on R-moduulin M toiminta $R \times M \to M$, niin erityisesti $rx \in M$, jolloin $(rx) + N \in M/N$. Näin ollen $r(x + N) = (rx) + N$ on todellakin kuvaus $R \times M/N \to M/N$. Olkoon $x, y \in M$ saman tekijämoduulin M/N sivuluokan edustajia, eli $x + N = y + N$. Tällöin

$$x - y + N = 0 + N = N,$$

eli $x-y \in N$. Nyt, koska N on moduulin M alimoduulina R-moduuli, niin määritelmän 4.4 mukaan $r(x-y) \in N$, jolloin lauseen 4.3 ja moduulin määritelmän mukaan

$$\begin{aligned} rx - (ry) &= rx + r(-y) \\ &= r(x-y) \in N. \end{aligned}$$

Tällöin lauseen 2.28 mukaan $rx + N = ry + N$, eli toiminta $r(x+N)$ on hyvin määritelty.

Olkoon $r, s \in R$ ja $x, y \in M$. Osoitetaan seuraavaksi, että tekijämoduulin toiminta $r(x+N) = (rx)+N$ toteuttaa moduulin määritelmän kohdat (1)–(4). Koska rx on R-moduulin M toiminta, niin saadaan

$$\begin{aligned} (r+s)(x+N) &= (r+s)x + N \\ &= (rx+sx) + N \\ &= (rx+N) + (sx+N) \\ &= r(x+N) + s(x+N), \end{aligned} \tag{1}$$

$$\begin{aligned} (rs)(x+N) &= (rs)x + N \\ &= r(sx) + N \\ &= r(sx+N) \\ &= r(s(x+N)), \end{aligned} \tag{2}$$

$$\begin{aligned} r((x+N)+(y+N)) &= r((x+y)+N) \\ &= r(x+y) + N \\ &= (rx+ry) + N \\ &= (rx+N) + (ry+N) \\ &= r(x+N) + r(y+N), \text{ sekä} \end{aligned} \tag{3}$$

$$1(x+N) = (1x) + N = x + N. \tag{4}$$

Näin ollen tekijämoduuli M/N on R-moduuli.

Osoitetaan lisäksi, että π on surjektiivinen R-moduulihomomorfismi jonka ydin on N. Koska $N \trianglelefteq M$, niin π on abelin ryhmän M luonnollinen projektio tekijäryhmälle M/N ja täten lauseen 2.33 mukaan π on surjektiivinen ryhmähomomorfismi, jolle pätee $\ker \pi = N$. Riittää siis näyttää, että $\pi(rm) = r\pi(m)$ kaikilla $m \in M$, $r \in R$. Toiminnan $r(x+N)$ määritelmän mukaan

$$\begin{aligned} \pi(rm) &= rm + N \\ &= r(m+N) \\ &= r\pi(m), \end{aligned}$$

joten π on myös R-moduulihomomorfismi, joka todistaa väitteen. □

Tarkastellaan seuraavaksi moduulien isomorfismilauseita. Edellisen lauseen todistuksessa huomasimme että, koska R-moduulin $(M, R, +, \cdot)$ aliryhmä N on

abelin ryhmän aliryhmänä abelin ryhmä, niin N on myös lauseen 2.19 mukaan additiivisen ryhmän $(M, +)$ normaali aliryhmä. Näin ollen monet ryhmäteorian normaaleja aliryhmiä koskevista tuloksista voidaan yleistää moduuleja koskeviksi, kunhan osoitamme, että moduulien toiminnat toteuttavat halutut ehdot.

LAUSE 4.12 (Moduulien ensimmäinen isomorfismilause). *Olkoot M, N R-moduuleja, sekä $\varphi : M \to N$ R-moduulihomomorfismi. Tällöin $\ker\varphi$ on moduulin M alimoduuli ja $M/\ker\varphi \cong \varphi(M)$.*

TODISTUS. Koska M on abelin ryhmä ja φ on ryhmähomomorfismi, niin $\ker\varphi$ on ryhmän M aliryhmänä abelin ryhmä. Tällöin $\ker\varphi$ on normaali aliryhmä, eli $M/\ker\varphi$ on hyvin määritelty. Nyt, koska ryhmien ensimmäinen isomorfismilause 2.35 antaa ryhmien välisen isomorfismin $\phi : M/\ker\varphi \to \varphi(M)$, jossa $\phi(x + \ker\varphi) = \varphi(x) + \ker\varphi$, niin riittää osoittaa, että ϕ on myös R-moduulihomomorfismi. Täten riittää osoittaa, että kaikilla $x + \ker\varphi \in M/\ker\varphi$ pätee

$$\phi(r(x + \ker\varphi)) = r\phi(x + \ker\varphi).$$

Olkoon $x + \ker\varphi \in M/\ker\varphi$. Koska M on R-moduuli ja φ on moduulihomomorfismi, niin

$$\begin{aligned}\phi(r(x + \ker\varphi)) &= \phi(rx + \ker\varphi)\\ &= \varphi(rx)\\ &= r\varphi(x)\\ &= r(\varphi(x))\\ &= r\phi(x + \ker\varphi).\end{aligned}$$

Näin ollen ϕ on ryhmäisomorfismi $M/\ker\varphi \to \varphi(M)$, joka toteuttaa moduulihomomorfismin määritelmän kohdan (2), eli ϕ on R-moduulien välinen isomorfismi ja $M/\ker\varphi \cong \varphi(M)$. □

LAUSE 4.13. *Olkoon $\varphi : M \to N$ surjektiivinen R-moduulihomomorfismi, sekä $N' \subset N$ alimoduuli. Tällöin $M/\varphi^{-1}(N') \cong N/N'$.*

TODISTUS. Koska M ja N ovat R-moduuleina abelin ryhmiä ja φ on surjektiivisena R-moduulihomomorfismina surjektiivinen ryhmähomomorfismi, niin lauseen 2.37 mukaan kuvaus $\pi \circ \varphi : M \to N/N'$, jossa π on luonnollinen projektio $G \to M/\varphi^{-1}(N')$, on surjektiivinen ryhmähomomorfismi, joka määrää isomorfismin $M/\varphi^{-1}(N') \cong N/N'$. Nyt, koska luonnollinen projektio π on lauseen 4.11 mukaan myös surjektiivinen R-moduulihomomorfismi, niin $\pi \circ \varphi$ on myös surjektiivinen R-moduulihomomorfismi, jolloin lauseen 2.37 päättely antaa moduulien ensimmäisen isomorfismilauseen 4.12 mukaan halutun isomorfismin. □

4.3. Vapaat moduulit ja suorat summat

Seuraavaksi yleistämme vektoriavaruuksien lineaarisen riippumattomuuden ja kannan käsitteet [**1**, s. 87] yleisille moduuleille. Aloitamme määrittelemällä viritetyn moduulin käsitteen viritetyn ryhmän ja viritetyn renkaan määritelmiä 2.14 ja 3.22 mukaillen.

MÄÄRITELMÄ 4.14. Olkoon M R-moduuli ja $A \subseteq M$. Tällöin renkaan R ja joukon A alkioiden välisistä tuloista ra, $r \in R$, $a \in A$ koostuvien äärellisten summien joukko

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ka_k \mid r_i \in R,\, a_i \in A,\, k \in \mathbb{Z}^+\},$$

on *joukon A virittämä alimoduuli*, jossa $RA = \{0\}$, jos $A = \varnothing$. Jos A on äärellinen joukko $\{a_1, a_2, \ldots, a_k\}$, niin merkitään $RA = Ra_1 + Ra_2 + \cdots + Ra_k$.

Jos N on R-moduulin M alimoduuli siten, että $N = RA$, jollain $A \subseteq M$ niin sanotaan, että A *on alimoduulin N virittäjien joukko* tai, että A *virittää alimoduulin N*. Tällöin jokainen $n \in N$ voidaan esittää joukon A alkioiden *lineaarikombinaationa*, eli äärellisenä summana

$$n = r_1a_1 + r_2a_2 + \cdots + r_ka_k,$$

jossa $r_i \in R$, sekä $a_i \in A$ jollain $k \in \mathbb{Z}^+$.

Jos N on R-moduulin M äärellisen joukon $A \subseteq M$ virittämä, niin sanotaan, että N on *äärellisesti viritetty*. Moduulin M alimoduuli N on *syklinen* moduuli, jos se on yhden alkion virittämä, eli jos on olemassa jokin $a \in M$ siten, että $N = Ra = \{ra \mid r \in R\}$.

MÄÄRITELMÄ 4.15. Olkoon M R-moduuli ja $A \subseteq M$. Jos jokaiselle äärelliselle osajoukolle $\{a_1, a_2, \ldots, a_n\} \subseteq A$, jossa $a_i \neq a_j$ kaikilla $i, j \in \{1, \ldots n\}$ pätee, että yhtälöstä

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 0, \text{ joillain } r_i \in R,$$

seuraa $r_i = 0$ kaikilla $i \in \{1, \ldots, n\}$, niin joukko A on *lineaarisesti riippumaton*. Jos joukko ei ole lineaarisesti riippumaton, niin sanotaan, että se on *lineaarisesti riippuva*.

Määritelmästä seuraa suoraan, että lineaarisesti riippumattoman joukon jokainen osajoukko on myös lineaarisesti riippumaton, sillä jokainen osajoukon alkioiden lineaarikombinaatio on myös kyseisen lineaarisesti riippumattoman joukon alkioiden lineaarikombinaatio.

MÄÄRITELMÄ 4.16. Moduulin M *kanta* on sen osajoukko $A \subseteq M$, joka on lineaarisesti riippumaton ja virittää moduulin M. Moduulia, jolla on kanta kutsutaan *vapaaksi moduuliksi*.

MÄÄRITELMÄ 4.17. Olkoon R on kommutatiivinen rengas. Tällöin vapaan R-moduulin M *aste* $\operatorname{rank}(M)$ on sen jonkin kannan mahtavuus.

Tulemme myöhemmin osoittamaan, että kommutatiivisen renkaan äärellisesti viritetyn vapaan moduulin aste on yksikäsitteinen. Tarkastellaan seuraavaksi moduulin kannan ominaisuuksia.

ESIMERKKI 4.18. Esimerkin 2.15 mukaan $\mathbb{Z}$-moduulin $\mathbb{Z}$ kanta on $\{1\}$, sillä yhden nollasta poikkeavan alkion joukko on aina lineaarisesti riippumaton. Eräs $\mathbb{R}$-moduulin $\mathbb{R}^2$, eli vektoriavaruuden $\mathbb{R}^2$ kannoista on esimerkiksi joukko $\{(1,0),(0,1)\}$. Äärellisesti viritetyllä syklisellä $\mathbb{Z}$-moduulilla $\mathbb{Z}/n\mathbb{Z}$, $n > 1$ ei ole kantaa, sillä kaikilla $x \in \mathbb{Z}/n\mathbb{Z}$ pätee $n(x + n\mathbb{Z}) = nx + n\mathbb{Z} = 0_{\mathbb{Z}/n\mathbb{Z}}$, jolloin mikä vain moduulin $\mathbb{Z}/n\mathbb{Z}$ virittävien alkioiden lineaarikombinaatioista saadaan nollaksi kertoimilla $n \in \mathbb{Z}^+$.

ESIMERKKI 4.19. Olkoon $\{0\}$ *triviaali R-moduuli*, jota usein kutsutaan myös *nolla moduuliksi*. Tällöin, koska viritetyn moduulin määritelmän 4.14 mukaan tyhjä joukko virittää nolla moduulin M ja joukossa $\varnothing$ ei ole lineaarisesti riippuvia alkioita, niin tyhjä joukko $\varnothing$ on nolla moduulin $\{0\}$ kanta.

Koska $0 = \sum_{i=1}^{n} 0a_i$, kaikilla $i \in \{1, \ldots, n\}$, niin vapaan moduulin nolla-alkiolla ei ole koskaan yksikäsitteistä kannan alkioiden lineaarikombinaatioesitystä, ellei summattavien termien määrää kiinnitetä. Seuraava lause kuitenkin osoittaa, että jokaisella nollasta poikkeavalla vapaan modulin alkiolla on olemassa kyseinen lineaarikombinaatio esitys.

LAUSE 4.20. *Olkoon M R-moduuli ja $A \subseteq M$ sen kanta. Tällöin $0 \notin A$ ja jokaisella $x \in M - \{0\}$ on yksikäsitteinen esitys $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, jossa $r_i \in R\{0\}$ ja $a_i \in A$.*

TODISTUS. Olkoon $x \in M - \{0\}$. Koska A on moduulin M kanta, niin alkiolla x on esitys $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, joillain $r_i \in R$, $a_i \in A$ ja $n \in \mathbb{Z}^+$. Oletetaan, että tämä esitys ei ole yksikäsitteinen. Tällöin alkiolla x on myös esitys

$$x = s_1b_1 + s_2b_2 + \cdots + s_mb_m$$

joillain $s_i \in R$, $b_i \in A$, $m \in \mathbb{Z}^+$. Koska $0 = 0a_1 + 0a_2 + \cdots + 0a_n + r0$ kaikilla $a_1, a_2, \ldots, a_n \in A$, $r \in R$, niin nolla on aina lineaarisesti riippuva alkio. Näin ollen $0 \notin A$, eli erityisesti $a_i, b_j \neq 0$ kaikilla $i \in \{1, \ldots, n\}$ ja $j \in \{1, \ldots, m\}$. Samoin voidaan olettaa, että $r_i, s_i \neq 0$ kaikilla i, j, sillä muuten alkiot r_i, s_i voitaisiin vain unohtaa kyseisistä esityksistä. Täten on nollasta poikkeavat alkiot $r_i, s_i \in R$, $a_i, b_i \in A$ siten, että

$$x = r_1a_1 + r_2a_2 + \cdots + r_na_n = s_1b_1 + s_2b_2 + \cdots + s_mb_m,$$

jolloin, abelin ryhmän M ominaisuuksien mukaan

$$0 = r_1a_1 + r_2a_2 + \cdots + r_na_n - (s_1b_1 + s_2b_2 + \cdots + s_mb_m).$$

Olkoon $A_a = \{a_1, \ldots, a_n\}$ ja $A_b = \{b_1, \ldots, b_m\}$. Tällöin, jos $A_a \cap A_b = \varnothing$, niin $a_i \neq b_j$ kaikilla $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$. Täten edellinen yhtälö on kannan A äärellisen osajoukon $A_a \cup A_b$ erillisten alkioiden lineaarikombinaatio, jolloin kannan lineaarinen riippuvuus takaa, että kertoimille $r_i, s_i \in R$ pätee $r_i = 0 = s_i$ kaikilla i, j. Tällöin siis $x = 0$, joka on ristiriita.

Täten pätee $A_a \cap A_b \neq \varnothing$. Järjestetään joukot A_a ja A_b siten, että luvulla $k \in \{1, \ldots, \min\{n, m\}\}$ pätee $a_i, b_i \in A_a \cap A_b$ ja $a_i = b_i$ kaikilla $i \leqslant k$. Tällöin

$$0 = \sum_{i=1}^{k}(r_i - s_i)a_i + \sum_{i=k+1}^{n} r_ia_i + \sum_{i=k+1}^{m} s_ib_i.$$

Näin ollen, koska kyseessä on taas äärellinen lineaarikombinaatio erillisistä kannan alkioista, niin $r_i = 0$ kaikilla $k + 1 \leqslant i \leqslant n$, $s_i = 0$ kaikilla $k + 1 \leqslant i \leqslant m$ ja $r_i = s_i$ kaikilla $1 \leqslant i \leqslant k$. Täten alkion x esitykset ovat täsmälleen samat, eli haluttu lineaarikombinaatioesitys on yksikäsitteinen. □

Seuraava lause osoittaa, että vapaiden moduulien väliset isomorfismit kuvaavat kannat kannoiksi.

LAUSE 4.21. *Olkoot M ja N vapaita R-moduuleja ja $\varphi : M \to N$ niiden välinen isomorfismi. Tällöin φ kuvaa moduulin M kannan joksikin moduulin N kannaksi.*

TODISTUS. Olkoon A moduulin M kanta. Tällöin jos alkioille $a_1, \ldots, a_n \in A$ ja $r_1, \ldots, r_n \in R$ pätee

$$r_1\varphi(a_1) + \ldots r_n\varphi(a_n) = 0_N,$$

niin isomorfismin φ ominaisuuksien mukaan $\varphi(r_1a_1 + \cdots + r_na_n) = 0_N$. Nyt, koska φ on injektio, niin $r_1a_1 + \ldots r_na_n = 0_M$, jolloin alkioiden $a_1, \ldots, a_n$ lineaarisen riippumattomuuden nojalla $r_i = 0$ kaikilla $i \in \{1, \ldots, n\}$. Täten $\varphi(A)$ on lineaarisesti riippumaton joukko.

Koska A virittää moduulin M, niin jokaisella $x \in M$ on alkiot $r_1, \ldots, r_n \in R$ ja $a_1, \ldots, a_n \in A$ siten, että $x = r_1a_1 + \cdots + r_na_n$. Tällöin, koska φ on isomorfismi, niin jokaisella $y \in N$ on $x \in M$ siten, että $\varphi(x) = y$, jolloin

$$y = \varphi(x) = \varphi(r_1a_1 + \cdots + r_na_n) = r_1\varphi(a_1) + \cdots + r_n\varphi(a_n),$$

eli joukko $\varphi(A)$ virittää moduulin N. Näin ollen kuvajoukko $\varphi(A)$ on moduulin N kanta. □

Tarkastellaan seuraavaksi miten moduuleista voidaan muodostaa uusia moduuleita ja kuinka moduuli voidaan esittää alimoduuliensa avulla.

MÄÄRITELMÄ 4.22. Olkoon $k \in \mathbb{Z}^+$. R-moduulien $M_1, M_2, \ldots M_k$ *suora tulo* $M_1 \times M_2 \times \cdots \times M_k$ on abelin ryhmien $M_1, M_2, \ldots, M_k$ suora tulo 2.6 varustettuna komponenteittain määritellyllä toiminnalla, jolle pätee

$$r(x_1, x_2, \ldots, x_k) = (rx_1, rx_2, \ldots, rx_k)$$

kaikilla $(x_1, x_2, \ldots, x_k) \in M_1 \times M_2 \times \ldots M_k$ ja $r \in R$, jossa komponentin i toiminta on vastaavan moduulin M_i toiminta kaikilla $i \in \{1, \ldots, k\}$. Moduulin M suoraa tuloa itsensä kanssa merkitään

$$\underbrace{M \times \cdots \times M}_{\text{n kertaa}} = M^n,$$

kaikilla $n \in \mathbb{N}$, jossa määritellään, että $M^0 = \{0\}$.

Tarkastellaan seuraavaksi kuinka R-moduuleiden avulla voidaan rakentaa uusia R-moduuleja, sekä kuinka R-moduulit voidaan esittää alimoduuleittensa avulla.

LAUSE 4.23. *R-moduulien $M_1, M_2, \ldots, M_k$ suora tulo on R-moduuli*

TODISTUS. Määritelmän mukaan R-moduulien suora tulo on abelin ryhmä. Koska $M_1, \ldots, M_k$ ovat R-moduuleja, niin niiden toiminnot toteuttavat moduulin toiminnon vaatimukset (1)–(4). Koska suoran tulon yhteenlasku ja toiminta on määritelty komponenteittain alkioille $(m_1, m_2, \ldots, m_k) \in M_1 \times M_2 \times \ldots M_k$ ja vaatimukset (1)–(4) toteutuvat komponenteittain, niin suoran tulon toiminta toteuttaa R-moduulin toiminnan vaatimukset. □

SEURAUS 4.24. *Olkoon R rengas ja $n \in \mathbb{Z}^+$. Tällöin moduuli R^n on n-asteinen vapaa moduuli, jonka kanta koostuu alkioista $e_i \in R^n$, jossa paikan i alkio on 1 ja muiden paikkojen alkiot ovat nollia kaikilla $i \in \{1, \ldots, n\}$.*

TODISTUS. Edellisen lauseen perusteella R^n on R-moduuli. Koska jokaiselle $(r_1, r_2, \ldots, r_n) \in R^n$ pätee

$$\begin{aligned}(r_1, r_2, \ldots, r_n) &= (r_1, 0, \ldots, 0) + (0, r_2, \ldots, 0) + \cdots + (0, 0, \ldots, r_n)\\ &= r_1(1, 0, \ldots, 0) + r_2(0, 1, \ldots, 0) + \cdots + r_n(0, 0, \ldots, 1),\end{aligned}$$

niin alkiot $(0,\dots,1,\dots,0)$ virittävät moduulin R^n. Edellisestä yhtälöstä nähdään myös, että jos alkioiden e_i mielivaltainen lineaarikombinaatio on nolla, eli muotoa $(0,0,\dots,0)$, niin $r_i = 0$ kaikilla $i \in \{1,\dots,n\}$, eli alkiot e_i ovat lineaarisesti riippumattomat. Täten alkiot e_i muodostavat moduulin R^n kannan. □

MÄÄRITELMÄ 4.25. Vapaan n-asteisen moduulin R^n kantaa $\{e_i \mid i \in \{1,\dots,n\}\}$ kutsutaan sen *luonnolliseksi kannaksi*.

MÄÄRITELMÄ 4.26. R-moduulin M alimoduulien $N_1, N_2, \dots, N_k$ *summa* on joukko

$$N_1 + N_2 + \cdots + N_k = \{a_1 + a_2 + \cdots + a_k \mid a_i \in N_i \text{ kaikilla } i \in \{1,\dots,k\}\}.$$

LAUSE 4.27. *Olkoot $N_1, N_2, \dots N_k$ R-moduulin M alimoduuleja. Tällöin seuraavat väittämät ovat yhtäpitäviä.*

(1) Kuvaus $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$, jossa

$$\pi(a_1, a_2, \dots, a_k) = a_1 + a_2 + \cdots + a_k$$

on isomorfismi, eli $N_1 \times N_2 \times \cdots \times N_k \cong N_1 + N_2 + \cdots + N_k$.

(2) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = \{0\}$ kaikilla $j \in \{1,\dots k\}$.

(3) Jokaisella $x \in N_1 + N_2 + \cdots + N_k$ on yksikäsitteinen esitys

$$x = a_1 + a_2 + \cdots + a_k,$$

jossa $a_i \in N_i$ kaikilla $i \in \{1,\dots,k\}$.

TODISTUS. (1)⇒(2): Oletetaan, että kohta (1) pätee, mutta kohta (2) ei päde. Merkitään $N_{k,j}^+ = N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Tällöin on $a_j \in N_j \cap N_{k,j}^+$, $a_j \neq 0$ eli $a_j \in N_j - \{0\}$, jolla on esitys

$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k.$$

Tällöin alkion $(a_1,\dots,-a_j,\dots,a_k)$ kuva isomorfismissa π on

$$\begin{aligned}\pi(a_1,\dots,-a_j,\dots,a_k) &= a_1 + \cdots + a_{j-1} - a_j + a_{j+1} + \cdots + a_k \\ &= (a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k) - a_j \\ &= a_j - a_j = 0.\end{aligned}$$

Kuitenkin, sillä π on homomorfismi, niin myös $\pi(0) = 0$ joten, koska $a_j \neq 0$, niin myös $(a_1,\dots,-a_j,\dots,a_k) \neq (0_1,\dots,0_k) = 0$. Näin ollen kuvaus π ei ole injektio, joka on ristiriita, eli kohdan (2) väitteen on pädettävä.

(2)⇒(3): Oletetaan, että kohta (2) pätee. Jos nyt on $x \in M$, jolla on esitykset $a_1 + a_2 + \cdots + a_k$ ja $b_1 + b_2 + \cdots + b_k$, niin

$$a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k.$$

Tällöin erityisesti jokaisella $j \in \{1,\dots,k\}$ pätee

$$a_j - b_j = (a_1 - b_1) + \cdots + (a_{j-1} - b_{j-1}) + (a_{j+1} - b_{j+1}) + \cdots + (a_k - b_k).$$

Nyt, koska $a_j - b_j \in N_j$ kaikilla $j \in \{1,\dots,k\}$, niin edellisen yhtälön summa kuuluu joukkoon $N_{k,j}^+$, jolloin $a_j - b_j \in N_j \cap N_{k,j}^+$. Tällöin kohdan (2) mukaan $N_j \cap N_{k,j}^+ = \{0\}$, niin $a_j - b_j = 0$, eli $a_j = b_j$ kaikilla $j \in \{1,\dots,k\}$. Näin ollen alkion x esitykset ovat täsmälleen samat.

(3)⇒(1): Oletetaan, että kohta (3) pätee. Kuvaus π on määritelmän mukaan selvästi R-moduulihomomorfismi. Koska kuvauksen π määritelmän mukaan jokaisen alkion $a_1 + a_2 + \cdots + a_k \in N_1 + N_2 + \cdots + N_k$ alkukuva sisältää alkion

$(a_1, \ldots, a_k) \in M_1 \times \cdots \times M_k$, niin π on surjektiivinen homomorfismi. Tällöin, koska jokainen $x \in N_1 + N_2 + \cdots + N_k$ voidaan esittää yksikäsitteisesti muodossa $x = a_1 + a_2 + \cdots + a_k$, niin π on myös injektio. Näin ollen π on bijektiivinen R-moduulihomomorfismi. □

Koska edellisen lauseen tilanteessa $0 \in N_i$ kaikilla i, niin kohdan (2) tapauksessa tarkastelemalla osajoukkoa

$$N_l = \{a_l \mid a_l \in N_l\} \subset N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k,$$

jollain $l \in \{1, \ldots, k\}$, $l \neq j$, eli asettamalla summan alkiot nollaksi kaikilla muilla, paitsi yhdellä indeksillä saadaan $N_j \cap N_l = \{0\}$ kaikilla $j, l \in \{1, \ldots, k\}$, $l \neq j$. Toisin sanoen, alimoduulit $N_1, \ldots, N_k$ ovat pareittain erillisiä, nollaa lukuunottamatta. Vastaavalla päättelyllä myös edellisen lauseen ehdosta (2) seuraa, $N_j \cap N_l = \{0\}$ kaikilla $j, l \in \{1, \ldots, k\}$, $l \neq j$, joten ehto (2) on yhtäpitävä moduulien pareittaisen erillisyyden kanssa nollaa lukuunottamatta.

MÄÄRITELMÄ 4.28. Jos R-moduuli M on lauseen 4.27 yhtäpätevien ehtojen toteuttavien alimoduuleiden $N_1, \ldots, N_k$ summa, eli $M = N_1 + N_2 + \cdots + N_k$ niin sanotaan, että M on alimoduulien $N_1, \ldots, N_k$ *suora summa*, jota merkitään

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k = \bigoplus_{i=1}^{k} N_i.$$

Edellisen määritelmän R-moduulin M alimoduuleiden $N_1, N_2, \ldots, N_k$ suoraa summaa $N_1 \oplus N_2 \oplus \cdots \oplus N_k$ kutsutaan joskus myös *sisäiseksi suoraksi summaksi*. Samoin, ehkä hieman sekaannusta aiheuttavasti, moduuleiden $N_1, N_2, \ldots, N_k$ suoraa tuloa $N_1 \times N_2 \times \cdots \times N_k$ kutsutaan joskus niiden *ulkoiseksi suoraksi summaksi*, jolloin symbolit $\times$ korvataan symboleilla $\oplus$ [**2**, s. 353], [**4**, s. 60]. Hieman täsmällisemmin ulkoisien suorien summien määritellään olevan suoria tuloja, joissa vain äärellinen määrä tulon tekijöistä on nollasta poikkeavia [**2**, s. 357]. Näin ollen moduulien äärelliset suorat tulot ja ulkoiset suorat summat ovat täsmälleen samat. Koska äärelliset suorat tulot ja summat ovat lauseen 4.27 mukaan isomorfiset, niin kyseessä oleva merkintä ei ole täysin aiheeton. On kuitenkin aiheellista huomioida, että sisäisillä, sekä ulkoisilla suorilla summilla on joitain perustavanlaatuisia eroja.

Suoran tulon määritelmässä vaadittiin vain, että suoran tulon tekijät ovat R-moduuleita. Näin ollen suora tulo tai ulkoinen suora summa yhdistää mielivaltaiset moduulit uudeksi moduuliksi. Kuitenkin sisäinen suora summa olettaa, että summattavat moduulit ovat summa moduulin alimoduuleita, jotka toteuttavat lauseen 4.27 yhtäpitävät ehdot, eli että esimerkiksi niiden leikkaus on nolla-alkio. Tämä merkintä voi aiheuttaa pientä sekaannusta esimerkiksi tarkasteltaessa R-moduulia R ja ulkoista suoraa summaa $R \oplus R$. Tällöin selvästi $R \cap R = R \neq \{0\}$, joten kyseessä ei ole hyvin määritelty sisäinen suora summa. Kuitenkin tulomoduulin $R \times R$ osajoukot $R \times \{0\}$ ja $\{0\} \times R$ ovat selvästi sen alimoduuleita, joiden leikkaus on $(0, 0) = 0_{R \times R}$, jolloin isomorfismit $R \times \{0\} \cong R$ ja $\{0\} \times R \cong R$ takaavat, että sisäinen suora summa on myös hyvin määritelty ja vastaa ulkoista suoraa summaa lauseen 4.27 tavoin. Täten sisäiset- sekä ulkoiset suorat summat ovat aina isomorfisia, jonka vuoksi niistä puhutaan yleensä sekaisin määrittelemättä kummasta on milloinkin kyse.

Tarkastellaan seuraavaksi joitain suorien summien ominaisuuksia.

LAUSE 4.29. *Olkoot $M_1, M_2, \ldots, M_n$ R-moduuleja ja $N_1, N_2, \ldots, N_n$ niiden alimoduuleja. Tällöin*

$$(M_1 \oplus M_2 \oplus \cdots \oplus M_n)/(N_1 \oplus N_2 \oplus \cdots \oplus N_n) \cong M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_n/N_n.$$

TODISTUS. Olkoon $\varphi : M_1 \times \cdots \times M_n \to M_1/N_1 \times \cdots \times M_n/N_n$, kuvaus jossa $(m_1, \ldots, m_n) \mapsto (\pi_1(m_1), \ldots, \pi_n(m_n))$ luonnollisien projektiohomomorfismien $\pi_i : M_i \to M_i/N_i$ avulla. Koska π_i on lauseen 4.12 mukaan surjektiivinen R-moduulihomomorfismi, niin φ on komponenteittain määriteltynä myös surjektiivinen R-moduulihomomorfismi. Koska jokaisen komponentin projektiohomomorfismin ydin $\ker \pi_i = N_i$ kaikilla $i \in \{1, \ldots, n\}$, niin $\varphi(m_1, m_2, \ldots, m_n) = 0$, jos ja vain jos $m_i \in N_i$ kaikilla i, eli $\ker \varphi = N_1 \times \cdots \times N_n$. Näin ollen ensimmäisen isomorfismilauseen mukaan

$$(M_1 \times M_2 \times \cdots \times M_n)/(N_1 \times N_2 \times \cdots \times N_n) \cong M_1/N_1 \times M_2/N_1 \times \cdots \times M_n/N_n.$$

Nyt, koska määritelmän ja lauseen 4.29 mukaan äärelliset suorat tulot ja suorat summat ovat isomorfisia, niin väite pätee myös suorille summille. □

Tarkastellaan seuraavaksi tilannetta, jossa vapaan moduulin kanta on äärellinen joukko, eli moduuli on äärellisesti viritetty vapaa moduuli.

LAUSE 4.30. *Olkoon $\{a_1, a_2, \ldots, a_n\}$ vapaan moduulin M kanta. Tällöin $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.*

TODISTUS. Olkoon $\{a_1, a_2, \ldots, a_n\}$ on moduulin M kanta. Tällöin lauseen 4.20 mukaan jokaisella moduulin alkiolla $x \in M - \{0\}$ on yksikäsitteinen lineaarikombinaatioesitys $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, jossa $r_ia_i \in Ra_i$ kaikilla $i \in \{1, \ldots, n\}$. Samoin myös nolla-alkiolla on yksikäsitteinen n-summatermin lineaarikombinaatio esitys $0 = 0a_1 + 0a_2 + \cdots + 0a_n$. Tällöin, koska kanta virittää moduulin M, niin $M = Ra_1 + Ra_2 + \cdots + Ra_n$, jolloin lauseen 4.27 mukaan kyseessä on suora summa. Sillä kuvaus $R \to Ra_i$, jossa $r \mapsto ra_i$ on isomorfismi kaikilla $i \in \{1, \ldots, n\}$ ja summa $r_1a_1 + r_2a_2 + \cdots + r_na_n$ on yksikäsitteinen, niin kuvaus

$$R^n \to Ra_1 + Ra_2 + \cdots + Ra_n, \qquad \pi(r_1, r_2, \ldots, r_n) = ra_1 + ra_2 + \cdots + ra_n$$

on isomorfismi, jolloin $Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$. □

LAUSE 4.31. *Olkoon M moduuli jolle $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$, joillain $a_i \in R - \{0\}$, $i \in \{1, \ldots, n\}$. Tällöin joukko $\{a_1, a_2, \ldots, a_n\}$ muodostaa moduulin M kannan.*

TODISTUS. Koska M on syklisien moduulien $Ra_1, Ra_1, \ldots, Ra_n$ suora summa, niin lauseen 4.27 mukaan jokaisella $x \in M$ on yksikäsitteinen summaesitys $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, jossa $r_ia_i \in Ra_i$ kaikilla $i \in \{1, \ldots, n\}$. Näin ollen jokainen moduulin M alkio voidaan esittää joukon $\{a_1, a_2, \ldots, a_n\}$ lineaarikombinaationa, eli joukko $\{a_1, a_2, \ldots, a_n\}$ virittää moduulin M. Osoitetaan vielä, että alkiot $a_1, a_2, \ldots, a_n$ ovat lineaarisesti riippumattomat. Jos näin ei ole, niin alkoiden $\{a_1, \ldots, a_n\}$ lineaarikombinaatio $r_1a_1 + r_2a_2 + \cdots + r_na_n$ on nolla siten, että kaikki lineaarikombinaation kertoimet $r_1, r_2, \ldots, r_n \in R$ eivät ole nollia. Olkoon $r_j \neq 0$ jokin tällainen kerroin. Tällöin pätee

$$-r_ja_j = r_1a_1 + \ldots r_{j-1}a_{j-1} + r_{j+1}a_{j+1} \cdots + r_na_n.$$

Näin ollen pätee $(-r_j)a_j \in Ra_j \cap (Ra_1 + \cdots + Ra_{j-1} + Ra_{j+1} + \cdots + Ra_n)$, jossa $(-r_j)a_j \in Ra_j$. Koska $r_j \neq 0$, niin $(-r_j)a_j \neq 0$, jolloin kyseinen leikkausjoukko ei ole nollamoduuli. Tämä on lauseen 4.27 kohdan (2) mukaan ristiriidassa oletuksen $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$ kanssa, joten joukko $\{a_1, a_2, \ldots, a_n\}$ on myös lineaarisesti riippumaton, eli se on moduulin M kanta. □

Näin ollen joukko $\{a_1, a_2, \ldots, a_n\}$ on vapaan moduulin M kanta jos ja vain jos se voidaan esittää syklisien moduulien $Ra_1, Ra_2 \ldots, Ra_n$ suorana summana.

4.4. Vektoriavaruudet

Moduulin määritelmän 4.2 vektoriavaruudet vastaavat täsmälleen kuntakertoimisen moduulin määritelmää. Näin ollen kaikki edellä mainitut moduuliteorian tulokset pätevät myös vektoriavaruuksille.

Koska jokaisella kunnan nollasta poikkeavalla alkiolla on käänteisalkio kyseisen kunnan kertolaskun suhteen, niin vektoriavaruuksilla on kuntakertoimisina moduuleina joitain miellyttäviä ominaisuuksia, jotka eivät päde yleisille moduuleille. Tulemme esimerkiksi osoittamaan, että äärellisesti viritetyllä vektoriavaruudella on aina kanta vaikkakin äärellisesti viritetylle moduulille tämä ei aina päde.

Vektoriavaruuksista puhuttaessa käytetään yleensä niiden seuraavassa määritelmässä esiintyvää terminologiaa.

MÄÄRITELMÄ 4.32. K-kertoiminen *vektoriavaruus* V on K-moduuli, jossa rengas K on kunta. Jos kunta K on kontekstista selvä, niin sanotaan vain, että V on vektoriavaruus tai avaruus. K-moduulin V alkio on vektoriavaruuden V *vektori* ja kunnan K alkio on avaruuden V vektoreiden *kerroin* tai *skalaari*. Vektoriavaruuden V *aliavaruus* A on K-moduulin V alimoduuli. K-kertoimisten vektoriavaruuksien V ja W välinen K-moduulihomomorifismi on vektoriavaruuksien V ja W välinen *lineaarikuvaus*. Jos $B \subset V$ virittää K-moduulin V, niin sanotaan, että B virittää vektoriavaruuden V. Jos V on vapaa K-moduuli, niin vektoriavaruuden V *dimensio* on K-moduulin V aste.

Tarkastellaan seuraavaksi joitain vektoriavaruuksien perusominaisuuksia.

LAUSE 4.33. *Olkoon V K-kertoiminen vektoriavaruus. Jos vektoriavaruuden V osajoukko $B = \{v_1, v_2, \ldots, v_n\}$ virittää avaruuden V siten, että mikään sen aito osajoukko ei viritä vektoriavaruutta V, niin B on vektoriavaruuden V kanta.*

TODISTUS. Koska joukko $B = \{v_1, v_2, \ldots, v_n\}$ virittää vektoriavaruuden V, niin B on kanta, jos se on lineaarisesti riippumaton joukko. Oletetaan, että B on lineaarisesti riippuva. Tällöin on kertoimet $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ siten, että

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0,$$

ja ainakin yksi kertoimista α_i on nollasta poikkeava. Järjestetään joukko B uudelleen siten, että vektoria v_1 vastaava kerroin α_1 on nollasta poikkeava. Tällöin edellisen yhtälön mukaan $-\alpha_1 v_1 = \alpha_2 v_2 + \cdots + \alpha_n v_n$. Nyt, koska K on kunta, niin $\alpha_1^{-1} \in K$, jolloin

$$v_1 = -\alpha_1^{-1}(\alpha_2 v_2 + \cdots + \alpha_n v_n) = (-\alpha_1^{-1}\alpha_2)v_2 + \cdots + (-\alpha_1^{-1}\alpha_n)v_n.$$

Koska $-\alpha_1^{-1}\alpha_i \in K$ kaikilla $i \in \{2, \ldots, n\}$, niin edellisen yhtälön mukaan v_1 voidaan esittää vektoreiden $v_2, \ldots, v_n$ lineaarikombinaationa. Nyt, koska B virittää vektoriavaruuden V, niin jokaisella $v \in V$ on jotkin kunnan K kertoimet $\beta_1, \beta_2, \ldots, \beta_n$ siten, että

$$\begin{aligned} v &= \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n \\ &= \beta_1((-\alpha_1^{-1}\alpha_2)v_2 + \ldots (-\alpha_1^{-1}\alpha_n)v_n) + \beta_2 v_2 + \cdots + \beta_n v_n \\ &= (-\beta_1\alpha_2\alpha_1^{-1} + \beta_2)v_2 + \cdots + (-\beta_1\alpha_n\alpha_1^{-1} + \beta_n)v_n. \end{aligned}$$

Nyt, koska $-\beta_1\alpha_i\alpha_1^{-1} + \beta_i \in K$ kaikilla $i \in \{2, \ldots, n\}$, niin joukon B aito osajoukko $\{v_2, \ldots, v_n\}$ virittää vektoriavaruuden V, joka on ristiriidassa oletuksen kanssa. Näin ollen B on lineaarisesti riippumaton, eli se on vektoriavaruuden V kanta. □

Seuraus 4.34. *Jos äärellinen joukko $A \subset V$ virittää vektoriavaruuden V, niin A sisältää avaruuden V kannan. Tosin sanoen äärellisesti viritetyllä vektoriavaruudella on äärellinen kanta.*

Todistus. Jos A on äärellinen joukko joka virittää vektoriavaruuden V, niin poistamalla äärellinen määrä joukon v vektoreita saadaan äärellinen joukko $B \subset A$ joka virittää avaruuden V siten, että mikään sen aito osajoukko ei viritä avaruutta V. Tällöin edellisen lauseen mukaan B on äärellisesti viritetyn vektoriavaruuden V kanta. □

Osoitetaan seuraavaksi, että äärellisesti viritetyn vektoriavaruuden kannan alkiot voidaan korvata minkä vaan lineaarisesti riippumattoman osajoukon alkioilla. Toisin sanoen jokainen äärellisesti viritetyn vektoriavaruuden lineaarisesti riippumaton osajoukko sisältyy johonkin kyseisen avaruuden kantaan.

Lause 4.35. *Olkoon $\{a_1, a_2, \ldots, a_n\}$ on K-kertoimisen vektoriavaruuden V kanta ja $\{b_1, b_2, \ldots, b_m\}$ lineaarisesti riippumaton vektoriavaruuden V osajoukko. Tällöin $n \geqslant m$ ja vektorit $a_1, a_2, \ldots, a_n$ voidaan järjestää uudelleen siten, että joukko $\{b_1, b_2, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ on vektoriavaruuden V kanta kaikilla $k \in \{1, \ldots, m\}$.*

Todistus. Osoitetaan väite induktioperiaatteen avulla. Jos $k = 0$, niin $\{a_1, a_2, \ldots, a_n\}$ on oletuksen mukaan vektoriavaruuden V kanta, joten väite pätee kun $k = 0$. Oletetaan siis, että alkiot $a_1, a_2, \ldots, a_n$ voidaan järjestää siten, että joukko $B = \{b_1, b_2, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ on vektoriavaruuden V kanta, jollain $k \in \mathbb{Z}^+$. Tällöin, koska kanta virittää avaruuden V, niin b_{k+1} voidaan esittää sen lineaarikombinaationa, eli on kertoimet $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ siten, että

$$\star \qquad b_{k+1} = \alpha_1 b_1 + \cdots + \alpha_k b_k + \alpha_{k+1} a_{k+1} + \cdots + \alpha_n a_n.$$

Nyt, jos vektoreiden $a_{k+1}, \ldots, a_n$ kertoimet $\alpha_{k+1}, \ldots, \alpha_n$ ovat kaikki nollia, niin edellisen yhtälön mukaan vektori b_{k+1} voidaan esittää vektoreiden $b_1, \ldots, b_k$ lineaarikombinaationa, jolloin joukko $\{b_1, \ldots, b_k, b_{k+1}\}$ on lineaarisesti riippuva. Koska tämä on ristiriidassa oletuksen kanssa, niin ainakin yksi kertoimista $\alpha_{k+1}, \ldots, \alpha_n$ on nollasta poikkeava. Järjestetään äärellinen joukko $\{a_1, \ldots, a_n\}$ siten, että vektoria a_{k+1} vastaavalle kertoimelle pätee $\alpha_{k+1} \neq 0$. Tällöin kunnan

K ominaisuuksien mukaan $-\alpha_{k+1}^{-1} \in K$, jolloin edellisestä yhtälöstä saadaan

$$\begin{aligned} a_{k+1} &= -\alpha_{k+1}^{-1}(\alpha_1 b_1 + \dots \alpha_k b_k + (-1)b_{k+1} + \cdots + \alpha_n a_n) \\ &= (-\alpha_{k+1}^{-1}\alpha_1)b_1 + \dots (-\alpha_{k+1}^{-1}\alpha_k)b_k + \alpha_{k+1}^{-1}b_{k+1} + \cdots + (-\alpha_{k+1}^{-1}\alpha_n)a_n. \end{aligned}$$

Näin ollen a_{k+1} voidaan esittää vektoreiden $b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n$ lineaarikombinaationa. Nyt lauseen 4.33 todistuksen tavoin, koska oletuksen mukaan joukko $\{b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n\}$ virittää vektoriavaruuden V ja a_{k+1} voidaan esittää vektoreiden $b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n$ lineaarikombinaationa, niin joukko $\{b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n\}$ virittää vektoriavaruuden V.

Nyt, jos $m > n$, niin edellä olevan päättelyn mukaan $\{b_1, \dots, b_n\}$ on vektoriavaruuden V kanta, jolloin vektori b_{n+1} voidaan esittää alkioiden $b_1, \dots, b_n$ lineaarikombinaationa. Täten joukko $\{b_1, \dots, b_m\}$ on lineaarisesti riippuva, joka on ristiriita. Näin ollen $n \geqslant m$.

Osoitetaan vielä, että joukko $\{b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n\}$ on lineaarisesti riippumaton. Jos $\beta_1, \dots, \beta_n$ ovat kunnan K kertoimet siten, että

$$\beta_1 b_1 + \cdots + \beta_k b_k + \beta_{k+1} b_{k+1} + \beta_{k+2} a_{k+2} \cdots + \beta_n a_n = 0.$$

Nyt, koska b_{k+1} voidaan esittää kannan $\{b_1, \dots, b_k, a_{k+1}, \dots, a_n\}$ lineaarikombinaationa, niin yhtälön $\bigstar$ mukaan on kertoimet $\alpha_1, \dots, \alpha_n$, jossa $\alpha_{k+1} \neq 0$ siten, että edellisen yhtälön mukaan

$$\begin{aligned} 0 &= \sum_{i=1}^{k} \beta_i b_i + \beta_{k+1}\Big(\sum_{i=1}^{k} \alpha_i b_i + \sum_{i=k+1}^{n} \alpha_i a_i\Big) + \sum_{i=k+2}^{n} \beta_i a_i \\ &= \sum_{i=1}^{k} (\beta_i + \beta_{k+1}\alpha_i) b_i + \beta_{k+1}\alpha_{k+1} a_{k+1} + \sum_{i=k+2}^{n} (\beta_{k+1}\alpha_i + \beta_i) a_i. \end{aligned}$$

Nyt, koska joukko $\{b_1, \dots, b_{k+1}, a_{k+1}, \dots, a_n\}$ on lineaarisesti riippumaton, niin erityisesti $\beta_{k+1}\alpha_{k+1} = 0$. Koska K on kuntana kokonaisalue ja oletimme aikaisemmin, että $\alpha_{k+1} \neq 0$, niin tällöin välttämättä pätee $\beta_{k+1} = 0$. Täten

$$\begin{aligned} 0 &= \beta_1 b_1 + \cdots + \beta_k b_k + \beta_{k+1} b_{k+1} + \beta_{k+2} a_{k+2} + \cdots + \beta_n a_n \\ &= \beta_1 b_1 + \cdots + \beta_k b_k + \beta_{k+2} a_{k+2} + \cdots + \beta_n a_n \end{aligned}$$

jolloin, koska joukko $\{b_1, \dots, b_k, a_{k+2}, \dots, a_n\}$ on kannan B osajoukkona lineaarisesti riippumaton, niin niitä vastaavat kertoimet $\beta_1, \dots, \beta_k, \beta_{k+2}, \dots, \beta_n$ ovat myös kaikki nolla. Täten $\beta_i = 0$ kaikilla $i \in \{1, \dots, n\}$ ja näin ollen joukko $\{b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_n\}$ on lineaarisesti riippumaton, joten se on vektoriavaruuden V kanta. □

Koska edellisen lauseen nojalla jokainen äärellisesti viritetyn vektoriavaruuden lineaarisesti riippumaton osajoukko voidaan sisällyttää sen johonkin kantaan niin osoittautuu, että jokaisella äärellisesti viritetyn vektoriavaruuden kannalla on sama mahtavuus ja näin ollen kyseisen avaruuden dimensio on yksikäsitteinen.

Seuraus 4.36. *Olkoon V äärellisesti viritetty K-kertoiminen vektoriavaruus. Tällöin jokaisessa avaruuden V kannassa on yhtä monta alkiota.*

Todistus. Koska lauseen 4.34 mukaan äärellisesti viritetyllä vektoriavaruudella V on kanta, niin olkoot A ja B vektoriavaruuden V vastaavasti n- ja m-alkioiset kannat. Nyt, koska A ja B ovat avaruuden V kantoja, niin ne ovat

eritysesti lineaarisesti riippumattomia joukkoja. Näin ollen lineaarisesti riippumaton joukko A voidaan lauseen 4.35 mukaan sisällyttää vektoriavaruuden V kantaan B korvaamalla jotkin kannan B alkioista joukon A alkioilla. Täten erityisesti $n \leqslant m$. Käyttämällä vastaavaa päättelyä lineaarisesti riippumattomalle joukolle B ja vektoriavaruuden kannalle A saadaan vastaavasti $m \leqslant n$, joten $n = m$. Näin ollen äärellisesti viritetyn vektoriavaruuden jokaisessa kannassa on yhtä monta alkiota. □

Yhdistämällä aikaisemmin käsiteltyä moduulien teoriaa vektoriavaruuksien teoriaan saamme seuraavan tuloksen.

LAUSE 4.37. *K-kertoimiset äärellisesti viritetyt vektoriavaruudet V ja W ovat isomorfisia jos ja vain jos niillä on samat dimensiot.*

TODISTUS. Jos $V \cong W$ isomorfismilla φ, niin lauseen 4.21 mukaan φ kuvaa vektoriavaruuden V kannan A joksikin vektoriavaruuden W kannaksi B. Tällöin, koska kyseessä on isomorfismi, niin kannoissa A ja B on täsmälleen yhtä monta alkiota. Täten, koska seurauksen 4.33 mukaan jokaisessa vektoriavaruuden W kannassa on yhtä monta alkiota, niin avaruuksilla V ja W on samat dimensiot.

Jos taas vektoriavaruuksilla V ja W on sama dimensio $n \in \mathbb{N}$, niin lauseen 4.30 mukaan $V \cong K^n \cong W$. □

Edellinen lause antaa tehokkaan tavan osoittaa, että tarkasteltavilla isomorfisilla moduuleilla on samat asteet. Nimittäin, jos tarkastelemme isomorfisia R-moduuleja, joiden välisestä isomorfismista seuraa sama-asteisien vektoriavaruuksien välinen isomorfismi, niin edellisen lauseen mukaan kyseisillä moduuleilla on samat asteet. Tulemme käyttämään tätä päättelyä esimerkiksi seuraavassa lauseessa, joka osoittaa äärellisesti viritetyn kommutatiivisen renkaan asteen yksikäsitteisyyden.

SEURAUS 4.38. *Jos R on kommutatiivinen rengas, niin $R^n \cong R^m$ jos ja vain jos $n = m$, kaikilla $n, m \in \mathbb{Z}^+$.*

TODISTUS. Jos $n = m$, niin selvästi $R^n \cong R^n$. Oletetaan siis, että $R^n \cong R^m$. Olkoon nyt $\mathcal{M}$ renkaan R maksimaalinen ideaali ja

$$\mathcal{M}R = \{m_1 r_1 + \cdots + m_n r_n \mid m_i \in \mathcal{M}, r_i \in R, n \in \mathbb{N}\}.$$

Tällöin $\mathcal{M}R \subseteq \mathcal{M}$, sillä ideaalin määritelmän mukaan $mr \in \mathcal{M}$ kaikilla $m \in \mathcal{M}$, $r \in R$. Täten, koska ideaalit ovat alirenkaita, niin alkioiden mr äärelliset summat sisältyvät myös ideaaliin $\mathcal{M}$. Samoin, koska $m = m1$ kaikilla $m \in \mathcal{M}$, niin $m \in \mathcal{M}R$, jolloin $\mathcal{M} \subseteq \mathcal{M}R$. Näin ollen $\mathcal{M} = \mathcal{M}R$, eli $\mathcal{M}R$ on myös renkaan R maksimaalinen ideaali.

Tällöin $\mathcal{M}R^n$ koostuu alkioista $\sum_{i=1}^{k} m_i(r_{1,i}, \ldots, r_{n,i})$, missä $m_i \in \mathcal{M}$, sekä $r_{j,i} \in R$ kaikilla $j \in \{1, \ldots, n\}$ ja $k \in \mathbb{Z}^+$. Näin ollen, koska ideaali $(\mathcal{M}R)^n$ koostuu alkioista $(\sum_{i=1}^{k_1} m_{1,i} r_{1,i}, \ldots, \sum_{i=1}^{k_n} m_{n,i} r_{n,i})$, jossa $n, k_1, \ldots, k_n \in \mathbb{Z}^+$, niin

jokaisella ideaalin MR^n alkiolla pätee

$$\begin{aligned}\sum_{i=1}^{k} m_i(r_{1,i},\ldots,r_{n,i}) &= \sum_{i=1}^{k}(m_i r_{1,i},\ldots,m_i r_{n,i})\\ &= (\sum_{i=1}^{k} m_i r_{1,i},\ldots,\sum_{i=1}^{k} m_i r_{n,i}) \in (\mathcal{M}R)^n,\end{aligned}$$

eli $\mathcal{M}R^n \subseteq (\mathcal{M}R)^n$. Vastaavasti, koska renkaan R ideaalin $\mathcal{M}$ määritelmän mukaan $m'_j = \sum_{i=1}^{k_j} m_{j,i}r_{j,i} \in \mathcal{M}$ kaikilla $n, k_j \in \mathbb{Z}^+$, niin jokaisella ideaalin $(\mathcal{M}R)^n$ alkiolla $(m'_1,\ldots,m'_n)$ pätee

$$\begin{aligned}(m'_1,\ldots,m'_n) &= (m'_1,0,\ldots,0) + \cdots + (0,\ldots,0,m'_n)\\ &= m'_1(1,0,\ldots,0) + \cdots + m'_n(0,\ldots,0,1)\\ &= m'_1e_1 + \cdots + m'_ne_n \in \mathcal{M}R^n\end{aligned}$$

eli $(\mathcal{M}R)^n \subseteq \mathcal{M}R^n$. Täten siis $\mathcal{M}R^n = (\mathcal{M}R)^n$ kaikilla $n \in \mathbb{Z}^+$. Nyt, koska oletuksen mukaan $R^n \cong R^m$ isomorfismilla $\varphi : R^n \to R^m$, niin $\mathcal{M}R^n \cong \mathcal{M}R^m$ kuvaamalla moduulin $\mathcal{M}R$ alkioiden äärellisissä summissa esiintyvät moduulin R^n alkiot isomorfisesti moduulin R^m alkioksi. Täten $\varphi^{-1}(\mathcal{M}R^m) = \mathcal{M}R^n$, jolloin lause 4.13 antaa tekijämoduulien isomorfismin

$$R^n/\mathcal{M}R^n \cong R^m/\mathcal{M}R^m.$$

Näin ollen, koska lauseen 4.29 mukaan

$$R^n/\mathcal{M}R^n = R^n/(\mathcal{M}R)^n \cong (R/\mathcal{M}R)^n,$$

niin oletuksesta $R^n \cong R^m$ seuraa isomorfismi $(R/\mathcal{M}R)^n \cong (R/\mathcal{M}R)^m$, jossa tekijämoduuli $R/\mathcal{M}R$ on lauseen 3.29 mukaan kunta. Näin ollen, sillä tekijärengas $R/\mathcal{M}R$ on kuntana $R/\mathcal{M}R$-kertoiminen vektoriavaruus ja vektoriavaruuksien $(R/\mathcal{M}R)^n$ ja $(R/\mathcal{M}R)^m$ dimensiot ovat vastaavasti n ja m, niin lauseen 4.37 mukaan isomorfismista $(R/\mathcal{M}R)^n \cong (R/\mathcal{M}R)^m$ seuraa $n = m$. □

Edellinen seuraus osoittaa, että kommutatiivisen renkaan äärellisesti viritettyjen vapaiden moduulien aste on yksikäsitteinen.

LAUSE 4.39. *Olkoon R kommutatiivinen rengas ja M äärellisesti viritetty vapaa R-moduuli. Tällöin, jos A ja B ovat moduulin M kannat, joiden alkioiden lukumäärät ovat vastaavasti n ja m, niin $n = m$.*

TODISTUS. Koska A on moduulin M kanta, jonka alkioiden lukumäärä n, niin moduulin asteen määritelmän 4.17 mukaan M on n-asteinen R-moduuli, jolloin lauseen 4.30 mukaan $M \cong R^n$. Samoin, koska myös B on moduulin M m-asteinen kanta, niin myös $M \cong R^m$. Näin ollen $R^n \cong R^m$, jolloin seurauksen 4.38 mukaan $n = m$, eli moduulin M aste on yksikäsitteinen. □

LUKU 5

Moduulit pääideaalialueessa

Tässä kappaleessa tarkastelemme pääideaalialueiden moduulien ominaisuuksia ja todistamme niiden rakennetta kuvaavan tuloksen, jota kutsutaan *pääideaalialueiden moduulien päälauseeksi*.

Kappaleessa 2 näimme, että pääideaalialueet ovat renkaita, joiden jokainen ideaali on jonkin yhden renkaan alkion virittämä, eli syklinen ideaali. Tulemme huomaamaan, että näin ollen jokainen syklinen pääideaalialueen R-moduuli on itse asiassa tekijämoduuli $R/(a)$, jossa (a) on alkion $a \in R$ virittämä pääideaali.

Tällöin pääideaalialueiden moduulien päälause kertoo, että jokainen äärellisesti viritetty R-moduuli voidaan esittää syklisien moduulien $R/(a_1), \ldots, R/(a_n)$, $n \geqslant 0$, sekä vapaan moduulin R^r, $r \geqslant 0$ äärellisenä suorana summana. Päälause kertoo myös, että pääideaalien (a_i) virittäjäalkiot $a_i \in R$ muodostavat jonon $a_1, a_2, \ldots, a_n$ siten, että jokainen jonon alkio jakaa jokaisen myöhemmin jonossa esiintyvän alkion. Tällaisiä alkioita $a_1, a_2, \ldots, a_n$ kutsutaan kyseisen moduulin *invarianteiksi tekijöiksi*.

Tulemme myös osoittamaan, että kyseinen suora summaesitys voidaan pääideaalialueen ominaisuuksia käyttäen muuttaa niin sanottuun *alkeisjakajamuotoon* alkioiden $a \in R$ alkulukuhajotelmien avulla ja että kyseiset esitykset ovat yksikäsitteisiä. Kappale perustuu lähteisiin [**1**], [**2**] ja [**4**].

5.1. Noetherin moduulit ja vapaiden moduulien kannat

Tarkastellaan ensiksi joitain R-moduulien äärellisyysehtoja, jotka ovat hyödyllisiä vapaiden moduulien kantojen tarkastelussa.

MÄÄRITELMÄ 5.1. R-moduuli M on *Noetherin R-moduuli* jos se toteuttaa niin sanotun *kasvavien ketjujen ehdon* eli, jos

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

on osajoukkojen inkluusiorelaation $\subseteq$ suhteen kasvava ketju moduulin M alimoduuleja M_i, niin on $m \in \mathbb{Z}^+$ siten, että $M_k = M_m$ kaikilla $k \geqslant m$. Toisin sanottuna ei ole olemassa äärettömiä moduulin M alimoduulien kasvavia ketjuja. Rengas R on *Noetherin rengas* jos se on itsessään Noetherin R-moduuli.

Koska esimerkin 4.7 mukaan R-moduulin R alimoduulit ovat täsmälleen sen ideaaleja, niin yhtäpitävästi R on Noetherin rengas jos siinä ei ole äärettömästi kasvavia ideaalien ketjuja $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$.

LAUSE 5.2. *Olkoon R rengas ja M R-moduuli. Tällöin seuraavat väittämät ovat yhtäpäteviä.*

(1) M on Noetherin R-moduuli

(2) Jokaisella epätyhjällä joukolla $\mathcal{M}$ moduulin M alimoduuleja N on inkluusion suhteen maksimaalinen alkio, eli on olemassa alkio $M_{max} \in \mathcal{M}$ siten, että ehdosta $M_{max} \subseteq N$ seuraa $N = M_{max}$ kaikilla $N \in \mathcal{M}$.

(3) Jokainen moduulin M alimoduuli on äärellisesti viritetty.

TODISTUS. (1) $\Rightarrow$ (2): Oletetaan, että M on Noetherin R-moduuli. Olkoon $\mathcal{M}$ epätyhjä kokoelma moduulin M alimoduuleja. Koska osajoukkojen inkluusio $\subseteq$ on epätyhjän joukon $\mathcal{M}$ osittainen järjestys ja Noetherin moduulin jokaisella kasvavalla ketjulla on yläraja, niin Zornin lemman [**4**, s. 13] mukaan joukossa $\mathcal{M}$ on maksimaalinen alkio.

(2)$\Rightarrow$(3): Olkoon N R-moduulin M alimoduuli ja $\mathcal{M}$ moduulin N äärellisesti viritettyjen alimoduulien kokoelma. Koska $\{0\} \in \mathcal{M}$, niin $\mathcal{M} \neq \varnothing$. Tällöin kohdan (2) mukaan kokoelmassa $\mathcal{M}$ on maksimaalinen alkio N_{max}. Oletetaan, että $N \neq N_{max}$. Olkoon nyt $x \in N - N_{max}$. Koska $N_{max} \in \mathcal{M}$ on äärellisesti viritetty, niin moduuli $N_{max} \cup \{x\}$ on myös äärellisesti viritetty, jolloin pätee inkluusio $N_{max} \subseteq N_{max} \cup \{x\} \in \mathcal{M}$. Kuitenkin N_{max} oli kokoelman $\mathcal{M}$ maksimaalinen alkio, joten tämä on ristiriita. Näin ollen $N_{max} = N$, eli toisin sanoen N on äärellisesti viritetty.

(3)$\Rightarrow$(1): Olkoon $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ moduulin M alimoduulien ketju ja

$$N = \bigcup_{i=1}^{\infty} M_i.$$

Tällöin kohdan (3) mukaan N on äärellisesti viritettyjen moduulin M alimoduulien yhdisteenä äärellisesti viritetty alimoduuli. Olkoon $\{x_1, x_2, \ldots, x_n\}$ moduulin N virittäjien joukko. Koska $x_i \in N$ kaikilla i, niin $x_i \in M_{j_i}$ jollain $j_i \in \mathbb{Z}^+$. Olkoon nyt $m = \max\{j_1, j_2, \ldots, j_n\}$. Tällöin moduulien M_i muodostaman ketjurakenteen mukaan $x_i \in M_m$ kaikilla $i \in \{1, \ldots, n\}$, jolloin koska alkiot x_i virittävät moduulin N, niin $N \subseteq M_m$. Näin ollen $N = M_m = M_k$, kaikilla $k \geqslant m$, eli toisin sanoen N on Noetherin R-moduuli. □

SEURAUS 5.3. *Jos R on pääideaalialue, niin jokaisella kokoelmalla $\mathcal{I} \neq \varnothing$ renkaan R ideaaleja I on maksimaalinen alkio ja R on Noetherin rengas.*

TODISTUS. Koska esimerkin 4.7 mukaan jokainen renkaan R alimoduuli on ideaali ja pääideaalialueen jokainen ideaali on pääideaalina yhden alkion virittämä, niin R toteuttaa edellisen lauseen kohdan (3). □

Yleistetään seuraavaksi aikaisemmin annettu vapaan moduulin asteen määritelmä 5.14 yleisille moduuleille, joilla ei ole välttämättä kantaa.

MÄÄRITELMÄ 5.4. *R-moduulin M lineaarinen aste* on sen maksimaalisen lineaarisesti riippumattoman osajoukon mahtavuus.

LAUSE 5.5. *Olkoon R rengas ja N R-moduulin M alimoduuli. Tällöin alimoduulin N lineaarinen aste on enintään moduulin M lineaarinen aste.*

TODISTUS. Olkoon r_M R-moduulin M lineaarinen aste ja $A \subseteq N$ lineaarisesti riippumaton joukko. Koska $A \subseteq N \subseteq M$, niin A on myös moduulin M lineaarisesti riippumaton osajoukko, jolloin lineaarisen asteen määritelmän mukaan pätee $|A| \leqslant r_M$. □

LAUSE 5.6. *Olkoon R kokonaisalue, M m-asteinen vapaa R-moduuli, sekä $A \subset M$ siten, että $|A| = m + 1$. Tällöin joukko A on lineaarisesti riippuva.*

TODISTUS. Todistus löytyy esimerkiksi teoksesta [**2**, s.459]. □

Täten erityisesti kokonaisalueen R vapaan moduulin M vapaan alimoduulin N astelle pätee $\operatorname{rank}(N) \leqslant \operatorname{rank}(M)$, sillä alimoduulin N kanta on moduulin M lineaarisesti riippumaton osajoukko. Edelliset lauseet osoittavat, että moduulin lineaarisen asteen määritelmä 5.4 on kokonaisalueen vapaiden moduulien tapauksessa täsmälleen kyseessä olevan vapaan moduulin aste.

SEURAUS 5.7. *Olkoon R kokonaisalue ja M vapaa R-moduuli Tällöin alimoduulin M lineaariselle asteelle r_M pätee $r_M = \operatorname{rank}(M)$, missä $\operatorname{rank}(M)$ on vapaana moduulin M aste.*

TODISTUS. Olkoon A vapaan moduulin M kanta. Tällöin, koska $A \subset M$ on lineaarisesti riippumaton osajoukko, niin sen alkioiden lukumäärä $\operatorname{rank}(M)$ on enintään moduulin M maksimaalisen lineaarisesti riippumattoman osajoukon alkioiden lukumäärä, eli $\operatorname{rank}(A) \leqslant r_M$. Nyt, koska edellisen lauseen mukaan jokaisen kannan A lineaarisesti riippumattoman osajoukon alkioiden lukumäärä on enintään kannan mahtavuus $\operatorname{rank}(M)$, niin pätee $\operatorname{rank}(A) \geqslant r_M$, eli toisin sanottuna $\operatorname{rank}(A) = r_M$. □

Näin ollen kokonaisalueen R moduulin M lineaarista-, sekä vapaata astetta tullaan kutsumaan vain moduulin M *asteeksi*, jolle käytetään merkintää $\operatorname{rank}(M)$.

LAUSE 5.8. *Olkoon R rengas ja A, sekä B R-moduuleita, joiden asteet ovat $r_A, r_B > 0$. Tällöin moduulin $A \oplus B$ asteelle $r_{A\oplus B}$ pätee $r_A + r_B \leqslant r_{A\oplus B}$.*

TODISTUS. Olkoon $\{a_1, \ldots, a_n\} \subset A$ ja $\{b_1, \ldots, b_m\} \subset B$ moduulien A ja B jotkin maksimaaliset lineaarisesti riippumattomat joukot. Tällöin, jos

$$0 = \sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{m} r_i' b_i,$$

missä $r_i, r_i' \in R$ kaikilla i, niin $\sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{m} (-r')_i b_i$. Nyt, sillä moduulit A ja B ovat moduulin $A \oplus B$ alimoduuleita, joiden leikkaus on vain nolla-alkio, niin täytyy olla

$$\sum_{i=1}^{n} r_i a_i = 0 \qquad \text{ja} \qquad \sum_{i=1}^{m} (-r')_i b_i = 0,$$

joka joukkojen $\{a_1, \ldots, a_n\}$ ja $\{b_1, \ldots, b_m\}$ lineaarisen riippumattomuuden mukaan pätee vain, kun $r_i, r_i' = 0$ kaikilla i. Täten joukko $\{a_1, \ldots, a_n, b_1, \ldots, b_m\}$ on lineaarisesti riippumaton moduulin $A \oplus B$ osajoukko, eli toisin sanottuna pätee $r_A + r_B \leqslant r_{A\oplus B}$. □

Tarkastellaan seuraavaksi kokonaisalueen moduulin *torsiota* ja sen ominaisuuksia.

MÄÄRITELMÄ 5.9. Olkoon R kokonaisalue ja M R-moduuli. Moduulin M *torsioalkioiden joukko* on

$$\operatorname{Tor}(M) = \{x \in M \mid rx = 0, \text{ jollain } r \in R,\ r \neq 0\}.$$

Jos $\operatorname{Tor}(M) = M$, eli jokaisella $x \in M$ on $r \in R$, $r \neq 0$, jolle $rx = 0$, niin M on *torsiomoduuli*. Jos $\operatorname{Tor}(M) = \{0\}$, niin sanotaan, että moduuli M on .

LAUSE 5.10. *Olkoon R kokonaisalue. Tällöin R-moduulin M torsioalkioiden joukko $Tor(M)$ on sen alimoduuli.*

TODISTUS. Koska lauseen 4.3 mukaan $r0 = 0$ kaikilla $r \in R$, niin erityisesti $0 \in \mathrm{Tor}(M)$, eli torsioalimoduuli on epätyhjä. Olkoon $x, y \in \mathrm{Tor(M)}$. Tällöin on $r_1, r_2 \in R - \{0\}$ siten, että $r_1 x = 0$ ja $r_2 y = 0$. Nyt, koska R on kokonaisalue, niin ehdosta $r_1, r_2 \neq 0$ seuraa $r_1 r_2 \neq 0$, jolloin kaikilla $r \in R$ pätee

$$\begin{aligned} r_1 r_2(x + ry) &= r_1 r_2 x + (r_1 r_2) ry \\ &= r_2(r_1 x) + r r_1(r_2 y) \\ &= r_2 0 + r r_1 0 = 0, \end{aligned}$$

niin myös $x + ry \in \mathrm{Tor}(M)$. Tällöin alimoduulitestin 4.5 mukaan $\mathrm{Tor}(M)$ on moduulin M alimoduuli. □

LAUSE 5.11. *Kokonaisalueen R vapaan moduulin alimoduuli on torsiovapaa.*

TODISTUS. Olkoon M vapaa R-moduuli, jonka kanta on joukko A ja N sen alimoduuli. Jos $A = \varnothing$, niin M on nollamoduuli, jolloin se on määritelmän mukaan torsiovapaa. Voidaan siis olettaa, että $A \neq \varnothing$. Jos $\mathrm{Tor}(N) \neq \{0\}$, niin on $x \in N$, $x \neq 0$ siten, että $rx = 0$, jollain $r \in R$, $r \neq 0$. Tällöin lauseen 4.20 mukaan on olemassa yksikäsitteiset $a_1, a_2, \ldots, a_n \in R$ siten, että $a_i \neq 0$ kaikilla $i \in \{1, \ldots, n\}$ ja $x_1, x_2, \ldots, x_n \in A$ siten, että

$$x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

Täten, jos $r \in R$, niin pätee

$$\begin{aligned} rx &= r(a_1 x_1 + a_2 x_2 + \cdots + a_n x_n) \\ &= r(a_1 x_1) + r(a_2 x_2) + \cdots + r(a_n x_n) \\ &= (ra_1)x_1 + (ra_2)x_2 + \cdots + (ra_n)x_n. \end{aligned}$$

Nyt, koska R on kokonaisalue ja $r, a_i \neq 0$, niin $ra_i \neq 0$, jolloin myös $(ra_i)x_i \neq 0$ kaikilla i. Nyt, koska joukko $\{x_1, \ldots, x_n\}$ on moduulin M kannan osajoukko, niin määritelmän 4.16 mukaan se on lineaarisesti riippumaton, jolloin yhtälöstä $rx = 0$ seuraa $ra_i = 0$ kaikilla $i \in \{1, \ldots, n\}$. Kuitenkin, koska rengas R on kokonaisalue, niin siinä ei ole nollanjakajia, eli tämä on ristiriita. Näin ollen $x \notin \mathrm{Tor}(N)$, eli N on torsiovapaa. □

LAUSE 5.12. *Olkoon R kokonaisalue ja M R-moduuli. Tällöin $M/\mathrm{Tor}(M)$ on torsiovapaa moduuli.*

TODISTUS. Olkoon $x + \mathrm{Tor}(M)$ tekijämoduulin $M/\mathrm{Tor}(M)$ alkio. Tällöin, jos $x \notin \mathrm{Tor}(M)$, niin $rx \neq 0$ kaikilla $r \in R$, jolloin

$$r(x + \mathrm{Tor}(M)) = rx + \mathrm{Tor}(M) \neq 0 + \mathrm{Tor}(M),$$

eli $x \notin \mathrm{Tor}(M/\mathrm{Tor}(M))$. Jos taas $x \in \mathrm{Tor}(M)$, niin lauseen 2.28 mukaan

$$x + \mathrm{Tor}(M) = 0 + \mathrm{Tor}(M) = 0_{M/\mathrm{Tor}(M)}.$$

Näin ollen tekijämoduulissa $M/\mathrm{Tor}(M)$ ei ole nollasta poikkeavaa torsio-alkiota, eli $M/\mathrm{Tor}(M)$ on torsiovapaa. □

LAUSE 5.13. *Jos R-moduulin $M \neq \{0\}$ aste on 0, niin M on torsiomoduuli.*

TODISTUS. Olkoon M R-moduuli, jonka aste on 0. Tällöin moduulissa M ei ole lineaarisesti riippumattomia alkioita, jolloin jokaisella joukolla $\{x_1, x_2, \ldots, x_n\}$ on renkaan R alkiot $r_1, r_2, \ldots, r_n$ siten, että $r_i \neq 0$ ainakin yhdellä $i \in \{1, \ldots, n\}$

ja $0 = r_1x_1 + r_2x_2 + \dots r_nx_n$. Tällöin erityisesti jokaisella $x \in M$ on $r \in R - \{0\}$ siten, että $rx = 0$, joten $\mathrm{Tor}(M) = M$. □

Osoitetaan seuraavaksi ensimmäinen vapaita pääideaalialueen moduuleja koskeva tärkeä tulos, joka osoittaa, että pääideaalialueen vapaan moduulin alimoduuli on myös vapaa moduuli.

LAUSE 5.14. *Olkoon R pääideaalialue ja N vapaan m-asteisen R-moduulin M alimoduuli. Tällöin*

(1) N on n-asteinen vapaa moduuli siten, että $n \leqslant m$ ja
(2) on olemassa moduulin M kanta $\{x_1, x_2, \dots, x_m\}$ siten, että

$$\{r_1x_1, r_2x_2, \dots, r_nx_n\}$$

on alimoduulin N kanta, joillain $r_i \in R$, $r_i \neq 0$, jotka toteuttavat jaollisuusrelaation

$$r_1 \mid r_2 \mid \cdots \mid r_n.$$

TODISTUS. Jos $N = \{0\}$, niin N on vapaa moduuli, jonka kanta on tyhjä joukko ja täten $\mathrm{rank}(N) = 0 \leqslant m$. Oletaan siis, että $N \neq \{0\}$. Olkoon tällöin $\varphi : M \to R$ jokin R-moduulihomomorfismi. Tällöin, koska lauseen 4.10 mukaan alimoduulin N kuva $\varphi(N)$ on R moduulin R alimoduuli ja R on kommutatiivinen rengas, niin esimerkin 4.7 mukaan $\varphi(N)$ on renkaan R ideaali. Koska R on pääideaalialue, niin ideaali $\varphi(N)$ on pääideaali, eli $\varphi(N) = (a_\varphi)$, jollain $a_\varphi \in R$. Olkoon nyt

$$\mathcal{I} = \{(a_\varphi) \mid \varphi \in \mathrm{Hom}_R(M, R)\}$$

tällaisten R-moduulihomomorfismien määräämien pääideaalien kokoelma. Koska triviaali homomorfismi $M \to R$, $x \mapsto 0$ on R-moduulihomomorfismi, jolle $\varphi(N) = \{0\}$, niin $(0) \in \mathcal{I}$, eli $\mathcal{I} \neq \varnothing$. Tällöin seurauksen 5.3 mukaan kokoelmalla $\mathcal{I}$ on maksimaalinen alkio, eli on olemassa R-moduulihomomorfismi $\nu : M \to R$ siten, että ei ole $I \in \mathcal{I}$ siten, että $\nu(N) = (a_\nu) \subset I$.

Olkoon nyt $a_1 = a_\nu$ ja $y \in N$ siten, että $\nu(y) = a_1$. Koska vapaalla moduulilla M on kanta $\{x_1, x_2, \dots, x_m\}$, niin lauseen 4.20 mukaan jokaisella $x \in M - \{0\}$ on yksikäsitteinen esitys $x = r_1x_1 + r_2x_2 + \cdots + r_mx_m$, joillain $r_i \in R$. Tällöin luonnolliset koordinaattiprojektiot $\pi_i : M \to R$,

$$\pi_i(x) = \pi_i(r_1x_1 + r_2x_2 + \cdots + r_mx_m) = r_i,$$

missä $i \in \{1, \dots, n\}$ ovat R-moduulihomomorfismeja, sillä jos $x, x' \in M$, niin

$$\begin{aligned}\pi_i(x + x') &= \pi_i((r_1x_1 + \cdots + r_ix_i + \cdots + r_mx_m) + (r'_1x_1 + \cdots + r'_ix_i + \cdots + r'_mx_m)) \\ &= \pi_i((r_i + r'_i)x_i + (r_1 + r'_1)x_1 + \cdots + (r_m + r'_m)x_m) \\ &= r_i + r'_i = \pi_i(x) + \pi_i(x'),\end{aligned}$$

sekä kaikilla $r \in R$ pätee

$$\begin{aligned}\pi_i(rx) &= \pi(rr_1x_1 + \cdots + rr_ix_i + \cdots + rr_mx_m) \\ &= rr_i = r\pi_i(x).\end{aligned}$$

Nyt, koska $N \neq \{0\}$, niin on jokin $x \in M$, jolla on lineaarikombinaatioesitys $x = r_1x_1 + \cdots + r_mx_m$, jossa $r_i, x_i \neq 0$ ainakin yhdellä $i \in \{1, \dots, m\}$. Täten $\pi_i(N) \neq 0$, eli kuvauksen π_i määräämälle ideaalille pätee $(a_{\pi_i}) = \pi_i(N) \neq (0)$. Nyt, koska nollaideaali (0) sisältyy jokaiseen ideaaliin, sekä (a_1) on pääideaalien

kokoelman $\mathcal{I}$ maksimaalinen alkio ja $(a_{\pi_i}) \in \mathcal{I}$ kaikilla $i \in \{1, \ldots, m\}$, niin $(a_1) \supsetneq (0)$, eli $a_1 \neq 0$.

Osoitetaan seuraavaksi, että $a_1 \mid \varphi(y)$, jokaisella $\varphi \in \mathrm{Hom}_R(M, R)$. Olkoon I alkioiden a_1 ja $\varphi(y)$ virittämä ideaali. Nyt, koska R on pääideaalialue, niin $I = (d)$, jollain $d \in R$. Tällöin lauseen 3.39 mukaan $d \mid a_1$ ja $d \mid \varphi(y)$, sekä $d = r_1 a_1 + r_2 \varphi(y)$, joillain $r_1, r_2 \in R$. Olkoon $\psi : M \to R$,

$$\psi(m) = r_1 \nu(m) + r_2 \varphi(m),$$

joka on R-moduulihomomorfismien pisteittäisenä summana R-moduulihomomorfismi. Tällöin erityisesti $d = \psi(y)$, eli $d \subset \psi(N)$. Näin ollen $(d) \subseteq \psi(N)$ ja koska $d \mid a_1$, niin myös $(a_1) \subseteq (d)$. Kuitenkin, koska (a_1) on joukon $\mathcal{I}$ maksimaalinen alkio, niin myös $(d) \subseteq (a_1)$, jolloin $(a_1) = (d) = \psi(N)$. Tällöin erityisesti $d = r a_1$ jollain $r \in R$. Nyt, koska $d \mid \varphi(y)$, niin $\varphi(y) = r' d$ jollain $r' \in R$, joten $\varphi(y) = r' r a_1$, eli $a_1 \mid \varphi(y)$.

Koska edellä oleva päättely pätee mielivaltaiselle R-moduulihomomorfismille $\varphi \in \mathrm{Hom}_R(M, R)$ ja $\pi_i \in \mathrm{Hom}_R(M, R)$, niin erityisesti $a_1 \mid \pi_i(y)$ kaikilla $i \in \{1, \ldots, n\}$. Täten $\pi_i(y) = a_1 b_i$, jollain $b_i \in R$, $i \in \{1, \ldots, m\}$. Olkoon nyt

$$y_1 = \sum_{i=1}^{m} b_i x_i.$$

Tällöin kuvauksen π_i määritelmän mukaan

$$a_1 y_1 = a_1 \sum_{i=1}^{m} b_i x_i = \sum_{i=1}^{m} (a_1 b_i) x_i = \sum_{i=1}^{m} \pi_i(y) x_i = y.$$

Nyt, koska R on kokonaisalue ja $a_1 \neq 0$, niin supistussäännön 3.13 mukaan yhtälöstä

$$a_1 = \nu(y) = \nu(a_1 y_1) = a_1 \nu(y_1)$$

seuraa $\nu(y_1) = 1$. Osoitetaan seuraavaksi, että moduuli M, sekä sen alimoduuli N voidaan esittää suorina summina

(a) $M = R y_1 \oplus \ker \nu$, sekä
(b) $N = R a_1 y_1 \oplus (N \cap \ker \nu)$.

Osoitetaan kohta (a). Olkoon $x \in M$. Tällöin

$$x = x + \nu(x) y_1 - \nu(x) y_1 = \nu(x) y_1 + (x - \nu(x) y_1)$$

joten, koska $\nu \in \mathrm{Hom}_R(M, R)$, niin saadaan

$$\begin{aligned} \nu(x - \nu(x) y_1) &= \nu(x) + \nu(-\nu(x) y_1) \\ &= \nu(x) - \nu(x) \nu(y_1) \\ &= \nu(x) - \nu(x) 1 = 0. \end{aligned}$$

Täten $x - \nu(x) y_1 \in \ker \nu$, eli $M = R y_1 + \ker \nu$. Osoitetaan vielä, että kyseinen summa on suora summa. Jos $r y_1 \in \ker \nu$, $r \in R$, niin

$$r = r \nu(y_1) = \nu(r y_1) = 0,$$

eli $r y_1 = 0$. Täten $R y_1 \cap \ker \nu = \{0\}$, jolloin lauseen 4.27 nojalla $M = R y_1 \oplus \ker \nu$.

Osoitetaan seuraavaksi kohta (b). Olkoon $x' \in N$. Koska $\nu(N) = (a_1)$, niin $a_1 \mid \nu(x')$, eli $\nu(x') = b a_1$, jollain $b \in R$. Tällöin (a)-kohdan tapaan saadaan

$$x' = \nu(x') y_1 + (x' - \nu(x') y_1) = b a_1 y_1 + (x' - b a_1 y_1).$$

Nyt, koska N on moduulin M alimoduuli ja $y \in N$, niin

$$x' - \nu(x')y_1 = x' - ba_1y_1 = x'by \in N$$

ja tällöin (a) kohdan mukaan $x' \in Ra_1y_1 + (N \cap \ker\varphi)$. Koska $N \subset M$, niin (a) kohdan mukaan jos $a_1y_1 \in \ker\nu$, niin $a_1y_1 = 0$, eli $Ra_1y_1 \cap \ker\nu = \varnothing$. Tällöin $N = Ra_1y_1 \oplus (N \cap \ker\nu)$.

Osoitetaan nyt lauseen kohta (1) induktiolla alimoduulin N asteen suhteen. Jos moduulin N asteelle n pätee $n = 0 \leqslant m$, niin lauseen 5.13 mukaan N on torsiomoduuli. Kuitenkin, koska moduuli M on vapaa moduuli, niin lauseen 5.11 mukaan alimoduuli N on torsiovapaa. Tällöin välttämättä $N = \{0\}$, joka on tyhjän joukon virittämä vapaa moduuli, jonka aste on $0 \leqslant m$. Näin ollen väite (1) pätee tapauksessa $n = 0$, eli voidaan olettaa, että $0 < n$.

Tehdään induktio-oletus. Oletetaan, että jos alimoduulin N aste on enintään $k \in \mathbb{Z}$, niin tällöin N on vapaa moduuli. Olkoon täten alimoduulin N aste $k+1$. Koska kohdan (b) mukaan $N = Ra_1y_1 \oplus (N \cap \ker\nu)$, niin lauseen 5.8 mukaan

$$\operatorname{rank}(Ra_1y_1) + \operatorname{rank}(N \cap \ker\nu) \leqslant \operatorname{rank}(N) = k + 1.$$

Nyt, koska lauseen 4.31 mukaan Ra_1y_1 on vapaa moduuli, jonka kanta on alkio a_1y_1, niin $\operatorname{rank}(Ry_1) = 1$ ja näin ollen $\operatorname{rank}(N \cap \ker\nu) \leqslant k$. Tällöin induktio-oletuksen mukaan $N \cap \ker\nu$ on vapaa moduuli, jonka aste on k. Näin ollen, koska $N \cap \ker\nu$ on vapaa moduuli, niin sillä on kanta $\{z_1, z_2, \ldots, z_k\}$, jolloin lauseen 4.30 mukaan $N = Ra_1y_1 \oplus Rz_1 \oplus \cdots \oplus Rz_k$. Täten lauseen 4.31 mukaan $\{a_1y_1, z_1, \ldots, z_k\}$ on moduulin M kanta, jolloin M on myös vapaa moduuli, jonka aste on $k+1$. Näin ollen m-asteisen vapaan moduulin M alimoduuli N on n-asteinen vapaa moduuli kaikilla $n \in \mathbb{Z}^+$, jossa lauseen 5.6 mukaan $n \leqslant m$.

Osoitetaan kohta (2) induktion avulla. Jos vapaan moduulin M asteelle pätee $m = 0$, niin M on taas triviaali moduuli $\{0\}$, jolloin sen ainoa kanta on tyhjä joukko ja tällöin väite pätee. Oletetaan, että $0 < m$ ja tehdään induktio-oletus: Oletetaan, että väite (2) pätee jollain $k-1 \in \mathbb{Z}^+$. Olkoon $\operatorname{rank}(M) = k$. Tällöin koska $\ker\nu$ on moduulin M alimoduuli, niin se on kohdan (1) mukaan vapaa moduuli, jonka aste on kohdan (a) mukaan $k-1$. Näin ollen induktio-oletuksen perusteella moduuli $\ker\nu$ ja sen alimoduuli $\ker\nu \cap N$ toteuttavat kohdan (2), eli on olemassa moduulin $\ker\nu$ kanta $y_1, y_2, \ldots, y_{k-1}$ siten, että $a_1y_2, \ldots, a_ly_l$, $l \leqslant k-1$ on moduulin $\ker\nu \cap N$ kanta, jossa $a_i \in R$ ja $a_1 \mid a_2 \mid \cdots \mid a_l$. Nyt, koska kohtien (a) ja (b) mukaan $M = Ry_1 \oplus \ker\nu$ ja $N = Ra_1y_1 \oplus (N \cap \ker\nu)$, niin $y_1, y_2, \ldots, y_k$ on moduulin M kanta ja $a_1y_1, a_2y_2, \ldots a_ly_l$ on alimoduulin N kanta. Riittää siis osoittaa, että $a_1 \mid a_2$.

Olkoon $\varphi : M \to R$, $\varphi(x) = \pi_1(x) + \pi_2(x)$. Tällöin φ on R-moduulien välinen homomorfismi siten, että $\varphi(y_1) = \varphi(y_2) = 1$ ja $\varphi(y_i) = 0$ kaikilla $i > 2$. Täten $a_1 = \varphi(a_1y_1)$, eli $a_1 \in \varphi(N)$. Näin ollen $(a_1) \subseteq \varphi(N)$ jolloin, koska (a_1) on joukon $\mathcal{I}$ maksimaalinen alkio, niin $(a_1) = \varphi(N)$. Nyt, koska myös $a_2 = \varphi(a_2y_2)$, niin $(a_2) \in \varphi(N) = (a_1)$, eli toisin sanoen $a_2 = ra_1$ jollain $r \in R$. Täten $a_1 \mid a_2$. Näin ollen väite (2) pätee jokaisella moduulin M asteella $n \in \mathbb{Z}^+$. □

5.2. Pääideaalialueen moduulien päälause

Seuraavaksi todistamme niin sanotun pääideaalialueen moduulien päälauseen, joka antaa meille tietoa äärellisesti viritettyjen pääideaalialueen moduulien rakenteesta. Osoitamme ensiksi, että äärellisesti viritetty moduuli on isomorfinen

vapaan moduulin ja syklisien moduulien suoran summan kanssa, joka voidaan esittää kahdessa eri muodossa. Tämän jälkeen näytämme, että kyseiset esitykset ovat yksikäsitteisiä. Tarkastellaan ensiksi R-moduuleiden *annihilaattoreita* ja niiden ominaisuuksia.

MÄÄRITELMÄ 5.15. Moduulin M alimoduulin N *annihilaattori* on renkaan R ideaali

$$\mathrm{Ann}(N) = \{r \in R \mid rn = 0, \text{ kaikilla } n \in N\}.$$

Koska moduulin M alimoduulin N alkiolle n pätee $0n = 0$, niin alimoduulin annihilaattori sisältää aina joukon $\{0\}$. Seuraava lause osoittaa, että alimoduulin annihilaattori antaa tietoa sen torsiosta.

LAUSE 5.16. *Olkoon R rengas. Jos R-moduulin M alimoduulin N annihilaattori $Ann(N) \neq \{0\}$, niin N on torsioalimoduuli. Vastaavasti, jos N on torsiovapaa, niin $Ann(N) = \{0\}$.*

TODISTUS. Jos $r \in \mathrm{Ann}(N) - \{0\}$, niin kaikilla $n \in N$ pätee $rn = 0$, jolloin torsiomoduulin määritelmän 5.9 mukaan N on torsioalimoduuli. Vastaavasti, jos N on torsiovapaa, niin soveltamalla edellä olevaa päättelyä nollasta poikkeavalle annihilaattorin alkiolle saadaan $\mathrm{Tor}(N) = N$, joka on ristiriita. Näin ollen $\mathrm{Ann}(N) = \{0\}$. □

Seuraava lause osoittaa, että moduulien väliset isomorfismit säilyttävät niiden annihilaattoreiden rakenteen.

LAUSE 5.17. *Isomorfisilla moduuleilla on sama annihilaattori.*

TODISTUS. Olkoon $\varphi : M \to N$ R-moduulien välinen isomorfismi. Tällöin, koska jokaisella $n \in N$ on $m \in M$ siten, että $\varphi(m) = n$, niin lauseen 2.21 nojalla kaikilla $r \in \mathrm{Ann}(M)$ pätee

$$\begin{aligned} rn &= r\varphi(m) \\ &= \varphi(rm) \\ &= \varphi(0_M) \\ &= 0_N, \end{aligned}$$

eli $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(N)$. Käyttämällä vastaavaa päättelyä moduulin N annihilaattorille saadaan $\mathrm{Ann}(N) \subseteq \mathrm{Ann}(M)$, joten moduulien M ja N annihilaattorit ovat täsmälleen samat. □

LAUSE 5.18. *Olkoon R pääideaalialue ja (a) sen pääideaali jollain nollasta poikkeavalla alkiolla $a \in R$, $a \notin R^\times$. Tällöin tekijämoduulin $R/(a)$ annihilaattori on $Ann(R/(a)) = (a)$.*

TODISTUS. Jos $r \in (a)$, niin ideaalin määritelmän 3.17 mukaan jokaisella $x \in R$ pätee $rx \in (a)$. Tällöin lauseen 2.28 mukaan jokaisella $x + (a) \in R/(a)$ pätee

$$r(x + (a)) = rx + (a) = 0 + (a).$$

Näin ollen $(a) \subseteq \mathrm{Ann}(R/(a))$. Jos taas $r \in \mathrm{Ann}(R/(a))$, niin jokaisella tekijämoduulin alkiolla $x + (a) \in R/(a)$ pätee $r(x + (a)) = 0 + (a)$, joten tekijämoduulin ja moduulin toiminnan määritelmien 4.11, sekä 4.2 nojalla saadaan erityisesti

$$r + (a) = r1 + (a) = r(1 + (a)) = 0 + (a),$$

joka pätee jos ja vain jos $r \in (a)$. Näin ollen myös $\mathrm{Ann}(R/(a)) \subseteq (a)$, joten siis $\mathrm{Ann}(R/(a)) = (a)$. □

SEURAUS 5.19. *Olkoon R pääideaalialue ja $a \in R - \{0\}$, $a \notin R^\times$. Tällöin $R/(a)$ on torsiomoduuli.*

TODISTUS. Koska edellisen lauseen mukaan $\mathrm{Ann}(R/(a)) = (a) \neq \{0\}$, niin lauseen 5.16 mukaan $R/(a)$ on torsiomoduuli. □

Edellisien lauseiden oletus siitä, että pääideaalialueen R pääideaalin (a) virittäjä alkio a ei ole renkaan R yksikkö takaa, ettei kyseisistä lauseista päädytä ristiriitaan nollamoduulien tapauksessa. Nimittäin, jos a on yksikkö, niin lauseen 3.25 mukaan pääideaali (a) on koko rengas R, jolloin edellä olevien lauseiden nojalla $R/(a) = R/R = \{0\}$ on torsiomoduuli.

Kuitenkin esimerkissä 4.19 totesimme, että nollamoduuli on vapaa moduuli, jonka kanta on tyhjä joukko, jolloin lauseen 5.11 nojalla se on torsiovapaa. Täten edelläolevat lauseet pätevät pääideaalialueen R aidoille pääideaaleille (a), eli nollasta poikkeaville tekijämoduuleille $R/(a)$.

Osoitetaan seuraavaksi, että pääideaalialueen sykliset moduulit ovat isomorfisia tekijämoduuleiden $R/(a)$ kanssa.

LAUSE 5.20. *Olkoon R pääideaalialue ja C syklinen R-moduuli. Tällöin pätee isomorfismi $C \cong R/(a)$, missä $(a) = Ann(C)$.*

TODISTUS. Olkoon $\varphi : R \to C$, $\varphi(r) = rc$, missä $c \in C$. Koska C on syklinen moduuli, eli $C = Rc$, jollain $c \in C$, niin jokaisella $c' \in C$ on $r \in R$ siten, että $rc = c'$. Täten kuvaus φ on surjektio. Nyt, koska myös

$$\varphi(r + s) = (r + s)c = rc + sc = \varphi(r) + \varphi(s)$$

ja $\varphi(sr) = (sr)c = s(rc) = s\varphi(r)$, niin φ on surjektiivinen R-moduulihomomorfismi. Täten moduulinen ensimmäisen isomorfismilauseen 4.12 mukaan

$$R/\ker\pi \cong C.$$

Koska R on pääideaalialue, niin $\ker\pi$ on renkaan R ideaalina pääideaali (a) jollain $a \in R$, joka todistaa väitteen. Koska $\mathrm{Ann}(R/(a)) = (a)$, niin lauseen 5.17 mukaan isomorfismista $C \cong R/(a)$ seuraa $(a) = \mathrm{Ann}(C)$. □

Ensiksi todistamme pääideaalialueiden moduulien päälauseesta niin sanotun *invarianttien tekijöiden* esityksen. Koska lauseen 4.24 mukaan R^n, $n \in \mathbb{N}$ on n-asteinen vapaa moduuli ja lauseen 5.19 mukaan sykliset moduulit $R/(a)$, missä $a \neq 0$, $a \notin R^\times$ ovat torsiomoduuleja. Näin ollen edellä oleva invarianttien tekijöiden esitys antaa jokaiselle äärellisesti viritetylle pääideaalialueen moduulille suoran summaesityksen, joka koostuu vapaasta moduulista sekä äärellisen monesta syklisestä torsiomoduulista.

LAUSE 5.21 (Invariantit tekijät). *Olkoon R pääideaalialue ja M äärellisesti viritetty R-moduuli.*

(1) Moduuli M on isomorfinen vapaan moduulin ja äärellisen monen syklisen moduulin suoran summan kanssa, eli

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

jollain $r \in \mathbb{N}$ *ja* $a_i \in R$, $a_i \neq 0$ *siten, että* a_i *ei ole yksikkö ja*

$$a_1 \mid a_2 \mid \cdots \mid a_m,$$

kaikilla $i \in \{1, \ldots, m\}$, $m \in \mathbb{N}$.

(2) *Moduuli* M *on torsiovapaa jos ja vain jos se on vapaa moduuli.*

(3) *Kohdan (1) esityksessä pätee*

$$Tor(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

eli toisin sanoen M *on torsiomoduuli jos ja vain jos* $r = 0$ *ja tällöin* $Ann(M) = (a_m)$.

TODISTUS. (1) Olkoon $\{x_1, x_2, \ldots, x_n\}$ pienin äärellisesti viritetyn moduulin M virittävä joukko ja R^n n-asteinen vapaa R-moduuli, jonka kanta on joukko $\{e_1, e_2, \ldots, e_n\}$. Olkoon $\pi : R^n \to M$ kuvaus, missä

$$\pi(x) = \pi(r_1e_1 + r_2e_2 + \cdots + r_ne_n) = r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

Tällöin, koska joukko $\{x_1, x_2, \ldots, x_n\}$ virittää moduulin M, niin jokainen moduulin M alkio voidaan esittää alkioiden $x_1, \ldots, x_n$ lineaarikombinaationa ja näin ollen π on määritelmän mukaan surjektiivinen R-moduulihomomorfismi. Näin ollen moduulien ensimmäinen isomorfismilause 4.12 antaa isomorfismin $R^n/\ker\pi \cong M$. Tällöin, koska $\ker\pi$ on moduulin R^n alimoduuli, niin lauseen 5.14 perusteella voidaan valita moduulin R^n kanta $\{y_1, y_2, \ldots, y_n\}$ siten, että $\{a_1y_1, a_2y_2, \ldots, a_my_m\}$ on alimoduulin $\ker\pi$ kanta jollain $m \leqslant n$ ja $a_i \in R$, jossa $a_1 \mid a_2 \mid \cdots \mid a_m$. Tällöin lause 4.30 antaa esityksen

$$(i)\quad M \cong R^n/\ker\pi = (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m).$$

Nyt, koska lauseen 4.11 mukaan luonnollisen surjektiivisen R-moduulihomomorfismin $\pi_i : Ry_i \to R/(a)$, $\alpha_iy_i \to \alpha_i + (a_i)$ ydin on (a_i), niin kuvaus

$$(ii)\quad \varphi : Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$
$$\varphi(r_1y_1, r_2y_2, \ldots, r_ny_n) = (r_1 + (a_1), r_2 + (a_2), \ldots, r_n + (a_m), r_{m+1}, \ldots, r_n)$$

on surjektiivinen R-moduulihomomorfismi, jonka ydin on joukko

$$\{(r_1, r_2, \ldots, r_n) \mid r_i \in (a_i),\ 1 \leqslant i \leqslant m, \text{ ja } r_i = 0,\ m < i \leqslant n\},$$

eli toisin sanoen $a_i \mid r_i$ kaikilla $1 \leqslant i \leqslant m$ ja $r_i = 0$ muulloin. Täten

$$\begin{aligned}\ker\varphi &= Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m \oplus \{0\}^{n-m}\\ &\cong Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m,\end{aligned}$$

isomorfismilla $(r_1a_1y_1, r_2a_2y_2, \ldots r_na_ny_n, 0, \ldots, 0) \to (r_1a_1y_1, r_2a_2y_2, \ldots r_na_ny_n)$. Tällöin moduulien ensimmäisen isomorfismilauseen 4.12 mukaan

$$(Ry_1 \oplus \cdots \oplus Ry_n)/\ker\varphi \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

Nyt, koska yhtälön (i) mukaan $M \cong R^n/\ker\pi$ ja koska $\ker\pi = \ker\varphi$, niin saadaan isomorfismi $M \cong R^n/\ker\varphi$. Näin ollen yhtälö (ii) antaa isomorfismin

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

Jos a_i on yksikkö, niin lauseen 3.25 mukaan pääideaali (a_i) on rengas R, jolloin $R/(a) = 0$. Näin ollen, jos a_i on yksikkö jokaisella $i \in \{1, \ldots, m\}$, niin

$M \cong R^r$, eli moduuli M on vapaa moduuli. Jos joukossa $\{a_1, \ldots, a_m\}$ on k-kappaletta yksiköitä, jollain $1 \leqslant k \leqslant m$, niin joukko $\{a_1, \ldots, a_m\}$ voidaan järjestää siten, että a_i ei ole yksikkö, kun $1 \leqslant i \leqslant m-k$ ja a_i on yksikkö kun $m-k \leqslant i \leqslant m$. Tällöin (1) kohdan yhtälö saadaan muotoon

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_{m'}) \oplus R^r,$$

jossa a_i ei ole yksikkö, $a_1 \mid \cdots \mid a_{m'}$ ja $r \in \mathbb{Z}^+$, kun merkitään $m' = m-k$ ja $r = n-m$.

(2) Seurauksen 5.19 mukaan tekijämoduuli $R/(a)$ on torsiomoduuli jokaisella $a \neq 0$. Tällöin, koska R^r on vapaa R-moduuli, jonka aste on r, niin kohdan (1) mukaan M on torsiovapaa jos ja vain jos $M \cong R^r$.

(3) Edellisen kohdan perusteella M on torsiomoduuli jos ja vain jos M on isomorfinen syklisien moduulien suoran summan kanssa, eli

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

joka vastaa tilannetta $r = 0$.

Koska $a_1 \mid a_2 \mid \cdots \mid a_m$, niin $a_1 = r_2a_2 = r_3a_3 = \ldots r_na_n$, missä $r_i \in R$ kaikilla $i \in \{2, \ldots, n\}$. Tällöin, koska pääideaalit (a_i) ovat alkion a_i virittämiä ideaaleja kaikilla $i \in \{1, \ldots, n\}$, niin $(a_i) = ra_i$, missä $r \in R$. Täten, koska myös $a_i \in (a_{i+1})$, niin saadaan inkluusiot $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_m)$. Nyt, koska lauseen 5.18 mukaan tekijämoduulien $R/(a_i)$ annihilaattorit ovat täsmälleen pääideaalit (a_i) ja $(a_i) \subseteq (a_m)$ kaikilla $i \in \{1, \ldots, m\}$, niin kohdan (1) suoran summaesityksen mukaan kaikilla $x \in M$ ja $r \in (a_m)$ pätee

$$\begin{aligned} rx &= r((r_1 + (a_1)) + (r_2 + (a_2)) + \cdots + (r_m + (a_m))) \\ &= (rr_1 + (a_1)) + (rr_2 + (a_2)) + \cdots + (rr_m + (a_m)) \\ &= (0 + (a_1)) + (0 + (a_2)) + \cdots + (0 + (a_m)) \\ &= 0_M, \end{aligned}$$

eli $(a_m) \subseteq \operatorname{Ann}(\bigoplus_{i=1}^m R/(a_i))$. Näin ollen kohdan (1), sekä lauseen 5.17 mukaan $(a_m) \subseteq \operatorname{Ann}(M)$.

Jos taas $r \in \operatorname{Ann}(M)$, niin lauseen 5.17 ja kohdan (1) esityksen mukaan $r \in \operatorname{Ann}(\bigoplus_{i=1}^m R/(a_i))$. Tällöin erityisesti alkiolle $1 + (a_m) \in \bigoplus_{i=1}^m R/(a_i)$ pätee

$$r(1 + (a_m)) = r1 + (a_m) = 0 + (a_m),$$

eli $r1 = r \in (a_m)$. Näin ollen $\operatorname{Ann}(\bigoplus_{i=1}^m R/(a_i)) \subseteq (a_m)$. Nyt, koska kohdan (1) mukaan $M \cong \bigoplus_{i=1}^m R/(a_i)$ ja koska lauseen 5.17 mukaan isomorfismilla moduuleilla on samat annihilaattorit, niin $\operatorname{Ann}(M) \subseteq (a_m)$. Näin ollen $\operatorname{Ann}(M) = (a_m)$. □

MÄÄRITELMÄ 5.22. Edellisessä lauseessa esiintyvä luku $r \in \mathbb{Z}^+$ on moduulin M *vapaa aste*, jota joskus kutsutaan myös sen *Bettin luvuksi* [**2**, s. 464]. Lauseessa esiintyvät alkiot $a_1, a_2, \ldots, a_m \in R$ ovat moduulin M *invariantit tekijät*. Tulemme myöhemmin osoittamaan, että pääideaalialueen äärellisesti viritetyn moduulin vapaa aste sekä invariantit tekijät ovat yksikäsitteiset.

Koska lauseen 5.11 mukaan vapaa moduuli on torsiovapaa, niin lauseen 5.23 antaman alkeisjakajaesityksen mukaan vapaan moduulin M aste n on sen vapaa aste ja $M \cong R^n$, joka sopii yhteen lauseen 4.30 kanssa.

Koska R on pääideaalialue, niin lauseen 3.50 mukaan se on myös yksikäsitteisen tekijäjaon alue, jolloin jokainen pääideaalialueen nollasta poikkeava alkio voidaan esittää yksiköllä kertomista vailla yksikäsitteisenä alkulukujen tulona. Soveltamalla tätä huomiota ja kiinalaista jakojäännöslausetta 3.33 äärellisesti viritetyn pääideaalialueen moduulin invarianttien tekijöiden esitykseen saamme niin sanotun äärellisesti viritetyn pääideaalialueen moduulin *alkeisjakajaesityksen.*

LAUSE 5.23 (Alkeisjakajaesitys). *Olkoon R pääideaalialue ja M äärellisesti viritetty R-moduuli. Tällöin*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t}),$$

jossa $r \in \mathbb{Z}^+$ ja $p_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}^+$ ovat renkaan R alkulukujen p_i positiivisia potensseja kaikilla $i \in \{1, \ldots, t\}$.

TODISTUS. Lauseen 5.21 mukaan $M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^r$, jollain $r \in \mathbb{Z}^+$. Koska lauseen 3.50 mukaan pääideaalialue R on yksikäsitteisen tekijänjaon alue, niin jokaisella $a_i \neq 0$ on yksiköllä kertomista vaille yksikäsitteinen esitys

$$a_i = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

jollain $s \in \mathbb{Z}^+$, jossa p_i ovat erillisiä renkaan R alkulukuja kaikilla $i \in \{1, \ldots, s\}$ ja $u \in R^\times$. Tällöin, koska alkuluvut $p_i^{\alpha_i}$ ovat yksiköllä kertomista vailla yksikäsitteiset ja pääideaalille $up_i^{\alpha_i} \in (p_i^{\alpha_i})$ kaikilla $u \in R^\times$, niin alkulukujen määräämät pääideaalit $(p_i^{\alpha_i})$ ovat yksikäsitteiset.

Olkoon $i \neq j$. Koska lauseen 3.39 mukaan pääideaaleille $(p_i^{\alpha_i})$ ja $(p_j^{\alpha_j})$ pätee $xp_i^{\alpha_i} + yp_j^{\alpha_j} = \operatorname{syt}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ joillain $x, y \in R$, niin erityisesti jokaisella $r \in R$ pätee

$$r = r1 = r(xp_i^{\alpha_i} + yp_j^{\alpha_j}) = x'p_i^{\alpha_i} + y'p_j^{\alpha_j}.$$

Näin ollen $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$, eli ideaalit $(p_i^{\alpha_i})$ ja $(p_j^{\alpha_j})$ ovat pareittain komaksimaaliset jokaisella $i, j \in \{1, \ldots, s\}$. Koska $a_i = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, niin $p_i^{\alpha_i} \mid a_i$, jokaisella i. Näin ollen $\cap_i (p_i^{\alpha_i}) \subseteq (a_i)$. Jos taas $x \in (a_i)$, niin $x = ra_i$, jollain $r \in R$, jolloin edellä saadun tuloesityksen mukaan

$$x = ra_i = r(up_1^{\alpha_1} \ldots p_s^{\alpha_s}) = r(up_1^{\alpha_1} \ldots p_{j-1}^{\alpha_{j-1}} p_{j+1}^{\alpha_{j+1}} \ldots p_s^{\alpha_s}) p_j^{\alpha_j} = r'p_j^{\alpha_j},$$

eli $x \in (p_j^{\alpha_j})$ kaikilla $j \in \{1, \ldots, s\}$. Näin ollen saadaan $\cap_j p_j^{\alpha_j} = (a_i)$.

Nyt, koska lauseen 3.25 mukaan yksikön $u \in R$ virittämä pääideaali (u) on koko rengas R, niin $R/(u) = \{0\}$, jolloin kiinalainen jakojäännöslause 3.33 antaa tekijämoduulille $R/(a_i)$ esityksen

$$\begin{aligned} R/(a_i) &= R/(up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}) \cong R/(u) \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s}) \\ &\cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s}). \end{aligned}$$

Näin ollen soveltamalla edellä olevaa päättelyä jokaiseen lauseen 5.21 antamaan pääideaaliin (a_i), $i \in \{1, \ldots, m\}$ ja numeroimalla indeksit uudelleen saadaan

$$M \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t}) \oplus R^r,$$

jossa $p_i^{\alpha_i}$ ovat renkaan R alkulukuja ja $r \in \mathbb{Z}^+$ on moduulin M vapaa aste. □

MÄÄRITELMÄ 5.24. Edellisen lauseen alkulukupotenssit $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_t}$ ovat moduulin M *alkeisjakajat*. Tulemme myöhemmin osoittamaan, että pääideaalialueen äärellisesti viritetyn moduulin alkeisjakat ovat yksikäsitteiset.

Osoitetaan seuraavaksi, että alkeisjakajaesityksen antamat alkulukujen potenssit voidaan ryhmitellä eri alkulukujen mukaan niin sanoituksi p-primäärisiksi komponenteiksi.

MÄÄRITELMÄ 5.25. Olkoon R pääideaalialue ja M äärellisesti viritetty R-torsiomoduuli siten, että $M \neq \{0\}$ ja $\mathrm{Ann}(M) = (a) \neq (0)$. Olkoon myös $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ renkaan R annihilaattorin virittäjän a alkulukutekijäesitys. Tällöin joukko

$$N_i = \{x \in M \mid p_i^{\alpha_i} x = 0\},$$

missä $i \in \{1, \ldots, n\}$ on torsiomoduulin M *p_i-primäärinen komponentti*.

LAUSE 5.26. *Olkoon $N_1, N_2, \ldots, N_t$ torsiomoduulin M p_i-primäärisiä komponentteja. Tällöin alimoduuleille N_i pätee $Ann(N_i) = (p_i^{\alpha_i})$ ja*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_t.$$

TODISTUS. Lauseiden 5.21 ja 5.23 mukaan torsiomoduulille M pätee

$$M \cong R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t}),$$

alkulukujen $p_i \in R$ potensseilla $p_i^{\alpha_i}$. Olkoon $p \in R$ alkuluku ja $\beta \in \mathbb{Z}^+$ Nyt, jos $x + (p_i^{\beta}) \in R/p_i^{\beta}$, niin tällöin $p^{\beta} x \in (p^{\beta})$, eli $p_i^{\beta} x + (p_i^{\beta}) = 0 + (p_i^{\beta}) = 0_{R/(p^{\beta})}$. Näin ollen $\mathrm{Ann}(R/(p^{\beta})) = (p_i^{\beta})$. Täten alkeisjakajaesityksen 5.23 mukaan jos $x \in M$, niin $x \in R/(p_i^{\alpha_i})$ jollain $i \in \{1, \ldots, t\}$, jolloin

$$\begin{aligned}(up_1^{\alpha_1} \ldots p_t^{\alpha_t})x &= (up_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_t^{\alpha_t}) p_i^{\alpha_i} x \\ &= (up_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_t^{\alpha_t}) 0 \\ &= 0.\end{aligned}$$

Näin ollen $\mathrm{Ann}(M) = up^{\alpha_1} \ldots p^{\alpha_t}$.

Jos alkuluvut p_i ovat renkaan R erillisiä alkioita, niin väite pätee. Olkoon näissä alkuluvuissa $1 \leqslant k \leqslant t$ eri alkulukua ja $\alpha_1^i, \ldots, \alpha_{t_i}^i$ niiden potenssit kaikilla $i \in \{1, \ldots, k\}$. Ryhmittelemällä sykliset moduulit $R/(p_i^{\alpha_i})$ uudelleen eri alkulukujen p_i suhteen saadaan

$$M \cong \bigoplus_{i=1}^{t_1} R/(p_1^{\alpha_i^1}) \oplus \bigoplus_{i=1}^{t_2} R/(p_2^{\alpha_i^2}) \oplus \cdots \oplus \bigoplus_{i=1}^{t_k} R/(p_k^{\alpha_i^k}).$$

Tällöin merkitsemällä $N_i = R/(p_i^{\alpha_1^i}) \oplus \cdots \oplus R/(p_i^{\alpha_{t_i}^i})$ ja soveltamalla edellä olevaa päättelyä moduuleille N_i saadaan annihilaattoreiksi $\mathrm{Ann}(N_i) = u_i p_i^{\alpha_1^i} \ldots p_i^{\alpha_{t_i}^i}$, jollain yksiköllä $u_i \in R^{\times}$. Täten siis alimoduulit N_i ovat moduulin M p_i-primääriset komponentit, jolloin kyseessä on haluttu esitys. □

Koska lauseen 3.44 mukaan alkuluvun $p \in R$ virittämä pääideaali (p) on maksimaalinen ideaali, niin lauseen 3.29 nojalla tekijärenkas $R/(p)$ on kunta. Tämä antaa meille keinon yhdistää pääideaalialueiden moduulien teoriaa kuntien teoriaan ja täten myös vektoriavaruuksien teoriaan.

LEMMA 5.27. *Olkoon R pääideaalialue ja $p \in R$ alkuluku. Tällöin tekijämoduuli $R/(p)$ on kunta ja seuraavat väittämät pätevät.*

(1) Jos $M = R^r$, niin $M/pM \cong (R/(p))^r$.

(2) Jos $M = R/(a)$, missä $a \in R$, $a \neq 0$, niin

$$M/pM \cong \begin{cases} R/(p) & jos\, p \mid a \\ 0 & jos\, p \nmid a. \end{cases}$$

(3) Jos $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ siten, että $p \mid a_i$ kaikilla $i \in \{1, \ldots, k\}$, niin $M/pM \cong (R/(p))^k$.

TODISTUS. (1) Koska projektiokuvaus

$$\varphi : R^r \to (R/(p))^r, (a_1, a_2, \ldots, a_r) \mapsto (a_1 + (p), a_2 + (p), \ldots, a_r + (p))$$

on surjektiivinen R-moduulihomomorfismi, jonka ydin koostuu moduulin R^r alkioista $(a_1, a_2, \ldots, a_r)$ jossa $a_i \in (p)$, eli toisin sanoen $a_i = r'p$ jollain $r' \in R$ ja kaikilla $i \in \{1, \ldots, r\}$, niin $\ker \varphi = pR^r$. Tällöin ensimmäisen isomorfismilauseen 4.12 mukaan

$$M/pM \cong (R/(p))^r.$$

(2) Olkoon $\varphi : R \to M/pM$, $\varphi(r) = (r + (a)) + pM$. Nyt, koska

$$pM = p(R/(a)) = pR + (a) = (p) + (a),$$

niin φ on luonnollisten projektio R-moduulihomomorfismien $\pi_1 : R \to R/(a)$, sekä $\pi_2 : R/(a) \to (R/(a))/p(R/(a))$ yhdisteenä $\varphi = \pi_2 \circ \pi_1$ surjektiivinen R-moduulihomomorfismi, jonka ydin on renkaan R alkioiden p ja a virittämä ideaali $\ker \varphi = (p) + (a)$.

Koska R on pääideaalialue, niin lauseen 3.39 mukaan alkioiden $a, p \in R$ suurin yhteinen tekijä $\text{syt}(a, p)$ virittää ideaalin $(a) + (p)$. Täten, jos $p \mid a$, niin $\text{syt}(a, p) = p$, jolloin p virittää ideaalin $(a) + (p)$ eli $(a) + (p) = (p)$. Tällöin ensimmäisen isomorfismilauseen 4.12 mukaan

$$R/(p) \cong M/pM.$$

Jos taas $p \nmid a$, niin $\text{syt}(a, p) = 1$, jolloin $1 \in R$ virittää ideaalin $(a) + (p)$, eli $(a) + (p) = (1) = R$. Tällöin ensimmäisen isomorfismilauseen mukaan

$$0 \cong R/R \cong M/pM.$$

(3) Jos $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ siten, että $p \mid a_i$ kaikilla $i \in \{1, \ldots, n\}$, niin $pM = pR/(a_1) \oplus pR/(a_2) \oplus \cdots \oplus pR/(a_k)$, jolloin lauseen 4.29 ja kohdan (2) mukaan saadaan

$$\begin{aligned} M/pM &= \bigoplus_{i=1}^{k} (R/(a_i)) / \bigoplus_{i=1}^{k} (pR/(a_i)) \\ &\cong \bigoplus_{i=1}^{k} (R/(a_i))/(pR/(a_i)) \\ &\overset{(2)}{\cong} \bigoplus_{i=1}^{k} R/(p) \cong (R/(p))^k. \end{aligned}$$

□

Osoitetaan seuraavaksi, että äärellisesti viritetyn pääideaalialueen moduulin alkeisjakaja, sekä invarianttien tekijöiden esitykset ovat yksikäsitteiset.

LAUSE 5.28 (Yksikäsitteisyys). *Olkoon R pääideaalialue ja M sekä N äärellisesti viritettyjä moduuleita. Moduulit M ja N ovat isomorfiset jos ja vain jos niillä on sama vapaa aste, sekä samat invariantit tekijät ja alkeisjakajat.*

TODISTUS. Jos moduuleilla M_1 ja M_2 on sama vapaa-aste, sekä samat invariantit tekijät tai alkeisjakajat, niin lauseiden 5.21 ja 5.23 mukaan saadaan isomorfismi $M_1 \cong M_2$.

Oletetaan, että $M_1 \cong M_2$. Olkoon nyt $x \in \mathrm{Tor}(M_1)$. Tällöin, jos kuvaus $\varphi : M_1 \to M_2$ on isomorfismi, niin $r\varphi(x) = \varphi(rx) = \varphi(0_{M_1}) = 0_{M_2}$, kun $r \in R$ siten, että $rx = 0_{M_1}$. Näin ollen $\varphi(\mathrm{Tor}(M_1)) = \mathrm{Tor}(M_2)$, eli $\mathrm{Tor}(M_1) \cong \mathrm{Tor}(M_2)$. Tällöin lauseen 4.13 mukaan

$$M_1/\mathrm{Tor}(M_1) \cong M_2/\mathrm{Tor}(M_2). \tag{1}$$

Olkoon nyt

$$M_1 \cong R^{r_1} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \cong R^{r_1} \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t}), \text{ sekä}$$
$$M_2 \cong R^{r_2} \oplus R/(b_1) \oplus \cdots \oplus R/(b_{m'}) \cong R^{r_2} \oplus R/(q_1^{\beta_1}) \oplus \cdots \oplus R/(q_{t'}^{\beta_{t'}})$$

moduulien M_1 ja M_2 lauseiden 5.23, sekä 5.21 mukaiset esitykset. Koska lauseen 5.21 kohdan (3) mukaan äärellisesti viritetyn moduulin torsio on sen invarianttien tekijöiden esityksessä esiintyvien syklisien moduulien suora summa, niin moduulille $\mathrm{Tor}(M_1) = R/(a_1) \oplus \cdots \oplus R/(a_m)$, jolloin $M_1/\mathrm{Tor}(M_1) = R^{r_1}$. Täten käyttämällä vastaavaa päättelyä moduulille M_2 saadaan $M_i/\mathrm{Tor}(M_i) \cong R^{r_i}$, kaikilla $i \in \{1, 2\}$. Näin ollen yhtälön (1) mukaan $R^{r_1} \cong R^{r_2}$, jossa r_i on moduulin M_i vapaa-aste.

Olkoon $p \in R$ alkuluku. Koska isomorfismista $R^{r_1} \cong R^{r_2}$ seuraa $pR^{r_1} \cong pR^{r_2}$ niin lauseen 4.13 mukaan

$$R^{r_1}/pR^{r_1} \cong R^{r_2}/pR^{r_2},$$

jolloin lemman 5.27 kohdan (1) mukaan

$$(R/(p))^{r_1} \cong (R/(p))^{r_2}.$$

Nyt, koska $R/(p)$ on kunta, niin lauseen 4.37 mukaan $r_1 = r_2$, eli moduuleilla M_1 ja M_2 on samat vapaat-asteet.

Riittää siis osoittaa, että moduuleilla M_1 ja M_2 on samat invariantit tekijät ja alkeisjakajat. Koska lauseiden 5.23 ja 5.21 mukaan moduulit voidaan esittää suorana summana vapaasta moduulista sekä torsiomoduuleista, niin voimme olettaa, että moduulit M_1 ja M_2 ovat torsiomoduuleita, Tällöin moduuleilla M_1 ja M_2 on esitykset

$$M_1 \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t}), \text{ sekä}$$
$$M_2 \cong R/(b_1) \oplus \cdots \oplus R/(b_{m'}) \cong R/(q_1^{\beta_1}) \oplus \cdots \oplus R/(q_{t'}^{\beta_{t'}}).$$

Osoitetaan, että moduuleilla M_1 ja M_2 on samat alkeisjakajat. Olkoon p jonkin renkaan R alkuluku. Tällöin, koska moduulien M_1 ja M_2 alkeisjakajat ovat renkaan R alkulukujen potensseja, niin riittää osoittaa, että niillä on samat alkuluvun p potensseja vastaavat alkeisjakajat.

Koska moduulien M_1 ja M_2 annihilaattorit ovat määritelmän 5.15 mukaan renkaan R ideaaleja, niin renkaan R ollessa pääideaali saadaan $\mathrm{Ann}(M_i) = (r_i)$, jollain $r_i \in R$, $i \in \{1, 2\}$. Olkoot N_p^1 ja N_p^2 moduulien M_1 ja M_2 p-primääriset

komponentit. Koska lauseen 5.17 mukaan isomorfisien moduulien annihilaattorit ovat täsmälleen samat ja moduulien M_1 ja M_2 p-primäärisien komponenttien annihilaattorit ovat alkuluvun p potensseja, niin esityksen 5.26 mukaan moduulien M_1 ja M_2 p-primääriset komponentit ovat isomorfisia, eli $N_p^1 \cong N_p^2$. Täten riittää osoittaa, että jos R-moduulien N_1 ja N_2 annihiliaattori on jokin alkuluvun p potenssi ja $N_1 \cong N_2$, niin moduuleilla N_1 ja N_2 on samat alkeisjakajat.

Olkoon moduulin N_1 ja N_2 annihilaattori $\mathrm{Ann}(N_1) = \mathrm{Ann}(N_2) = (p^q)$. Tehdään induktio alkuluvun p potenssin q suhteen. Tällöin, jos $q = 0$, niin $\mathrm{Ann}(N_1) = (p^0) = (1)$, jolloin $1x = x = 0$ kaikilla $x \in N_1$. Näin ollen $N_1 = \{0\}$. Koska isomorfisien moduulien annihilaattorit ovat samat, niin myös $N_2 = \{0\}$, jolloin moduulit M_1 ja M_2 ovat vapaita moduuleita, eli niillä ei ole alkeisjakajia. Täten väite pätee kun $q = 0$.

Olkoon siis $q > 0$. Oletetaan, että tällöin moduuleilla N_1 ja N_2 on samat alkeisjakajat jollain $q \in \mathbb{Z}^+$. Lauseen 5.23 mukaan moduuli N_1 voidaan esittää suorana summana tekijämoduuleista $R/(p^\alpha)$, jossa p^α on renkaan R alkuluvun potenssi. Nyt, koska moduulin N_1 annihilaattori on (p^q) ja lauseen 5.18 mukaan tekijämoduulin $R/(p^\alpha)$ annihilaattori on (p^α), niin jokainen ideaaleista (p^α) sisältyy moduulin N_1 annihilaattoriin (p^q). Täten moduulin N_1 alkeisjakajat ovat jotain alkuluvun p potensseja, jossa jokaisen alkuluvun potenssi on enintään q. Olkoon täten moduulin N_1 alkeisjakajat muotoa

$$\underbrace{p, p, \ldots, p}_{\text{n kertaa}}, p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_s},$$

jossa $2 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_s = q$, jolloin moduulilla N_1 on alkeisjakajaesitys

$$N_1 \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{\text{n kertaa}} \oplus R/(p^{\alpha_1}) \oplus \cdots \oplus R/(p^{\alpha_s}),$$

jossa moduulien $R/(p), R/(p^{\alpha_i})$ annihilaattorit ovat lauseen 5.18 mukaan

$$(p), \ldots, (p), (p^{\alpha_1}), \ldots, (p^{\alpha_s}).$$

Tällöin moduuli $pN_1 = \{px \mid x \in N_1\}$ voidaan esittää syklisien moduulien suorana summana

$$pN_1 \cong \underbrace{pR/(p) \oplus \cdots \oplus pR/(p)}_{\text{n kertaa}} \oplus pR/(p^{\alpha_1}) \oplus \cdots \oplus pR/(p^{\alpha_s}).$$

Koska lauseen 5.18 mukaan tekijämoduulin $R/(p^q)$, $q \in \mathbb{Z}$ annihilaatori on ideaali (p^q) ja jokaisella $px + (p^q) \in pR/(p^q)$ ja $rp^{q-1} \in (p^{q-1})$ pätee

$$rp^{q-1}(px + (p^q)) = rp^{q-1}px + (p^q) = r(p^q x) + (p^q) = 0 + (p^q),$$

niin tekijämoduulien $pR/(p), pR/(p_i^{\alpha_i})$ annihilaattorit ovat vastaavasti ideaalit

$$\underbrace{(1), \ldots, (1)}_{\text{n kertaa}}, (p^{\alpha_1 - 1}), \ldots, (p^{\alpha_s - 1}).$$

Nyt, koska lauseen 5.20 mukaan moduulit $R/(p), R/(p^{\alpha_i})$, $i \in \{1, \ldots, s\}$ ovat syklisiä moduuleja, joiden virittäjät ovat vastaavasti $x, x_i \in R$, niin moduulit $pR/(p), pR/(p^{\alpha_i})$ ovat syklisiä moduuleja, joiden virittäjät ovat $px, px_i \in R$.

Tällöin, koska sykliset moduulit C ovat isomorfisia tekijämoduulin $R/\mathrm{Ann}(C)$ kanssa, niin moduulin pN_1 alkeisjakajaesitys antaa isomorfismin

$$\begin{aligned} pN_1 &\cong \underbrace{R/(1) \oplus \cdots \oplus R/(1)}_{\text{n kertaa}} \oplus R/(p^{\alpha_1-1}) \oplus \cdots \oplus R/(p^{\alpha_s-1}) \\ &\cong R/(p^{\alpha_1-1}) \oplus \cdots \oplus R/(p^{\alpha_s-1}), \end{aligned}$$

sillä lauseen mukaan 3.25 $R/(1) = R/R = \{0\}$. Näin ollen moduulin pN_1 alkeisjakajat ovat

$$p^{\alpha_1-1}, p^{\alpha_2-1}, \ldots, p^{\alpha_s-1}.$$

Samoin, jos moduulin N_2 alkeisjakajat ovat

$$\underbrace{p, p, \ldots, p}_{\text{m kertaa}}, p^{\beta_1}, p^{\beta_2}, \ldots, p^{\beta_t},$$

niin vastaavalla päättelyllä sen alimoduulin pN_1 alkeisjakajat ovat

$$p^{\beta_1-1}, p^{\beta_2-1}, \ldots, p^{\beta_t-1}.$$

Koska $N_1 \cong N_2$, niin $pN_1 \cong pN_2$. Tällöin, koska moduulin pN_1 annihilaattorin alkuluvun p potenssi on $q-1$, niin induktio-oletuksen mukaan moduuleilla pN_1 ja pN_2 on samat alkeisjakajat. Täten $s = t$ ja $\alpha_i - 1 = \beta_t - 1$, eli $\alpha_i = \beta_i$ kaikilla $i \in \{1, \ldots, s\}$. Nyt, koska lauseen 4.13 mukaan $N_1/pN_1 \cong N_2/pN_2$, niin lemman 5.27 kohdan (3) mukaan kunnalle $R/(p)$ pätee $R/(p)^{n+s} \cong R/(p)^{s+t}$. Täten $n + s = m + t$ eli $n = m$. Näin ollen moduulien N_1 ja N_2 alkeisjakajat ovat täsmälleen samat.

Osoitetaan lopuksi, että moduuleilla M_1 ja M_2 on samat invariantit tekijät. Jos $a_1 \mid a_2 \mid \cdots \mid a_n$ ovat moduulin M_1 invariantit tekijät, niin lauseen 5.23 todistuksen mukaisesti jokainen a_i voidaan esittää yksiköllä kertomista vaille yksikäsitteisenä alkulukujen tulona, josta saadaan moduulin M_1 alkeisjakajaesitys alkuluvuilla $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$. Samoin, jos $b_1 \mid b_2 \cdots \mid b_m$ ovat moduulin M_2 invariantit tekijät, niin $q_1^{\beta_1}, \ldots, q_t^{\beta_t}$ ovat sen alkeisjakajat. Nyt, koska $M_1 \cong M_2$, niin edellisen kohdan mukaan moduuleilla M_1 ja M_2 on samat alkeisjakajat, eli $s = t$ ja $p_i^{\alpha_i} = q_i^{\beta_i}$. Näin ollen $n = m$ ja $\alpha_i = \beta_i$ kaikilla $i \in \{1, \ldots, n\}$, jolloin moduulien yksikäsitteiset alkulukuesitykset antavat samat invariantit tekijät. □

Olemassaolo ja yksikäsitteisyyslauseet antavat yhdessä niin sanotun *äärellisesti viritettyjen pääideaalialueen moduulien päälauseen.*

Lause 5.29 (Päälause). *Olkoon R pääideaalialue ja M äärellisesti viritetty R-moduuli. Tällöin on olemassa yksikäsitteiset alkiot $r, m, t, \alpha_i \in \mathbb{Z}^+$, missä $i \in \{1, \ldots, t\}$ sekä alkiot $a_1, a_2, \ldots, a_m \in R - \{0\}$, joille pätee $a_1 \mid a_2 \mid \cdots \mid a_m$ ja $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_t} \in R$, jossa p_i on renkaan R alkuluku siten, että*

$$\begin{aligned} M &\cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \\ &\cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t}). \end{aligned}$$

Lisäksi moduuli M on torsiovapaa jos ja vain jos se on vapaa moduuli, sekä

$$Tor(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

eli toisin sanoen M on torsiomoduuli jos ja vain jos $r = 0$ ja tällöin moduulin M annihilaattori on $Ann(M) = (a_m)$.

5.3. Päälauseen sovelluksia

Tarkastellaan seuraavaksi joitain pääideaalialueen moduulien päälauseen sovelluksia. Koska jotkin käsittelemistämme sovelluksista nojaavat tässä tutkielmassa käsittelemättömään teoriaan, kuten matriisien, sekä polynomirenkaiden teoriaan niin tyydymme vain kuvailemaan sovelluksien ideoita täsmällisien todistuksien sijasta.

Koska esimerkin 4.8 mukaan abelin ryhmät ovat täsmälleen $\mathbb{Z}$ moduuleja, niin pääideaalialueen moduulien päälause pätee erityisesti äärellisesti viritetyille abelin ryhmille. Tämä sovellus antaa niin sanotun *äärellisesti viritettyjen abelin ryhmien päälauseen.*

Seuraus 5.30 (Äärellisesti viritettyjen abelin ryhmien päälause). *Olkoon G äärellisesti viritetty abelin ryhmä. Tällöin on olemassa yksikäsitteiset luvut $r, s, n_1, n_2, \ldots, n_s \in \mathbb{Z}$ siten, että*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

ja $r \geqslant 0$ ja $n_j \geqslant 2$ kaikilla $j \in \{1, \ldots, s\}$, sekä $n_{i+1} \mid n_i$ kaikilla $1 \leqslant i \leqslant s-1$.

Todistus. Olkoon G äärellisesti viritetty abelin ryhmä. Koska esimerkin 4.8 mukaan abelin ryhmät ovat täsmälleen $\mathbb{Z}$ moduuleja, niin G on $\mathbb{Z}$ moduuli. Esimerkin 3.24 mukaan $\mathbb{Z}$ on pääideaalialue, jolloin lauseen 5.29 mukaan on yksikäsitteiset luvut $q, a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$, $a_i \neq 0$ kaikilla $i \in \{1, \ldots, m\}$ siten, että ryhmä G voidaan esittää aliryhmiensä suorana summana

$$G \cong \mathbb{Z}^q \oplus \mathbb{Z}/\langle a_1 \rangle \oplus \mathbb{Z}/\langle a_2 \rangle \oplus \cdots \oplus \mathbb{Z}/\langle a_m \rangle$$

ja $a_1 \mid a_2 \mid \cdots \mid a_m$. Koska ideaalit (a_i) koostuvat alkioista $x = za_i$, jollain $z \in \mathbb{Z}$, niin ne koostuvat kokonaisluvuista, jotka ovat jaollisia luvulla a_i. Toisin sanoen $(a_i) = a_i\mathbb{Z}$ kaikilla $i \in \{1, \ldots, m\}$. Näin ollen tekijämoduulit $\mathbb{Z}/(a_i)$ ovat abelin tekijäryhmiä $\mathbb{Z}/a_i\mathbb{Z}$. Nyt, koska lauseen 2.36 mukaan $\mathbb{Z}/a_i\mathbb{Z} \cong \mathbb{Z}_{a_i}$ kaikilla $i \in \{1, \ldots, m\}$, niin lauseen 4.27 nojalla saadaan

$$\begin{aligned} G &\cong \mathbb{Z}^q \oplus \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_m} \\ &\cong \mathbb{Z}^q \times \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_m}. \end{aligned}$$

jossa $a_1 \mid a_2 \mid \cdots \mid a_m$. Jos $a_i = 1$ jollain i, niin $(1) = \mathbb{Z}$, joten $\mathbb{Z} = \mathbb{Z}_1$ ja tällöin

$$\mathbb{Z}^q \times \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_m} \cong \mathbb{Z}^{q+1} \times \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_m - 1}.$$

Jos nyt $0 \leqslant p \leqslant q$ on lukumäärä niistä a_i, joilla $a_i = 1$, niin merkitsemällä $r = q + p$, indeksoimalla loput $a_i \geqslant 2$ jakoyhtälön $a_1 \mid a_2 \mid \cdots \mid a_m$ mukaan kaikilla $i \in \{1, \ldots, s\}$, missä $s = m - p$, ja tämän jälkeen merkitsemällä $a_i = n_{s-i}$ saadaan

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s},$$

jossa $n_{i+1} \mid n_i$ kaikilla $i \in \{1, \ldots, s\}$ ja $r \geqslant 0$, sekä $n_i \geqslant 2$. □

Äärellisesti viritettyjen abelin ryhmien päälause antaa keinon selvittää kaikki isomorfismia vaille eri tietyn kokoiset äärelliset abelin ryhmät. Huomataan ensiksi, että ryhmä on äärellinen jos ja vain jos sen vapaa aste on nolla. Nimittäin, jos äärellisesti viritetyn abelin ryhmän G vapaa aste on $n > 0$, niin päälauseen 5.30 mukaan $G \cong R^n \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$, jollain $n_i, s \in \mathbb{Z}^+$, jossa $R^n \cong \mathbb{Z}^n$ lauseen 4.30 nojalla. Tällöin, koska R^n on numeroituvasti ääretön ja sykliset

ryhmät $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_s}$, ovat määritelmän 2.31 mukaan n_i-alkioisia ryhmiä, niin G on äärellinen jos ja vain jos $n = 0$.

Voidaan osoittaa, että ryhmien $G_1, \ldots, G_n$ suoran tulon mahtavuus on ryhmien $G_1, \ldots, G_n$ mahtavuuksien tulo [**2**, s. 153]. Nyt, jos G on äärellinen abelin ryhmä jonka mahtavuus on $n \in \mathbb{Z}^+$, niin päälauseen esityksen mukaan $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ $n = n_1 n_2 \ldots n_s$, jossa luvut n_i ovat ryhmän G invariantit tekijät. Tällöin ryhmän G mahtavuus on $n = n_1 n_2 \ldots n_s$.

Koska päälauseen yksikäsitteisyyden mukaan äärellisesti viritetyt abelin ryhmät ovat isomorfiset jos ja vain jos niillä on samat invariantit tekijät, niin jokaista eri jonoa lukuja $n_1, n_2, \ldots, n_s$ vastaa kokoelma moduuleita, jotka ovat isomorfiset vain toisten samoja invariantteja tekijöitä vastaavien ryhmien kanssa. Näin ollen, jos löydämme kaikki luvut $n_1, n_2, \ldots, n_s$, joille pätee $n = n_1 n_2 \ldots n_s$ ja jotka toteuttavat invarianttien tekijöiden vaatimukset $n_j \geqslant 2$, sekä $n_{j+1} \mid n_j$ kaikilla $j \in \{1, \ldots, s\}$, niin olemme löytäneet kaikki mahdolliset n-alkioiset abelin ryhmät samoja invariantteja tekijöitä vastaavien ryhmien isomorfismeja vaille. Täten jokainen n-alkioinen ryhmä on isomorfinen täsmälleen yhden löytämämme ryhmän kanssa. Seuraava esimerkki hahmottaa, kuinka tämä päättely toimii käytännössä ja esittelee aiheeseen liittyvän yleisen tuloksen.

Esimerkki 5.31. Etsitään kaikki 42-alkioiset abelin ryhmät isomorfismeja vaille. Huomataan, että luvulla $42 \in \mathbb{Z}$ on alkulukuesitys $42 = 2 \cdot 3 \cdot 7$. Olkoot nyt $n_1, n_2, \ldots, n_s$ 42-alkioisen ryhmän invariantteja tekijöitä. Tällöin luku 42 voidaan esittää kyseisien invarianttien tekijöiden tulona, eli $42 = n_1 n_2 \ldots n_s$. Koska luku 42 voidaan esittää myös alkulukujen tulona $42 = 2 \cdot 3 \cdot 7$, niin lauseen 3.46 mukaan jokainen alkuluvuista $2, 3$, sekä 7 jakaa jonkin invariantin tekijän n_i. Täten jakoyhtälön $n_1 \mid n_2 \mid \cdots \mid n_s$ mukaan pätee $2 \mid n_1$, $3 \mid n_1$, sekä $7 \mid n_1$. Tällöin, koska alkuluvuille $2, 3, 7$ pätee $\operatorname{syt}(2, 3) = 1 = \operatorname{syt}(2 \cdot 3, 7)$, niin käyttämällä lausetta 3.40 lukuihin $2, 3$ ja $2 \cdot 3, 7$ saadaan $42 = 2 \cdot 3 \cdot 7 \mid n_1$.

Koska myös $n_1 \mid 42$, niin on luvut $a, b \in \mathbb{Z}^+$ siten, että $42 = an_1 = ab(42)$, jolloin supistussäännön 3.13 mukaan $n_1 = 42$. Näin ollen ainoa mahdollinen invariantti tekijä on $n_1 = 2 \cdot 3 \cdot 7$, sillä ei ole toista invarianttia tekijää n_2, jolle pätee $n_1 n_2 = 2 \cdot 3 \cdot 7$. Täten ainoa 42-alkioinen äärellisesti viritetty abelin ryhmä on ryhmä $\mathbb{Z}_{42}$. Vastaava päättely yleisessä tapauksessa osoittaa, että jos kokonaisluvulla on erillisien alkulukujen tuloesitys, eli alkulukujen tuloesitys jossa jokaisen alkuluvun potenssi on yksi, niin kyseinen luku itse on ainoa invariantti tekijänsä, eli kyseisen kokoisia ryhmiä on vain yksi. [**2**, s. 159].

Pääideaalialueiden päälause antaa myös tavan esittää neliömatriisit diagonaalimatriiseja muistuttavien yläkolmiomatriisien avulla. Tätä kutsutaan *Jordanin kanoniseksi muodoksi*. Sovellus nojaa tietoon että, kun K-kertoimisen vektoriavaruuden V kanta on kiinnitetty, niin lineaarikuvausta $T : V \to V$ vastaa neliömatriisi, jonka alkiot ovat kunnan K alkioita. Samoin K-alkioista neliömatriisia vastaa lineaarikuvaus $V \to V$ [**1**, s. 111], [**2**, s. 415].

Voidaan osoittaa, että samoin kuten esimerkin 4.8 mukaan abelin ryhmät ovat täsmälleen $\mathbb{Z}$ moduuleita, niin kunnan K-kertoimisten polynomien renkaan $K[x]$ [**1**, s. 350] moduulit ovat täsmälleen K-kertoimisten vektoriavaruuksien lineaarikuvauksia $T : V \to V$, joille pätee $T(v) = xv$. [**1**, s. 476], [**2**, s. 340]. Voidaan myös osoittaa, että jos V on äärellisuloitteinen vektoriavaruus, niin lineaarikuvauksen T ominaisarvot $(x - \lambda)^n$, jossa $\lambda \in K$ ja $n \in \mathbb{Z}^+$ ovat täsmälleen

$K[x]$-moduulin V alkeisjakajat [**2**, s. 491]. Tällöin, koska polynomirengas $F[x]$ on pääideaalialue [**1**, s. 397], niin olettamalla, että lineaarikuvauksen T ominaisarvot sisältyvät vektoriavaruuteen V saadaan pääideaalialueen moduulien päälauseen 5.29 mukaan

$$V \cong F[x]/(x-\lambda_1)^{n_1} \oplus \cdots \oplus F[x]/(x-\lambda_s)^{n_s},$$

joillain $s, n_i \in \mathbb{Z}^+$ ja lineaarikuvauksen T ominaisarvoilla λ_i. Tällöin alkiot

$$(x'-\lambda_i)^{s_i-1}, (x'-\lambda_i)^{s_i-2}, \ldots, x'-\lambda_i, 1$$

muodostavat vektoriavaruuden $F[x]/(x-\lambda_i)^{n_i}$ kannan kaikilla $i \in \{1, \ldots, s\}$, jolloin lineaarikuvausta T vastaava matriisi tämän kannan suhteen on muotoa

$$J_i = \begin{bmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{bmatrix},$$

jossa matriisin alkiot ovat nollia alkioita λ_i ja 1 lukuunottamatta. Matriisia J_i kutsutaan lineaarikuvauksen T ominaisarvoa λ_i vastaavaksi *Jordanin lohkoksi*.

Näin ollen, koska vektoriavaruus V voidaan esittää tekijä aliavaruuksiensa $F[x]/(x-\lambda_i)^{n_i}$ suorana summana, niin lineaarikuvausta T vastaava matriisi vektoriavaruuden V jonkin kannan suhteen on muotoa

$$J = \begin{bmatrix} J_1 & & & & \\ & J_2 & & & \\ & & \ddots & & \\ & & & J_{s-1} & \\ & & & & J_s \end{bmatrix}$$

oleva matriisi, jota kutsutaan lineaarikuvausta T vastaavaksi *Jordan-matriisiksi*, joka on yksikäsitteinen Jordanin lohkojen J_i järjestystä vaille. [**2**, s. 492]. Tällöin, jos M on lineaarikuvausta T vastaava alkuperäinen matriisi, niin on kääntyvä neliömatriisi P siten, että $M = P^{-1}JP$ [**1**, s. 116].

Kirjallisuutta

[1] Artin, Michael: *Algebra*, Ensimmäinen laitos, Prentice-Hall, Inc., 1991.

[2] Dummit, David S. ja Foote, Richard M.: *Abstract Algebra*. Kolmas laitos, John Wiley and Sons, Inc., 2004.

[3] Herstein, I. N. *Topics in Algebra* Toinen laitos, John Wiley & sons, 1975

[4] Hungerford, Thomas W.: *Algebra*, Kolmas laitos, Springer-Verlag, 1984.

[5] Häsä, Jokke ja Rämö, Johanna: *Johdatus Abstraktiin Algebraan*. Ensimmäinen laitos, Gaudeamus Helsinki University Press, 2012.

[6] Ribenboim, Paulo: *Rings and Modules*, Ensimmäinen laitos, John Wiley & sons, 1969