TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Jyri Hiltunen

Pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennelause

Informaatiotieteiden yksikkö
Matematiikka
Helmikuu 2014

Tampereen yliopisto
Informaatiotieteiden yksikkö
HILTUNEN, JYRI: Pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennelause
Pro gradu -tutkielma, 58 s.
Matematiikka
Helmikuu 2014

Tiivistelmä

Tässä pro gradu -tutkielmassa tarkastellaan pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennetta. Yksinkertaistettuna rakennelause kertoo, että pääideaalialueen yli määritelty äärellisviritteinen moduli voidaan esittää yksikäsitteisen hajotelman avulla samaan tapaan kuin kokonaisluku voidaan esittää sen jaottomien tekijöiden tulona.

Tutkielman alussa esitellään rakennelauseen käsittelemisessä tarvittavia abstraktin algebran peruskäsitteitä, kuten esimerkiksi alkuideaali, maksimaalinen ideaali, pääideaalialue ja äärellisviritteisen vapaan modulin aste. Rakennelauseen tarkastelu aloitetaan esittelemällä käsite torsio sekä siihen liittyviä ominaisuuksia. Pääideaalialueen yli määritellyn äärellisviritteisen vapaan modulin rakenteeseen päästään käsiksi toteamalla jokaisen äärellisviritteisen vapaan modulin alimodulin olevan myöskin äärellisviritteinen ja vapaa, ja osoittamalla, että tämän modulin kannan avulla voidaan muodostaa sen alimodulin kanta, ja että tämän kannan alkioilla on tietty ominaisuus. Tiedetään, että itse modulin ja samaa astetta olevan vapaan modulin välillä on olemassa homomorfinen kuvaus, joten modulien isomorfialauseen ja edellä mainittujen kantojen ominaisuuksien avulla päästään osoittamaan, että alkuperäinen moduli on isomorfinen vapaan modulin ja torsiomodulin suoran summan kanssa. Lisäksi todetaan, että tämä esitysmuoto on pääideaalialueen yksiköitä vaille yksikäsitteinen. Rakennelauseen yhteydessä tutustutaan myöskin invariantteihin tekijöihin ja alkeisjakajiin.

Tutkielmassa tarkastellaan myös euklidisen alueen yli määritellyn matriisin Smithin normaalimuotoa, jonka avulla matriisin invariantit tekijät voidaan löytää. Lisäksi tarkastellaan kuinka matriisien similaarisuutta voidaan tutkia Smithin normaalimuodon avulla.

Tutkielman päälähdeteoksina toimivat J. J. Rotmanin teos Advanced Modern Algebra sekä D. S. Dummitin ja R. M. Footen teos Abstract Algebra.

Sisältö

1 Johdanto

Tämän tutkielman tavoitteena on esitellä pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennetta kuvaava lause. Sen avulla nähdään, että äärellisviritteisen modulin rakenne koostuu vapaan modulin ja torsiomodulin suorasta summasta.

Luvussa 2 käydään läpi abstraktin algebran peruskäsitteitä. Vaikka lukijalta odotetaan pohjatietoina kurssit Algebra 1 ja 2 sekä Lineaarialgebra 1 ja 2, on tässä luvussa käyty suurin osa tutkielmassa tarvittavista käsitteistä ja lauseista läpi melko tarkasti. Luvun lopussa tarkastellaan äärellisviritteisen vapaan modulin astetta, joka on keskeisessä osassa tässä tutkielmassa.

Luku 3 aloitetaan tutustumalla nopeasti muun muassa käsitteisiin torsiomoduli ja torsiovapaus, jonka jälkeen lähdetään tarkastelemaan itse rakennelausetta. Aluksi osoitetaan, että pääideaalialueen yli määritellyn äärellisviritteisen vapaan modulin jokainen alimoduli on myöskin vapaa sekä äärellisviritteinen, ja modulin kannan avulla voidaan muodostaa tälle alimodulille kanta, jonka alkioiden välillä on tietty ominaisuus. Tiedetään, että itse modulin ja samaa astetta olevan vapaan modulin välillä on olemassa homomorfinen kuvaus. Täten modulien isomorfialauseen ja edellä mainittujen kantojen ominaisuuksien avulla päästään osoittamaan, että alkuperäinen moduli on isomorfinen vapaan modulin ja torsiomodulin suoran summan kanssa. Itse asiassa tämä torsiomoduli on isomorfinen syklisten modulien suoran summan kanssa, josta saadaan rakennelauseen yleinen muoto. Nämä sykliset modulit voidaan esittää joko invarianttien tekijöiden tai alkeisjakajien avulla. Luvun lopuksi osoitetaan, että rakennelause on pääideaalialueen yksiköitä vaille yksikäsitteinen.

Luvussa 4 tutustutaan käsitteeseen Smithin normaalimuoto. Luvussa osoitetaan, että jokainen euklidisen alueen yli määritelty matriisi voidaan viedä sellaiseen diagonaalimuotoon, jossa diagonaalialkiot toteuttavat tietyn jakorelaation. Tätä muotoa sanotaan Smithin normaalimuodoksi ja näitä diagonaalialkioita sanotaan matriisin invarianteiksi tekijöiksi. Lisäksi luvussa osoitetaan, että kahden matriisin similaarisuutta voidaan tutkia myöskin Smithin normaalimuodon avulla.

Tutkielman päälähdeteoksina toimivat J. J. Rotmanin teos *Advanced Modern Algebra* [1] sekä D. S. Dummitin ja R. M. Footen teos *Abstract Algebra* [3]. Lisäksi joitakin viittauksia on myös muihin teoksiin, joiden tiedot löytyvät tutkielman lopusta. Myös kurssien Algebra 2 sekä Lineaarialgebra 2 luentomuistiinpanoja käytettiin hyödyksi tutkielmaa kirjoitettassa, mutta viittaukset näihin jätettiin tekemättä.

2 Abstraktin algebran peruskäsitteitä

Tässä luvussa käydään läpi abstraktiin algebraan liittyviä peruskäsitteitä.

2.1 Renkaat ja modulit

Määritelmä 2.1. Sanotaan, että joukko R, jossa on annettu kuvaukset

$$+ : R \times R \to R, (x, y) \mapsto x + y$$

sekä

$$\cdot : R \times R \to R, (x, y) \mapsto xy,$$

on *rengas*, mikäli seuraavat ehdot pätevät:

1. kaikilla alkioilla $x, y, z \in R$ pätee $x + (y + z) = (x + y) + z$,
2. on olemassa alkio $0 \in R$ siten, että $x + 0 = 0 + x = x$ pätee kaikilla alkioilla $x \in R$,
3. kaikilla alkioilla $x \in R$ on olemassa alkio $-x \in R$ siten, että $x + (-x) = (-x) + x = 0$,
4. kaikilla alkioilla $x, y \in R$ pätee $x + y = y + x$,
5. kaikilla alkioilla $x, y, z \in R$ pätee $x(yz) = (xy)z$,
6. on olemassa alkio $1 \in R$ siten, että $1 \cdot x = x \cdot 1 = x$ pätee kaikilla alkioilla $x \in R$,
7. kaikilla alkioilla $x, y, z \in R$ pätee $x(y + z) = xy + xz$ sekä $(x + y)z = xz + yz$.

Sanotaan, että rengas R on *kommutatiivinen*, mikäli

$$xy = yx$$

kaikilla alkioilla $x, y \in R$.

Alkiota $u \in R$ sanotaan kommutatiivisen renkaan R *yksiköksi*, mikäli $u \mid 1$.

Huomautus. Tässä tutkielmassa renkaalla tarkoitetaan aina yksiköllistä rengasta, mikäli toisin ei sanota.

Määritelmä 2.2. Kommutatiivista rengasta R sanotaan *kokonaisalueeksi*, mikäli seuraavat ehdot pätevät:

1. $1 \neq 0$,
2. jos $ab = ac$ ja $a \neq 0$, niin $b = c$ kaikilla alkioilla $a, b, c \in R$.

Lause 2.1. *Olkoon R kommutatiivinen rengas. Rengas R on kokonaisalue, jos ja vain jos kaikilla alkioilla $a, b \in R$ on voimassa tulon nollasääntö*

$$ab = 0 \quad \Rightarrow \quad a = 0 \quad \vee \quad b = 0.$$

Todistus. Olkoon $a, b \in R$. Oletetaan ensin, että rengas R on kokonaisalue. Tällöin jos $ab = 0$, mutta $a \neq 0$, niin täytyy olla $b = 0$, joten tulon nollasääntö on voimassa.

Oletetaan sitten, että tulon nollasääntö on voimassa. Oletetaan lisäksi, että $ab = ac$ ja $a \neq 0$, missä alkiot $a, b, c \in R$. Tällöin

$$\begin{aligned} & ab = ac \\ \therefore \quad & ab - ac = 0 \\ \therefore \quad & a(b - c) = 0. \end{aligned}$$

Koska tulon nollasääntö on voimassa, niin

$$\begin{aligned} & b - c = 0 \\ \therefore \quad & b = c. \end{aligned}$$

Siis tällöin rengas R on kokonaisalue. □

Määritelmä 2.3. Kommutatiivista rengasta R sanotaan *kunnaksi*, mikäli $1 \neq 0$ ja kaikilla nollasta eroavilla alkioilla $x \in R$ on olemassa alkio $x^{-1} \in R$ siten, että

$$x \cdot x^{-1} = 1 \quad \text{ja} \quad x^{-1} \cdot x = 1.$$

Määritelmä 2.4. Kokonaisaluetta R sanotaan *euklidiseksi alueeksi*, mikäli on olemassa kuvaus

$$d : R \setminus \{0\} \to \mathbb{N}$$

siten, että

1. $d(x) = d(xy)$ kaikilla alkioilla $x, y \in R \setminus \{0\}$,
2. kaikilla alkioilla $x, y \in R$, missä $x \neq 0$, on olemassa sellaiset alkiot $q, r \in R$, että
$$y = qx + r,$$
missä $r = 0$ tai $d(r) < d(x)$.

Kuvausta d kutsutaan *astefunktioksi*.

Määritelmä 2.5. Olkoon R kommutatiivinen rengas. Additiivista Abelin ryhmää M, jossa on annettu kuvaus

$$\cdot : R \times M \to M, (r, m) \mapsto rm,$$

sanotaan *R-moduliksi*, mikäli kaikilla alkioilla $m, m' \in M$ ja $r, r' \in R$ pätevät seuraavat ehdot:

1. $r(m + m') = rm + rm'$,
2. $(r + r')m = rm + r'm$,
3. $(rr')m = r(r'm)$,
4. $1m = m$.

Edellä mainittua kuvausta $\cdot : R \times M \to M$ kutsutaan usein *skalaarikertolaskuksi*.

Huomautus. Jos määritelmässä 2.5 esitelty kommutatiivinen rengas R on kunta K, merkitään $R = K$, niin R-modulia M sanotaan *(K-)vektoriavaruudeksi*.

Määritelmä 2.6. Olkoon R kommutatiivinen rengas. R-modulia M sanotaan *sykliseksi*, mikäli se on yhden alkion $x \in M$ virittämä. Toisin sanoen

$$M = Rx = \{rx \mid r \in R\}.$$

Jos $x = 0$, niin $M = \{0\}$. Tällöin R-modulia M kutsutaan *nollamoduliksi*.

Määritelmä 2.7. Olkoon R kommutatiivinen rengas ja M R-moduli. Epätyhjää joukkoa $N \subseteq M$ sanotaan R-modulin M *alimoduliksi*, mikäli ehdot

1. $x, y \in N \Rightarrow x + y \in N$,
2. $a \in R$ ja $x \in N \Rightarrow ax \in N$

pätevät.

Määritelmä 2.8. Olkoon R kommutatiivinen rengas. R-modulia M sanotaan *äärellisviritteiseksi*, mikäli on olemassa äärellinen joukko $X := \{x_1, \ldots, x_n\} \subseteq M$ siten, että $M = \langle X \rangle$.

Määritelmä 2.9. Olkoon R kommutatiivinen rengas ja M R-moduli. Kuvausta

$$f : I \to M, i \mapsto x_i,$$

missä I on epätyhjä indeksijoukko, sanotaan *perheeksi* R-modulin M alkioita. Merkintä M^I tarkoittaa joukkoa, joka sisältää kaikki kuvaukset joukolta I R-modulille M. Indeksoitua perhettä merkitään $(x_i)_{i \in I} \in M^I$, missä $x_i := f(i)$ kaikilla alkioilla $i \in I$.

Määritelmä 2.10. Olkoon R kommutatiivinen rengas, M R-moduli ja $N \subseteq M$ alimoduli. Koska R-moduli M on Abelin ryhmä, voidaan muodostaa *tekijäryhmä*

$$M/N := \{x + N \mid x \in M\}.$$

Määritellään tekijäryhmän M/N yhteenlasku asettamalla

$$(x + N) + (y + N) := (x + y) + N$$

ja skalaarikertolasku asettamalla

$$a \cdot (x + N) := ax + N$$

kaikilla alkioilla $a \in R$ ja $x, y \in M$.

Määritelmä 2.11. Olkoon R kommutatiivinen rengas ja $(M_i)_{i \in I}$, missä I on indeksijoukko, perhe R-moduleita. R-modulien M_i *karteesinen tulo*, merkitään $\prod_{i \in I} M_i$, koostuu perheistä $(a_i)_{i \in I}$, missä $a_i \in M_i$. Määritellään yhteenlasku asettamalla

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}$$

ja kertolasku

$$a(x_i)_{i \in I} = (ax_i)_{i \in I}$$

kaikilla perheillä $(x_i)_{i \in I}, (y_i)_{i \in I} \in M^I$ ja alkioilla $a \in R$.

Määritelmä 2.12. Olkoon R kommutatiivinen rengas ja $(M_i)_{i \in I}$, missä I on indeksijoukko, perhe R-moduleita. R-modulien M_i *ulkoinen suora summa*, merkitään $\oplus_{i \in I} M_i$, koostuu kaikista perheistä $(x_i)_{i \in I}$, missä $a_i \in M_i$ kaikilla $i \in I$ siten, että $a_i = 0$ kaikilla, paitsi äärellisen monella alkiolla i. Yhteen- ja kertolasku ulkoisessa suorassa summassa on määritelty kuten karteesisen tulon tapauksessa, kun indeksijoukko I on finiittinen.

Määritelmä 2.13. Olkoon R kommutatiivinen rengas ja $(M_i)_{i \in I}$, missä I on indeksijoukko, perhe R-modulin M alimoduleita. R-modulia M sanotaan alimodulien M_i *sisäiseksi suoraksi summaksi*, mikäli jokainen alkio $x \in M$ voidaan lausua yksikäsitteisesti muodossa $x_{i_1} + \cdots + x_{i_n}$, missä $x_{i_k} \in M_i$ ja $x_{i_k} \neq 0$ kaikilla $k \in \{1, \ldots, n\}$.

2.2 Isomorfismi

Määritelmä 2.14. Olkoon R kommutatiivinen rengas ja M, M' R-moduleita. Kuvausta $f : M \to M'$ sanotaan *(R-)homomorfismiksi*, mikäli

1. $f(x + y) = f(x) + f(y)$ ja
2. $f(ax) = af(x)$

kaikilla alkoilla $a \in R$ ja $x, y \in M$.

Määritelmä 2.15. Olkoon R kommutatiivinen rengas ja M, M' R-moduleita. Joukko

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

sisältää kaikki homomorfismit R-modulilta M R-modulille M'.

Määritelmä 2.16. Olkoon R kommutatiivinen rengas ja M, M' R-moduleita. Kuvaus $f : M \to M'$ on *(R-)isomorfismi*, mikäli f on bijektiivinen R-homomorfismi. Sanotaan, että tällöin R-modulit M ja M' ovat *isomorfiset*.

Määritelmä 2.17. Olkoon R kommutatiivinen rengas ja M, N R-moduleita. Jos kuvaus $f : M \to N$ on homomorfismi, niin tällöin homomorfismin f *ydin*

$$\ker(f) := \{m \in M \mid f(m) = 0\}$$

ja *kuva*

$$\mathrm{im}(f) := \{n \in N \mid \text{on olemassa alkio } m \in M \text{ siten, että } n = f(m)\}.$$

Lause 2.2. *Olkoon R kommutatiivinen rengas ja M, N R-moduleita. Jos kuvaus $f : M \to N$ on homomorfismi, niin tällöin homomorfismin f ydin* $\ker(f)$ *on R-modulin M alimoduli.*

Todistus. Tiedetään, että homomorfismin f ydin $\ker(f)$ on epätyhjä, sillä $f(0) = 0 \in \ker(f)$. Olkoot $x, y \in \ker(f)$. Tällöin

$$f(x + y) = f(x) + f(y) = 0 + 0 = 0,$$

joten $x + y \in \ker(f)$.

Olkoon lisäksi $a \in R$. Nyt

$$f(ax) = af(x) = a \cdot 0 = 0,$$

joten $ax \in \ker(f)$. Siis homomorfismin f ydin $\ker(f)$ on R-modulin M alimoduli. □

Lause 2.3. *Olkoon R kommutatiivinen rengas ja M, N R-moduleita. Jos kuvaus $f : M \to N$ on homomorfismi, niin tällöin homomorfismin f kuva $\mathrm{im}(f)$ on R-modulin M alimoduli.*

Todistus. Tiedetään, että homomorfismin f kuva $\mathrm{im}(f)$ on epätyhjä, sillä $f(0) = 0 \in \mathrm{im}(f)$. Olkoot $x, y \in \mathrm{im}(f)$. Tällöin

$$x + y = f(x') + f(y') = f(x' + y'),$$

joten $x + y \in \mathrm{im}(f)$.

Olkoon lisäksi $a \in R$. Nyt

$$ax = af(x') = f(ax'),$$

joten $ax \in \mathrm{im}(f)$. Siis täten homomorfismin f kuva $\mathrm{im}(f)$ on R-modulin M alimoduli. □

Määritelmä 2.18. Olkoon R kommutatiivinen rengas, M R-moduli ja $N \subseteq M$ R-modulin M alimoduli. Surjektiivista kuvausta $\varphi : M \to M/N, x \mapsto x+N$ sanotaan *luonnolliseksi surjektioksi.*

Lause 2.4. *Olkoon R kommutatiivinen rengas, M R-moduli ja $N \subseteq M$ R-modulin M alimoduli. Tällöin luonnollinen surjektio $\varphi : M \to M/N, x \mapsto x+N$ on homomorfismi, jonka ydin* $\ker(\varphi) = N$.

Todistus. Olkoot $x, y \in M$. Tällöin

$$\begin{aligned}\varphi(x+y) &= (x+y)+N \\ &= (x+N)+(y+N) \\ &= \varphi(x)+\varphi(y).\end{aligned}$$

Olkoon lisäksi $a \in R$. Nyt

$$\begin{aligned}\varphi(ax) &= (ax)+N \\ &= a(x+N) \\ &= a\varphi(x).\end{aligned}$$

Siis kuvaus φ on homomorfismi.

Lisäksi

$$\begin{aligned}\ker(\varphi) &= \{x \in M \mid \varphi(x) = 0\} \\ &= \{x \in M \mid x+N = 0+N\} \\ &= \{x \in M \mid x \in N\} \\ &= N,\end{aligned}$$

mistä väite seuraa. □

Lause 2.5 (Ensimmäinen isomorfialause)**.** *Olkoon R kommutatiivinen rengas ja M, N R-moduleita. Jos kuvaus $f : M \to N$ on homomorfismi, niin on olemassa isomorfismi*

$$g : M/\ker(f) \to im(f)$$

siten, että $g(m + \ker(f)) = f(m)$ kaikilla alkioilla $m \in M$.

Todistus. Osoitetaan ensin, että kuvaus g on mielekäs. Olkoot $x, y \in M$ sellaiset, että $x + \ker(f) = y + \ker(f)$. Tällöin

$$\begin{aligned}& x - y \in \ker(f) \\ \Rightarrow\quad & f(x-y) = 0 \\ \Rightarrow\quad & f(x) - f(y) = 0 \\ \Rightarrow\quad & f(x) = f(y) \\ \Rightarrow\quad & g(x+\ker(f)) = g(y+\ker(f)).\end{aligned}$$

Osoitetaan sitten kuvauksen g homomorfisuus. Olkoon $a \in R$ ja $x, y \in M$. Tällöin

$$\begin{aligned} g((x + \ker(f)) + (y + \ker(f))) &= g((x + y) + \ker(f)) \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= g(x + \ker(f)) + g(y + \ker(f)). \end{aligned}$$

ja

$$\begin{aligned} g(a(x + \ker(f)) &= g(ax + \ker(f)) \\ &= f(ax) \\ &= af(x) \\ &= ag(x + \ker(f)). \end{aligned}$$

Osoitetaan vielä kuvauksen g bijektiivisyys. Olkoon $x \in M$. Tällöin

$$\begin{aligned} & g(x + \ker(f)) = 0 \\ \Rightarrow \quad & f(x) = 0 \\ \Rightarrow \quad & x \in \ker(f) \\ \Rightarrow \quad & x + \ker(f) = 0 + \ker(f), \end{aligned}$$

joten kuvaus g on injektio. Olkoon sitten $y \in \mathrm{im}(f)$. Tällöin $y = f(x)$ jollakin alkiolla $x \in R$. Siis

$$y = g(x + \ker(f)),$$

joten kuvaus g on myös surjektio ja täten bijektio. □

Lause 2.6 (Toinen isomorfialause)**.** *Olkoon R kommutatiivinen rengas, M R-moduli ja $S, T \subseteq M$ alimoduleita. Tällöin on olemassa isomorfismi*

$$S/(S \cap T) \to (S + T)/T.$$

Todistus. Koska $S, T \subseteq M$ ovat R-modulin M alimoduleita, lauseen 2.4 nojalla on olemassa luonnollinen homomorfismi

$$f : M \to M/T, m \mapsto m + T,$$

missä $\ker(f) = T$. Määritellään rajoittumakuvaus h siten, että

$$h : S \to M/T, s \mapsto s + T$$

rajoittamalla kuvauksen f lähtöjoukko alimoduliin S. Tällöin

$$\begin{aligned} \ker(h) &= \{s \in S \mid h(s) = 0\} \\ &= \{s \in S \mid s + T = 0 + T = T\} \\ &= \{s \in S \mid s \in T\} \\ &= S \cap T \end{aligned}$$

ja

$$\begin{aligned}\mathrm{im}(h) &= \{h(x) \mid x \in S\} \\ &= \{x + T \mid x \in S\} \\ &= (S + T)/T.\end{aligned}$$

Täten ensimmäisen isomorfialauseen nojalla on olemassa isomorfismi

$$\bar{h} : S/(S \cap T) \cong (S + T)/T,$$

missä $\bar{h}(x + S \cap T) = x + T$ kaikilla alkioilla $x \in S$. □

Lause 2.7 (Kolmas isomorfialause)**.** *Olkoon R kommutatiivinen rengas, M R-moduli ja $N, P \subseteq M$ alimoduleita siten, että $P \subseteq N$. Tällöin on olemassa isomorfismi*

$$(M/P)/(N/P) \to M/N.$$

Todistus. Määritellään kuvaus $g : M/P \to M/N$, missä $g(m + P) = m + N$ kaikilla alkioilla $m \in M$. Olkoon alkiot $m, m' \in M$ siten, että $m + P = m' + P$. Tällöin $m - m' \in P$. Mutta koska $P \subseteq N$, niin $m + N = m' + N$. Siis kuvaus g on hyvinmääritelty.

Olkoon sitten $a \in R$ ja $m, n \in M$. Nyt

$$\begin{aligned}g((m + P) + (n + P)) &= g((m + n) + P) \\ &= (m + n) + N \\ &= (m + N) + (n + N) \\ &= g(m + P) + g(n + P)\end{aligned}$$

ja

$$\begin{aligned}g(a(m + P)) &= g((am) + P) \\ &= (am) + N \\ &= a(m + N) \\ &= ag(m + P).\end{aligned}$$

Siis kuvaus g on homomorfismi. Lisäksi

$$\begin{aligned}\ker(g) &= \{m + P \in M/P \mid g(m + P) = 0\} \\ &= \{m + P \in M/P \mid m + N = 0 + N = N\} \\ &= \{m + P \in M/P \mid m \in N\} \\ &= N/P\end{aligned}$$

ja

$$\begin{aligned}\mathrm{im}(g) &= \{g(n + P) \mid n + P \in M/P\} \\ &= \{n + N \mid n + P \in M/P\} \\ &= M/N.\end{aligned}$$

Nyt ensimmäisen isomorfialauseen nojalla on olemassa isomorfismi

$$h : (M/P)/(N/P) \to M/N,$$

missä $h((x + P) + (N/P)) = x + N$ kaikilla alkioilla $x \in M$. □

2.3 Pääideaalialueet

Määritelmä 2.19. Olkoon R kommutatiivinen rengas. Joukkoa $I \subseteq R$ sanotaan renkaan R *ideaaliksi*, mikäli

1. $0 \in I$,
2. kaikilla alkioilla $a, b \in I$ pätee $a + b \in I$,
3. kaikilla alkioilla $a \in I$ ja $r \in R$ pätee $ra \in I$.

Jos ideaali $I \neq R$, sanotaan, että se on *aito ideaali*.

Määritelmä 2.20. Olkoon R kommutatiivinen rengas. Ideaali $I \subseteq R$ on *maksimaalinen ideaali*, jos se on aito ideaali ja ei ole olemassa ideaalia $J \subseteq R$ siten, että $I \subset J \subset R$.

Zornin lemma. Jos X on epätyhjä osittain järjestetty joukko siten, että sen jokaisella ketjulla on yläraja, niin joukossa X on olemassa maksimaalinen alkio.

Lause 2.8. *Olkoon R kommutatiivinen rengas. Tällöin renkaassa R on maksimaalinen ideaali.*

Todistus. (Vrt. [2, kappale 2 s. 13]) Olkoon $I \subseteq R$ on renkaan R aito ideaali. Oletetaan, että joukko X sisältää kaikki renkaan R aidot ideaalit, jotka sisältävät ideaalin I, ja että joukko X on osittain järjestetty sisältyvyysrelaation $\subset$ suhteen. Tällöin jokaisella aitojen ideaalien ketjulla

$$J := \{J_t \mid J_t \subset R \text{ on aito ideaali kaikilla alkioilla } t \in T\},$$

joka sisältää ideaalin I, on yläraja, ketjun ideaalien yhdiste $\bigcup_{J_t \in J} J_t$ kaikilla alkioilla $t \in T$. Havaitaan, että yhdiste $\bigcup_{J_t \in J} J_t$ on myöskin aito ideaali, sillä renkaan R ykkösalkio ei sisälly mihinkään ketjun J alkioon niiden ollessa aitoja ideaaleja, ja täten myöskään se ei sisälly yhdisteeseen $\bigcup_{J_t \in J} J_t$.

Nyt Zornin lemman nojalla osittain järjestetyssä joukossa X on olemassa maksimaalinen alkio, joka tällöin on maksimaalinen ideaali, joka sisältää ideaalin I. Valitsemalla ideaaliksi I joukko $\{0\}$, on osoitettu, että jokaisessa renkaassa on olemassa vähintään yksi maksimaalinen ideaali. □

Lause 2.9. *Olkoon R kommutatiivinen rengas ja $I \subseteq R$ sen aito ideaali. Tällöin I on maksimaalinen ideaali, jos ja vain jos tekijäryhmä R/I on kunta.*

Todistus. (Vrt. [2, kappale 2 s. 14]) Oletetaan ensin, että I on renkaan R maksimaalinen ideaali. Olkoon $a+I \in R/I$ nollasta eroava alkio. Pitää siis osoittaa, että on olemassa alkio $b+I \in R/I$ siten, että $(a+I)(b+I) = 1+I$. Merkitään

$$I' := \{ar + s \mid \text{ joillakin alkioilla } r \in R \text{ ja } s \in I\}.$$

Koska $0 \in R$ ja $0 \in I$, niin tällöin $0 \in I'$. Olkoot $ar + s, ar' + s' \in I'$. Tällöin

$$(ar + s) + (ar' + s') = a(r + r') + (s + s'),$$

missä $r + r' \in R$ ja $s + s' \in I$, joten $(ar + s) + (ar' + s') \in I'$. Olkoon lisäksi $x \in R$. Tällöin

$$x(ar + s) = axr + xs,$$

missä $xr \in R$ ja $xs \in I$, joten $x(ar + s) \in I'$. Siis täten I' on ideaali. Lisäksi havaitaan, että $I \subset I'$, sillä $a \in I'$, mutta $a \notin I$. Täten täytyy olla $I' = R$, sillä oletuksen mukaan I on renkaan R maksimaalinen ideaali. Erityisesti $1 \in I'$ ja $1 = ab + m$ joillakin $b \in R$ ja $m \in I$, joten $ab - 1 \in I'$ ja

$$(a + I)(b + I) = ab + I = (1 - m) + I = 1 + I$$

tekijäryhmässä R/I. Siis alkiolla $a + I$ on käänteisalkio tekijäryhmässä R/I, joten R/I on kunta.

Oletetaan sitten, että tekijäryhmä R/I on kunta ja olkoon $J \subseteq R$ sellainen ideaali, että $I \subset J$. Olkoon lisäksi alkio $a \in J$ siten, että $a \notin I$. Täten $a+I \neq 0$ tekijäryhmässä R/I, joten $(a+I)(b+I) = 1+I$ jollakin alkiolla $b \in R$. Tällöin $ab - 1 \in I$. Nyt $1 = ab - (ab - 1)$, joten $1 \in J$ koska $a \in J$ ja $ab - 1 \in J$. Täytyy siis olla $J = R$, joten I on renkaan R maksimaalinen ideaali. □

Määritelmä 2.21. Olkoon R kommutatiivinen rengas. Ideaalia $I \subseteq R$ sanotaan *alkuideaaliksi*, mikäli se on aito ideaali sekä ehto

$$ab \in I \quad \Rightarrow \quad a \in I \quad \vee \quad b \in I$$

pätee kaikilla alkioilla $a, b \in I$.

Määritelmä 2.22. Olkoon R kommutatiivinen rengas. Yhden alkion virittämää ideaalia $I \subseteq R$ sanotaan *pääideaaliksi*. Jos rengas R on kokonaisalue ja sen kaikki ideaalit ovat pääideaaleja, sitä sanotaan *pääideaalialueeksi*.

Esimerkki 2.1. Kokonaislukujen rengas $\mathbb{Z}$ on pääideaalialue, sillä se on kokonaisalue ja sen kaikki ideaalit ovat yhden alkion virittämiä.

Lause 2.10. *Pääideaalialueessa ei ole olemassa ääretöntä nousevaa ideaalien ketjua.*

Todistus. Olkoon R pääideaalialue. Tehdään vastaoletus, että on olemassa ideaalit $I_k \in R$, missä $k \in \mathbb{N}$, joille pätee

$$I_0 \subset I_1 \subset I_2 \subset \dots$$

Tarkastellaan ideaalien yhdistettä

$$I = \cup_{k\in\mathbb{N}} I_k.$$

Huomataan, että tällöin joukko I on selvästi ideaali, sillä

- $0 \in I$, sillä $0 \in I_k$ kaikilla $k \in \mathbb{N}$.
- kaikilla $a, b \in I$ pätee $a + b \in I$, sillä $a \in I_i$ ja $b \in I_j$ joillakin $i, j \in \mathbb{N}$ ja $I_0 \subset I_1 \subset I_2 \subset \dots$
- kaikilla $r \in R$ ja $a \in I$ pätee $ra \in I$, sillä $a \in I_k$ jollakin $k \in \mathbb{N}$ ja I_k on ideaali.

Koska R on pääideaalialue, niin on olemassa $x \in R$ siten, että $I = \langle x \rangle$. Lisäksi, koska

$$I = \cup_{k\in\mathbb{N}} I_k,$$

niin $a \in I_l$ jollakin $l \in \mathbb{N}$. Täten

$$I = \langle a \rangle \subseteq I_l \subset I_{l+1} \subseteq I,$$

mikä on ristiriita. Siis alkuperäinen väite pätee. □

Lause 2.11. *Olkoon R pääideaalialue. Tällöin jokaisessa pääideaalialueen R ideaalien kokoelmassa on maksimaalinen alkio.*

Todistus. Olkoon K epätyhjä kokoelma pääideaalialueen R ideaaleja. Tehdään vastaoletus, että kokoelmassa K ei ole maksimaalista alkiota. Olkoon $I_1 \in K$. Nyt vastaoletuksen nojalla on olemassa ideaali $I_2 \in K$ siten, että $I_1 \subset I_2$. Vastaavasti on olemassa ideaali $I_3 \in K$ siten, että $I_2 \subset I_3$. Jatkamalla näin päästään ideaaliin $I_n \in K$, jolloin on olemassa ideaali $I_{n+1} \in K$ siten, että $I_n \subset I_{n+1}$. Toisin sanoen kokoelman $K \subseteq R$ alkioista voidaan muodostaa ääretön nousevien ideaalien ketju

$$I_1 \subset I_2 \subset \dots \subset I_n \subset I_{n+1} \subset \dots,$$

jolloin saadaan siis ristiriita lauseen 2.10 kanssa. Täten vastaoletus on väärä ja alkuperäinen väite pätee. □

Lause 2.12. *Jokainen euklidinen alue on pääideaalialue.*

Todistus. Olkoon R euklidinen alue, jonka astefunktio on kuvaus $d : R/\{0\} \to \mathbb{N}$. Osoitetaan, että jokainen euklidisen alueen R ideaali on pääideaali. Olkoon $I \subseteq R$ mielivaltainen ideaali siten, että $I \neq \{0\}$, ja olkoon $x \in I$ sellainen alkio, että $x \neq 0$ ja $d(x) < d(y)$ kaikilla alkioilla $y \in I$, missä $y \neq x$. Nyt astefunktion määritelmän nojalla kuvauksen d maalijoukko on joukon $\mathbb{N}$ osajoukko. Koska joukon $\mathbb{N}$ osajoukossa on olemassa pienin alkio ja $d(x) \in \mathbb{N}$, niin tällainen alkio x todellakin on olemassa.

Olkoon $a \in I$. Kirjoitetaan $a = xq + s$, missä $s = 0$ tai $d(s) < d(x)$ joillakin $q, s \in R$. Tällöin $s = a - xq$, joten $s \in I$. Oletetaan, että $x \neq 0$, jolloin $d(s) < d(x)$. Mutta oletuksen mukaan $d(x)$ on pienin ideaalin I alkioiden joukossa, joten tämä on ristiriita. Täytyy siis olla $s = 0$, jolloin $a = qx$. Täten ideaalin I jokainen alkio on alkion d lineaarikombinaatio, joten ideaali I on alkion x virittämä pääideaali. Koska ideaali I valittiin mielivaltaisesti, väite pätee kaikille euklidisen alueen R ideaaleille, joten R on pääideaalialue. □

Määritelmä 2.23. Olkoon R kokonaisalue.

1. Nollasta eroavaa alkiota $r \in R$, joka ei ole yksikkö, sanotaan *jaottomaksi*, jos kaikilla alkioilla $a, b \in R$ pätee ehto

$$r = ab \quad \Rightarrow \quad a \text{ on yksikkö} \quad \vee \quad b \text{ on yksikkö.}$$

2. Nollasta eroavaa alkiota $p \in R$ sanotaan *alkualkioksi*, mikäli se ei ole kokonaisalueen R yksikkö ja kaikilla alkioilla $a, b \in R$ pätee ehto

$$p \mid ab \quad \Rightarrow \quad p \mid a \quad \vee \quad p \mid b.$$

3. Alkioita $a, b \in R$ sanotaan *liittoalkioiksi*, mikäli $a = ub$ jollakin yksiköllä $u \in R$.

Apulause 2.13. *Olkoon R pääideaalialue. Jokainen nollasta eroava alkio $a \in R$, joka ei ole yksikkö, voidaan kirjoittaa jaottomien alkioiden tulona. Toisin sanoen on olemassa alkion a esitysmuoto*

$$a = a_1 a_2 \cdots a_n,$$

missä alkiot $a_1, \ldots, a_n \in R$ ovat jaottomia.

Todistus. Olkoon $X \subset R$ sellainen joukko, joka sisältää sellaiset alkiot $a \in R$, että $a \neq 0$, a ei ole yksikkö ja alkiota a ei voida kirjoittaa väitteessä annetussa esitysmuodossa jaottomien alkioiden tulona. Tehdään vastaoletus, että joukko $X \neq \emptyset$.

Nyt mikään alkio $x \in X$ ei ole jaoton, joten $x = bc$, missä alkiot $b, c \in R$ eivät ole yksiköitä eivätkä alkion a liittoalkioita. Tällöin ainakin toinen alkioista b ja c kuuluu joukkoon X. Täten jokaisella alkiolla $x \in X$ on aito tekijä $b \in X$,

jolloin $\langle a \rangle \subset \langle b \rangle$. Toistamalla tätä prosessia saadaan muodostettua jono alkioita $x_i \in X$, missä $i \in \mathbb{N}$, jotka toteuttavat ehdot $x_{i+1} \mid x_i$ ja $x_i \mid x_{i+1}$ kaikilla $i \in \mathbb{N}$. Toisin sanoen on olemassa ääretön ideaalien ketju

$$\langle x_0 \rangle \subset \langle x_1 \rangle \subset \langle x_2 \rangle \subset \ldots,$$

mikä on ristiriidassa lauseen 2.10 kanssa, jonka mukaan pääideaalialueessa ei ole olemassa ääretöntä nousevien ideaalien ketjua. Täten alkuperäinen väite pätee. □

Määritelmä 2.24. Kokonaisaluetta R sanotaan *faktoriaaliseksi*, mikäli

1. jokainen nollasta eroava alkio $r \in R$, joka ei ole yksikkö, voidaan kirjoittaa muodossa
$$r = p_1 p_2 \cdots p_n,$$
missä alkiot $p_1, \ldots, p_n \in R$ ovat jaottomia,
2. kohdassa 1 oleva alkion r esitysmuoto on siinä mielessä yksikäsitteinen, että jos $r = p'_1 p'_2 \cdots p'_m$, missä alkiot $p'_1, \ldots, p'_m \in R$ ovat jaottomia, niin $m = n$ ja tekijät voidaan numeroida uudelleen siten, että alkiot p_i ja p'_i ovat liittoalkioita kaikilla $i \in \{1, \ldots, n\}$.

Lause 2.14. *Jokainen pääideaalialue on faktoriaalinen.*

Todistus. Olkoon R pääideaalialue. Apulauseen 2.13 mukaan jokainen nollasta eroava alkio $a \in R$, joka ei ole yksikkö, voidaan kirjoittaa muodossa

$$a = p_1 p_2 \cdots p_n,$$

missä alkiot $p_1, \ldots, p_n \in R$ ovat jaottomia. Riittää siis osoittaa, että tämä esitysmuoto on oleellisesti yksikäsitteinen.

Olkoot alkio $a \in R$ kuten edellä ja

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

alkion a esitysmuotoja jaottomien alkioiden $p_1, \ldots, p_m, q_1, \ldots, q_n \in R$ tuloina. Osoitetaan esitysmuodon yksikäsitteisyys induktiolla luvun $s := min\{m, n\}$ suhteen.

Jos $s = 1$, niin alkio $a = p_1$ on jaoton. Tällöin täytyy siis olla myöskin $m = 1$ ja $a = p_1 = q_1$.

Oletetaan nyt, että $s > 1$ ja väite pätee lukua s pienemmillä luvuilla. Koska $p_m \mid q_1 \cdots q_n$, niin $q_1 \cdots q_n \in \langle p_m \rangle$. Toisaalta ideaali $\langle p_m \rangle$ on alkuideaali, joten jollakin $i \in \{1, \ldots, n\}$ pätee $q_i \in \langle p_m \rangle$. Täten $p_m \mid q_i$. Mutta koska alkio q_1 on jaoton, niin alkiot p_m ja q_i ovat välttämättä liittoalkiot, toisin sanoen

$$p_m = u q_i,$$

missä $u \in R$ on yksikkö. Siis

$$\begin{aligned} ap_m^{-1} &= p_1 \cdots p_{m-1} \\ &= q_1 \cdots q_n p_m^{-1} \\ &= q_1 \cdots q_{i-1}(q_i p_m^{-1}) q_{i+1} \cdots q_n \\ &= q_1 \cdots q_{i-1}(u q_{i+1}) q_{i+2} \cdots q_n. \end{aligned}$$

Nyt induktio-oletuksen nojalla on olemassa indeksijoukon $\{1, \ldots, m\}$ permutaatio ρ siten, että $\rho(m) = i$, ja p_k ja $p_{\rho(k)}$ ovat liittoalkioita, kun $k \in \{1, \ldots, m\}$. Erityisesti siis $m = n$, mistä väite seuraa. □

Lause 2.15. *Olkoon R faktoriaalinen kokonaisalue. Tällöin jokainen kokonaisalueen R jaoton alkio on alkualkio.*

Todistus. Olkoon $p \in R$ jaoton alkio. Oletetaan, että $a, b \in R$ siten, että $p \mid ab$. Tällöin on olemassa $c \in R$ siten, että $ab = pc$. Jakamalla alkiot a, b ja c jaottomien alkioiden tuloiksi, yksikäsitteisyyden nojalla nähdään, että on olemassa joko alkion a tai alkion b jaoton tekijä, joka on alkion p liittoalkio. Toisin sanoen $p \mid a$ tai $p \mid b$. Siis p on alkualkio. □

2.4 Kiinalainen jäännöslause

Määritelmä 2.25. Olkoon R kommutatiivinen rengas. Renkaan R ideaaleja I ja J sanotaan *komaksimaalisiksi*, mikäli $I + J = R$.

Lause 2.16 (Kiinalainen jäännöslause)**.** *Olkoon R kommutatiivinen rengas ja $A_1, \ldots, A_n \subseteq R$ ideaaleja. Kuvaus*

$$\psi : R \to R/A_1 \times \cdots \times R/A_n, r \mapsto (r + A_1, \ldots, r + A_n)$$

on rengashomomorfismi, jonka ydin $\ker(\varphi) = A_1 \cap \cdots \cap A_n$. Jos jokaisella $i, j \in \{1, \ldots, n\}$, missä $i \neq j$, ideaalit A_i ja A_j ovat komaksimaalisia, niin kuvaus φ on surjektio ja $A_1 \cap \cdots \cap A_n = A_1 \cdots A_n$, joten

$$R/(A_1 \cdots A_n) = R/(A_1 \cap \cdots \cap A_n) \cong R/A_1 \times \cdots \times R/A_n.$$

Todistus. (Vrt. [3, s. 266]) Osoitetaan ensin, että väite pätee, kun $n = 2$. Olkoon $A = A_1$ ja $B = A_2$. Tarkastellaan kuvausta

$$\varphi : R \to R/A \times R/B,$$

missä $\varphi(r) = (r \bmod A, r \bmod B)$, ja $r \bmod A \equiv r + A \in R/A$. Olkoot $x, y \in R$. Nyt

$$\begin{aligned} \varphi(x + y) &= ((x + y) \bmod A, (x + y) \bmod B) \\ &= (x \bmod A, x \bmod B) + (y \bmod A, y \bmod B) \\ &= \varphi(x) + \varphi(y) \end{aligned}$$

ja

$$\begin{aligned}\varphi(xy) &= (xy \bmod A, xy \bmod B)\\ &= (x \bmod A, x \bmod B)(y \bmod A, y \bmod B)\\ &= \varphi(x)\varphi(b).\end{aligned}$$

Lisäksi $\varphi(1) = (1 \bmod A, 1 \bmod B)$, joten kuvaus φ on selvästi rengashomomorfismi. Nyt homomorfismin φ ydin

$$\begin{aligned}\ker(\varphi) &= \{r \in R \mid \varphi(r) = 0\}\\ &= \{r \in R \mid (r \bmod A, r \bmod B) = (0 \bmod A, 0 \bmod B\}\\ &= \{r \in R \mid r \in A, r \in B\}\\ &= A \cap B.\end{aligned}$$

Oletetaan, että ideaalit A ja B ovat komaksimaalisia eli $A+B = R$. Tällöin on olemassa alkiot $x \in A$ ja $y \in B$ siten, että $x + y = 1 \in R$. Koska $x \in A$ ja $x = 1 - y \in 1 + B$, niin $\varphi(x) = (0, 1)$. Vastaavasti $\varphi(y) = (1, 0)$. Oletetaan, että $(r_1 \bmod A, r_2 \bmod B) \in R/A \times R/B$ on mielivaltainen. Tällöin

$$\begin{aligned}\varphi(r_2x + r_1y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y)\\ &= (r_2 \bmod A, r_2 \bmod B)(0, 1) + (r_1 \bmod A, r_1 \bmod B)(1, 0)\\ &= (0, r_2 \bmod B) + (r_1 \bmod A, 0)\\ &= (r_1 \bmod A, r_2 \bmod B),\end{aligned}$$

missä $r_2x + r_1y \in R$. Täten kuvaus φ on surjektio.

Oletetaan edelleen, että ideaalit A ja B ovat komaksimaalisia, ja alkiot $x \in A$ ja $y \in B$ ovat kuten edellä. Jos mielivaltainen alkio $c \in A \cap B$, niin

$$c = c1 = c(x + y) = cx + cy,$$

joten $c \in AB$. Siis $A \cap B \subseteq AB$. Suoraan ideaalin määritelmästä seuraa, että $AB \subseteq A \cap B$. Siis $AB = A \cap B$ ja täten väite pätee, kun $n = 2$.

Merkitään nyt, että $A = A_1$ ja $B = A_2 \cdots A_n$. Oletuksen nojalla A on ideaali. Merkitään

$$B = A_2 \cdots A_n := \{\sum_{i \in I} a_{2i} \cdots a_{ni} \mid a_{ji} \in A_j \text{ kaikilla } j \in \{2, \ldots, n\}\},$$

missä I on äärellinen epätyhjä indeksijoukko. Nyt koska $0 \in A_i$ kaikilla $i \in \{2, \ldots, n\}$, niin tällöin $0 \in B$. Olkoot $a, b \in B$. Tällöin

$$a + b = \sum_{i \in I} a_{2i} \cdots a_{ni} + \sum_{j \in I} a_{2j} \cdots a_{nj}.$$

Siis myös $a + b$ on äärellinen summa, missä summattavat alkiot ovat ideaalien $A_2, \ldots, A_n$ alkioiden tuloja, joten $a + b \in B$. Vastaavasti $ra \in B$, missä $r \in R$, sillä

$$ra = r \sum_{i \in I} a_i a_i' = \sum_{i \in I} (ra_i)b_i,$$

missä $ra_i \in A$. Siis B on ideaali.

Osoitetaan vielä, että ideaalit A ja B ovat komaksimaalisia. Koska oletuksen nojalla ideaalit A_1 ja A_i ovat komaksimaalisia jokaisella $i \in \{2, \ldots, n\}$, on olemassa alkiot $x_i \in A_1$ ja $y_i \in A_i$ siten, että $x_i + y_i = 1 \in R$ kaikilla $i \in \{2, \ldots, n\}$. Koska $x_i \in A_1$, niin $x_i + y_i \equiv y_i \mod A_1$, joten

$$1 = (x_2 + y_2) \cdots (x_n + y_n).$$

Siis $(x_2 + y_2) \cdots (x_n + y_n) \in A_1 + (A_2 \cdots A_n)$. Täten $A_1 + (A_2 \cdots A_n) = R$.

Osoitetaan nyt induktiolla, että väite pätee myös, kun $n = k$. Oletetaan, että väite pätee, kun $n = k - 1$. Tiedetään, että ideaalit A_1 ja $A_2 \cdots A_k$ ovat komaksimaalisia. Täten tapauksen $n = 2$ nojalla kuvaus

$$\varphi : R \to R/A_1 \times R/(A_2 \cdots A_k), r \mapsto (r + A_1, r + (A_2 \cdots A_k))$$

on surjektiivinen ja

$$A_1 \cap (A_2 \cdots A_k) = A_1 \cdot (A_2 \cdots A_k).$$

Toisaalta induktio-oletuksen nojalla $A_2 \cap \cdots \cap A_k = A_2 \cdots A_k$, joten

$$A_1 \cap (A_2 \cdots A_k) = A_1 \cap (A_2 \cap \cdots \cap A_k) = A_1 \cap A_2 \cap \cdots \cap A_k.$$

Pitää siis vielä osoittaa, että kuvaus

$$\psi : R \to R/A_1 \times \cdots \times R/A_k, r \mapsto (r + A_1, \ldots, r + A_k)$$

on surjektio. Mutta koska induktio-oletuksen nojalla

$$R/(A_2 \cap \cdots \cap A_k) \cong R/A_2 \times \cdots \times R/A_k,$$

niin täten myös kuvaus ψ on surjektio. □

2.5 Kanta

Määritelmä 2.26. Olkoon R kommutatiivinen rengas ja M R-moduli. Perhe $(x_i)_{i \in I} \in M^I$, missä I on epätyhjä joukko, on *vapaa* (eli *lineaarisesti riippumaton*), mikäli

$$\sum_{i \in I} c_i x_i = 0 \quad \Rightarrow \quad c_i = 0$$

kaikilla alkioilla $i \in I$, kun $(c_i)_{i \in I}$ on perhe renkaan R alkioita. Jos perhe $(x_i)_{i \in I}$ ei ole vapaa, se on *sidottu* (eli *lineaarisesti riippuva*).

Määritelmä 2.27. Olkoon R kommutatiivinen rengas ja M R-moduli. Sanotaan, että perhe $(x_i)_{i\in I} \in M^I$, missä I on epätyhjä joukko, on R-modulin M *kanta*, mikäli

1. perhe $(x_i)_{i\in I}$ on vapaa,
2. perhe $(x_i)_{i\in I}$ virittää R-modulin M.

Esimerkki 2.2. Perhe $((1,0,0),(0,1,0),(0,0,1))$ on vektoriavaruuden $\mathbb{R}^3$ kanta.

Määritelmä 2.28. Olkoon R kommutatiivinen rengas. R-moduli M on *vapaa*, mikäli sillä on kanta.

Määritelmä 2.29. Olkoon K kunta. K-vektoriavaruuden V *dimensio* on sen kannan alkioiden lukumäärä.

Lause 2.17 (Steinitzin vaihtolause)**.** *Olkoon K kunta ja V K-vektoriavaruus. Jos $(v_1,\ldots,v_n) \in V^n$ on vapaa ja $V = \langle w_1,\ldots,w_m\rangle$, missä $w_1,\ldots,w_m \in V$, niin $n \leq m$.*

Todistus. (Vrt. [1, s. 168]) Oletetaan, että $(v_1,\ldots,v_n) \in V^n$ on vapaa ja $V = \langle w_1,\ldots,w_m\rangle$, missä $w_1,\ldots,w_m \in V$, ja tehdään vastaoletus, että $n > m$. Koska vektoriavaruus $V = \langle w_1,\ldots,w_m\rangle$, niin voidaan kirjoittaa $v_1 = a_1w_1 + \cdots + a_mw_m$, missä alkiot $a_1,\ldots,a_m \in R$. Koska $(v_1,\ldots,v_n)$ on vapaa, niin alkio $v_1 \neq 0$. Täten jollakin alkiolla $j \in \{1,\ldots,m\}$ pätee $a_j \neq 0$. Koska vektorit $w_1,\ldots,w_n$ voidaan uudelleennumeroida, voidaan olettaa, että $a_1 \neq 0$. Tällöin

$$\begin{aligned}
& v_1 = a_1w_1 + \cdots + a_mw_m \\
\Rightarrow\quad & w_1 = a_1^{-1}v_1 - a_1^{-1}a_2w_2 - \cdots - a_1^{-1}a_mw_m \\
\Rightarrow\quad & w_1 \in \langle v_1, w_2,\ldots,w_m\rangle \\
\Rightarrow\quad & \langle w_1,\ldots,w_m\rangle \subset \langle v_1,w_2,\ldots,w_m\rangle \\
\Rightarrow\quad & V = \langle v_1,w_2,\ldots,w_m\rangle.
\end{aligned}$$

Nyt voidaan kirjoittaa $v_2 = b_1v_1+b_2w_2+\cdots+b_mw_m$, missä alkiot $b_1,\ldots,b_m \in R$. Oletuksen mukaan perhe $(v_1,\ldots,v_n)$ on vapaa, joten ei voi olla $b_2 = b_3 = \cdots = b_m = 0$, sillä tällöin olisi $v_2 = u_1v_1$, joka on ristiriita. Täten jollakin alkiolla $j \in \{2,\ldots,m\}$ pätee $b_j \neq 0$. Koska vektorit $w_2,\ldots,w_n$ voidaan uudelleennumeroida, voidaan olettaa, että $b_2 \neq 0$. Tällöin

$$\begin{aligned}
& v_2 = b_1v_1 + b_2w_2 + \cdots + a_mw_m \\
\Rightarrow\quad & w_2 = b_2^{-1}v_2 - b_2^{-1}b_1v_1 - \cdots - b_2^{-1}b_mw_m \\
\Rightarrow\quad & w_2 \in \langle v_1, v_2, w_3,\ldots,w_m\rangle \\
\Rightarrow\quad & \langle v_1,w_2,\ldots,w_m\rangle \subset \langle v_1,v_2,w_3\ldots,w_m\rangle \\
\Rightarrow\quad & V = \langle v_1,v_2,w_3,\ldots,w_m\rangle.
\end{aligned}$$

Vastaoletuksen nojalla $n > m$, joten vastaavalla tavalla jatkamalla päädyttäisiin tulokseen $V = \langle v_1, \ldots, v_m \rangle$. Mutta tällöin vektori v_{m+1} voitaisiin esittää vektoreiden $v_1, \ldots, v_m$ lineaarikombinaationa, joka taas on ristiriita sillä perhe $(v_1, \ldots, v_n)$ oletettiin vapaaksi.

Täten vastaoletus on väärä ja alkuperäinen väite pätee. □

Lause 2.18. *Olkoon K kunta ja V K-vektoriavaruus. Tällöin vektoriavaruus V on äärellisviritteinen, jos ja vain jos sillä on äärellinen kanta.*

Todistus. Oletetaan ensin, että vektoriavaruus V on äärellisviritteinen. Tällöin $V = \langle x_1, \ldots, x_m \rangle$, missä vektorit $x_1, \ldots, x_m \in V$. Olkoon $S \subseteq V$ vektoriavaruuden V kanta ja $y_1, \ldots, y_n \in S$, missä $y_1, \ldots, y_n$ ovat eri vektoreita. Koska S on kantana vapaa, niin tällöin myöskin perhe $(y_1, \ldots, y_n)$ on vapaa. Nyt Steinitzin vaihtolauseen nojalla $n \leq m$, joten kanta S on äärellinen.

Oletetaan sitten, että vektoriavaruudella V on äärellinen kanta. Vektoriavaruuden kanta virittää kannan määritelmän nojalla vektoriavaruuden, joten selvästi vektoriavaruus V on äärellisviritteinen. □

Lause 2.19. *Olkoon K kunta ja V K-vektoriavaruus. Jos $(x_1, \ldots, x_n) \in V^n$ ja $(y_1, \ldots, y_m) \in V^m$ ovat vektoriavaruuden V kantoja, niin tällöin $m = n$.*

Todistus. (Vrt. [1, s. 169]) Oletuksen mukaan $(x_1, \ldots, x_n) \in V^n$ ja $(y_1, \ldots, y_m) \in V^m$ ovat vektoriavaruuden V kantoja, joten $(x_1, \ldots, x_n)$ on vapaa ja $V = \langle y_1, \ldots, y_m \rangle$. Nyt Steinitzin vaihtolauseen nojalla $n \leq m$.

Vastaavasti $(y_1, \ldots, y_m)$ on vapaa ja $V = \langle x_1, \ldots, x_n \rangle$, joten Steinizin vaihtolauseen nojalla myöskin $m \leq n$. Siis täten n=m. □

Lause 2.20. *Olkoon K kunta ja V, W K-vektoriavaruuksia siten, että $V \cong W$. Tällöin vektoriavaruuksien V ja W dimensiot ovat samat.*

Todistus. Olkoon kuvaus $f : V \to W$ isomorfismi ja $(v_1, \ldots, v_n) \in V^n$ vektoriavaruuden V kanta. Osoitetaan, että $(f(v_1), \ldots, f(v_n))$ on vektoriavaruuden W kanta.

Olkoon $w \in W$. Koska kuvaus f on surjektio, on olemassa alkio $v \in V$ siten, että $w = f(v)$. Tällöin

$$w = f(v) = f(a_1 v_1 + \cdots + a_n v_n) = a_1 f(v_1) + \cdots + a_n f(v_n),$$

joten $(f(v_1), \ldots, f(v_n))$ virittää vektoriavaruuden W.

Oletetaan sitten, että

$$c_1 f(v_1) + \cdots + c_n f(v_n) = 0,$$

missä $c_1, \ldots, c_n \in K$. Koska kuvaus f on injektio, niin $f(0) = 0$, joten

$$c_1 f(v_1) + \cdots + c_n f(v_n) = f(c_1 v_1 + \cdots + c_n v_n) = 0.$$

Lisäksi $(v_1, \ldots, v_n)$ on vektoriavaruuden V kanta, joten $c_1 = \cdots = c_n = 0$. Siis $(f(v_1), \ldots, f(v_n))$ on myöskin vapaa ja täten vektoriavaruuden W kanta. Täten vektoriavaruuksien V ja W dimensiot ovat samat. □

2.6 Äärellisviritteisen vapaan modulin aste

Määritelmä 2.30. Olkoon R rengas ja M äärellisviritteinen vapaa R-moduli. R-modulin M *asteeksi*, merkitään $rank(M)$, sanotaan sen kannan alkioiden lukumäärää.

Huomautus. Määritelmässä 2.30 esitetty äärellisviritteisen vapaan R-modulin asteen määritelmä on mielekäs, sillä mitkä tahansa kaksi R-modulin eri kantaa sisältävät täsmälleen saman määrän alkioita. Tämä tulos esitetään lauseessa 2.21.

Lause 2.21. *Olkoon R epätyhjä kommutatiivinen rengas ja M äärellisviritteinen vapaa R-moduli. Tällöin R-modulin M mitkä tahansa kaksi eri kantaa sisältävät täsmälleen saman määrän alkioita.*

Todistus. (Vrt. [2, kappale 4 s. 10]) Olkoon I renkaan R maksimaalinen ideaali. Lauseen 2.8 mukaan tällainen maksimaalinen ideaali I on olemassa. Koska I on maksimaalinen ideaali, lauseen 2.9 nojalla tekijäryhmä R/I on kunta.

Havaitaan, että joukko

$$IM := \sum_{i=1}^{n} a_i x_i,$$

missä $a_i \in I$ ja $x_i \in M$ kaikilla alkioilla $i \in \{1, \ldots, n\}$, täyttää määritelmän 2.7 ehdot, joten ryhmä IM on R-modulin M alimoduli. Tällöin määritelmän 2.10 nojalla voidaan muodostaa tekijäryhmä M/IM.

Määritellään nyt yhteenlasku ja skalaarikertolasku tekijäryhmässä M/IM. Olkoot $x + IM, y + IM \in M/IM$. Tällöin

$$(x + IM) + (y + IM) := (x + y) + IM.$$

Olkoon lisäksi $r + I \in R/I$. Tällöin

$$(r + I)(x + IM) := rx + IM.$$

Havaitaan, että

$$r \in I \quad \text{tai} \quad x \in IM \Rightarrow rx \in IM,$$

joten skalaarikertolasku on hyvinmääritelty.

Tekijäryhmä M/IM on R-moduli, mutta voidaan osoittaa, että se on aina myöskin R/I-moduli edellä mainituilla skalaarikertolaskulla varustettuna. Olkoot $r + I, s + I \in R/I$ siten, että $r + I = s + I$. Tällöin $r - s \in I$, joten

$$\begin{aligned}(rm + IM) - (sm + IM) &= rm - sm + IM \\ &= (r - s)m + IM,\end{aligned}$$

missä $m \in M$. Koska $(r - s)m \in IM$, niin

$$(r - s)m + IM = 0 + IM.$$

Täten

$$\begin{aligned}(r+I)(m+IM) &= rm+IM\\ &= sm+IM\\ &= (s+I)(m+IM).\end{aligned}$$

Siis skalaarikertolasku on mielekäs ja tällöin R-moduli M/IM on myöskin R/I-moduli.

Osoitetaan, että tekijäryhmä M/IM on kunnan R/I yli muodostettu vektoriavaruus. Olkoot $a+I, b+I \in R/I$ ja $x+IM, y+IM \in M/IM$. Tällöin

1. $$\begin{aligned}(a+I)((x+IM)+(y+IM)) &= (a+I)((x+y)+IM)\\ &= (a(x+y))+IM\\ &= (ax+ay)+IM\\ &= (ax+IM)+(ay+IM),\end{aligned}$$
2. $$\begin{aligned}((a+I)+(b+I))(x+IM) &= ((a+b)+I)(x+IM)\\ &= ((a+b)x)+IM\\ &= (ax+bx)+IM\\ &= (ax+IM)+(bx+IM),\end{aligned}$$
3. $$\begin{aligned}(a+I)((b+I)(x+IM)) &= (a+I)(bx+IM)\\ &= (a(bx))+IM\\ &= ((ab)x)+IM\\ &= (ab+I)(x+IM)\\ &= ((a+I)(b+I))(x+IM),\end{aligned}$$
4. $$\begin{aligned}(1+I)(x+IM) &= 1x+IM\\ &= x+IM.\end{aligned}$$

Olkoon perhe $(x_i)_{i\in J} \in M^J$ R-modulin M kanta. Merkitään $\bar{x_i} := x_i + IM$. Koska kanta $(x_i)_{i\in J}$ virittää R-modulin M, perhe $(\bar{x}_i)_{i\in J} \in (M/IM)^J$ virittää vektoriavaruuden M/IM. Tutkitaan vielä perheen $(\bar{x}_i)_{i\in J}$ vapautta. Oletetaan, että

$$\sum_{i\in J} \bar{a}_i\bar{x}_i = 0,$$

missä $\bar{a}_i = a_i + I \in R/I$ kaikilla alkioilla $i \in J$, joten

$$\sum_{i\in J} a_i x_i \in IM.$$

Tällöin on olemassa alkiot $b_j \in I$ ja $y_j \in M$ siten, että

$$\sum_{i\in J} a_i x_i = \sum_{j=1}^{n} b_j y_j.$$

Nyt alkiot y_j voidaan lausua R-modulin M kannan avulla, jolloin

$$y_j = \sum_{i \in J} a_{ij} x_i$$

kaikilla alkioilla $j \in J$. Tällöin

$$\begin{aligned} \sum_{i \in J} a_i x_i &= \sum_{j=1}^{n} b_j \sum_{i \in J} a_{ij} x_i \\ &= \sum_{i \in J} \sum_{j=1}^{n} a_{ij} b_j x_i. \end{aligned}$$

Vertaamalla yhtälöä puolittain, saadaan

$$a_i = \sum_{j=1}^{n} a_{ij} b_j \in I$$

siten, että $\bar{a}_i = 0$ kunnassa R/I kaikilla alkioilla $i \in J$. Siis perhe $(\bar{x}_i)_{i \in J}$ on vapaa ja täten vektoriavaruuden M/IM kanta.

Oletusten mukaan R-moduli M on äärellisviritteinen, joten myöskin vektoriavaruus M/IM on äärellisviritteinen. Täten lauseen 2.18 nojalla vektoriavaruuden M/IM kannan $(\bar{x}_i)_{i \in J}$ indeksijoukon J täytyy olla äärellinen.

Oletetaan nyt, että perhe $(x'_j)_{j \in J} \in M^J$ on R-modulin M toinen kanta. Tällöin vastaavasti perhe $(\bar{x}'_j)_{j \in J} \in (M/IM)^J$ on myöskin kunnan R/I yli muodostetun vektoriavaruuden M/IM kanta, missä indeksijoukko J on äärellinen. Nyt lauseen 2.19 mukaan minkä tahansa vektoriavaruuden kaksi eri äärellistä kantaa sisältävät täsmälleen saman määrän alkioita, joten tällöin myöskin niitä vastaavat R-modulin M eri kannat $(x_i)_{i \in J}$ ja $(x'_j)_{j \in J}$ sisältävät täsmälleen saman määrän alkioita. □

Esitetään vielä asteen määritelmä kokonaisalueen yli määritellylle modulille, joka ei välttämättä ole vapaa.

Määritelmä 2.31. Olkoon R kokonaisalue. R-modulin M *asteeksi* sanotaan sen lineaarisesti riippumattomien alkioiden maksimaalista lukumäärää, jota merkitään $\operatorname{rank}(M)$.

3 Pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennelause

Aloitetaan tarkastelemalla pääideaalialuetta ja sen yli määriteltyä äärellisviritteistä modulia. Pääideaalialueen yli määriteltyjen äärellisviritteisten modulien rakennelause kertoo, että tämä moduli on isomorfinen vapaan modulin ja torsiomodulin suoran summan kanssa. Edellä mainittu vapaa moduli taasen on isomorfinen pääideaalialueen kopioiden suoran summan kanssa ja torsiomoduli on isomorfinen syklisten modulien suoran summan kanssa. Tutustutaan kuitenkin ennen rakennelauseen esittelyä käsitteeseen *torsio*.

3.1 Torsioista

Määritelmä 3.1. Olkoon R kokonaisalue ja M R-moduli. Alkiota $x \in M$ sanotaan *torsioalkioksi*, mikäli on olemassa sellainen nollasta eroava alkio $r \in R$, että $rx = 0$. R-modulin M osajoukkoa, joka sisältää kaikki R-modulin M torsioalkiot, merkitään $\mathrm{Tor}_R(M)$.

Esimerkki 3.1. Tarkastellaan kokonaisaluetta $\mathbb{Z}$ ja $\mathbb{Z}$-modulia $\mathbb{Z}/6\mathbb{Z}$. Havaitaan, että alkiot $2, 3 \in \mathbb{Z}/6\mathbb{Z}$ ovat torsioalkioita, sillä

$$3 \cdot 2 = 0$$

ja

$$2 \cdot 3 = 0.$$

Täten $\mathrm{Tor}_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = \{2, 3\}$.

Määritelmä 3.2. Olkoon R kokonaisalue. R-modulia M sanotaan *torsiomoduliksi*, mikäli jokainen alkio $x \in M$ on torsioalkio.

Määritelmä 3.3. Olkoon R kokonaisalue. R-modulia M sanotaan *torsiovapaaksi*, mikäli $\mathrm{Tor}_R(M) = \{0\}$.

Lause 3.1. *Olkoon R kokonaisalue ja M vapaa R-moduli. Tällöin M on torsiovapaa R-moduli.*

Todistus. Oletetaan, että perhe $(x_i)_{i\in I} \in M^I$, missä I on epätyhjä joukko, on R-modulin M kanta. Olkoon alkio $x \in M$. Tällöin voidaan kirjoittaa

$$x = \sum_{i\in I} a_i x_i,$$

missä $a_i \in R$ kaikilla alkioilla $i \in I$. Oletetaan, että $ax = 0$, missä alkio $a \in R$ siten, että $a \neq 0$. Nyt

$$\begin{aligned} & ax = 0 \\ \Rightarrow \quad & a\sum_{i\in I} a_i x_i = 0 \\ \Rightarrow \quad & \sum_{i\in I} a a_i x_i = 0 \\ \Rightarrow \quad & aa_i = 0 \text{ kaikilla } i \in I, \end{aligned}$$

sillä perhe $(x_i)_{i\in I}$ on kantana vapaa. Koska R on kokonaisalue, niin $a_i = 0$ kaikilla $i \in I$. Siis täten R-moduli M on torsiovapaa. □

Lause 3.2. *Olkoon R kokonaisalue ja M R-moduli. Tällöin $Tor_R(M)$ on R-modulin M alimoduli ja tekijämoduli $M/\,Tor_R(M)$ on torsiovapaa.*

Todistus. (Vrt. [4, s. 88]) Osoitetaan ensin, että $\mathrm{Tor}_R(M)$ on R-modulin alimoduli. Selvästi torsioalkion määritelmän nojalla $0 \in \mathrm{Tor}_R(M)$. Olkoot $t_1, t_2 \in \mathrm{Tor}_R(M)$. Tällöin on olemassa nollasta eroavat alkiot $r_1, r_2 \in R$ siten, että $r_1 t_1 = 0$ ja $r_2 t_2 = 0$. Nyt

$$\begin{aligned} r_1 r_2(t_1 - t_2) &= (r_2 r_1)t_1 - (r_1 r_2)t_2 \\ &= r_2(r_1 t_1) - r_1(r_2 t_2) \\ &= r_2 \cdot 0 - r_1 \cdot 0 \\ &= 0. \end{aligned}$$

Koska kokonaisalue R ei sisällä nollanjakajia ja alkiot r_1 ja r_2 ovat nollasta eroavia, niin $t_1 - t_2 \in \mathrm{Tor}_R(M)$. Olkoon lisäksi $r \in R$. Tällöin

$$r_1(rt_1) = r(r_1 t_1) = r \cdot 0 = 0,$$

joten $rt_1 \in \mathrm{Tor}_R(M)$. Siis $\mathrm{Tor}_R(M)$ on R-modulin M alimoduli.

Osoitetaan sitten, että $M/\mathrm{Tor}_R(M)$ on torsiovapaa. Olkoon $m+\mathrm{Tor}_R(M) \in M/\mathrm{Tor}_R(M)$ ja oletetaan, että on olemassa nollasta eroava alkio $r \in R$ siten, että $r(m + \mathrm{Tor}_R(M)) = \mathrm{Tor}_R(M)$. Tällöin $rm \in \mathrm{Tor}_R(M)$, joten on olemassa nollasta eroava alkio $s \in R$ siten, että $s(rm) = 0$. Mutta $s(rm) = (sr)m$ ja koska R on kokonaisalue, niin $sr \in R/\{0\}$ ja $m \in \mathrm{Tor}_R(M)$. Täten $m+\mathrm{Tor}_R(M) = \mathrm{Tor}_R(M)$ ja tekijämoduli $M/\mathrm{Tor}_R(M)$ ei sisällä yhtään torsioalkiota. Siis tekijämoduli $M/\mathrm{Tor}_R(M)$ on torsiovapaa. □

3.2 Rakennelause

Määritelmä 3.4. Olkoon R kokonaisalue ja M R-moduli. Alimodulin $N \subseteq M$ *annihilaattori* on kokonaisalueen R ideaali

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

Apulause 3.3. *Olkoon R kommutatiivinen rengas, M, N R-moduleita, $M' \subseteq M$ R-modulin M alimoduli ja $N' \subseteq N$ R-modulin N alimoduli. Tällöin*

$$(M \times N)/(M' \times N') \cong (M/M') \times (N/N').$$

Todistus. Määritellään kuvaus

$$\varphi : M \times N \to (M/M') \times (N/N')$$

asettamalla $\varphi(m, n) = (m + M', n + N')$ kaikilla alkioilla $m \in M$ ja $n \in N$.

Olkoot $(a_1, b_1), (a_2, b_2) \in M \times N$ siten, että $(a_1, b_1) = (a_2, b_2)$. Toisin sanoen $a_1 = a_2$ ja $b_1 = b_2$. Tällöin

$$\begin{aligned}
\varphi(a_1, b_1) - \varphi(a_2, b_2) &= (a_1 + M', b_1 + N') - (a_2 + M', b_2 + N') \\
&= ((a_1 + M') - (a_2 + M'), (b_1 + N') - (b_1 + N')) \\
&= ((a_1 - a_2) + M', (b_1 - b_2) + N') \\
&= (0 + M', 0 + N') \\
&= 0,
\end{aligned}$$

joten $\varphi(a_1, b_1) = \varphi(a_2, b_2)$. Siis kuvaus φ on hyvinmääritelty.

Oletetaan nyt, että alkiot (a_1, b_1) ja (a_2, b_2) ovat mielivaltaiset, ja olkoon $r \in R$. Tällöin

$$\begin{aligned}
\varphi((a_1, b_1) + (a_2, b_2)) &= \varphi((a_1 + a_2, b_1 + b_2)) \\
&= ((a_1 + a_2) + M', (b_1 + b_2) + N') \\
&= (a_1 + M', b_1 + N') + (a_2 + M', b_2 + N') \\
&= \varphi(a_1, b_1) + \varphi(a_2, b_2)
\end{aligned}$$

ja

$$\begin{aligned}
\varphi(r(a_1, b_1)) &= \varphi((ra_1, rb_1)) \\
&= (ra_1 + M', rb_1 + N') \\
&= r(a_1 + M', b_1 + N') \\
&= r\varphi(a_1, b_1),
\end{aligned}$$

joten kuvaus φ on homomorfismi. Lisäksi

$$\begin{aligned}
\ker(\varphi) &= \{(m, n) \in M \times N \mid \varphi(m, n) = 0\} \\
&= \{(m, n) \in M \times N \mid (m + M', n + N') = (0 + M', 0 + N')\} \\
&= \{(m, n) \in M \times N \mid m \in M', n \in N'\} \\
&= M' \times N'
\end{aligned}$$

ja kuvaus φ on surjektio, sillä kaikilla alkioilla $(x + M', y + N') \in (M/M') \times (N/N')$

$$(x + M', y + N') = \varphi((x + y)),$$

missä $x + y \in M \times N$. Täten $\mathrm{im}(\varphi) = (M/M') \times (N/N')$. Nyt ensimmäisen isomorfialauseen nojalla

$$(M \times N)/(M' \times N') \cong (M/M') \times (N/N').$$

□

Lause 3.4. *Olkoon R kokonaisalue ja M R-moduli.*

1. *Oletetaan, että R-modulin M aste on n, ja $S := \{m_1, \ldots, m_m\} \subseteq M$ maksimaalinen lineaarisesti riippumaton joukko. Olkoon $N \subseteq M$ joukon S virittämä R-modulin M alimoduli. Tällöin alimoduli N on vapaa, $\mathrm{rank}(N) = n$ ja M/N on torsiomoduli.*
2. *Oletetaan, että on olemassa R-modulin M alimoduli $N \subseteq M$, joka on vapaa, sen aste on n ja M/N on torsiomoduli. Tällöin $\mathrm{rank}(M) = n$.*

Todistus. 1. Koska alimodulin N vapaa virittäjäjoukko S on lineaarisesti riippumaton, myöskin alimoduli itse on vapaa. Siis joukko S on alimodulin kanta ja täten $\mathrm{rank}(N) = n$.

Olkoon $x + N \in M/N$. Erityisesti alkio x ja joukko S ovat vapaita, sillä S on lineaarisesti riippumaton maksimaalinen joukko. Täten on olemassa alkiot $s, r_i \in R$ siten, että vähintään yksi joukon $\{s, r_1, \ldots, r_m\}$ alkioista on nollasta eroava ja $sx + \sum_{i=1}^{m} r_i m_i = 0$. Oletetaan, että $s = 0$. Tällöin $\sum_{i=1}^{m} r_i m_i = 0$, joten $r_i = 0$ kaikilla $i \in \{1, \ldots, m\}$, joka on ristiriita. Siis täytyy olla $s \neq 0$.

Nyt $sx \in N$, joten $s(x+N) = 0 \in M/N$. Täten $x+N$ on torsioalkio. Koska $x + N$ on mielivaltainen, niin M/N on torsiomoduli.

2. Olkoon $S \subseteq N$ alimodulin N vapaa virittäjäjoukko, jossa on n alkiota. Joukko S on lineaarisesti riippumaton R-modulissa M, joten R-modulin M aste on vähintään n.

Olkoon $T := \{t_1, \ldots, t_{n+1}\} \subseteq M$. Koska M/N on torsiomoduli, jokaista alkiota t_i kohti on olemassa nollasta eroava alkio $r_i \in R$ siten, että $r_i t_i + N = 0 + N$ eli $r_i t_i \in N$ kaikilla alkioilla $i \in \{1, \ldots, n+1\}$. Jos joillakin alkioilla i ja j, missä $i \neq j$, pätisi $r_i t_i = r_j t_j$, niin joukko T olisi lineaarisesti riippuvainen. Oletetaan, ettei näin ole, jolloin $\{r_1 t_1, \ldots, r_{n+1} t_{n+1}\} \subseteq N$. Koska alimoduli N on vapaa ja sen aste on n, jollakin $i \in \{1, \ldots, n+1\}$ on olemassa nollasta eroava alkio s_i siten, että $\sum_{i=1}^{n+1} s_i r_i t_i = 0$. Erityisesti joukko T on lineaarisesti riippuvainen R-modulissa M. Täten R-modulin M aste on enintään n. Mutta aiemmin osoitettiin, että R-modulin M aste on vähintään n, joten sen aste on täsmälleen n. □

Lause 3.5. *Olkoon R kokonaisalue ja M, N R-moduleita siten, että R-modulin M aste on m ja R-modulin N aste on n. Tällöin R-modulien M ja N suoran summan $M \oplus N$ aste on $m + n$.*

Todistus. Oletetaan, että $M' \subseteq M$ on R-modulin M alimoduli ja $N' \subseteq N$ on R-modulin N alimoduli. Nyt lauseen 3.4 kohdan 1 nojalla alimodulit M' ja N' ovat vapaita sekä niiden asteet $\operatorname{rank}(M') = m$ ja $\operatorname{rank}(N') = n$, ja lisäksi tekijämodulit M/M' ja N/N' ovat torsiomoduleita.

Olkoon nyt $(m', n') \in M' \oplus N'$. Koska $m' \in M' \subseteq M$ ja $n' \in N' \subseteq N$, niin $M' \oplus N' \subseteq M \oplus N$. Lisäksi koska alimodulit M' ja N' ovat vapaita, niin myöskin niiden suora summa $M' \oplus N'$ on vapaa, sillä minkä tahansa alkion $s := (s_1, s_2) \in M' \oplus N'$ komponentit $s_1 \in M'$ ja $s_2 \in N'$ voidaan kirjoittaa alimodulien M' ja N' kantojen avulla. Täten näistä kannoista saadaan muodostettua alimodulien suoran summan $M' \oplus N'$ kanta. Toisin sanoen alimodulien suoran summan $M' \oplus N'$ kanta on alimodulien M' ja N' kantojen yhdiste, joten sen alkioiden lukumäärä on $m + n$.

Koska modulien suora summa on määritelty karteesisen tulon avulla, apulauseen 3.3 nojalla

$$(M \oplus N)/(M' \oplus N') \cong (M/M') \oplus (N/N').$$

Nyt koska R on pääideaalialueena kokonaisalue, torsiomodulien äärellinen suora summa on torsiomoduli, sillä tämä suora summa ei sisällä muita kuin torsioalkioita. Tällöin $(M \oplus N)/(M' \oplus N')$ on myöskin torsiomoduli.

Koska alimodulien M' ja N' suoran summan $M' \oplus N'$ kannan alkioiden lukumäärä on $m + n$, niin $\operatorname{rank}(M' \oplus N') = m + n$. Nyt lauseen 3.4 kohdan 2 nojalla myös R-modulien M ja N suoran summan $M \oplus N$ aste on $m + n$. □

Lause 3.6. *Olkoon R pääideaalialue, M äärellisviritteinen vapaa R-moduli, jonka aste $\operatorname{rank}(M) = n$ ja $N \subseteq M$ R-modulin M alimoduli. Tällöin*

1. *alimoduli N on vapaa ja sen aste $\operatorname{rank}(N) = m$, missä $m \leq n$.*
2. *on olemassa R-modulin M kanta $(x_1, \ldots, x_n) \in M$ siten, että $(a_1x_1, \ldots, a_mx_m)$, $m \leq n$, on alimodulin N kanta, missä nollasta eroavat alkiot $a_1, \ldots, a_m \in R$ toteuttavat ehdon $a_1 \mid \cdots \mid a_m$.*

Todistus. (Vrt. [3, s. 460]) Jos R-modulin M alimoduli $N = \{0\}$, niin väite pätee triviaalisti. Voidaan siis olettaa, että $N \neq \{0\}$.

Osoitetaan ennen varsinaisen väitteen todistamista, että $M = Ry_1 \oplus \ker(\psi)$ ja $N = Ra_1y_1 \oplus (N \cap \ker(\psi))$, missä alkio $y_1 \in M$ ja kuvaus ψ on homomorfismi R-modulilta M pääideaalialueelle R.

Oletetaan, että kuvaus $\varphi : M \to R$ on homomorfismi. Osoitetaan ensin, että alimodulin N kuva

$$\varphi(N) = \{r \in R \mid \text{on olemassa alkio } n \in N \text{ siten, että } \varphi(n) = r\}$$

on ideaali pääideaalialueessa R. Nyt on olemassa alkiot $n, n' \in N$ siten, että $\varphi(n) = r$ ja $\varphi(n') = r'$, missä alkiot $r, r' \in R$. Koska N on R-modulin M alimoduli, niin $n+n' \in N$, ja koska kuvaus φ on homomorfismi, niin $\varphi(n+n') = \varphi(n) + \varphi(n') = r + r' \in R$. Vastaavasti havaitaan, että $a\varphi(n) = \varphi(an) =$

ar, missä alkio $a \in R$. Siis alimodulin N kuva $\varphi(N)$ on pääideaalialueen R alimoduli. Koska lisäksi $0 \in R$, niin on olemassa alkio $m \in N$ siten, että $\varphi(m) = 0$. Siis alimodulin N kuva $\varphi(N)$ on ideaali pääideaalialueessa R.

Koska R on pääideaalialue, ideaali $\varphi(N) := \langle a_\varphi \rangle$ on tällöin pääideaali. Olkoon

$$\Sigma := \{\langle a_\varphi \rangle \mid \varphi \in \mathrm{Hom}_R(M, R)\}$$

pääideaalialueen R pääideaalien joukko, missä pääideaalit $\langle a_\varphi \rangle$ on muodostettu edellä kuvatulla tavalla. Osoitetaan, että joukossa Σ on maksimaalinen alkio. Joukko Σ on epätyhjä, sillä homomorfismiksi $\varphi : M \to R$ voidaan valita triviaali homomorfismi $M \to R : x \mapsto 0$. Täten $\langle 0 \rangle \in \Sigma$ ja joukko Σ on epätyhjä. Lauseen 2.11 mukaan pääideaalialueen R ideaalien kokoelmassa on maksimaalinen alkio, joten joukossa Σ on maksimaalinen alkio. Toisin sanoen on olemassa ainakin yksi homomorfismi $\psi : M \to R$ siten, että pääideaali $\psi(N) := \langle a_\psi \rangle$ ei sisälly aidosti mihinkään muuhun joukon Σ alkioon. Merkitään tätä virittäjäalkiota $a_1 := a_\psi$.

Osoitetaan sitten, että $a_1 \neq 0$. Olkoon perhe $(x_1, \ldots, x_n)$ R-modulin M kanta ja kuvaus

$$\pi_i : M \to R, a_1x_1 + \cdots + a_nx_n \mapsto a_i$$

luonnollinen homomorfismi kaikilla alkioilla $i \in \{1, \ldots, n\}$. Koska alimoduli $N \neq \{0\}$, jollakin $i \in \{1, \ldots, n\}$ pätee $\pi_i(N) \neq 0$. Täten joukko Σ sisältää triviaalin ideaalin lisäksi myös jonkin muun ideaalin. Koska pääideaali $\langle a_1 \rangle$ on joukon Σ maksimaalinen alkio, täytyy olla $a_1 \neq 0$.

Olkoon alkio $y \in N$ sellainen, että $\psi(y) = a_1$. Osoitetaan sitten, että $a_1 \mid \varphi(y)$ kaikilla homomorfismeilla $\varphi \in \mathrm{Hom}_R(M, R)$. Tarkastellaan ideaalia $\langle a_1, \varphi(y) \rangle$. Koska R on pääideaalialue, niin $\langle a_1, \varphi(y) \rangle = \langle d \rangle$ jollakin alkiolla $d \in R$. Täten alkio d jakaa molemmat alkiot a_1 ja $\varphi(y)$, ja $d = r_1a_1 + r_2\varphi(y)$ joillakin alkioilla $r_1, r_2 \in R$. Oletetaan, että kuvaus $\nu = r_1\psi + r_2\varphi$ on homomorfismi R-modulilta M pääideaalialueelle R. Tämä todella on homomorfismi, sillä olkoot $a, b \in M$ ja $a \in R$. Nyt

$$\begin{aligned}
\nu(a) + \nu(b) &= (r_1\psi + r_2\varphi)(a) + (r_1\psi + r_2\varphi)(b) \\
&= (r_1\psi(a) + r_2\varphi(a)) + (r_1\psi(b) + r_2\varphi(b)) \\
&= r_1\psi(a + b) + r_2\varphi(a + b) \\
&= (r_1\psi + r_2\varphi)(a + b) \\
&= \nu(a + b)
\end{aligned}$$

ja

$$\begin{aligned}
\nu(ra) &= (r_1\psi + r_2\varphi)(ra) \\
&= r_1\psi(ra) + r_2\varphi(ra) \\
&= rr_1\psi(a) + rr_2\varphi(a) \\
&= r(r_1\psi + r_2\varphi)(a) \\
&= r\nu(a).
\end{aligned}$$

Tällöin $\nu(y) = (r_1\psi + r_2\varphi)(y) = r_1\psi(y) + r_2\varphi(y) = r_1a_1 + r_2\varphi(y) = d$, joten alkio $d \in \nu(N)$ ja myöskin $\langle d\rangle \subseteq \nu(N)$. Koska alkio d jakaa alkion a_1, pätee myöskin $\langle a_1\rangle \subseteq \langle d\rangle$. Täten pääideaalin $\langle a_1\rangle$ maksimaalisuuden perusteella yhtälö $\langle a_1\rangle = \langle d\rangle = \langle a_1, \varphi(y)\rangle$ pätee, ja alkio d jakaa alkion $\varphi(y)$, joten myöskin alkio a_1 jakaa alkion $\varphi(y)$, koska $\langle a_1\rangle = \langle d\rangle$.

Koska $a_1 \mid \varphi(y)$ kaikilla homomorfismeilla $\varphi \in \mathrm{Hom}_R(M, R)$, niin tällöin myöskin $a_1 \mid \pi_i(y)$ kaikilla alkioilla $i \in \{1, \ldots, n\}$. Voidaan siis kirjoittaa $\pi_i(y) = a_1b_i$ jollakin alkiolla $b_i \in R$, missä $i \in \{1, \ldots, n\}$. Kirjoitetaan

$$y_1 := b_1x_1 + \cdots + b_nx_n,$$

missä alkiot $x_1, \ldots, x_n$ ovat R-modulin M kannan alkioita. Koska $x_j = 1 \cdot x_j$, niin $\pi_i(x_j) = 1$, kun $i = j$, ja $\pi_i(x_j) = 0$, kun $i \neq j$. Nyt kaikilla $i \in \{1, \ldots, n\}$ pätee

$$\begin{aligned}\pi_i(a_1y_1) &= \pi_i(a_1b_1x_1 + \cdots + a_1b_nx_n)\\ &= a_1b_i.\end{aligned}$$

Siis $\pi_i(a_1y_1) = \pi_i(y)$ kaikilla $i \in \{1, \ldots, n\}$, joten $a_1y_1 = y$. Täten $a_1 = \psi(y) = \psi(a_1y_1) = a_1\psi(y_1)$. Siis $a_1(1 - \psi(y_1)) = 0$. Koska $a_1 \neq 0$ ja pääideaalialue R on myöskin kokonaisalue, niin

$$\psi(y_1) = 1.$$

Osoitetaan vielä, että alkiota y_1 voidaan käsitellä R-modulin M kannan alkiona ja alkiota a_1y_1 voidaan käsitellä alimodulin N kannan alkiona. Toisin sanoen osoitetaan, että seuraavat kohdat ovat voimassa:

- $M = Ry_1 \oplus \ker(\psi)$,
- $N = Ra_1y_1 \oplus (N \cap \ker(\psi))$.

Oletetaan ensin, että alkio $x \in M$ ja kirjoitetaan $x = \psi(x)y_1 + (x - \psi(x)y_1)$. Koska

$$\begin{aligned}\psi(x - \psi(x)y_1) &= \psi(x) - \psi(x)\psi(y_1)\\ &= \psi(x) - \psi(x) \cdot 1\\ &= 0,\end{aligned}$$

niin $x - \psi(x)y_1 \in \ker(\psi)$. Koska lisäksi $\psi(x)y_1 \in Ry_1$, niin $M = Ry_1 + \ker(\psi)$. Oletetaan lisäksi, että myös $ry_1 \in \ker(\psi)$. Tällöin $0 = \psi(ry_1) = r\psi(y_1) = r$, joten $Ry_1 \cap \ker(\psi) = \{0\}$. Siis

$$M = Ry_1 \oplus \ker(\psi).$$

Koska $\psi(N) = \langle a_1\rangle$, niin $a_1 \mid \psi(x')$ kaikilla alkioilla $x' \in N$. Kirjoittamalla $\psi(x') = ba_1$, missä $b \in R$, ja $x' = \psi(x')y_1 + (x' - \psi(x')y_1)$, saadaan

$$x' = ba_1y_1 + (x' - ba_1y_1),$$

missä $x' - ba_1y_1 \in \ker(\psi)$. Toisaalta $x' - ba_1y_1 \in N$, joten

$$N = Ra_1y_1 + (N \cap \ker(\psi)).$$

Oletetaan lisäksi, että $r'a_1y_1 \in N \cap \ker(\psi)$. Erityisesti $r'a_1y_1 \in \ker(\psi)$, joten $0 = \psi(r'a_1y_1) = r'a_1\psi(y_1) = r'a_1$. Siis $Ra_1y_1 \cap (N \cap \ker(\psi)) = \{0\}$, joten

$$N = Ra_1y_1 \oplus (N \cap \ker(\psi)).$$

1. Todistetaan väite induktiolla alimodulin N asteen m suhteen. Jos $m = 0$, niin N on torsiomoduli. Koska vapaa moduli on torsiovapaa, niin $N = \{0\}$. Siis tällöin väite pätee triviaalisti.

Oletetaan, että $m > 0$ ja väite pätee kaikilla vapailla alimoduleilla, joiden aste on pienempi kuin m. Koska summa $Ra_1y_1 \oplus (N \cap \ker(\psi))$ on suora ja termin Ra_1y_1 aste on 1, lauseen 3.5 nojalla termin $N \cap \ker(\psi)$ aste on $m - 1$. Nyt induktio-oletuksen nojalla $N \cap \ker(\psi) \subseteq N$ on astetta $m - 1$ oleva vapaa R-moduli. Riittää siis näyttää, että yhdistämällä termi a_1y_1 R-modulin $N \cap \ker(\psi)$ kantaan, saadaan koko alimodulin N kanta. Olkoon $(z_1, \ldots, z_{m-1})$ R-modulin $N \cap \ker(\psi)$ kanta. Osoitetaan, että $(a_1y_1, z_1, \ldots, z_{m-1})$ on alimodulin N kanta. Koska $Ra_1y_1 = \langle a_1y_1 \rangle$ ja $N = Ra_1y_1 \oplus (N \cap \ker(\psi))$, niin selvästi perhe $(a_1y_1, z_1, \ldots, z_{m-1})$ virittää alimodulin N. Se myöskin on vapaa, sillä jos

$$sa_1y_1 + \sum_{i=1}^{m-1} r_iz_i = 0$$

joillakin alkioilla $s, r_1, \ldots, r_{m-1} \in R$, niin koska $N = Ra_1y_1 \oplus (N \cap \ker(\psi))$, täytyy olla $s = 0$ ja $\sum_{i=1}^{m-1} r_iz_i = 0$. Lisäksi koska $(z_1, \ldots, z_{m-1})$ on R-modulin $N \cap \ker(\psi)$ kanta, niin täytyy olla $r_i = 0$ kaikilla $i \in \{1, \ldots, m-1\}$. Siis $(a_1y_1, z_1, \ldots, z_{m-1})$ on alimodulin N kanta ja näin ollen alimoduli N on astetta m oleva vapaa R-moduli.

2. Todistetaan väite induktiolla R-modulin M asteen n suhteen. Käyttämällä lauseen 3.6 kohtaa 1 alimoduliin $\ker(\psi)$, nähdään, että $\ker(\psi)$ on vapaa ja sen aste on $m \leq n$. Jos $n = 0$, niin tällöin $m = 0$ ja väite pätee triviaalisti.

Oletetaan, että $n > 0$ ja väite pätee kaikilla R-moduleilla, joiden aste on pienempi kuin n. Koska summa $Ry_1 \oplus \ker(\psi)$ on suora, lauseen 3.5 nojalla vapaan alimodulin $\ker(\psi)$ aste on $n - 1$. Merkitsemällä R-modulina $\ker(\psi)$ ja alimodulina $\ker(\psi) \cap N$, induktio-oletuksen nojalla on olemassa R-modulin $\ker(\psi)$ kanta $(y_2, \ldots, y_n)$ siten, että perhe $(a_2y_2, \ldots, a_my_m)$ on alimodulin $\ker(\psi) \cap N$ kanta, joillakin alkioilla $a_2, \ldots, a_m \in R$, jotka toteuttavat ehdon $a_2 \mid \cdots \mid a_m$. Summien $M = Ry_1 \oplus \ker(\psi)$ ja $N = Ra_1y_1 \oplus (N \cap \ker(\psi))$ suoruuden nojalla perhe $(y_1, \ldots, y_n)$ on R-modulin M kanta ja perhe $(a_1y_1, \ldots, a_my_m)$ on alimodulin N kanta.

Osoitetaan vielä, että ehto $a_1 \mid a_2$ pätee. Määritellään homomorfismi $\rho : M \to R$ asettamalla $\rho(y_1) = \rho(y_2) = 1$ ja $\rho(y_i) = 0$ kaikilla alkioilla $i > 2$, missä alkiot y_j ovat R-modulin M kannan alkioita kaikilla alkioilla $j \in \{1, \ldots, n\}$.

Tällöin $a_1 = a_1\rho(y_1) = \rho(a_1y_1)$, joten $a_1 \in \rho(N)$ ja myöskin $\langle a_1\rangle \subseteq \rho(N)$. Koska $\langle a_1\rangle$ on maksimaalinen ideaali perheessä Σ, on oltava $\langle a_1\rangle = \rho(N)$. Nyt vastaavasti $a_2 = \rho(y_2a_2) \in \rho(N)$, niin tällöin $a_2 \in \langle a_1\rangle$. Toisin sanoen $a_1 \mid a_2$, mistä väite seuraa. □

Lause 3.7 (Rakennelause invarianttien tekijöiden avulla)**.** *Olkoon R pääideaalialue ja M äärellisviritteinen R-moduli. Tällöin R-moduli M on isomorfinen äärellisen monen syklisen modulin suoran summan kanssa. Toisin sanoen*

$$M \cong R^r \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle$$

jollakin kokonaisluvulla $r \geq 0$ ja nollasta eroavilla alkioilla $a_1, \ldots, a_m \in R$, jotka toteuttavat ehdon $a_1 \mid \cdots \mid a_m$.

Todistus. (Vrt. [3, s. 463]) Koska R-moduli M on äärellisviritteinen, on olemassa äärellinen joukko $X := \{x_1, \ldots, x_n\} \subseteq M$ siten, että $M = \langle X\rangle$. Olkoon R^n astetta n oleva vapaa R-moduli, jonka kantana on perhe $(b_1, \ldots, b_n)$. Määritellään nyt kuvaus

$$f : R^n \to M$$

asettamalla $f(b_i) = x_i$ kaikilla alkioilla $i \in \{1, \ldots, n\}$. Kuvaus f on selvästi homomorfismi, sillä kaikilla alkioilla $a \in R$ ja $x, y \in R^n$ pätee

$$\begin{aligned} f(x+y) &= f((r_1b_1 + \cdots + r_nb_n) + (r_1'b_1 + \cdots + r_n'b_n)) \\ &= f((r_1 + r_1')b_1 + \cdots + (r_n + r_n')b_n) \\ &= (r_1 + r_1')x_1 + \cdots + (r_n + r_n')x_n \\ &= (r_1x_1 + \cdots + r_nx_n) + (r_1'x_1 + \cdots + r_n'x_n) \\ &= f(r_1b_1 + \cdots + r_nb_n) + f(r_1'b_1 + \cdots + r_n'b_n) \\ &= f(x) + f(y) \end{aligned}$$

sekä

$$\begin{aligned} f(ax) &= f(a(r_1b_1 + \cdots + r_nb_n)) \\ &= f(ar_1b_1 + \cdots + ar_nb_n) \\ &= ar_1x_1 + \cdots + ar_nx_n \\ &= a(r_1x_1 + \cdots + r_nx_n) \\ &= af(r_1b_1 + \cdots + r_nb_n) \\ &= af(x). \end{aligned}$$

Koska alkiot $x_1, \ldots, x_n \in R$ virittävät R-modulin M, huomataan, että homomorfismi f on surjektio. Nyt ensimmäisen isomorfialauseen nojalla on olemassa isomorfismi $R^n/\ker(f) \cong M$. Lauseen 2.2 nojalla $\ker(f)$ on R-modulin R^n alimoduli, joten R-moduliin R^n ja alimoduliin $\ker(f)$ voidaan soveltaa lauseen 3.6 kohtaa 2. Siis R-modulille R^n voidaan valita toinen kanta $(y_1, \ldots, y_n)$ siten,

että $(a_1y_1, \ldots, a_my_m)$ on alimodulin $\ker(f)$ kanta joillakin nollasta eroavilla alkioilla $a_1, \ldots, a_m \in R$, jotka toteuttavat ehdon $a_1 \mid \cdots \mid a_m$. Tällöin

$$R^n/\ker(f) \cong (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m).$$

Lauseen 2.4 nojalla on olemassa luonnollinen surjektiivinen homomorfismi

$$\pi : Ry_1 \oplus \cdots \oplus Ry_n \to R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle \oplus R^{n-m},$$

missä $\pi(\alpha_1y_1, \ldots, \alpha_ny_n) = (\alpha_1 \bmod \langle a_1\rangle, \ldots, \alpha_m \bmod \langle a_m\rangle, \alpha_{m+1}, \ldots, \alpha_n)$. Nyt

$$\ker(\pi) = \{(\alpha_1y_1, \ldots, \alpha_ny_n) \in Ry_1 \oplus \cdots \oplus Ry_n \mid \pi(\alpha_1y_1, \ldots, \alpha_ny_n) = 0\},$$

missä

$$\begin{aligned}
& \pi(\alpha_1y_1, \ldots, \alpha_ny_n) = 0 \\
\Rightarrow\ & (\alpha_1 \bmod \langle a_1\rangle, \ldots, \alpha_m \bmod \langle a_m\rangle, \alpha_{m+1}, \ldots, \alpha_n) = 0 \\
\Rightarrow\ & \alpha_i \bmod \langle a_i\rangle = 0 \text{ kaikilla alkioilla } i \in \{1, \ldots, m\} \\
\Rightarrow\ & \langle a_i\rangle \mid \alpha_i \text{ kaikilla alkioilla } i \in \{1, \ldots, m\}.
\end{aligned}$$

Siis täten $\ker(\pi) = Ra_1y_1 \oplus \cdots \oplus Ra_my_m$. Nyt soveltamalla ensimmäistä isomorfialausetta kuvaukseen π, saadaan isomorfismi

$$(Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m) \cong R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle \oplus R^{n-m},$$

joten

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

Mikäli alkio a on yksikkö, niin $R/\langle a\rangle = 0$. Tällöin kaikki sellaiset termit, joissa alkio a_i on yksikkö, missä alkio $i \in \{1, \ldots, m\}$, voidaan poistaa. Valitsemalla $r = n - m$, väite on todistettu. □

Huomautus. Lauseen 3.7 esitysmuoto on pääideaalialueen R yksiköitä vaille yksikäsitteinen, sillä jos on olemassa isomorfismi

$$M \cong R^{r'} \oplus R/\langle b_1\rangle \oplus \cdots \oplus R/\langle b_{m'}\rangle$$

jollakin kokonaisluvulla $r' \geq 0$ ja nollasta eroavilla alkioilla $b_1, \ldots, b_{m'} \in R$, jotka toteuttavat ehdon $b_1 \mid \cdots \mid b_{m'}$, niin ehdosta $a_1 \mid \cdots \mid a_m$ seuraa, että $r = r'$, $m = m'$ ja $\langle a_i\rangle = \langle b_i\rangle$ kaikilla alkioilla $i \in \{1, \ldots, m\}$. Rakennelauseen yksikäsitteisyys todistetaan tarkemmin lauseessa 3.13.

Määritelmä 3.5. Lauseessa 3.7 esiteltyä kokonaislukua r sanotaan R-modulin *M vapaaksi asteeksi* ja alkioita $a_1, \ldots, a_n \in R$ sanotaan R-modulin *M invarianteiksi tekijöiksi.*

Lause 3.8 (Rakennelause alkeisjakajien avulla)**.** *Olkoon R pääideaalialue ja M äärellisviritteinen R-moduli. Tällöin R-moduli M on suora summa äärellisen monesta syklisestä modulista, joiden annihilaattorit ovat joko $\langle 0\rangle$ tai alkualkiopotenssien virittämiä eli*

$$M \cong R^r \oplus R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle,$$

missä kokonaisluku $r \geq 0$ ja alkualkiopotenssit $p_1^{\alpha_1}, \ldots, p_m^{\alpha_m} \in R$ ovat positiivisia.

Todistus. (Vrt. [3, s. 464]) Olkoon $a \in R$ nollasta eroava alkio. Lauseen 2.14 mukaan pääideaalialue R on faktoriaalinen, joten alkiolle a saadaan esitysmuoto

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m},$$

missä alkio $u \in R$ on yksikkö ja alkiot $p_i \in R$ ovat alkualkioita siten, että $p_i \neq p_j$ kaikilla $i \neq j$, missä $i, j \in \{1, \ldots, m\}$. Tämä esitysmuoto on yksikäsitteinen, joten ideaalit $\langle p_i^{\alpha_i}\rangle$ ovat yksikäsitteisesti määritettyjä kaikilla $i \in \{1, \ldots, m\}$.

Pääideaalialueessa jokainen ideaali on pääideaali. Täten alkualkioiden p_i ja p_j, missä $i \neq j$, suurin yhteinen tekijä on $1 \in R$, ja ideaalien $\langle p_i^{\alpha_i}\rangle$ ja $\langle p_j^{\alpha_j}\rangle$ muodostama summaideaali $\langle p_i^{\alpha_i}\rangle + \langle p_j^{\alpha_j}\rangle$ on alkion 1 virittämä, joten $\langle p_i^{\alpha_i}\rangle + \langle p_j^{\alpha_j}\rangle = R$. Toisin sanoen ideaalit $\langle p_i^{\alpha_i}\rangle$ ja $\langle p_j^{\alpha_j}\rangle$ ovat komaksimaaliset kaikilla $i \neq j$, missä $i, j \in \{1, \ldots, m\}$.

Koska alkualkiopotenssien $p_1^{\alpha_1}, \ldots, p_m^{\alpha_m}$ pienin yhteinen jaettava on $a \in R$, niin

$$\langle p_1^{\alpha_1}\rangle \cap \cdots \cap \langle p_m^{\alpha_m}\rangle = \langle a\rangle.$$

Täten Kiinalaisen jäännöslauseen nojalla

$$R/\langle a\rangle = R/(\langle p_1^{\alpha_1}\rangle \cap \cdots \cap \langle p_m^{\alpha_m}\rangle) \cong R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle.$$

pätee renkaiden lisäksi myöskin R-modulille. Nyt tätä seikkaa voidaan käyttää jokaiseen lauseessa 3.7 esiintyvään termiin $R/\langle a_i\rangle$, missä $i \in \{1, \ldots, m\}$, mistä väite seuraa. □

Määritelmä 3.6. Olkoon R pääideaalialue ja M sellainen äärellisviritteinen R-moduli kuin lauseessa 3.8. Alkualkiopotensseja $p_1^{\alpha_1}, \ldots, p_m^{\alpha_m} \in R$ kutsutaan R-modulin M *alkeisjakajiksi.*

Lause 3.9. *Olkoon R pääideaalialue ja M äärellisviritteinen torsiomoduli. Tällöin*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n,$$

missä $N_i = \{x \in M \mid p_i^{\alpha_i} x = 0$ jollakin $\alpha_i \geq 1\}$ on torsiomodulin M alimoduli ja $p_i \in R$ on alkualkio kaikilla $i \in \{1, \ldots, n\}$ siten, että $p_i \neq p_j$, kun $i \neq j$.

Todistus. (Vrt. [3, s. 465]) Osoitetaan, että N_i on torsiomodulin M alimoduli kaikilla $i \in \{1, \ldots, n\}$. Selvästi joukko N_i on epätyhjä. Olkoot $a, b \in N_i$. Tällöin $p_i^{\alpha_i} a = 0$ ja $p_i^{\alpha_i} b = 0$, joten

$$0 = 0 + 0 = p_i^{\alpha_i} a + p_i^{\alpha_i} b = p_i^{\alpha_i}(a + b).$$

Siis $a+b \in N_i$. Olkoot lisäksi $r \in R$. Tällöin $p_i^{\alpha_i}(ra) = r(p_i^{\alpha_i}a) = r \cdot 0 = 0$, joten myöskin $ra \in N_i$. Siis N_i on torsiomodulin M alimoduli kaikilla $i \in \{1, \ldots, n\}$.

Olkoon $M \cong R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle$, missä nollasta eroavat alkiot $a_1, \ldots, a_m \in R$ toteuttavat ehdon $a_1 \mid \cdots \mid a_m$. Tällöin $\mathrm{Ann}_R(M) = \langle a_m\rangle$, missä $a_m \neq 0$. Olkoon

$$a_m = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{a_n}.$$

Olkoon lisäksi $P = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{a_n}$ ja $P_i = P/p_i^{\alpha_i}$. Havaitaan, että alkioiden $P_1, \ldots, P_n$ suurin yhteinen tekijä on 1, joten on olemassa $Q_1, \ldots, Q_n \in R$ siten, että

$$\sum_{i=1}^{n} P_iQ_i = 1.$$

Olkoon $x \in M$. Tällöin $x = 1 \cdot x = \sum_{i=1}^{n} P_iQ_ix$. Nyt

$$p_i^{\alpha_i}(P_iQ_ix) = PQ_ix = Q_iPx = Q_i \cdot 0 = 0,$$

joten $P_iQ_ix \in N_i$ kaikilla $i \in \{1, \ldots, n\}$ ja edelleen $M = N_1 + \cdots + N_n$.

Olkoon $y \in N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_n)$. Tällöin $p_j^{\alpha_j}y = 0$ ja $P_jy = 0$. Koska alkioiden $p_j^{\alpha_j}$ ja P_j suurin yhteinen tekijä on 1, niin on olemassa alkiot $r, s \in R$ siten, että $p_j^{\alpha_j}r + P_js = 1$. Täten

$$y = p_j^{\alpha_j}ry + P_jsy = 0$$

ja $M = N_1 \oplus \cdots \oplus N_n$. □

Määritelmä 3.7. Lauseessa 3.9 mainittua alimodulia N_i sanotaan torsiomodulin M *p-primääriseksi komponentiksi.*

Apulause 3.10. *Olkoon R kokonaisalue ja M, N R-moduleita. Tällöin $Tor_R(M \oplus N) = Tor_R(M) \oplus Tor_R(N)$.*

Todistus. Olkoon $(m, n) \in \mathrm{Tor}_R(M \oplus N)$. Siis on olemassa nollasta eroava alkio $r \in R$ siten, että $r(m, n) = (0, 0)$. Siis $(rm, rn) = (0, 0)$, joten täytyy olla $rm = 0$ ja $rn = 0$. Mutta torsioalkion määritelmän nojalla tällöin $m \in \mathrm{Tor}_R(M)$ ja $n \in \mathrm{Tor}_R(N)$, joten $\mathrm{Tor}_R(M \oplus N) \subseteq \mathrm{Tor}_R(M) \oplus \mathrm{Tor}_R(N)$.

Olkoon sitten $(m, n) \in \mathrm{Tor}_R(M) \oplus \mathrm{Tor}_R(N)$. Tällöin on olemassa nollasta eroavat alkion $u, v \in R$ siten, että $um = 0$ ja $vn = 0$. Koska R on kokonaisalue, niin myöskin tulo $uv \in R$ on nollasta eroava. Nyt $uv(m, n) = (u(vm), v(um)) = (0, 0)$, joten $(m, n) \in \mathrm{Tor}_R(M \oplus N)$. Siis $\mathrm{Tor}_R(M \oplus N) = \mathrm{Tor}_R(M) \oplus \mathrm{Tor}_R(N)$. □

Apulause 3.11. *Olkoon R pääideaalialue ja $p \in R$ alkualkio. Merkitään kuntaa $F := R/(p)$.*

1. *Olkoon $M = R^r$. Tällöin $M/pM \cong F^r$.*
2. *Olkoon $M = R/\langle a\rangle$, missä $a \in R$ on nollasta eroava alkio. Tällöin*

$$M/pM \cong \begin{cases} F, \text{ jos alkio } p \text{ jakaa alkion } a. \\ 0, \text{ jos alkio } p \text{ ei jaa alkiota } a. \end{cases}$$

3. Olkoon $M = R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_n\rangle$, missä alkio p jakaa alkion a_i kaikilla $i \in \{1, \ldots, n\}$. Tällöin $M/pM \cong F^n$.

Todistus. (Vrt [3, s. 466]) 1. Koska $\langle p\rangle \subseteq M$ on alimoduli, niin lauseen 2.4 nojalla on olemassa surjektiivinen homomorfismi

$$\varphi : R^r \to (R/\langle p\rangle)^r, (a_1, \ldots, a_r) \mapsto (a_1 \bmod \langle p\rangle, \ldots, a_r \bmod \langle p\rangle),$$

jonka ydin

$$\begin{aligned}\ker(\varphi) &= \{(a_1, \ldots, a_r) \in R^r \mid \varphi((a_1, \ldots, a_r)) = 0\} \\ &= \{(a_1, \ldots, a_r) \in R^r \mid (a_1 \bmod \langle p\rangle, \ldots, a_r \bmod \langle p\rangle) = (0, \ldots, 0)\} \\ &= \{(a_1, \ldots, a_r) \in R^r \mid \langle p\rangle \mid a_i \text{ kaikilla } i \in \{1, \ldots, r\}\} \\ &= pR^r.\end{aligned}$$

Nyt ensimmäisen isomorfialauseen nojalla

$$R^r/pR^r \cong (R/\langle p\rangle)^r.$$

2. Tarkastellaan homomorfismia $\varphi : R \to R/\langle a\rangle, r \mapsto r + \langle a\rangle$. Kuvauksen ydin

$$\begin{aligned}\ker(\varphi) &= \{r \in R \mid \varphi(r) = 0\} \\ &= \{r \in R \mid r + \langle a\rangle = 0 + \langle a\rangle\} \\ &= \{r \in R \mid r \in \langle a\rangle\} \\ &= \langle a\rangle.\end{aligned}$$

Jos alkio p jakaa alkion a, niin tällöin $\langle a\rangle \subseteq \langle p\rangle$ ja ideaalin $\langle p\rangle$ kuva tekijärenkaassa $R/\langle a\rangle$ on $p(R/\langle a\rangle)$. Nyt kolmannen isomorfialauseen nojalla $M/pM \cong R/\langle p\rangle$.

Koska ideaalin $\langle p\rangle + \langle a\rangle$ virittää alkioiden p ja a suurin yhteinen tekijä, niin $\langle p\rangle + \langle a\rangle = \langle 1\rangle = R$, kun alkio p ei jaa alkiota a. Tällöin $M/pM = M/M \cong 0$.

3. Merkitään $M_i := R/\langle a_i\rangle$. Koska alkio p jakaa jokaisen alkion a_i kaikilla $i \in \{1, \ldots, n\}$, niin kohdan 2 nojalla $M_i/pM_i \cong F$ kaikilla $i \in \{1, \ldots, n\}$. Siis

$$\begin{aligned}M_1/pM_1 \oplus \cdots \oplus M_n/pM_n &\cong \underbrace{F \oplus \cdots \oplus F}_{\text{n kappaletta}} \\ &\cong F^n,\end{aligned}$$

joten

$$\begin{aligned}M_1/pM_1 \oplus \cdots \oplus M_n/pM_n &\cong M/pM \\ &\cong F^n.\end{aligned}$$

□

Apulause 3.12. *Olkoon R kokonaisalue. Tällöin jokaisella äärellisviritteisellä torsiomodulilla on nollasta eroava annihilaattori.*

Todistus. Olkoon M kokonaisalueen R yli määritelty äärellisviritteinen torsiomoduli. Tällöin on olemassa sellainen äärellinen joukko $A \subseteq M$, missä jokainen $x \in A$ on nollasta eroava, että $M = RA$. Olkoon $A = \{a_1, \ldots, a_n\}$. Koska M on torsiomoduli, on olemassa nollasta eroavat alkiot $r_1, \ldots, r_n \in R$, siten, että $r_i a_i = 0$ kaikilla $i \in \{1, \ldots, n\}$.

Olkoot $q = r_1 \cdots r_n$ ja $m \in M$. Koska $M = RA$, niin on olemassa alkiot $s_1, \ldots, s_n \in R$, siten, että

$$m = s_1 a_1 + \cdots + s_n a_n.$$

Koska R on kokonaisalueena kommutatiivinen, niin $q = pr_j$ jollakin alkiolla $j \in \{1, \ldots, n\}$, missä

$$p = r_1 \cdots r_{j-1} \cdot r_{j+1} \cdots r_n.$$

Tällöin

$$qa_j = (pr_j)a_i = p(r_j a_j) = p(0) = 0.$$

Täten $qa_1 = qa_2 = \cdots = qa_n = 0$, joten

$$\begin{aligned} qm &= q(s_1 a_1 + \cdots + s_n a_n) \\ &= s_1(qa_1) + \cdots + s_n(qa_n) \\ &= s_1(0) + \cdots + s_n(0) \\ &= 0. \end{aligned}$$

Koska alkio $m \in M$ on mielivaltaisesti valittu, on näytetty, että $qm = 0$ kaikilla alkioilla $m \in M$. Lisäksi koska kokonaisalueessa R ei ole nollantekijöitä, niin $q \neq 0$, sillä $r_i \neq 0$ kaikilla alkioilla $i \in \{1, \ldots, n\}$. □

Lause 3.13 (Rakennelauseen yksikäsitteisyys)**.** *Olkoon R pääideaalialue.*

1. *Äärellisviritteiset R-modulit M_1 ja M_2 ovat isomorfiset, jos ja vain jos niillä on sama vapaa aste ja samat alkeisjakajat.*
2. *Äärellisviritteiset R-modulit M_1 ja M_2 ovat isomorfiset, jos ja vain jos niillä on sama vapaa aste ja samat invariantit tekijät.*

Todistus. (Vrt. [3, s. 466])
1. " $\Rightarrow$ " Oletetaan, että R-modulit M_1 ja M_2 ovat isomorfiset. Osoitetaan ensin, että R-moduleilla M_1 ja M_2 on sama vapaa aste. Nyt mikä tahansa isomorfinen kuvaus R-modulilta M_1 R-modulille M_2 on bijektiivinen, joten se kuvaa joukon $\mathrm{Tor}_R(M_1)$ joukolle $\mathrm{Tor}_R(M_2)$. Täten myöskin joukot $\mathrm{Tor}_R(M_1)$ ja $\mathrm{Tor}_R(M_2)$ ovat isomorfiset, ja edelleen $M_1/\mathrm{Tor}_R(M_1) \cong M_2/\mathrm{Tor}_R(M_2)$.

Olkoon nyt $r_1 \geq 0$ R-modulin M_1 vapaa aste ja $r_2 \geq 0$ R-modulin M_2 vapaa aste. Nyt lauseen 3.8 nojalla

$$M_1 \cong R^{r_1} \oplus R/\langle p_1^{\alpha_1} \rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m} \rangle,$$

missä alkualkiopotenssit $p_1^{\alpha_1}, \ldots, p_m^{\alpha_m} \in R$ ovat positiivisia. Apulauseen 3.10 nojalla

$$\begin{aligned}\mathrm{Tor}_R(M_1) &= \mathrm{Tor}_R(R^{r_1} \oplus (R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle)) \\ &= \mathrm{Tor}_R(R^{r_1}) \oplus \mathrm{Tor}_R(R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle).\end{aligned}$$

Koska R on pääideaalialueena kokonaisalue, niin siinä ei ole nollantekijöitä. Täten R^{r_1} on torsiovapaa ja $\mathrm{Tor}_R(R^{r_1}) = \{0\}$. Nyt $R/\langle p_i^{\alpha_i}\rangle$ on torsiomoduli kaikilla $i \in \{1, \ldots, m\}$, sillä jokainen syklinen moduli $R/\langle p_i^{\alpha_i}\rangle$ on alkion $p_i^{\alpha_i}$ annihiloima. Siis

$$\mathrm{Tor}_R(M_1) = \mathrm{Tor}_R(R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle) = R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle.$$

Nyt siis apulauseen 3.3 nojalla

$$\begin{aligned}M_1/\mathrm{Tor}_R(M_1) &\cong (R^{r_1} \oplus R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle)/(R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle) \\ &\cong R^{r_1} \oplus [(R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle)/(R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle)] \\ &\cong R^{r_1}.\end{aligned}$$

Vastaavalla tavalla nähdään, että $M_2/\mathrm{Tor}_R(M_2) \cong R^{r_2}$, joten $R^{r_1} \cong R^{r_2}$.

Olkoon nyt $p \in R$ nollasta eroava alkualkio. Tällöin isomorfismin $R^{r_1} \cong R^{r_2}$ nojalla myöskin $R^{r_1}/pR^{r_1} \cong R^{r_2}/pR^{r_2}$, sillä $pR^{r_1} \cong pR^{r_2}$. Tällöin apulauseen 3.11 kohdan 1 nojalla $F^{r_1} \cong F^{r_2}$, missä $F := R/pR$ on kunta. Toisin sanoen kunnan F yli määritetty r_1-dimensioinen vektoriavaruus on isomorfinen kunnan F yli määritetyn r_2-dimensioisen vektoriavaruuden kanssa. Täten lauseen 2.20 nojalla täytyy olla $r_1 = r_2$ ja näin ollen R-moduleilla M_1 ja M_2 on sama vapaa aste.

Osoitetaan sitten, että R-moduleilla M_1 ja M_2 on samat alkeisjakajat. Riittää siis tarkastella vain torsiomoduleita $\mathrm{Tor}_R(M_1)$ ja $\mathrm{Tor}_R(M_2)$, jotka osoitettiin aiemmin isomorfisiksi keskenään. Voidaankin olettaa, että R-modulit M_1 ja M_2 ovat torsiomoduleita.

Koska M_1 ja M_2 ovat torsiomoduleita, ne koostuvat syklisten modulien $R/\langle p_i^{\alpha_i}\rangle$, missä alkualkiopotenssi $p_i^{\alpha_i}$ on positiivinen kaikilla $i \in \{1, \ldots, m\}$, suorista summista. Oletetaan, että x on torsiomodulin M_1 p-primäärisen alimodulin alkio ja kirjoitetaan

$$x = \sum_{i=1}^{m} x_i,$$

missä $x_i \in R/\langle p_i^{\alpha_i}\rangle$ kaikilla $i \in \{1, \ldots, m\}$. Nyt $p^\alpha x = 0$ jollakin $\alpha \geq 1$. Koska summa

$$M_1 = R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle$$

on suora, $p^\alpha x_i = 0$ kaikilla $i \in \{1, \ldots, m\}$. Mutta jos $x_i \neq 0$, missä $i \in \{1, \ldots, m\}$, niin täytyy olla $p = p_i$. Tämä pätee, sillä x_i on muotoa $a + \langle p_i^{\alpha_i}\rangle$ kaikilla $i \in \{1, \ldots, m\}$, missä $a \in R$. Jos $p^\alpha x_i = 0$, niin tällöin $p^\alpha a \in \langle p_i^{\alpha_i}\rangle$. Mutta mikäli $p \neq p_i$, niin täytyy olla $a \in \langle p_i^{\alpha_i}\rangle$ eli $x_i = 0$. Vastaava tulos

pätee myöskin torsiomodulin M_2 p-primääriselle alimodulille. Täten torsiomodulien M_1 ja M_2 p-primääriset alimodulit ovat suoria summia niistä syklisistä moduleista, missä alkeisjakajat ovat alkualkion p potensseja.

Osoitetaan sitten, että torsiomodulien M_1 ja M_2 p-primääriset alimodulit ovat isomorfisia keskenään. Olkoon M_{1p} torsiomodulin M_1 p-primäärinen alimoduli ja M_{2p} torsiomodulin M_2 p-primäärinen alimoduli. Oletuksen nojalla on olemassa isomorfinen kuvaus $f : M_1 \to M_2$. Tällöin $f(M_{1p}) \subseteq M_{2p}$ kaikilla alkualkioilla p, sillä jos $p^\alpha x = 0$ jollakin $\alpha \geq 1$ ja $x \in M_1$, niin tällöin

$$0 = f(p^\alpha x) = p^\alpha f(x),$$

missä $f(x) \in M_2$. Nyt kaikilla alkualkioilla p myöskin pätee $p^\beta y = 0$, missä $\beta \geq 1$ ja $y \in M_2$. Koska f on isomorfismina surjektio, niin on olemassa $x' \in M_1$ siten, että $y = f(x')$. Tällöin

$$0 = p^\beta y = p^\beta f(x') = f(p^\beta x'),$$

ja koska $f(0) = 0$, niin $p^\beta x' = 0$. Täten $M_{2p} \subseteq f(M_{1p})$, joten $f(M_{1p}) = M_{2p}$.

Koska kuvaus f on isomorfismi, niin on olemassa isomorfinen kuvaus $f^{-1} : M_2 \to M_1$. Tällöin jokainen rajoittumakuvaus $f' : M_{1p} \to M_{2p}$ on isomorfismi, jonka käänteiskuvaus on $f'^{-1} : M_{2p} \to M_{1p}$ myöskin on isomorfismi. Toisin sanoen $M_{1p} \cong M_{2p}$. Nyt torsiomodulit M_1 ja M_2 voidaan korvata p-primäärisillä alimoduleilla M_{1p} ja M_{2p}. Merkitään tästä eteenpäin $M_1 = M_{1p}$ ja $M_2 = M_{2p}$.

Apulauseen 3.12 nojalla torsiomoduleilla M_1 ja M_2 on nollasta eroavat annihilaattorit, jotka tällöin koostuvat alkualkion p joistakin potensseista. Koska $M_1 \cong M_2$, niin tämä potenssi täytyy olla sama kummallekin torsiomodulille. Olkoon n pienin mahdollinen tällainen alkualkion p potenssi.

Todistetaan nyt väite induktiolla edellä mainitun alkualkion p potenssin n suhteen. Jos $n = 0$, niin tällöin $M_1 = \{0\}$ ja $M_2 = \{0\}$, joten triviaalisti väite on tosi.

Oletetaan sitten, että väite pätee, kun $n = \alpha_s - 1$ ja osoitetaan, että väite pätee myös, kun $n = \alpha_s$. Olkoon

$$M_1 \cong \underbrace{R/\langle p\rangle \oplus R/\langle p\rangle \oplus \cdots \oplus R/\langle p\rangle}_{\text{m kappaletta}} \oplus R/\langle p^{\alpha_1}\rangle \oplus R/\langle p^{\alpha_2}\rangle \oplus \cdots \oplus R/\langle p^{\alpha_s}\rangle,$$

missä $2 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_s$. Siis torsiomoduli M_1 on syklisten modulien suora summa, missä syklisten modulien virittäjät ovat $x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_{m+s} \in M_1$ ja niitä vastaavat annihilaattorit ovat

$$\underbrace{\langle p\rangle, \langle p\rangle, \ldots, \langle p\rangle}_{\text{m kappaletta}}, \langle p^{\alpha_1}\rangle, \ldots, \langle p^{\alpha_s}\rangle.$$

Tällöin

$$pM_1 \cong R/\langle p^{\alpha_1 - 1}\rangle \oplus R/\langle p^{\alpha_2 - 1}\rangle \oplus \cdots \oplus R/\langle p^{\alpha_s - 1}\rangle.$$

Siis alimoduli pM_1 on syklisten modulien suora summa, missä syklisten modulien virittäjät ovat $px_1, px_2, \ldots, px_m, px_{m+1}, \ldots, px_{m+s}$ ja niitä vastaavat annihilaattorit ovat

$$\underbrace{\langle 1\rangle, \langle 1\rangle, \ldots, \langle 1\rangle}_{\text{m kappaletta}}, \langle p^{\alpha_1-1}\rangle, \ldots, \langle p^{\alpha_s-1}\rangle.$$

Vastaavasti olkoon

$$M_2 \cong \underbrace{R/\langle p\rangle \oplus R/\langle p\rangle \oplus \cdots \oplus R/\langle p\rangle}_{\text{n kappaletta}} \oplus R/\langle p^{\beta_1}\rangle \oplus R/\langle p^{\beta_2}\rangle \oplus \cdots \oplus R/\langle p^{\beta_t}\rangle$$

missä $2 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_t$. Tällöin

$$pM_2 \cong R/\langle p^{\beta_1-1}\rangle \oplus R/\langle p^{\beta_2-1}\rangle \oplus \cdots \oplus R/\langle p^{\beta_t-1}\rangle.$$

Koska $M_1 \cong M_2$, niin täten myöskin $pM_1 \cong pM_2$. Nyt $\mathrm{Ann}_R(pM_1) = \langle p^{\alpha_s-1}\rangle$ ja $\mathrm{Ann}_R(M_1) = \langle p^{\alpha_s}\rangle$. Nähdään siis, että alkualkion p potenssi n alimodulin pM_1 annihilaattorissa on yhden vähemmän kuin alkualkion p potenssi n torsiomodulin M_1 annihilaattorissa. Koska induktio-oletuksen nojalla väite pätee, kun $n = \alpha_s - 1$, niin alimodulin pM_1 alkeisjakajat ovat samat kuin alimodulin pM_2 alkeisjakajat. Toisin sanoen täytyy olla $s = t$ ja $\alpha_i - 1 = \beta_i - 1$ kaikilla alkioilla $i \in \{1, \ldots, s\}$. Täten $\alpha_i = \beta_i$ kaikilla alkioilla $i \in \{1, \ldots, s\}$. Koska $M_1/pM_1 \cong M_2/pM_2$, niin apulauseen 3.11 kohdan 3 nojalla

$$F^{m+s} \cong M_1/pM_1 \cong M_2/pM_2 \cong F^{n+t}.$$

Tällöin lauseen 2.20 nojalla $m+s = n+t$, ja koska aiemmin jo osoitettiin, että vapaat asteet m ja n ovat samat, niin täytyy olla $s = t$. Siis torsiomodulin M_1 alkeisjakajat ovat samat kuin torsiomodulin M_2.

" $\Leftarrow$ " Oletetaan, että R-moduleilla M_1 ja M_2 on sama vapaa aste $s \geq 0$ ja samat alkeisjakajat $p_1^{\alpha_1}, \ldots, p_m^{\alpha_m} \in R$. Tällöin lauseen 3.8 nojalla

$$M_1 \cong R^s \oplus R/\langle p_1^{\alpha_1}\rangle \oplus \cdots \oplus R/\langle p_m^{\alpha_m}\rangle \cong M_2.$$

2. " $\Rightarrow$ " Oletetaan nyt, että R-modulit M_1 ja M_2 ovat isomorfiset ja osoitetaan, että R-moduleilla M_1 ja M_2 on samat invariantit tekijät. Vastaavasti kuin kohdassa 1 nähdään, että R-moduleilla M_1 ja M_2 on sama vapaa aste. Oletetaan, että alkiot $a_1, \ldots, a_m \in R$, missä $a_1 \mid \cdots \mid a_m$ ovat R-modulin M_1 invariantit tekijät. Nyt lauseen 2.13 mukaan pääideaalialue R on faktoriaalinen, joten jokaiselle alkiolle a_i, missä $i \in \{1, \ldots, m\}$, saadaan esitysmuoto

$$a_i = u p_{i_1}^{\alpha_{i_1}} p_{i_2}^{\alpha_{i_2}} \cdots p_{i_n}^{\alpha_{i_n}},$$

missä $u \in R$ on yksikkö ja alkiot $p_{ij} \in R$ ovat alkualkioita siten, että $p_{ij} \neq p_{ik}$ kaikilla $j \neq k$, missä $j, k \in \{1, \ldots, n\}$. Tämä esitysmuoto on yksikäsitteinen, joten ideaalit $\langle p_{il}^{\alpha_{il}}\rangle$ ovat yksikäsitteisesti määritettyjä kaikilla alkioilla

$l \in \{1, \ldots, n\}$. Toisin sanoen invariantit tekijät voidaan esittää alkeisjakajien avulla. Nyt koska $a_i \mid a_{i+1}$ kaikilla $i \in \{1, \ldots, m-1\}$, niin invariantti tekijä a_m voidaan esittää alkeisjakajien korkeimpien potenssien tulona ja invariantti tekijä a_{m-1} voidaan esittää alkeisjakajien korkeimpien potenssien tulona, kun invariantin tekijän a_m tekijät ovat poistettu. Näin jatkamalla saadaan kaikille invarianteille tekijöille a_i, missä $i \in \{2, \ldots, m\}$ vastaava esitysmuoto. Oletetaan lisäksi, että alkiot $b_1, \ldots, b_n \in R$, missä $b_1 \mid \cdots \mid b_n$ ovat R-modulin M_2 invariantit tekijät. Näille invarianteille tekijöille saadaan vastaavat esitysmuodot kuin R-modulin M_1 invarianteille tekijöille. Nyt lauseen kohdan 1 nojalla R-modulien M_1 ja M_2 alkeisjakajat ovat samat, joten tällöin myöskin niiden invariantit tekijät ovat samat.

" $\Leftarrow$ " Oletetaan, että R-moduleilla M_1 ja M_2 on sama vapaa aste $r \in R$ ja samat invariantit tekijät $a_1, \ldots, a_m \in R$, missä $a_i \neq 0$ kaikilla $i \in \{1, \ldots, m\}$ ja $a_1 \mid \cdots \mid a_m$. Tällöin lauseen 3.7 nojalla

$$M_1 \cong R^r \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_m \rangle \cong M_2.$$

□

Esimerkki 3.2. (Vrt. [6, s. 397]) Tarkastellaan euklidista aluetta $\mathbb{Q}[x]$. Olkoon $f(x), g(x) \in \mathbb{Q}[x]$ siten, että

$$f(x) = (x-2)^4(x-1)$$

ja

$$g(x) = (x-2)^2(x-1)^2(x^2+1)^3$$

ovat esitettynä jaottomien tekijöiden avulla. Koska lauseen 2.12 nojalla euklidinen alue on pääideaalialue, niin apulauseen 2.13 nojalla tällaiset esitysmuodot on olemassa. Nyt koska jokainen pääideaalialue on faktoriaalinen lauseen 2.14 nojalla, niin lauseen 2.15 nojalla jokainen jaoton tekijä on alkualkio. Merkitään $\mathbb{Q}[x]$-modulia

$$M := \mathbb{Q}[x]/\langle f \rangle \oplus \mathbb{Q}[x]/\langle g \rangle.$$

Tällöin

$$\begin{aligned} M \cong\ & \mathbb{Q}[x]/\langle (x-2)^4 \rangle \oplus \mathbb{Q}[x]/\langle x-1 \rangle \oplus \mathbb{Q}[x]/\langle (x-2)^2 \rangle \\ & \oplus \mathbb{Q}[x]/\langle (x-1)^2 \rangle \oplus \mathbb{Q}[x]/\langle (x^2+1)^3 \rangle. \end{aligned}$$

Nyt lauseen 3.8 nojalla $\mathbb{Q}[x]$-modulin M alkeisjakajat ovat $(x-2)^4$, $(x-2)^2$, $(x-1)^2$, $x-1$ ja $(x^2+1)^3$. Järjestelemällä uudelleen edellä mainittu suora summa, saadaan

$$\begin{aligned} M &\cong \mathbb{Q}[x]/\langle (x-2)^2 \rangle \oplus \mathbb{Q}[x]/\langle x-1 \rangle \oplus \mathbb{Q}[x]/\langle (x-2)^4 \rangle \oplus \mathbb{Q}[x]/\langle (x-1)^2 \rangle \\ &\quad \oplus \mathbb{Q}[x]/\langle (x^2+1)^3 \rangle \\ &\cong \mathbb{Q}[x]/\langle (x-2)^2(x-1) \rangle \oplus \mathbb{Q}[x]/\langle (x-2)^4(x-1)^2(x^2+1)^3 \rangle. \end{aligned}$$

Nyt koska $(x-2)^2(x-1) \mid (x-2)^4(x-1)^2(x^2+1)^3$, niin lauseen 3.7 nojalla $\mathbb{Q}[x]$-modulin invariantit tekijät ovat $(x-2)^2(x-1)$ ja $(x-2)^4(x-1)^2(x^2+1)^3$.

4 Smithin normaalimuoto

Edellisessä luvussa osoitettiin, että pääideaalialueen yli määritellyt äärellisviritteiset modulit ovat isomorfisia vapaan modulin ja torsiomodulin suoran summan kanssa. Tiedetään, että vapaiden modulien väliseen homomorfismiin voidaan liittää matriisi, joka määräytyy niiden kantojen alkioiden välisestä yhtälöstä. Tässä luvussa perehdytään siihen, kuinka annetun matriisin invariantit tekijät voidaan löytää.

4.1 Valmistelevia tarkasteluja

Tässä kappaleessa esitellään lyhyesti vektoriavaruuksien välisten homomorfismien ominaisuuksia. Koska asia on tuttua jo lineaarialgebran peruskursseilta, todistukset sivuutetaan.

Lause 4.1. *Olkoon K kunta ja V sellainen K-vektoriavaruus, jonka kantana on perhe $(v_1, \ldots, v_n)$. Jos W on K-vektoriavaruus, johon perhe $(w_1, \ldots, w_n)$ kuuluu, niin on olemassa yksikäsitteinen homomorfismi $T : V \to W$, missä $T(v_i) = w_i$ kaikilla $i \in \{1, \ldots, n\}$.*

Todistus. Sivuutetaan. Kts. [1, s. 172]. □

Lause 4.2. *Olkoon K kunta. Jos $T : K^n \to K^m$ on homomorfismi, niin on olemassa sellainen $m \times n$-matriisi A, että*

$$T(y) = Ay$$

kaikilla $y \in K^n$. Tässä y on $n \times 1$-matriisi ja Ay matriisi y kerrottuna skalaarilla A.

Todistus. Sivuutetaan. Kts. [1, s. 173]. □

Määritelmä 4.1. Olkoon K kunta, $X := (v_1, \ldots, v_n)$ K-vektoriavaruuden V kanta ja $Y := (w_1, \ldots, w_m)$ K-vektoriavaruuden W kanta. Jos $T : V \to W$ on homomorfismi, niin *kuvauksen T matriisi* on $m \times n$-matriisi $A := [a_{ij}]$, jonka sarakkeen j alkiot $a_{1j}, \ldots, a_{mj}$ määräytyvät yhtälöstä

$$T(v_j) = \sum_{i=1}^{m} a_{ij} w_i.$$

Matriisi A riippuu kantojen X ja Y valinnoista. Tätä riippuvuutta merkataan $A = {}_Y[T]_X$.

Esimerkki 4.1. Olkoon K kunta, $X := (v_1, \ldots, v_n)$ K-vektoriavaruuden V kanta ja $Y := (w_1, \ldots, w_m)$ K-vektoriavaruuden W kanta. Olkoon lisäksi $T : V \to W$ homomorfismi. Tällöin kuvauksen T matriisin $A = {}_Y[T]_X$ alkiot määräytyvät yhtälöstä

$$T(v_j) = a_{1j}w_1 + a_{2j}w_2 + \cdots + a_{mj}w_m.$$

Siis

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}.$$

4.2 Smithin normaalimuoto

Nyt edellisessä kappaleessa kunnan yli määritetyille äärellisulotteisille vektoriavaruuksille annetut tulokset voidaan yleistää kommutatiivisen renkaan yli määritetyille moduleille.

Määritelmä 4.2. Olkoon R kommutatiivinen rengas ja $T : R^t \to R^n$ homomorfismi, missä R^t on astetta t oleva vapaa R-moduli ja R^n astetta n oleva vapaa R-moduli. Jos $Y := (y_1, \ldots, y_t)$ on R-modulin R^t kanta ja $Z := (z_1, \ldots, z_n)$ on R-modulin R^n kanta, niin

$${}_Z[T]_Y = [a_{ij}]$$

on renkaan R yli määritetty $n \times t$-matriisi, jonka sarakkeen j alkiot $a_{1j}, \ldots, a_{mj}$ määräytyvät yhtälöstä

$$T(y_j) = \sum_{i=1}^{m} a_{ij}z_i.$$

Määritelmä 4.3. Olkoon R kommutatiivinen rengas ja Γ sekä Γ' $n \times t$-matriiseja, joiden alkiot kuuluvat renkaaseen R. Matriisit Γ ja Γ' ovat *R-ekvivalentteja*, mikäli on olemassa kääntyvät matriisit P ja Q, joiden alkiot kuuluvat renkaaseen R, siten, että

$$\Gamma' = Q\Gamma P.$$

Apulause 4.3. *Olkoon P euklidisen alueen $K[x]$ yli määritetty $n \times n$-matriisi ja A kunnan K yli määritetty $n \times n$-matriisi. Tällöin on olemassa euklidisen alueen $K[x]$ yli määritetyt $n \times n$-matriisit Q_1 ja Q_2 sekä kunnan K yli määritetyt $n \times n$-matriisit R_1 ja R_2 siten, että*

$$P = (xI - A)Q_1 + R_2 \quad ja \quad P = Q_2(xI - A) + R_2.$$

Todistus. (Vrt. [5, s. 201]) Jos P on kunnan K yli määritetty $n \times n$-matriisi, niin tällöin valitsemalla $Q_1 = Q_2 = 0$ ja $R_1 = R_2 = P$ väite pätee.

Oletetaan, että P on euklidisen alueen $K[x]$ yli määritetty $n \times n$-matriisi. Tällöin jollakin $k \geq 1$ on olemassa matriisin P esitysmuoto

$$P = x^k C_k + x^{k-1} C_{k-1} + \cdots + C_0,$$

missä $C_k \neq 0$. Määritellään

$$Q_1 := x^{k-1} D_{k-1} + x^{k-2} D_{k-2} + \cdots + x D_1 + D_0,$$

missä

$$D_j = \sum_{m=0}^{k-1-j} A^m C_{m+1+j}$$

kaikilla $j \in \{0, \ldots, k-1\}$, ja

$$Q_2 := x^{k-1} E_{k-1} + x^{k-2} E_{k-2} + \cdots + x E_1 + E_0,$$

missä

$$E_j = \sum_{m=0}^{k-1-j} C_{m+1+j} A^m$$

kaikilla $j \in \{0, \ldots, k-1\}$. Määritellään lisäksi

$$R_1 := A^k C_k + A^{k-1} C_{k-1} + \cdots + A C_1 + C_0$$

ja

$$R_2 := C_k A^k + C_{k-1} A^{k-1} + \cdots + C_1 A + C_0.$$

Nyt sijoittamalla edellä olevat merkinnät väitteen yhtälöihin $P = (xI - A)Q_1 + R_2$ ja $P = Q_2(xI - A) + R_2$ havaitaan, että väite pätee. □

Määritelmä 4.4. Polynomimatriisia A sanotaan *unimodulaariseksi*, mikäli sen determinantti on nollasta eroava vakioarvoinen alkio. Toisin sanoen polynomimatriisilla A on olemassa käänteismatriisi, joka myöskin on polynomimatriisi.

Määritelmä 4.5. Kunnan K yli määritetyt $n \times n$-matriisit A ja B ovat *similaariset*, mikäli on olemassa sellainen kääntyvä matriisi P, jonka alkiot kuuluvat kuntaan K, että

$$B = PAP^{-1}.$$

Lause 4.4. *Olkoon A ja B kunnan K yli määriteltyjä $n \times n$-matriiseja. Matriisit A ja B ovat similaariset, jos ja vain jos matriisit $\Gamma = xI - A$ ja $\Gamma' = xI - B$ ovat $K[x]$-ekvivalentteja.*

Todistus. (Vrt. [5, s. 203]) Oletetaan ensin, että matriisit A ja B ovat similaariset. Tällöin on olemassa kääntyvä matriisi T siten, että $A = T^{-1}BT$. Täten $xI - A = T^{-1}(xI - B)T$, joten matriisit $xI - A$ ja $xI - B$ ovat määritelmän mukaan $K[x]$-ekvivalentit.

Oletetaan sitten, että matriisit $xI - A$ ja $xI - B$ ovat $K[x]$-ekvivalentit. Tällöin on olemassa unimodulaariset $n \times n$-matriisit P ja Q siten, että $xI - A = P(xI - B)Q$. Nyt

$$P^{-1}(xI - A) = (xI - B)Q,$$

joten apulauseen 4.3 nojalla on olemassa $n \times n$-matriisit Q_1, Q_1, R_1 ja R_2 siten, että

$$P^{-1} = (xI - B)Q_1 + R_1$$

sekä

$$Q = Q_2(xI - A) + W_2.$$

Nyt sijoittamalla nämä esitysmuodot edellä olevaan yhtälöön, saadaan

$$((xI - B)Q_1 + R_1)(xI - A) = (xI - B)(Q_2(xI - A) + W_2),$$

joka voidaan sieventää muotoon

$$(xI - B)(Q_1 - Q_2)(xI - A) = x(R_2 - R_1) + R_1A - BR_2.$$

Jos $Q_1 - Q_2 \neq 0$, niin edellä olevan yhtälön vasemman puolen aste on vähintään 2, kun taas oikean puolen aste on enintään 1, mikä johtaa ristiriitaan. Täten täytyy siis olla $Q_1 - Q_2 = 0$, joten

$$x(R_2 - R_1) + R_1A - BR_2 = 0.$$

Tästä seuraa, että $R_2 - R_1 = 0$ ja $R_1A - BR_2 = 0$, joten $R_2 = R_1$ ja $R_1A = BR_1$. Siis

$$R_1(xI - A) = (xI - B)R_1.$$

Osoitetaan vielä, että matriisi R_1 on kääntyvä. Apulauseen 4.3 nojalla on olemassa $n \times n$-matriisit Q_3 ja R_3 siten, että

$$P = (xI - A)Q_3 + R_3.$$

Nyt koska $P^{-1} = (xI - B)Q_1 + R_1$, voidaan kirjoittaa

$$\begin{aligned}
I &= P^{-1}P \\
&= [(xI - B)Q_1 + R_1][(xI - A)Q_3 + R_3] \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + R_1(xI - A)Q_3 + R_1R_3 \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + (xI - B)R_1Q_3 + R_1R_3 \\
&= (xI - B)[Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3] + R_1R_3.
\end{aligned}$$

Täten saadaan

$$I - R_1R_3 = (xI - B)[Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3].$$

Koska $n \times n$-matriisien tulo R_1R_3 on $n \times n$-matriisi, ja erotus $I - R_1R_3$ on myöskin $n \times n$-matriisi, joissa kummassakin tapauksessa alkiot kuuluvat kuntaan K, niin täytyy olla $Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3 = 0$. Jos näin ei olisi, niin

edellä olevan yhtälön vasen puoli olisi vakioarvoinen matriisi ja oikean puolen aste olisi vähintään yksi, mikä johtaa ristiriitaan. Täten $R_1R_3 = I$ ja matriisi R_1 on kääntyvä. Siis yhtälöstä $R_1A = BR_1$ saadaan

$$A = R_1^{-1}BR_1,$$

mistä väite seuraa. □

Huomautus. Olkoon R kommutatiivinen rengas ja A matriisi, jonka alkiot kuuluvat renkaaseen R. Merkitään matriisin A riviä j merkinnällä ROW(j) ja saraketta j merkinnällä COL(j).

Määritelmä 4.6. Olkoon R kommutatiivinen rengas ja A matriisi, jonka alkiot kuuluvat renkaaseen R. Tällöin matriisille A voidaan tehdä kolme eri tyyppistä *alkeisrivioperaatiota*:

1. ROW(i) voidaan kertoa renkaan R yksiköllä.
2. ROW(i) voidaan korvata summalla ROW(i) + c_jROW(j), missä $j \neq i$ ja alkio $c_j \in R$.
3. ROW(i) ja ROW(j) voidaan vaihtaa keskenään.

Matriisille A voidaan tehdä myös kolme vastaavaa *alkeissarakeoperaatiota*.

Määritelmä 4.7. Matriisia, joka saadaan yksikkömatriisista yhdellä alkeisrivioperaatiolla, sanotaan *alkeismatriisiksi*. Jokainen määritelmässä 4.6 esitelty alkeisrivioperaatio voidaan esittää jonkin alkeismatriisin avulla.

Määritelmä 4.8. Olkoon R kommutatiivinen rengas. Tällöin matriisi Γ' matriisin Γ *Gaussin ekvivalentti*, jos voidaan suorittaa sarja alkeisrivi- ja alkeissarakeoperaatioita siten, että

$$\Gamma = \Gamma_0 \to \Gamma_1 \to \cdots \to \Gamma_r = \Gamma'.$$

Gaussin ekvivalenssi on ekvivalenssirelaatio kaikkien renkaan R yli määriteltyjen $n \times t$-matriisien perheessä.

Huomautus. Määritelmästä 4.8 seuraa, että jos matriisi Γ' on matriisin Γ Gaussin ekvivalentti, niin tällöin on olemassa alkeismatriiseiden tuloista saadut matriisit P ja Q, joille pätee $\Gamma' = P\Gamma Q$. Koska matriisit Γ ja Γ' ovat R-ekvivalentteja, kun on olemassa kääntyvät matriisit P ja Q, joille pätee $\Gamma' = P\Gamma Q$, niin matriisit Γ ja Γ' ovat R-ekvivalentteja, kun ne ovat Gaussian ekvivalentteja. Käänteinen tulos pätee vain, kun R on euklidinen alue. Tämä tulos osoitetaan lauseessa 4.6.

Lause 4.5 (Smithin normaalimuoto)**.** *Jokainen nollasta eroava $n \times t$-matriisi Γ, jonka alkiot kuuluvat euklidiseen alueeseen R, on muotoa*

$$\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix},$$

missä $\Sigma = diag(\sigma_1, \ldots, \sigma_q)$ ja nollasta eroavat alkiot $\sigma_1, \ldots, \sigma_q \in R$ toteuttavat ehdon $\sigma_1 \mid \cdots \mid \sigma_q$, olevan matriisin Gaussin ekvivalentti.

Huomautus. Lauseessa 4.5 esitetyssä matriisissa

$$\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix}$$

ei ole välttämättä esitetty koko matriisia.

Todistus. (Vrt. [1, s. 688]) Todistetaan väite induktiolla matriisin Γ rivien lukumäärän $n \geq 1$ suhteen. Merkitään $d(\sigma)$ alkion $\sigma \in R$ astetta euklidisessa alueessa R. Oletetaan, että alkion σ_1 aste on pienin kaikkien matriisin Γ Gaussin ekvivalenttien matriisien sisältämien alkioiden joukossa. Oletetaan lisäksi, että Δ on matriisin Γ Gaussin ekvivalentti matriisi, missä $\Delta_{kl} = \sigma_1$.

Osoitetaan, että $\sigma_1 \mid \eta_{kj}$ kaikilla matriisin Δ rivin k alkioilla η_{kj}. Jos näin ei olisi, pätisi $j \neq l$ ja $\eta_{kj} = \kappa\sigma_1 + \rho$, missä $d(\rho) < d(\sigma_1)$. Korvaamalla $\mathrm{COL}(j)$ summalla $\mathrm{COL}(j) + (-\kappa)\mathrm{COL}(l)$ saadaan matriisi Δ', jonka eräs alkio on ρ. Mutta koska matriisi Δ' on matriisin Γ Gaussin ekvivalentti ja se sisältää alkion ρ, jonka aste $d(\rho)$ on pienempi kuin alkion σ_1 aste $d(\sigma_1)$, saadaan muodostettua ristiriita. Vastaavasti voidaan osoittaa, että $\sigma_1 \mid \eta_{il}$ kaikilla matriisin Δ sarakkeen l alkioilla η_{il}.

Osoitetaan sitten, että alkio σ_1 jakaa jokaisen matriisin Δ' alkion. Olkoon a matriisin Δ' sellainen alkio, että se ei sijaitse samalla rivillä kuin alkio σ_1. Voidaan siis kirjoittaa

$$\Delta' = \begin{bmatrix} a & b \\ c & \sigma_1 \end{bmatrix},$$

missä $b = u\sigma_1$ ja $c = v\sigma_1$ joillakin alkioilla $u, v \in R$. Korvaamalla $\mathrm{ROW}(1)$ summalla $\mathrm{ROW}(1) + (1-u)\mathrm{ROW}(2)$ saadaan

$$\Delta' = \begin{bmatrix} a + (1-u)c & \sigma_1 \\ c & \sigma_1 \end{bmatrix}.$$

Mutta edellä osoitettiin, että alkio σ_1 jakaa jokaisen saman rivin alkion, joten $\sigma_1 \mid a + (1-u)c$. Koska $\sigma_1 \mid c$, niin $\sigma_1 \mid a$.

Nyt matriisille Δ voidaan suorittaa alkeisoperaatioita siten, että saadaan muodostettua matriisin Γ Gaussin ekvivalentti matriisi Δ' siten, että $\Delta'_{11} = \sigma_1$. Oletetaan, että alkio η_{1j} on jokin toinen rivin 1 alkio. Tällöin $\eta_{1j} = \kappa_j\sigma_1$. Korvaamalla $\mathrm{COL}(j)$ tulolla $(-\kappa_j)\mathrm{COL}(1)$ saadaan uusi matriisi Δ'', missä $\Delta''_{1j} = 0$. Täten matriisi Δ on Gaussin ekvivalentti sellaisen matriisin kanssa, jossa alkio σ_1 sijaitsee paikassa $(1,1)$ ja muut ensimmäisen rivin alkiot ovat nolla-alkioita. Ollaan siis osoitettu, että nollasta eroava $1 \times t$-matriisi on matriisin $[\sigma_1\, 0 \ldots 0]$ Gaussin ekvivalentti, joten lauseen väite pätee, kun matriisin Γ rivien lukumäärä $n = 1$.

Oletetaan sitten, että lauseen väite pätee, kun matriisin Γ rivien lukumäärä $n = q - 1$ ja osoitetaan, että väite pätee myös, kun $n = q$. Koska alkio σ_1 jakaa jokaisen ensimmäisen sarakkeen alkion, niin matriisi Γ on Gaussin ekvivalentti sellaisen matriisin kanssa, jossa kaikki muut ensimmäisen sarakkeen alkiot ovat

nolla-alkioita. Toisin sanoen, matriisi Γ on Gaussin ekvivalentti muotoa

$$\begin{bmatrix} \sigma_1 & 0 \\ 0 & \Omega \end{bmatrix}.$$

olevan matriisin kanssa. Nyt induktio-oletuksen nojalla matriisi Ω on matriisin

$$\begin{bmatrix} \Sigma' & 0 \\ 0 & 0 \end{bmatrix}$$

Gaussin ekvivalentti, missä $\Sigma' = \operatorname{diag}(\sigma_2, \ldots, \sigma_q)$ ja $\sigma_2 \mid \cdots \mid \sigma_q$. Täten matriisi Γ on matriisin

$$\Delta''' := \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \Sigma' & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Gaussin ekvivalentti. Koska matriisi Δ''' on matriisin Γ Gaussin ekvivalentti ja sisältää alkion σ_1, voidaan vastaavasti kuin edellä osoittaa, että $\sigma_1 \mid \sigma_2$. Täten väite pätee myös, kun matriisin Γ rivien lukumäärä $n = q$. □

Määritelmä 4.9. Lauseessa 4.5 esiteltyä matriisia

$$\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix}$$

sanotaan matriisin Γ *Smithin normaalimuodoksi.*

Esimerkki 4.2. Tarkastellaan kokonaislukujen renkaan $\mathbb{Z}$ yli määriteltyä matriisia

$$A := \begin{bmatrix} -2 & 3 & 0 \\ -3 & 3 & 0 \\ -12 & 12 & 6 \end{bmatrix}.$$

Etsitään matriisia A vastaava Smithin normaalimuodossa oleva matriisi. Korvataan COL(1) summalla COL(1) + COL(2), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 3 & 0 \\ 0 & 3 & 0 \\ 0 & 12 & 6 \end{bmatrix}.$$

Korvataan COL(2) summalla COL(2) + (-3)COL(1), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 12 & 6 \end{bmatrix}.$$

Korvataan ROW(3) summalla ROW(3)+(-4)ROW(2), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{bmatrix}.$$

Huomataan, että diagonaalialkiot $1, 3$ ja 6 toteuttavat lauseessa 4.5 mainitun ehdon, joten tämä matriisi on matriisia A vastaava Smithin normaalimuoto.

Esimerkki 4.3. Olkoon A Abelin ryhmä, jonka kanta on (m_1, m_2, m_3) siten, että yhtälöt

$$8m_1 + 4m_2 + 8m_3 = 0$$

ja

$$4m_1 + 8m_2 + 4m_3 = 0$$

ovat voimassa. Muodostetaan nyt relaatioalimoduli K, jonka virittäjät u_1 ja u_2 määräytyvät yhtälöistä

$$u_1 = 8m_1 + 4m_2 + 8m_3$$

ja

$$u_2 = 4m_1 + 8m_2 + 4m_3.$$

Näin saadaan muodostettua Abelin ryhmä $G = A/K$, jonka virittäjät ovat $m_1 + K, m_2 + K$ ja $m_3 + K$. Edellä olevista yhtälöistä saadaan muodostettua relaatiomatriisi

$$\begin{bmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \end{bmatrix}.$$

Viedään relaatiomatriisi nyt Smithin normaalimuotoon, jollainen on olemassa lauseen 4.5 nojalla. Aloitetaan korvaamalla ROW(1) summalla ROW(1) + (-2)ROW(2), jolloin saadaan

$$\begin{bmatrix} 0 & -12 & 0 \\ 4 & 8 & 4 \end{bmatrix}.$$

Korvataan sitten COL(2) summalla COL(2) + (-2)COL(1) ja COL(3) summalla COL(3) + (-2)COL(1). Täten

$$\begin{bmatrix} 0 & -12 & 0 \\ 4 & 0 & 0 \end{bmatrix}.$$

Vaihdetaan ROW(1) ja ROW(2) keskenään, jolloin

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & -12 & 0 \end{bmatrix}.$$

Kerrotaan vielä ROW(2) Abelin ryhmän A yksiköllä -1, jolloin relaatiomatriisin Smithin normaalimuodoksi saadaan

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & 12 & 0 \end{bmatrix}.$$

Täten ollaan saatu Abelin ryhmän A uusi kanta (n_1, n_2, n_3) ja relaatioalimodulin K uudet virittäjäalkiot $4n_1$ ja $12n_2$. Tekijäryhmän A/K virittäjät ovat siis $n_1 + K, n_2 + K$ ja $n_3 + K$, missä $4(n_1 + K) = 12(n_2 + K) = 0 + K$. Siis täytyy olla

$$A/K \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/12\mathbb{Z}) \oplus \mathbb{Z}.$$

Lause 4.6. *Olkoon R euklidinen alue.*

1. *Jokainen kääntyvä $n \times n$-matriisi Γ, jonka alkiot kuuluvat euklidiseen alueeseen R, koostuu alkeismatriisien tulosta.*
2. *Matriisit Γ ja Γ', joiden alkiot kuuluvat euklidiseen alueeseen R, ovat R-ekvivalentteja, jos ja vain jos ne ovat Gaussin ekvivalentteja.*

Todistus. (Vrt. [1, s. 689]) 1. Lauseen 4.5 nojalla muotoa

$$\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix}$$

oleva matriisi, missä $\Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_n)$, on matriisin Γ Gaussin ekvivalentti. Koska Γ on kääntyvä matriisi, niin se on matriisin Σ Gaussin ekvivalentti. Toisin sanoen on olemassa matriisit P ja Q, jotka koostuvat alkeismatriisien tulosta siten, että

$$P\Gamma Q = \Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_n).$$

Täten $\Gamma = P^{-1}\Sigma Q^{-1}$. Koska alkeismatriisin käänteismatriisi on edelleen alkeismatriisi, niin myöskin matriisit P^{-1} ja Q^{-1} koostuvat alkeismatriisien tulosta. Lisäksi koska matriisi Σ on kääntyvä ja R on euklidisena alueena kommutatiivinen rengas, niin $\det(\Sigma) = \sigma_1 \cdots \sigma_n$ on euklidisen alueen R yksikkö. Täten σ_i on euklidisen alueen R yksikkö jokaisella $i \in \{1, \ldots, n\}$, joten matriisi Σ koostuu n kappaleen alkeismatriisin tulosta.

2. Jos matriisit Γ ja Γ' ovat Gaussin ekvivalentteja, niin ne ovat myöskin R-ekvivalentteja. Toisin sanoen jos $\Gamma' = P\Gamma Q$, missä matriisit P ja Q koostuvat alkeismatriisien tuloista, niin matriisit P ja Q ovat kääntyviä.

Jos matriisit Γ ja Γ' ovat R-ekvivalentteja, niin $\Gamma' = P\Gamma Q$, missä matriisit P ja Q ovat kääntyviä. Tällöin kohdan 1 nojalla matriisit Γ ja Γ' ovat Gaussin ekvivalentteja. □

Lause 4.7. *Olkoon Γ sellainen $n \times n$-matriisi, että sen alkiot kuuluvat euklidiseen alueeseen R.*

1. *Jos Γ on Smithin normaalimuodossa olevan matriisin $\operatorname{diag}(\sigma_1, \ldots, \sigma_q) \oplus 0$ R-ekvivalentti, niin tällöin ne joukon $\{\sigma_1, \ldots, \sigma_q\}$ alkiot, jotka eivät ole euklidisen alueen R yksiköitä, ovat matriisin Γ invariantit tekijät.*
2. *Jos matriisi $\operatorname{diag}(\sigma_1, \ldots, \sigma_s) \oplus 0$ on matriisin Γ jokin toinen Smithin normaalimuoto, niin tällöin $s = q$ ja on olemassa euklidisen renkaan R yksiköt u_i, missä $\eta_i = u_i\sigma_i$ kaikilla $i \in \{1, \ldots, q\}$. Toisin sanoen matriisien diagonaalialkiot ovat toistensa liittoalkioita.*

Todistus. (Vrt. [1, s. 690]) 1. Merkitään, että Γ on homomorfismiin $\lambda : R^n \to R^n$ liittyvä matriisi joillakin kantojen valinnoilla. Olkoon $M = R^n/\operatorname{im}(\lambda)$ ja oletetaan, että $\operatorname{diag}(\sigma_1, \ldots, \sigma_q) \oplus 0$ on matriisin Γ Smithin normaalimuoto. Tällöin lauseen 3.6 kohdan 2 nojalla on olemassa kannat $(y_1, \ldots, y_n) \in R^n$ ja

$(z_1, \ldots, z_n) \in R^n$ siten, että $\lambda(y_1) = \sigma_1 z_1, \ldots, \lambda(y_q) = \sigma_q z_q$ ja $\lambda(y_j) = 0$ kaikilla alkioilla y_j, missä $j > q$. Oletetaan, että σ_p on ensimmäinen alkioiden σ_i, missä $i \in \{1, \ldots, q\}$, joukossa, joka ei ole euklidisen alueen R yksikkö. Tällöin

$$M \cong R^{n-q} \oplus R/\langle \sigma_p \rangle \oplus \cdots \oplus R/\langle \sigma_q \rangle,$$

missä $\sigma_p \mid \cdots \mid \sigma_q$. Lauseen 3.7 nojalla alkiot $\sigma_p, \ldots, \sigma_q$ ovat R-modulin M invariantit tekijät.

2. Muodostetaan R-modulille M esitysmuoto

$$M \cong R^{n-s} \oplus R/\langle \eta_p \rangle \oplus \cdots \oplus R/\langle \eta_s \rangle$$

vastaavalla tavalla kuin kohdan 1 todistuksessa. Koska lauseen 3.7 esitysmuoto on yksikäsitteinen, niin tällöin $s = q$ ja $\langle \eta_i \rangle = \langle \sigma_i \rangle$ kaikilla $i \in \{p, \ldots, q\}$. Toisin sanoen diagonaalialkiot ovat toistensa liittoalkioita. □

Lause 4.8. *Olkoon A ja B kunnan K yli määriteltyjä $n \times n$-matriiseja. Matriisit A ja B ovat similaariset, jos ja vain jos matriisien $xI - A$ ja $xI - B$ Smithin normaalimuodossa olevat matriisit ovat samat.*

Todistus. (Vrt. [1, s. 691]) Nyt lauseen 4.4 nojalla matriisit A ja B ovat similaariset, jos ja vain jos matriisit $xI - A$ ja $xI - B$ ovat $K[x]$-ekvivalentteja. Mutta lauseen 4.7 nojalla matriisit $xI - A$ ja $xI - B$ ovat $K[x]$-ekvivalentteja, jos ja vain jos niiden Smithin normaalimuodossa olevat matriisit ovat samat, mistä väite seuraa. □

Esimerkki 4.4. Tarkastellaan matriiseja

$$A := \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$$

ja

$$B := \begin{bmatrix} 1 & -2 \\ 1 & 4 \end{bmatrix}.$$

Etsitään ensin matriisin

$$xI - A = \begin{bmatrix} x-2 & 0 \\ 1 & x-3 \end{bmatrix}$$

Smithin normaalimuoto. Vaihdetaan ROW(1) ja ROW(2) keskenään, jolloin saadaan matriisi

$$\begin{bmatrix} 1 & x-3 \\ x-2 & 0 \end{bmatrix}$$

ja korvataan COL(2) summalla COL(2) + $(-(x-3))$COL(1), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 \\ x-2 & (x-2)(-x+3) \end{bmatrix}.$$

Korvaamalla vielä ROW(2) summalla ROW(2) + (−(x − 2))ROW(1), saadaan matriisi

$$\begin{bmatrix} 1 & 0 \\ 0 & (x-2)(-x+3) \end{bmatrix},$$

joka on Smithin normaalimuodossa.

Etsitään myös matriisin

$$xI - B = \begin{bmatrix} x-1 & -2 \\ 1 & x-4 \end{bmatrix}$$

Smithin normaalimuoto. Korvataan COL(2) summalla COL(2) + COL(1), jolloin saadaan matriisi

$$\begin{bmatrix} x-1 & x-3 \\ 1 & x-3 \end{bmatrix},$$

ja korvataan ROW(1) summalla ROW(1) + (−1)ROW(2), jolloin saadaan matriisi

$$\begin{bmatrix} x-2 & 0 \\ 1 & x-3 \end{bmatrix}.$$

Vaihtamalla ROW(1) ja ROW(2) keskenään, saadaan matriisi

$$\begin{bmatrix} 1 & x-3 \\ x-2 & 0 \end{bmatrix}.$$

Korvataan COL(2) summalla COL(2) + (−(x − 3))COL(1), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 \\ x-2 & (x-2)(-x+3) \end{bmatrix}.$$

Korvaamalla vielä ROW(2) summalla ROW(2) + (−(x − 2))ROW(1), saadaan matriisi

$$\begin{bmatrix} 1 & 0 \\ 0 & (x-2)(-x+3) \end{bmatrix},$$

joka on Smithin normaalimuodossa.

Havaitaan, että matriisien $xI - A$ ja $xI - B$ Smithin normaalimuodossa olevat matriisit ovat samat, joten lauseen 4.8 nojalla matriisit A ja B ovat similaariset.

Huomautus. Kunnan K yli määritetyn $n \times n$-matriisin A invariantteja tekijöitä etsiessä lauseen 4.8 nojalla riittää etsiä matriisin $xI - A$ Smithin normaalimuodossa oleva matriisi. Lauseen 4.7 nojalla matriisin $xI - A$ ne diagonaalialkiot, jotka eivät ole yksiköitä, ovat matriisin A invariantit tekijät.

Esimerkki 4.5. Etsitään kunnan $\mathbb{Q}$ yli määritellyn matriisin

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

invariantit tekijät.

Invariantit tekijät löydetään viemällä matriisi

$$xI - A = \begin{bmatrix} x-2 & 0 & 0 & 0 \\ 1 & x-1 & 0 & 0 \\ 0 & 1 & x & 1 \\ -1 & -1 & -1 & x-2 \end{bmatrix}$$

Smithin normaalimuotoon. Aloitetaan korvaamalla matriisin $xI - A$ ROW(1) summalla ROW(1) + $(-(x-2)$ROW(2)), jolloin saadaan

$$\begin{bmatrix} 0 & -(x-1)(x-2) & 0 & 0 \\ 1 & x-1 & 0 & 0 \\ 0 & 1 & x & 1 \\ -1 & -1 & -1 & x-2 \end{bmatrix}.$$

Vaihdetaan ROW(1) ja ROW(2) paikkoja, jolloin saadaan matriisi

$$\begin{bmatrix} 1 & x-1 & 0 & 0 \\ 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & 1 & x & 1 \\ -1 & -1 & -1 & x-2 \end{bmatrix},$$

ja korvataan ROW(4) summalla ROW(4) + ROW(1), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & x-1 & 0 & 0 \\ 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & x-2 & -1 & x-2 \end{bmatrix}.$$

Korvataan sitten COL(2) summalla COL(2) + COL(1) ja korvataan sitten COL(2) summalla COL(2) + $(-x)$COL(1), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & x-2 & -1 & x-2 \end{bmatrix}.$$

Nyt vaihdetaan ROW(2) ja ROW(3) paikkoja, jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & x-2 & -1 & x-2 \end{bmatrix}$$

ja vaihdetaan COL(2) ja COL(4) paikkoja, jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & 0 & 0 & -(x-1)(x-2) \\ 0 & x-2 & -1 & x-2 \end{bmatrix}.$$

Korvataan COL(4) summalla COL(4) + (-1)COL(2), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x & 0 \\ 0 & 0 & 0 & -(x-1)(x-2) \\ 0 & x-2 & -1 & 0 \end{bmatrix}.$$

Korvataan COL(3) summalla COL(3) + $(-x)$COL(2), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -(x-1)(x-2) \\ 0 & x-2 & -1-x(x-2) & 0 \end{bmatrix},$$

ja korvataan vielä ROW(4) summalla ROW(4) + $(-(x-2))$ROW(2), jolloin saadaan matriisi

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x & 0 \\ 0 & 0 & 0 & -(x-1)(x-2) \\ 0 & 0 & -(x-1)^2 & 0 \end{bmatrix}.$$

Nyt voidaan siirtyä tarkastelemaan edellä olevan matriisin osamatriisia

$$\begin{bmatrix} 0 & -(x-1)(x-2) \\ -(x-1)^2 & 0 \end{bmatrix},$$

sillä muu osa matriisista on jo diagonaalimuodossa. Vaihtamalla tämän osamatriisin COL(1) ja COL(2) paikkoja, saadaan matriisi

$$\begin{bmatrix} -(x-1)(x-2) & 0 \\ 0 & -(x-1)^2 \end{bmatrix},$$

ja kertomalla ROW(1) yksiköllä -1, saadaan matriisi

$$\begin{bmatrix} (x-1)(x-2) & 0 \\ 0 & -(x-1)^2 \end{bmatrix}.$$

Korvaamalla ROW(1) summalla ROW(1) + (-1)ROW(2), saadaan matriisi

$$\begin{bmatrix} (x-1)(x-2) & (x-1)^2 \\ 0 & -(x-1)^2 \end{bmatrix},$$

ja korvaamalla COL(2) summalla COL(2) − COL(1), saadaan matriisi

$$\begin{bmatrix} (x-1)(x-2) & x-1 \\ 0 & -(x-1)^2 \end{bmatrix}.$$

Vaihtamalla COL(1) ja COL(2) paikkoja, saadaan matriisi

$$\begin{bmatrix} x-1 & (x-1)(x-2) \\ -(x-1)^2 & 0 \end{bmatrix},$$

ja korvaamalla COL(2) summalla COL(2)+(−(x−2))COL(1), saadaan matriisi

$$\begin{bmatrix} x-1 & 0 \\ -(x-1)^2 & (x-2)(x-1)^2 \end{bmatrix}.$$

Vielä lopuksi korvaamalla ROW(2) summalla ROW(2) + (x − 1)ROW(1), saadaan matriisi

$$\begin{bmatrix} x-1 & 0 \\ 0 & (x-2)(x-1)^2 \end{bmatrix},$$

joka on Smithin normaalimuodossa. Siis matriisin $xI - A$ Smithin normaalimuoto on

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-1 & 0 \\ 0 & 0 & 0 & (x-2)(x-1)^2 \end{bmatrix},$$

joten matriisin A invariantit tekijät ovat $(x-1)$ ja $(x-2)(x-1)^2$.

Viitteet

[1] J. J. Rotman, *Advanced Modern Algebra, 2nd edition*. Prentice Hall, 2003.

[2] R. B. Ash, *Abstract Algebra: The Basic Graduate Year, Revised edition*, 2002. URL http://www.math.uiuc.edu/~r-ash/Algebra.html

[3] D. S. Dummit, R. M. Foote, *Abstract Algebra, 3rd edition*. John Wiley and Sons, Inc., 2003.

[4] B. Hartley, T. O. Hawkes, *Rings, Modules and Linear Algebra*. Chapman and Hall, 1970.

[5] P. J. Davis, *Circulant matrices, 2nd edition*. Chelsea Pub Co, 1994.

[6] F. M. Goodman, *Algebra: Abstract and Concrete, Edition 2.6*.
URL http://homepage.math.uiowa.edu/~goodman/algebrabook.dir/book.2.6.pdf