Johdanto moduleihin

Netta Hietala

LuK-tutkielma
Marraskuu 2024

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Netta Hietala: Johdanto moduleihin
LuK-tutkielma, 9 s.
Matematiikka
Marraskuu 2024

Tässä tutkielmassa tutustutaan lineaarialgebran vektoriavaruutta laajentavaan käsitteeseen, jota kutsutaan moduliksi. Määritellään modulit aksioomien avulla ja käsitellään myös alimoduleja. Lopuksi tarkastellaan vapaita moduleja sekä laajennetaan tarkastelua matriiseihin ja Smithin normaalimuotoon.

Asiasanat: moduli, vapaa moduli, matriisi, Smithin normaalimuoto.

Sisällys

1 Johdanto **1**

2 Modulin määritelmä **1**
2.1 Modulit poikkeavat vektoriavaruuksista 2
2.2 Esimerkki 3

3 Hyödyllisiä määritelmiä ja lauseita **3**
3.1 Määritelmiä 3
3.2 Lauseita 4

4 Vapaat modulit **5**

5 Matriisit ja Smithin normaalimuoto **7**
5.1 Homomorfismin muuttaminen matriisiksi 7
5.2 Smithin normaalimuodon idea 7
5.3 Smithin normaalimuoto 8

1 Johdanto

Modulit ovat vektoriavaruuksien yleistyksiä [1]. Niiden historia ulottuu 1800-luvun puolelle. Richard Dedekind käytti modulin käsitettä algebrallisen lukuteorian yhteydessä ensimmäisen kerran vuonna 1871. Dedekind kuitenkin tarkoitti käsitteellä vain kompleksilukujen additiivisen ryhmän aliryhmää eli $\mathbb{Z}$-modulia. 1900-luvun alussa Emanuel Lasker käytti modulin käsitettä ideaalin käsitteen kanssa synonyymin tavoin. Vasta myöhemmin 1900-luvulla Emmy Noether käytti modulin käsitettä samalla tavalla kuin se nykyään ymmärretään. Noether oli ensimmäinen, joka käytti modulin käsitettä oikeassa merkityksessään [2].

Moduleilla on paljon sovelluksia. Muun muassa lineaariavaruuksien tarkastelu moduleina yhdestä vektoriavaruudesta toiseen polynomirenkaan $F(x)$ yli, missä F on vektoriavaruuksien skalaareiden kunta, johtaa esimerkiksi Jordanin kanoniseen muotoon [1]. Moduleja voi hyödyntää myös esimerkiksi koodausteoriassa, erityisesti lineaaristen koodien yhteydessä [3].

Tutkielman tarkoituksena on opettaa lukijalle, millaisia algebrallisia rakenteita modulit ovat. Lisäksi tutkielma pyrkii herättämään lukijan kiinnostuksen moduleja kohtaan ja sitä kautta innostamaan lukijaa tutkimaan niitä lisää. Tutkielma pohjautuu lähteeseen [1].

2 Modulin määritelmä

Yksinkertaisesti moduli on vektoriavaruus, jonka määritelmässä kertoimien kunta korvataan renkaalla.

Määritellään vasen R-moduli. Oikea R-moduli määritellään samankaltaisten aksioomien avulla.

Määritelmä 1. *Vasen R-moduli M* yli renkaan R, jossa 1_R on ykkösalkio, on Abelin ryhmä varustettuna skalaaritulolla

$$\cdot : R \times M \to M,$$

missä $\cdot(\alpha, m) = \alpha \cdot m$, kaikilla $\alpha \in R$ ja $m \in M$, ja missä α ja M täyttävät seuraavat aksioomat:

- $\alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m$
- $(\alpha + \beta) \cdot m = (\alpha \cdot m) + (\beta \cdot m)$
- $\alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n$
- $1_R \cdot m = m$,

missä $\alpha, \beta \in R$ ja $m, n \in M$.

2.1 Modulit poikkeavat vektoriavaruuksista

Tarkastellaan rationaalilukuja $\mathbb{Q}$ $\mathbb{Z}$-modulina. Nyt $\mathbb{Q}$ on $\mathbb{Z}$-moduli, sillä $\mathbb{Q}$ muodostaa Abelin ryhmän. Lisäksi moduliaksioomat pätevät, koska alkioille $a, b, c, d, m, n, \in \mathbb{Z}$ ja $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ pätevät laskulait

- $n(m\frac{a}{b}) = (nm)\frac{a}{b}$
- $(n+m)\frac{a}{b} = n\frac{a}{b} + m\frac{a}{b}$
- $n(\frac{a}{b} + \frac{c}{d}) = n\frac{a}{b} + n\frac{c}{d}$
- $1_{\mathbb{Z}}\frac{a}{b} = \frac{a}{b}$,

missä on käytetty kokonaislukujen $\mathbb{Z}$ ja rationaalilukujen $\mathbb{Q}$ tuttuja ominaisuuksia.

Seuraavaksi osoitetaan, että $\mathbb{Z}$-modulilla $\mathbb{Q}$ ei ole kantaa. Käytetään apuna lineaarisen riippumattomuuden määritelmää ja kannan määritelmää, jossa vektoriavaruus korvataan modulilla ja skalaarikunta renkaalla.

Modulin $\mathbb{Q}$ alkiot eivät pysty muodostamaan modulin $\mathbb{Q}$ kantaa. Modulin $\mathbb{Q}$ kanta ei voi muodostua yhdestä alkiosta, sillä jos näin olisi, olisi olemassa elementti $a/b \in \mathbb{Q}, a, b \in \mathbb{Z}$ ja $b \neq 0$, missä jokainen modulin $\mathbb{Q}$ alkio voitaisiin esittää tämän alkion kokonaislukukerronnalla eli jollekin $r \in \mathbb{Z}$,

$$r\frac{a}{b} = \frac{a}{b+1}. \tag{1}$$

Tämä ei ole mahdollista, koska yhtälön 1 mukaan

$$r(b+1) = b$$

eli

$$r = \frac{b}{b+1},$$

missä $b \neq 0$ eli $r \notin \mathbb{Z}$. Päädytään siis ristiriitaan. Seuraavaksi osoitetaan, että kaksi modulin $\mathbb{Q}$ alkiota eivät voi muodostaa modulin $\mathbb{Q}$ kantaa. Olkoon $a_1/b_1, a_2/b_2 \in \mathbb{Q}$ ja $a_1/b_1 \neq a_2/b_2$, missä $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ ja $b_1, b_2 \neq 0$. Nyt $r_1, r_2 \in \mathbb{Z}$ ja lineaarisen riippumattomuuden mukaan

$$r_1\frac{a_1}{b_1} + r_2\frac{a_2}{b_2} = 0,$$

jos ja vain jos kertoimet r_1 ja r_2 ovat 0. Jos valitaan $r_1 = b_1a_2$ ja $r_2 = -b_2a_1$, niin $r_1, r_2 \in \mathbb{Z}$ ja edellä mainittu lauseke on lineaarisesti riippuva. Joten, kun valitaan mitkä tahansa kaksi modulin $\mathbb{Q}$ alkiota, niin ne ovat lineaarisesti riippuvia ja täten eivät voi muodostaa modulin $\mathbb{Q}$ kantaa. Induktiotodistuksesta seuraa laajennus: mikä tahansa kahta suurempi alkioiden määrä modulilla $\mathbb{Q}$ on lineaarisesti riippuva eikä täten voi muodostaa modulin $\mathbb{Q}$ kantaa.

2.2 Esimerkki

Modulien aksioomat ovat hyvin samankaltaiset kuin vektoriavaruuksien, mutta pienien muutoksien seuraukset ovat monipuoliset. Monet objektit osoittautuvat moduleiksi. Esimerkiksi Abelin ryhmä G, jossa on ryhmäoperaatio $+$, on $\mathbb{Z}$-moduli, jonka skalaarinen kertolasku on määritelty seuraavasti: $g \in G$ ja $n \in \mathbb{Z}$,

$$ng = \begin{cases} \underbrace{g + g + \cdots + g}_{n \text{ kertaa}}, \text{ jos } n > 0 \\ \underbrace{(-g) + (-g) + \cdots + (-g)}_{n \text{ kertaa}}, \text{ jos } n < 0, \end{cases}$$

missä $-g$ on alkion g käänteisalkio. Voidaan myös osoittaa, että renkaan R vasemmanpuoleiset ihanteet ovat R-moduleja, ja että vektroriavaruudet ovat modulien erikoistapauksia tilanteissa, joissa rengas R on kunta.

3 Hyödyllisiä määritelmiä ja lauseita

3.1 Määritelmiä

Monet ryhmiin, renkaisiin ja vektoriavaruuksiin liittyvät määritelmät pätevät myös moduleihin, koska modulit ovat näiden käsitteiden yleistyksiä. Seuraavaksi määritellään alimodulin käsite sekä tutkitaan vastaavan osajoukon ominaisuuksia.

Määritelmä 2. Olkoon R rengas ja olkoon M R-moduli. R-modulin M osajoukko N on *R-alimoduli*, jos ja vain jos N on Abelin ryhmän M aliryhmä ja N on R-moduli, missä skalaarikertolasku $\cdot$ on määritelty kuten modulissa M ja $\alpha \cdot n \in N$ kaikilla $a \in R$ ja $n \in N$.

Esimerkkejä alimoduleista ovat Abelin ryhmän aliryhmät, jotka ovat $\mathbb{Z}$-alimoduleita ja renkaan R ihanteet, joissa rengas R on R-moduli.

Määritelmä 3. Olkoot R rengas, M R-moduli sekä N R-modulin M R-alimoduli. *Osamäärämoduli* M/N on Abelin ryhmän M tekijäryhmä, joka on myös R-moduli, missä skalaarikertolasku $\circ$ määritellään

$$\alpha \circ (m + N) = \alpha \cdot m + N,$$

kaikilla $\alpha \in R$, $m + N \in M/N$.

Jos $m + N = m' + N$ niin $m - m' \in N$, mistä saadaan $\alpha \cdot m - \alpha \cdot m' = \alpha \cdot (m - m') \in N$, koska N on alimoduli ja siten suljettu skalaarikertolaskussa. Siis $\alpha \cdot m + N = \alpha \cdot m' + N$. Täten osamäärämodulin skalaarinen kertolasku on hyvin määritelty.

Seuraavaksi määritellään modulihomomorfismin ja moduli-isomorfismin käsitteet, jotka ovat tärkeitä ryhmien, renkaiden, kuntien ja vektoriavaruuksien tutkimisessa.

Määritelmä 4. Olkoon R rengas ja olkoon M ja N R-moduleita. Funktio $f : M \to N$ on *R-modulihomomorfismi* jos ja vain jos seuraavat ehdot pätevät:

- $f(m_1 + m_2) = f(m_1) + f(m_2)$ kaikilla $m_1, m_2 \in M$ ja
- $f(\alpha \cdot m) = \alpha \cdot f(m)$ kaikilla $\alpha \in R, m \in M$.

Määritelmä 5. Olkoot R rengas, M ja N R-moduleita sekä $f : M \to N$ R-modulihomomorfismi. Funktio f on R-modulin *isomorfismi* jos ja vain jos f on bijektio.

Määritellään vielä generoidun alimodulin käsite, joka on yleistys vektoreiden virittämästä aliavaruudesta lineaarialgebrassa ja ihanteen käsitteestä rengasteoriassa.

Määritelmä 6. Olkoot R rengas, M R-moduli sekä S R-modulin M osajoukko. Määritellään joukon S *generoima alimoduli* M seuraavasti:

$$\langle S \rangle = \{\sum_{i=1}^{n} a_i s_i \mid n \in N, a_i \in R, s_i \in S, 1 \leq i \leq n\}.$$

Määritelmä 7. Olkoot R rengas, M R-moduli sekä S R-modulin M osajoukko. Määritellään alimodulin $\langle S \rangle$ *generaattoreiksi* joukon S alkiot. Moduli M on *äärellinen* jos ja vain jos $M = \langle S \rangle$, missä S on äärellinen joukko. Moduli M on *syklinen* jos ja vain jos $M = \langle \{m\} \rangle$ jollekin $m \in M$.

Määritelmä 8. Olkoon R rengas, olkoon M R-moduli ja olkoon S R-modulin M osajoukko. Määritellään R-modulin M *aste* R-modulin M generaattoreiden vähimmäismääräksi. Merkitään R-modulin M astetta $rank(M)$.

Syklisen R-modulin käsite yleistää syklisen ryhmän käsitteen, koska Abelin ryhmä on syklinen jos ja vain jos se on syklinen $\mathbb{Z}$-moduli.

3.2 Lauseita

On olemassa kolme isomorfialausetta sekä ryhmille että renkaille. Koska modulit yleistävät sekä Abelin ryhmiä että renkaita, myös moduleille on olemassa kolme isomorfialausetta. Todistetaan vain ensimmäinen isomorfialause, sillä lauseet 2 ja 3 todistetaan samalla tavalla.

Lause 1. *(Ensimmäinen isomorfialause). Olkoot R rengas, M ja N R-moduleita sekä $f : M \to N$ R-modulihomomorfismi. Silloin $M/Ker(f) \cong Im(f)$.*

Todistus. Ryhmiä koskevasta ensimmäisestä isomorfialauseesta saamme kuvauksen $\hat{f} : M/Ker(f) \to Im(f)$, joka määritellään $\hat{f}(m + Ker(f)) = f(m)$. Kuvaus on hyvin määritelty Abelin ryhmän isomorfismi. Todistetaan vielä, että f on R-modulihomomorfismi kaikilla $\alpha \in R, m \in M$. Nyt

$$\hat{f}(\alpha \circ (m + Ker(f))) = \hat{f}(\alpha \cdot m + Ker(f)) = f(\alpha \cdot m) = \alpha \cdot f(m) = \alpha \cdot \hat{f}(m + Ker(f)).$$

□

Lause 2. *(Toinen isomorfialause). Olkoon R rengas, olkoon M R-moduli ja olkoon N ja P R-modulin M R-alimoduleita. Silloin*

$$(N + P)/P \cong N/(N \cap P).$$

Lause 3. *(Kolmas isomorfialause). Olkoot R rengas, M R-moduli sekä N ja P R-modulin M R-alimoduleita, missä $P \subset N$. Silloin*

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

4 Vapaat modulit

Soveltamalla samankaltaista ajattelutapaa äärellisesti generoiduille moduleille pääihannealueen yli kuin äärellisille Abelin ryhmille tarvitsemme suoran tulon vastaavan käsitteen moduleille.

Määritelmä 9. Olkoon R rengas ja $M_1, \ldots, M_n$ äärellinen määrä R-moduleja. Määritellään karteesiselle tulolle $M_1 \times \ldots \times M_n$ yhteenlasku, jota merkitään symbolilla $+$, ja skalaarikertolasku, jota merkitään symbolilla $\circ$, kun $x_i, y_i \in M, i \in \mathbb{N}, 1 \leq i \leq n$. Nyt

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

ja kaikilla $\alpha \in R$

$$\alpha \circ (x_1, \ldots, x_n) = (\alpha \cdot x_1, \ldots, \alpha \cdot x_n).$$

Tällöin karteesinen tulo $M_1 \times \ldots \times M_n$ on R-moduli, jossa on yhteenlasku $+$ ja skalaarikertolasku $\circ$. Tätä kutsutaan $M_1, \ldots, M_n$ *suoraksi summaksi*. Merkitään suoraa summaa $M_1, \ldots, M_n$ seuraavasti:

$$M_1 \oplus \cdots \oplus M_n.$$

Seuraava lause on hyödyllinen myöhemmin tutkielmassa.

Lause 4. *Olkoot R-rengas, M R-moduli ja $M_1, \ldots, M_n$ R-modulin M sellaiset alimodulit, että*

- $M = M_1 + \cdots + M_n$ *ja*
- *kun* $1 \leq i \leq n$,

$$M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}.$$

Silloin

$$M \cong M_1 \oplus \cdots \oplus M_n.$$

Todistus. Määritellään kuvaus $f_i : M_i \to M$, $f_i(x) = x$ kaikilla $x \in M_i$. Olkoon $f : M_1 \oplus \cdots \oplus M_n \to M$

$$f(x_1, \ldots, x_n) = f_i(x_1) + \cdots + f_n(x_n) = x_i + \cdots + x_n.$$

Selvästi nähdään, että f on R-modulihomomorfismi. Oletusten ensimmäisen ehdon perusteella f on surjektio. Valitaan nyt $(y_1, \ldots, y_n) \in Ker(f)$. Tällöin $y_1 + \cdots + y_n = 0$. Saadaan

$$y_i = -y_1 - \cdots - y_{i-1} - y_{i+1} - \cdots - y_n,$$

mistä seuraa

$$y_i \in M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}$$

oletusten toisen ehdon perusteella. Näin ollen $(y_1, \ldots, y_n) = 0$, joten $Ker(f) = 0$ ja siten f on injektio. Kuvaus f on siis sekä surjektio että injektio. Täten kuvaus f on bijektiivinen kuvaus eli isomorfismi. □

Kappaleessa 2.1 osoitettiin, ettei kaikilla moduleilla ole kantaa. Nyt kuitenkin rajoitetaan tarkastelu moduleihin, joilla on kanta. Kanta esittää äärettömän joukon äärellisellä määrällä alkioita.

Formalisoidaan kannan käsite aiemmin käytetystä lineaarialgebrallisesta kielestä.

Määritelmä 10. Olkoon R rengas ja olkoon S R-modulin M osajoukko. Joukko S on *lineaarisesti riippumaton* yli renkaan R, jos ehdosta

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$$

seuraa, että $\lambda_i = 0$, missä $\lambda_i \in R$ ja $x_i \in S$, kun $i \in \mathbb{N}, 1 \leq i \leq n$.

Määritelmä 11. Olkoon R rengas ja olkoon S R-modulin M äärellinen osajoukko. Silloin S on R-modulin M *kanta* jos ja vain jos $M = \langle S \rangle$ ja S on lineaarisesti riippumaton yli renkaan R.

Seuraavaksi määritellään vapaan modulin käsite.

Määritelmä 12. Olkoon R-rengas ja olkoon M R-moduli. R moduli M on *vapaa* jos ja vain jos R-modulilla M on kanta.

Osoitetaan, että vapaat modulit käyttäytyvät hyvin samalla tavalla kuin vektoriavaruudet. Oletetaan, että M on vapaa moduli, jonka kantana on v_i, missä $i \in \mathbb{N}$ ja $1 \leq i \leq n$. Tarkastellaan nyt alimodulia, jonka generoi v_j, $\langle \{v_j\} \rangle$, jollekin $j \in \mathbb{N}, 1 \leq j \leq n$. Tarkastellaan rengasta R R-modulina. Määritellään kuvaus $\phi_j : R \to \langle \{v_j\} \rangle$ lausekkeella

$$\phi_j(r) = rv_j.$$

Kuvaus ϕ_j on homomorfismi, koska

$$\phi_j(a_1 r_1 + a_2 r_2) = (a_1 r_1 + a_2 r_2)v_j = a_1 r_1 v_j + a_2 r_2 v_j = a_1 \phi_j(r_1) + a_2 \phi_j(r_2).$$

Oikeastaan ϕ_j on isomorfismi, koska selvästi nähdään, että kuvaus on surjektiivinen ja koska $\{v_j\}$ on lineaarisesti riippumaton joukko, kuvauksen ϕ_j ydin on 0, kuvaus on myös injektiivinen. Eli kuvaus on bijektiivinen ja täten ϕ_j on isomorfismi. Koska vektorit v_i generoivat R -modulin M, niin seuraavat yhtäsuuruudet pätevät vektoreiden v_i lineaarisen riippumattomuuden vuoksi:

$$M = \langle \{v_1\} \rangle + \cdots + \langle \{v_n\} \rangle$$

ja

$$\langle \{v_i\} \rangle \cap (\langle \{v_1\} \rangle + \cdots + \langle \{v_{i-1}\} \rangle + \langle \{v_{i+1}\} \rangle + \cdots + \langle \{v_n\} \rangle) = \{0\}.$$

Lauseen 4 mukaan R-moduli M on vektoreiden v_i generoimien alimodulien suora summa. Koska $\langle v_i \rangle$ on isomorfinen renkaan R kanssa, voimme tulkita vapaan modulin seuraavasti: Vapaa moduli on renkaan R isomorfisten kopioiden suora summa. Tällöin voimme tulkita vapaan modulin R listana n-alkioita, missä skalaarikertolasku ja yhteenlasku suoritetaan komponenteittain.

Keskeinen lause lineaarialgebrassa sanoo, että jokaisella vektoriavaruuden kannalla on sama määrä alkioita, mikä mahdollistaa vektoriavaruuden ulottuvuuden

hyvin määritellyn käsitteen. Jos vapaan modulin kerrointen renkaana on kommutatiivinen rengas, niin jokaisella kannalla on sama määrä alkioita, joka tarkoittaa, että vapaalla modulilla on hyvin määritelty aste. On olemassa kuitenkin esimerkkejä, jotka rikkovat tämän ominaisuuden, mutta niitä ei käsitellä tässä tutkielmassa.

Lopuksi todetaan, että annetulla renkaalla R mikä tahansa äärellinen R-moduli N voidaan esittää vapaan R-modulin R-homomorfisena kuvana. Otetaan R-modulin N generaattorijoukko $\{y_i | 1 \leq i \leq k, k \in \mathbb{N}\}$. Rakennetaan vapaa R-moduli, jonka kantana on k alkion joukko $\{x_i | 1 \leq i \leq k, k \in \mathbb{N}\}$. Lopuksi määritellään jokaiselle $i, 1 \leq i \leq k$, kuvaus, joka vie alkion x_i alkioksi y_i. Mikä tahansa äärellinen R-moduli on isomorfinen vapaan R-modulin osamäärämodulin kanssa, kuten ensimmäinen isomorfialause sanoo.

5 Matriisit ja Smithin normaalimuoto

Tutkitaan vielä matriiseja. Kuten matriisit lineaarialgebrassa esittävät lineaarikuvauksia vektoriavaruuksien välillä, matriisit modulien tutkimuksessa esittävät homomorfismeja vapaiden modulien välillä.

5.1 Homomorfismin muuttaminen matriisiksi

Esimerkki 1. Olkoot R rengas, M vapaa R-moduli, jonka aste on $rank(M) = m$ ja kanta $\{v_1, \ldots, v_m\}$. Olkoon lisäksi N vapaa R-moduli, jonka aste on $rank(N) = n$ ja kanta $\{w_1, \ldots, w_m\}$. Olkoon $f : M \to N$ R-modulihomomorfismi. Tällöin kaikille $1 \leq i \leq m$, $f(v_i) \in N$, ja siksi se voidaan esittää kantavektoreiden N lineaarikombinaationa

$$f(v_i) = \sum_{j=1}^{n} a_{ij} w_j,$$

missä $a_{ij} \in R$. Jos merkitään matriisin alkio a_{ij} rivillä i ja sarakkeessa j, saadaan homomorfismille matriisiesitys.

Matriisikertolasku voidaan käsittää vapaiden R-modulihomomorfismien yhdistelmänä, jos ja vain jos R on kommutatiivinen. Koska kommutatiivisilla renkailla on myös hyvin määritelty aste, rajataan käsittely jatkossa kommutatiivisiin renkaisiin.

5.2 Smithin normaalimuodon idea

Motivoidaan lineaarialgebrasta tutun kannan täydentämisen ajatuksella Smithin normaalimuoto tarkastelemalla seuraavaa ongelmaa: liitetään vapaan R-modulin M kanta $x_1, \ldots, x_n$ äärellisesti generoidun alimodulin generaattoreihin $\{u_1, \ldots, u_m\}$, missä $m \leq n$. Alimodulin generaattoreille voidaan luonnollisesti määritellä esitys kantavektoreiden suhteen. Kuten lineaarialgebrassa, kanta voidaan vaihtaa kannasta $x = (x_1 \ldots x_n)^T$ kantaan $y = (y_1 \ldots y_n)^T$ kertomalla säännöllisellä matriisilla P, jolloin $y = Px$. Myös generaattoreita voidaan vaihtaa generaattorista $v = (v_1 \ldots v_m)^T$

generaattoriin $w = (w_1 \dots w_n)^T$ kertomalla säännöllisellä matriisilla Q. Koska generaattorit ovat kantavektoreiden lineaarikombinaatioita, saadaan

$$U = AX,$$

missä A on kerroinmatriisi, joka koostuu kantavektoreiden lineaarikombinaatioiden kertoimista. Määritelmän mukaisesti:

$$V = QU = QAX = QAP^{-1}Y,$$

joten uusi kerroinmatriisi on QAP^{-1}. Smithin normaalimuodon perusidea on valita Q ja P niin, että uudet generaattorit liittyvät uusiin kantavektoreihin yksinkertaisella tavalla. Tarkemmin sanottuna Smithin normaalimuodossa kerroinmatriisilla $B = QAP^{-1}$ on seuraava ominaisuus: $b_{ij} = 0$, kun $i \neq j$, ja $b_{ii} = b_i \neq 0$, kun $i = j$. Lisäksi $b_i | b_{i+1}$ kaikilla i.

Seuraus 1. *Jokainen generaattori on uuden kantavektorin skalaarikerroin.*

Säännöllisen matriisin tapauksessa on syytä olla tarkkana, sillä renkaassa R olevan matriisin käänteismatriisilla tulee myös olla alkiot renkaasta R. Esimerkiksi kokonaislukujen tapauksessa matriisin käänteismatriisin alkioiden tulee olla myös kokonaislukuja, mikä rajoittaa kääntyvät matriisit kokonaslukujen tapauksessa niihin, joiden determinantti on ± 1. Determinantin tulee olla siis yksikkö eli alkio, jolla on käänteisalkio saman renkaan sisällä, jotta matriisi voi olla säännöllinen.

5.3 Smithin normaalimuoto

Rajoitetaan perusrengasta vielä kommutatiivisista renkaista pääihannealueeseen. Esimerkissä kertoimien renkaana on kokonaislukujen pääihannealue ja lopuksi päädytään Smithin normaalimuotoon. Smithin normaalimuodon olemassaoloa ei todisteta, mutta esimerkin avulla voi huomata, että prosessi päättyy äärellisen monen askeleen jälkeen. Jos tehdään samat rivitoimitukset identiteettimatriisille ja samat saraketoimitukset toiselle identiteettimatriisille, niin löydetään matriisit P ja Q, jotka muuttavat kannan ja generaattorit.

Oletetaan, että on olemassa $\mathbb{Z}$-moduli M, jonka kanta on $\{x_1, x_2, x_3, x_4\}$. Olkoon K $\mathbb{Z}$-alimoduli, jonka generaattorit ovat v_1, v_2 ja v_3, missä $v_1 = 2x_1 + x_2 - 3x_4 - x_4, v_2 = x_1 - x_2 - 3x_3 + x_4$ ja $v_3 = 4x_1 - 4x_2 + 16x_4$. Tällöin kerroinmatriisi on

$$A = \begin{pmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{pmatrix}.$$

Muutetaan nyt matriisi A Smithin normaalimuotoon:

$$\begin{matrix} I_3 & A & I_4 \end{matrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & -3 & 1 \\ 2 & 1 & -3 & -1 \\ 4 & -4 & 0 & 16 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{-2R_1+R_2;-4R_1+R_3} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & -3 & 1 \\ 0 & 3 & 3 & -3 \\ 0 & 0 & 12 & 12 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_1+C_2;3C_1+C_3;-1C_1+C_4} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 3 & -3 \\ 0 & 0 & 12 & 12 \end{pmatrix} \begin{pmatrix} 1 & 1 & 3 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{-C_2+C_3;C_2+C_4} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 12 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{-C_3+C_4} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= Q \quad B \quad P^{-1}.$$

Helposti voitaisiin myös tarkistaa, että $QAP^{-1} = B$. Nyt modulin M uusi kanta on $\{y_1, y_2, y_3, y_4\}$, ja alimodulin K generaattorit ovat $w_1 = y_1, w_2 = 3y_2$ ja $w_3 = 12y_3$. Koska generaattorit w_i generoivat $\mathbb{Z}$-alimodulin K ja alkiot y_i sekä w_i ovat lineaarisesti riippumattomia, muodostaa w_i kannan K. Näin ollen K on vapaa $\mathbb{Z}$-alimoduli.

Viitteet

[1] Poulsen, D. (2010). *Modules: An introduction*. University of Puget Sound.

[2] Kleiner, I., & Kleiner, I. (2007). *A History of Abstract Algebra (1st ed.)*. Springer Nature. https://doi.org/10.1007/978-0-8176-4685-1

[3] Faldiyan, M., & Sylviani, S. (2024). *Application of Module to Coding Theory: A Systematic Literature Review*. https://doi.org/10.48550/arxiv.2401.02489