PRO GRADU -TUTKIELMA

**Sasu Turunen**

# Gröbnerin kannat

TAMPEREEN YLIOPISTO
Luonnontieteiden tiedekunta
Matematiikka
Kesäkuu 2018

Tampereen yliopisto
Luonnontieteiden tiedekunta
TURUNEN, SASU: Gröbnerin kannat
Pro gradu -tutkielma, 56 s.
Matematiikka
Kesäkuu 2018

---

## Tiivistelmä

Gröbnerin kanta on kuntakertoimisen polynomirenkaan ideaalin virittäjäjoukko. Sen ominaisuus on, että valittaessa mielivaltainen ideaalin polynomi, löytyy Gröbnerin kannasta polynomi, jonka korkein termi jakaa kyseisen mielivaltaisesti valitun polynomin korkeimman termin. Jokaisella kuntakertoimisen polynomirenkaan ideaalilla on Gröbnerin kanta, ja itse asiassa jokaisella polynomirenkaan ideaalilla on yksikäsitteinen redusoitu Gröbnerin kanta, jossa on minimaalinen määrä polynomeja. Gröbnerin kannoilla on useita sovelluksia muun muassa laskennallisessa algebrassa. Tässä tutkielmassa tutustutaan Gröbnerin kantoihin ja niiden konstruktioon Buchbergerin algoritmin avulla. Sitä varten esitellään termijärjestyksen määritelmä sekä usean muuttujan polynomien jakoalgoritmi. Lisäksi käydään läpi muutamia sovelluksia Gröbnerin kannoille, kuten polynomiyhtälöryhmien ratkaiseminen sekä esitellään Gröbnerin kantojen laskemista tietokoneohjelmiston avulla.

# Sisältö

# 1 Johdanto

Gröbnerin kanta on kuntakertoimisen polynomirenkaan ideaalin virittäjäjoukko. Sen ominaisuus on, että valittaessa mielivaltainen polynomi ideaalista, löytyy Gröbnerin kannasta polynomi, jonka korkein termi jakaa kyseisen mielivaltaisesti valitun polynomin korkeimman termin. Jokaisella kuntakertoimisen polynomirenkaan ideaalilla on Gröbnerin kanta. Tässä tutkielmassa käydään ensin läpi Gröbnerin kantoja varten tarvittavaa teoriaa. Sen jälkeen esitellään Gröbnerin kannat sekä niiden ominaisuuksia ja selvitetään Gröbnerin kantojen konstruointia. Lopuksi esitellään joitain Gröbnerin kantojen sovelluksia.

Usean muuttujan polynomifunktioden hyvä järjestäminen ei ole yksikäsitteistä. Tämän vuoksi tarvitaan termijärjestys, joka järjestää joukon $\mathbb{N}^n$ alkioita. Nämä luonnollisten lukujen vektorit voidaan samaistaa usean muuttujan polynomifunktioiden kanssa, koska polynomifunktioiden eksponentit ovat luonnollisten lukujen vektoreita. Termijärjestykset eivät ole yksikäsitteisiä, jolloin on valittava kuhunkin tilanteeseen mahdollisimman hyvin sopiva järjestys. Tutkielmassa esitellään kertauksenomaisesti usean muuttujan polynomifunktiot ja tämän jälkeen tutustutaan termijärjestyksen määritelmään ja esitetään muutama yleisesti käytetty termijärjestys.

Usean muuttujan polynomien jakoalgoritmi on yhden muuttujan polynomin jakoalgoritmin laajennettu versio. Itse proseduuri on kuitenkin varsin samanlainen kuin yhden muuttujan polynomien jakaminen perinteisessä jakokulmassa. Erikoisemmaksi asian tekee se, että polynomeja jaetaan polynomijoukoilla eikä yksittäisellä polynomilla. Tällöin on myös merkitystä, missä järjestyksessä polynomia jaetaan muilla polynomeilla. Jakoalgoritmia varten tutustutaan polynomien johtaviin termeihin ja johtavien termien eksponentteihin sekä myöhemmin tarpeelliseen supistumisen käsitteeseen.

Kuten todettua, jos kuntakertoimisen polynomirenkaan ideaalista valitaan mielivaltainen polynomi, löytyy tämän ideaalin Gröbnerin kannasta polynomi, jonka korkeain termi jakaa tämän ideaalin polynomin korkeimman termin. Tämä määritelmä esitetään tutkielmassa formaalisti. Sen jälkeen selvitetään tärkeitä Gröbnerin kantoihin liittyviä tuloksia. Esimerkiksi kun polynomi jaetaan Gröbnerin kannalla, ei jakamisen järjestyksellä ole merkitystä ja mielivaltaisen ideaalin Gröbnerin kanta on myös tämän ideaalin virittäjäjoukko.

Gröbnerin kantoja voidaan muodostaa esimerkiksi Buchbergerin algoritmin avulla. Tätä varten esitellään tutkielmassa S-polynomien määritelmä. Itse algoritmi esitetään ja sen toimivuus todistetaan. Algoritmia havainnollistavat kaksi kaksi esimerkkiä, joista selviää myös se, että Gröbnerin kantojen laskeminen käsin voi olla varsin työlästä, vaikka lähtötilanne näyttäisikin yksinkertaiselta.

Gröbnerin kannat eivät ole yksikäsitteisiä. Itse asiassa mielivaltaisen ideaalin Gröbnerin kantaan voidaan lisätä mikä tahansa ideaalin alkio, ja edelleen kyseessä on määritelmän mukaisesti Gröbnerin kanta. Tämän takia tutkielmassa esitellään sekä minimaalisen Gröbnerin kannan että redusoidun Gröbnerin

kannan määritelmät. Lisäksi osoitetaan, että jokaisella ideaalilla on olemassa yksikäsitteinen redusoitu Gröbnerin kanta.

Gröbnerin kantojen sovelluksista esitellään tutkielmassa eliminointi, jossa muodostetaan eliminointi-ideaali, jolloin polynomirenkaan $k[X_1, \ldots, X_n]$ muuttujia voidaan poistaa muodostamalla ideaali $I \cap k[X_m, \ldots, X_n]$, missä $m > 1$. Eliminointi-ideaalin tärkeä ominaisuus on, että ideaalin $I$ Gröbnerin kannasta saatu joukko $G \cap k[X_m, \ldots, X_n]$ on ideaalin $I \cap k[X_m, \ldots, X_n]$ Gröbnerin kanta. Eliminointi-ideaalin avulla voidaan laskea jäännösideaaleja sekä esimerkiksi kahden polynomin suurin yhteinen tekijä ja pienin yhteinen monikerta. Toisena sovelluksena tutkielmassa esitetään polynomiyhtälöryhmien ratkaisu, jossa käytetään hyväksi sitä tulosta, että polynomijoukon ratkaisujoukko on sama kuin polynomijoukon generoiman ideaalin ratkaisujoukko. Tällöin myös tämän ideaalin Gröbnerin kannan ratkaisujoukko on sama kuin alkuperäisen polynomijoukon. Tämä on merkittävää, koska Gröbnerin kannan ratkaisujoukko on usein huomattavasti helpompi laskea kuin alkuperäisen joukon ratkaisujoukko.

Tutkielmassa on käytetty pääasiallisina lähteinä Lauritzenin teosta, ks. [3], jota käytetään erityisesti usean muuttujan polynomifunktioiden määrittelemisessä ja Gröbnerin kantojen perustulosten esityksessä, sekä Cox et al. kirjaa, ks. [2], jota käytettiin erityisesti algoritmien esittämiseen ja todistamiseen sekä eliminointiteoriaan. Lisäksi Adamsin ja Loustaunaun kirja, ks. [1], toimi lähteenä joissakin tuloksissa etenkin polynomiyhtälöryhmien ratkaisemisen osalta. Joissain esimerkeissä on sekä ajan että lukijan säästämiseksi tehty Gröbnerin kantojen laskeminen tietokoneen avulla niissä tilanteissa, joissa itse kannan laskemisen mekaaninen toiminta ei ole tuonut esimerkille lisäarvoa. Nämä laskut on tehty Sage-ohjelmaa, ks. [4], apuna käyttäen.

Lukijan odotetaan tuntevan matemaattisten perustietojen lisäksi algebran peruskäsitteet ryhmä- ja rengasteoriasta sekä erityisesti ideaaleihin liittyvät ominaisuudet.

# 2 Termijärjestykset

## 2.1 Usean muuttujan polynomifunktiot

**Määritelmä 2.1.** Olkoon $R$ kommutatiivinen rengas. Joukkoa

$$R[X] = R[\mathbb{N}] = \{f : \mathbb{N} \to R \mid f(n) = 0,\ n \gg 0\}$$

sanotaan *yhden muuttujan polynomirenkaaksi*, joka tavanomaisen yhteen- ja kertolaskun kanssa muodostaa kommutatiivisen renkaan $(R[X], +, \cdot)$. Lisäksi polynomirenkaan alkiot, $f \in R[X]$ ovat tuttua muotoa

$$f = a_n X^n + \cdots + a_1 X + a_0,$$

missä $a_i \in R$. *Usean muuttujan polynomirengas* on edeltävästä laajennettu joukko

$$R[X_1, \ldots, X_n] = R[\mathbb{N}^n] = \{f : \mathbb{N}^n \to R \mid f(v) = 0,\ |v| \gg 0\},$$

missä $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$ ja $|v| = v_1 + \cdots + v_n$. Polynomi $f \in R[X_1, \ldots, X_n]$ vastaa funktiota $f : \mathbb{N}^n \to R$, jonka arvo eroaa nollasta vain äärellisen monella $v \in \mathbb{N}^n$. Vastatkoon nyt $X^v \in R[\mathbb{N}^n]$ sellaista funktiota, jolle

$$X^v(w) = \begin{cases} 1 & \text{kun } v = w, \\ 0 & \text{kun } v \neq w. \end{cases}$$

Tällä notaatiolla voidaan jokainen polynomi $f \in R[\mathbb{N}^n]$ kirjoittaa äärellisenä summana

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v,$$

missä $a_v \in R$.

Jos $f$, $g \in R[\mathbb{N}^n]$, määritellään

$$f + g = (f + g)(v) = f(v) + g(v)$$

ja $fg$ summana

$$(fg)(v) = \sum_{v_1 + v_2 = v} f(v_1) g(v_2),$$

missä $v_1$, $v_2 \in \mathbb{N}^n$. Näin saadaan aikaan rengas $(R[\mathbb{N}^n], +, \cdot)$.

*Huomautus.* Notaatiossa $R[X_1, \ldots, X_n]$ $X_1$ vastaa merkintää $X^{(1,0,\ldots,0)}$ notaatiolle $R[\mathbb{N}^n]$, $X_2$ vastaa merkintää $X^{(0,1,\ldots,0)}$, $X_n$ vastaa merkintää $X^{(0,0,\ldots,1)}$ ja niin edelleen.

**Esimerkki 2.1.** Tässä esitetyn määritelmän mukainen notaatio useamman muuttujan polynomeille voidaan helposti muuttaa perinteiseen koulumatematiikan esitykseen polynomeista. Jos esimerkiksi

$$f = 3X^{(0,0,0)} + 5X^{(3,1,0)} - X^{(0,2,1)} + 2X^{(1,1,1)} \in \mathbb{Z}[\mathbb{N}^3],$$

niin voidaan merkitä $X = X^{(1,0,0)}$, $Y = X^{(0,1,0)}$ ja $Z = X^{(0,0,1)}$, jolloin saadaan

$$f = 3 + 5X^3Y - Y^2Z + 2XYZ \in \mathbb{Z}[X, Y, Z].$$

**Määritelmä 2.2.** Olkoon $R[X_1, \ldots, X_n]$ polynomirengas,
$f \in R[X_1, \ldots, X_n]$ ja $(a_1, \ldots, a_n) \in R^n$. Kuvausta
$(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$, $R^n \to R$, missä polynomin $f$ *arvo* saadaan sijoittamalla muuttujan $X_i$ paikalle alkio $a_i$ kaikilla $i \in \{1, \ldots, n\}$, sanotaan *polynomifunktioksi*.

**Lause 2.1.** *Usean muuttujan polynomirengas* $(R[\mathbb{N}^n], +, \cdot)$ *on rengas, jonka yhteenlaskun neutraalialkio on* $0 \in R$ *ja ykkösalkio on* $X^{(0,\ldots,0)}$.

*Todistus.* Jotta $R[\mathbb{N}^n]$ olisi rengas, sen on oltava Abelin ryhmä. Lisäksi kertolaskun täytyy olla suljettu, eli $fg \in R[\mathbb{N}^n]$ kaikilla $f, g \in R[\mathbb{N}^n]$. Kertolaskulla täytyy olla ykkösalkio $1 \in R[\mathbb{N}^n]$, jolle $1f = f$ kaikilla $f \in R[\mathbb{N}^n]$. Viimeiseksi osittelulakien pitää olla voimassa, eli

$$\begin{aligned}
&(fg)h = f(hg),\\
&f(g + h) = fg + hg \text{ ja}\\
&(f + g)h = fh + gh.
\end{aligned}$$

Jotta $R[\mathbb{N}^n]$ olisi Abelin ryhmä, täytyy sen ensinnäkin olla ryhmä laskutoimituksenaan polynomien yhteenlasku. Lisäksi yhteenlaskun täytyy olla vaihdannainen. Olkoot $f, g \in R[\mathbb{N}^n]$. Nyt $f + g = (f(v) + g(v)) \in R$, koska $R$ on rengas, ja tiedetään, että sen yhteenlasku on suljettu. Samoin siis polynomirenkaan $R[\mathbb{N}^n]$ yhteenlasku on suljettu. Täysin samalla perusteella polynomirenkaan yhteenlasku on myös liitännäinen, eli $f + (g + h) = (f + g) + h$, kun $f, g, h \in R[\mathbb{N}^n]$. Polynomirenkaan yhteenlaskun neutraalialkio on nollakuvaus. Olkoon $f \in R[\mathbb{N}^n]$, $f = \sum_{v \in R[\mathbb{N}^n]} a_v X^v$. Polynomin $f$ käänteisalkio on $-f = \sum_{v \in R[\mathbb{N}^n]} -a_v X^v$. Nyt

$$\begin{aligned}
f + (-f) &= \sum_{v \in R[\mathbb{N}^n]} a_v X^v + \sum_{v \in R[\mathbb{N}^n]} -a_v X^v\\
&= \sum_{v \in R[\mathbb{N}^n]} (a + (-a))_v X^v\\
&= \sum_{v \in R[\mathbb{N}^n]} 0 X^v\\
&= 0_{R[\mathbb{N}^n]}.
\end{aligned}$$

Polynomirengas on siis suljettu yhteenlaskunsa suhteen, sille on voimassa yhteenlaskun liitäntälaki, polynomirenkaassa on yhteenlaskun neutraalialkio, ja jokaiselle polynomille on olemassa käänteisalkio yhteenlaskun suhteen. Polynomirengas täyttää siis kaikki ryhmän määritelmän vaatimukset.

Olkoot sitten $f, g \in R[\mathbb{N}^n]$. Nyt

$$\begin{aligned} f + g &= \sum_{v_1+v_2=v} (f(v_1) + g(v_2)) \\ &= \sum_{v_1+v_2=v} (f(v_1)) + \sum_{v_1+v_2=v} (g(v_2)) \\ &= \sum_{v_1+v_2=v} (g(v_2)) + \sum_{v_1+v_2=v} (f(v_1)) \\ &= g + f. \end{aligned}$$

Polynomien yhteenlasku on siis vaihdannainen, joten polynomirengas on myös Abelin ryhmä.

Funktioiden ominaisuuksien perusteella voidaan todeta, että kertolasku on suljettu. Lisäksi

$$(fg)(v) = \sum_{v_1+v_2=v} f(v_1)g(v_2) = \sum_{v_1+v_2=v} g(v_2) = g(v),$$

kun $f = X^{(0,\ldots,0)}$, sillä tällöin $f(v) = 1$ kaikilla $v \in \mathbb{N}^n$. Huomataan, että $(f + g)h = fh + gh$ kaikilla $f, g, h \in R[\mathbb{N}^n]$, koska

$$\begin{aligned} ((f + g)(v))h(w) &= (f(v) + g(v))h(w) \\ &= \sum_{w_1+w_2=w} (f(v) + g(v))(w_1)h(w_2) \\ &= \sum_{w_1+w_2=w} ((f(v)(w_1))h(w_2) + (g(v))(w_1)h(w_2)) \\ &= f(v)h(w) + g(v)h(w), \end{aligned}$$

koska $(f(v) + g(v))(w_1)h(w_2) \in R$, joka on kommutatiivinen rengas. Täysin vastaavasti voidaan osoittaa, että $(fg)h = f(hg)$ ja $f(g + h) = fg + hg$, joten väite seuraa.

## 2.2 Järjestykset

**Määritelmä 2.3.** Olkoon $S$ joukko ja $x, y, z \in S$. Joukon $S$ relaatio $\leq$ on *järjestys*, jos se on

refleksiivinen, eli $x \leq x$,
antisymmetrinen, eli $x \leq y, y \leq x \Rightarrow x = y$ ja
transitiivinen, eli $x \leq y, y \leq z \Rightarrow x \leq z$.

**Määritelmä 2.4.** Joukon $S$ järjestystä $\leq$ sanotaan *täydelliseksi järjestykseksi*, jos $x \leq y$ tai $y \leq x$ kaikilla $x$, $y \in S$.

**Määritelmä 2.5.** Joukon $S$ järjestystä $\leq$ sanotaan *hyväksi järjestykseksi*, jos jokaisella epätyhjällä osajoukolla $M \subseteq S$ on pienin alkio $m \in M$, jolle $m \leq x$ kaikilla $x \in M$.

**Määritelmä 2.6.** Joukon $\mathbb{N}^n$ järjestystä $\leq$ sanotaan *termijärjestykseksi*, jos

$$\begin{aligned} &(i) \ \leq \text{ on täydellinen järjestys,} \\ &(ii) \ 0 \leq v \text{ ja} \\ &(iii) \ v_1 \leq v_2 \Rightarrow v_1 + v \leq v_2 + v \end{aligned}$$

kaikilla $v$, $v_1$, $v_2 \in \mathbb{N}^n$, kun yhteenlasku + vastaa luonnollisten lukujen tavanomaista yhteenlaskua alkioittain.

**Määritelmä 2.7.** Joukossa $\mathbb{N}^n$ määritellään relaatio $\leq_{lex}$ seuraavasti:

$$(v_1, \ldots, v_n) \leq_{lex} (w_1, \ldots, w_n),$$

jos jokin seuraavista ehdoista täyttyy:

$$\begin{aligned} &v_1 < w_1 \text{ tai} \\ &v_1 = w_1 \text{ ja } v_2 < w_2 \text{ tai} \\ &v_1 = w_1 \text{ ja } v_2 = w_2 \text{ ja } v_3 < w_3 \text{ tai} \\ &\vdots \\ &v_1 = w_1 \text{ ja } v_2 = w_2 \text{ ja } \ldots \text{ ja } v_{n-1} = w_{n-1} \text{ ja } v_n < w_n \text{ tai} \\ &v_1 = w_1 \text{ ja } v_2 = w_2 \text{ ja } \ldots \text{ ja } v_n = w_n, \end{aligned}$$

kun $<$ on luonnollisten lukujen tavanomainen järjestys. Relaatiota $\leq_{lex}$ sanotaan *sanakirjajärjestykseksi*.

**Määritelmä 2.8.** Joukossa $\mathbb{N}^n$ määritellään relaatio $\leq_{glex}$ seuraavasti:
$v \leq_{glex} w$, jos

$$\begin{aligned} &|v| < |w|, \text{ tai} \\ &|v| = |w| \text{ ja } v \leq_{lex} w, \end{aligned}$$

kun $v, w \in \mathbb{N}^n$, $|v| = v_1 + v_2 + \cdots + v_n$ ja $<$ on luonnollisten lukujen tavanomainen järjestys. Relaatiota $\leq_{glex}$ sanotaan *porrastetuksi sanakirjajärjestykseksi*.

**Lause 2.2.** *Sanakirjajärjestys on järjestys.*

*Todistus.* On siis todistettava, että sanakirjajärjestys on refleksiivinen, antisymmetrinen ja transitiivinen. Olkoon $\leq_{lex}$ sanakirjajärjestys ja
$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n) \in \mathbb{N}^n$. Nyt $x \leq_{lex} x$, koska $x_i = x_i$ kaikilla $i \in \{1, \ldots, n\}$. Sanakirjajärjestys on siis refleksiivinen.

Oletetaan nyt, että $x \leq_{lex} y$ ja $y \leq_{lex} x$. Nyt $x_1 < y_1$ tai $x_1 = y_1$ sekä $y_1 < x_1$ tai $y_1 = x_1$. On siis oltava $x_1 = y_1$. Induktiolla voidaan edeltävällä tavalla osoittaa, että $x_i = y_i$ aina, kun $i \in \{1, \ldots, n\}$, joten on oltava $x = y$. Sanakirjajärjestys on siis antisymmetrinen.

Oletetaan lopuksi, että $x \leq_{lex} y$ ja $y \leq_{lex} z$. Voidaan olettaa, että $x \neq y \neq z$. Nyt on olemassa $i \in \{1, \ldots, n\}$, jolle $x_i < y_i$ ja $x_k = y_k$, kun $k < i$. Samoin on olemassa $j \in \{1, \ldots, n\}$, jolle $y_j < z_j$ ja $y_l = z_l$, kun $l < j$. Jos $i < j$, niin $x_i < y_i = z_i$. Lisäksi $x_k = z_k$. kun $k < i$. Jos $i = j$, niin $x_i < y_i < z_i$ ja $x_k = z_k$, kun $k < i$. Jos $i > j$, niin $x_j = y_j < z_j$ ja $x_l = z_l$. kun $l < j$. On siis oltava $x \leq_{lex} z$. Sanakirjajärjestys on siis transitiivinen. On siis osoitettu, että sanakirjajärjestys täyttää kaikki järjestyksen ehdot, mistä väite seuraa.

**Lause 2.3.** *Porrastettu sanakirjajärjestys on järjestys.*

*Todistus.* On siis todistettava, että porrastettu sanakirjajärjestys on refleksiivinen, antisymmetrinen ja transitiivinen. Olkoon $\leq_{glex}$ porrastettu sanakirjajärjestys. ja $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n) \in \mathbb{N}^n$. Nyt $x \leq_{glex} x$, koska ensinnäkin $|x| = |x|$ ja toisekseen lauseen 2.2 perusteella tiedetään, että $x \leq_{lex} x$. Porrastettu sanakirjajärjestys on siis refleksiivinen.

Oletetaan nyt, että $x \leq_{glex} y$ ja $y \leq_{glex} x$. Tällöin on oltava $|x| = |y|$ ja sen perusteella on oltava $x \leq_{lex} y$ ja $y \leq_{lex} x$, mistä Lauseen 2.2 perusteella tiedetään, että tällöin $x = y$. Porrastettu sanakirjajärjestys on siis antisymmetrinen.

Oletetaan lopuksi, että $x \leq_{glex} y$ ja $y \leq_{glex} z$. Jos $|x| < |y|$, niin on oltava $|x| < |z|$, koska joko $|y| < |z|$ tai $|y| = |z|$. Jos taas $|x| = |y|$, niin joko $|x| < |z|$ tai $|x| = |z|$, koska joko $|y| < |z|$ tai $|y| = |z|$. Jos $|x| = |z|$, niin ensinnäkin $x \leq_{lex} y$ ja toisekseen $y \leq_{lex} z$. Lauseen 2.2 perusteella tiedetään, että tällöin $x \leq_{lex} z$. On siis oltava $x \leq_{glex} z$, joten porrastettu sanakirjajärjestys on transitiivinen. On siis osoitettu, että porrastettu sanakirjajärjestys täyttää kaikki järjestyksen ehdot, mistä väite seuraa.

**Lause 2.4.** *Sanakirjajärjestys ja porrastettu sanakirjajärjestys ovat termijärjestyksiä.*

*Todistus.* On siis osoitettava, että sanakirjajärjestykselle $\leq_{lex}$ ja porrastetulle sanakirjajärjestykselle $\leq_{glex}$ ovat voimassa termijärjestyksen määritelmän mukaiset kolme ehtoa:

$$
\begin{aligned}
&(i) \leq_{lex} \text{ ja } \leq_{glex} \text{ ovat täydellisiä järjestyksiä,}\\
&(ii)\ 0 \leq_{lex} v,\ 0 \leq_{glex} v \text{ ja}\\
&(iii)\ v_1 \leq_{lex} v_2 \Rightarrow v_1 + v \leq_{lex} v_2 + v,\\
&\qquad v_1 \leq_{glex} v_2 \Rightarrow v_1 + v \leq_{glex} v_2 + v,
\end{aligned}
$$

kaikilla $v, v_1, v_2 \in \mathbb{N}^n$.

Todistetaan ensin, että sanakirjajärjestys on termijärjestys. Olkoot $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{N}^n$. Olkoon $i \in \mathbb{N}$ pienin sellainen luku, jolla

$v_i \neq w_i$. Jos tällaista lukua $i$ ei löydy, on oltava $v = w$ ja sanakirjajärjestyksen määritelmän perusteella $v \leq_{lex} w$. Jos $i$ on olemassa, niin tällöin $v_k = w_k$, kun $k \in \mathbb{N}$ ja $k < i$. Lisäksi $v_i < w_i$ tai $w_i < v_i$. Ensimmäisessä tapauksessa $v_i < w_i$ ja $v_k = w_k$, joten sanakirjajärjestyksen määritelmän perusteella $v \leq_{lex} w$. Jälkimmäisessä tapauksessa $w_i < v_i$ ja $w_k = v_k$, joten sanakirjajärjestyksen määritelmän perusteella $w \leq_{lex} v$. On siis oltava joko $v \leq_{lex} w$ tai $w \leq_{lex} v$, joten sanakirjajärjestys on täydellinen järjestys.

$0_{\mathbb{N}^n} = (0, \ldots, 0) \leq_{lex} v$, koska $0 \leq v_i$ kaikilla $i \in \{0, \ldots, n\}$.

Oletetaan, että $v \leq_{lex} w$ ja olkoon $p \in \mathbb{N}^n$. Osoitetaan, että $v + p \leq_{lex} w + p$. Jos $v = w$, eli $v_i = w_i$ kaikilla $i \in \{1, \ldots, n\}$, niin samoin $v_i + p_i = w_i + p_i$ ja tällöin $v + p \leq_{lex} w + p$. Jos $v \neq w$, niin olkoon $j \in \{1, \ldots, n\}$ pienin sellainen luku, jolle $v_j < w_j$. Tällöin myös $v_j + p_j < w_j + p_j$. Sanakirjajärjestyksen määritelmän perusteella tiedetään, että $v_k = w_k$ aina, kun $k \in \mathbb{N}$ ja $k < j$. Tästä seuraa suoraan, että $v_k + p_k = w_k + p_k$ aina, kun $k \in \mathbb{N}$ ja $k < j$. Tällöin on siis oltava $v+p \leq_{lex} w+p$. Sanakirjajärjestys täyttää siis kaikki termijärjestyksen ehdot.

Todistetaan seuraavaksi, että porrastettu sanakirjajärjestys on termijärjestys. Olkoot $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{N}^n$. Nyt luonnollisten lukujen järjestyksen perusteella joko $|v| < |w|$, $|v| > |w|$ tai $|v| = |w|$. Jos $|v| = |w|$, niin tiedetään, että tällöin $v \leq_{lex}$ tai $w \leq_{lex}$, koska sanakirjajärjestys osoitettiin edellä täydelliseksi järjestykseksi. Tästä taas seuraa välittömästi porrastetun sanakirjajärjestyksen määritelmän perusteella, että $v \leq_{glex} w$ tai $w \leq_{glex}$. Jos taas $|v| < |w|$ tai $|v| > |w|$, niin porrastetun sanakirjajärjestyksen määritelmästä seuraa välittömästi, että ensimmäisessä tapauksessa $v \leq_{glex} w$ ja jälkimmäisessä $w \leq_{glex} v$. Porrastettu sanakirjajärjestys on siis täydellinen järjestys.

$0_{\mathbb{N}^n} = (0, \ldots, 0) \leq_{glex} v$, koska joko $|(0, \ldots, 0)| < v$ tai $v = (0, \ldots, 0)$ ja koska porrastettu sanakirjajärjestys on edellä todetun perusteella täydellinen järjestys, on oltava $(0, \ldots, 0) \leq_{glex} (0, \ldots, 0)$.

Jos $p \in \mathbb{N}^n$ ja $v \leq_{glex} w$, niin joko $|v| < |w|$ tai $|v| = |w|$ ja $v \leq_{lex} w$. Ensimmäisestä tapauksesta seuraa selvästi $|v + p| < |w + p|$, jolloin $v + p \leq_{glex} w + p$. Jälkimmäisessä tapauksessa taas ensinnäkin $|v + p| = |w + p|$ ja toiseksi, koska sanakirjajärjestys edellä osoitettiin termijärjestykseksi, niin $v + p \leq_{lex} w + p$, joten $v + p \leq_{glex} w + p$.

Porrastettu sanakirjajärjestys täyttää siis kaikki termijärjestyksen ehdot.

On siis osoitettu, että sanakirjajärjestys ja porrastettu sanakirjajärjestys täyttävät kaikki termijärjestyksen ehdot, mistä väite seuraa.

**Esimerkki 2.2.** Yhden muuttujan polynomirenkaassa polynomien termejä voidaan järjestää helposti totutulla tavalla niiden potenssien mukaan. Usean muuttujan polynomirenkaassa ei ole yksiselitteistä tapaa järjestää polynomien termejä. Kuitenkin joukolle $\mathbb{N}^n$ on määritelty termijärjestys, joten useamman muuttujan polynomeja ja niiden termejä voidaan järjestää minkä tahansa termijärjestyksen mukaan.

Olkoon $\leq_1$ sellainen polynomirenkaan $\mathbb{R}[X_1, \ldots, X_n]$ järjestys, jolle $aX^v \leq_1$

$bX^w$, jos ja vain jos $v \leq_{lex} w$, kun $a, b \in \mathbb{R}$ ja $v, w \in \mathbb{N}^n$. Tällöin esimerkiksi

$$3X^{(2,3,7)} \leq_1 X^{(3,2,4)} \text{ ja}$$
$$3X^{(2,1,6)} \leq_1 X^{(2,2,4)},$$

koska ensimmäisessä vertailussa $2 < 3$ ja jälkimmäisessä $2 = 2$ sekä $1 < 2$. Olkoon sitten $\leq_2$ sellainen joukon $\mathbb{R}[X_1, \ldots, X_n]$ järjestys, jolle $aX^v \leq_2 bX^w$, jos ja vain jos $v \leq_{glex} w$, kun $a, b \in R$ ja $v, w \in \mathbb{N}^n$. Tällöin taas

$$X^{(3,2,4)} \leq_2 3X^{(2,3,7)} \text{ ja}$$
$$X^{(2,2,4)} \leq_2 3X^{(2,1,6)},$$

koska ensimmäisessä vertailussa $3+2+4 < 2+3+7$ ja jälkimmäisessä $2+2+4 < 2+1+6$.

Järjestys $\leq_1$ on selvästi täydellinen järjestys, koska $\leq_{lex}$ on täydellinen järjestys. Samoin $\leq_1$ on hyvä järjestys, sillä $X^{(0,\ldots,0)} \leq_1 s$ kaikilla $s \in \mathbb{R}[X_1, \ldots, X_n]$. Vastaavasti myös järjestys $\leq_2$ on sekä täydellinen että hyvä järjestys.

**Lause 2.5.** *(Dicksonin lemma) Olkoon $S$ joukon $\mathbb{N}^n$ osajoukko. Tällöin on olemassa äärellinen joukko alkioita $v_1, \ldots, v_r \in S$ siten, että*

$$S \subseteq (v_1 + \mathbb{N}^n) \cup \cdots \cup (v_r + \mathbb{N}^n).$$

*Todistus.* Ks. [3, s. 192].

Todistetaan Dicksonin lemma induktiolla joukon $\mathbb{N}^n$ eksponentin $n$ suhteen. Jos $n = 1$ ja $S \subseteq \mathbb{N}$, niin olkoon $s$ joukon $S$ pienin luku. Tällöin selvästi $S \subseteq (s + \mathbb{N})$. Tehdään nyt induktio-oletus, eli oletetaan, että $n > 1$ ja että lause on tosi eksponenteilla $m < n$. Olkoon nyt $\pi : \mathbb{N}^n \to \mathbb{N}^{n-1}$ kuvaus siten, että

$$\pi(x_1, x_2, \ldots, x_n) = (x_2, \ldots, x_n).$$

Käyttämällä induktio-oletusta joukkoon

$$\pi(S) = \{\pi(s) \mid s \in S\} \subseteq \mathbb{N}^{n-1}$$

huomataan, että on olemassa vektorit $s_1, \ldots, s_r \in S$, joille pätee

$$\pi(S) \subseteq (\pi(s_1) + \mathbb{N}^{n-1}) \cup \ldots \cup (\pi(s_r) + \mathbb{N}^{n-1}).$$

Koska yleisesti ei pidä paikkaansa, että $S \subseteq (s_1 + \mathbb{N}^n) \cup \ldots \cup (s_r + \mathbb{N}^n)$, tarvitaan lisää vektoreita joukosta $S$.

Merkitään vektorin $s_i$ ensimmäistä alkiota $s_{i_1}$. Olkoon $M$ joukon $\{s_{1_1}, \ldots, s_{r_1}\}$ suurin luku. Määritellään

$$S_i = \{s \in S \mid \text{vektorin } s \text{ ensimmäinen koordinaatti on } i\}, \text{ kun } 0 \leq i < M$$

ja

$$S_{\geq M} = \{s \in S \mid \text{vektorin } s \text{ ensimmäinen koordinaatti on } \geq M\}.$$

Tällöin $S = S_0 \cup \cdots \cup S_{M-1} \cup S_{\geq M}$ ja

$$S_{\geq M} \subseteq (s_1 + \mathbb{N}^n) \cup \cdots \cup (s_r + \mathbb{N}^n).$$

Koska joukkojen $S_i$ vektoreiden ensimmäiset koordinaatit ovat kiinnitettyjä, voimme samaistaa joukon $S_i$ joukon $\mathbb{N}^{n-1}$ osajoukon kanssa, ja induktion perusteella voimme löytää äärellisen määrän vektoreita $s_1^i, \ldots, s_{r_i}^i \in S_i$, joille

$$S_i \subseteq (s_1^i + \mathbb{N}^n) \cup \cdots \cup (s_{r_i}^i + \mathbb{N}^n).$$

Nyt

$$\begin{aligned} S &= S_0 \cup \cdots \cup S_{M-1} \cup S_{\geq M} \\ &\subseteq S_0 \cup \cdots \cup S_{M-1} \cup (s_1 + \mathbb{N}^n) \cup \cdots \cup (s_r + \mathbb{N}^n) \\ &\subseteq (s_1^0 + \mathbb{N}^n) \cup \cdots \cup (s_{r_0}^0 + \mathbb{N}^n) \cup \cdots \cup (s_1^{M-1} + \mathbb{N}^n) \cup \cdots \cup (s_{r_{M-1}}^{M-1} + \mathbb{N}^n) \\ &\quad \cup S_{M-1} \cup (s_1 + \mathbb{N}^n) \cup \cdots \cup (s_r + \mathbb{N}^n), \end{aligned}$$

mikä on täsmälleen haluttu tulos, mistä väite seuraa.

**Lause 2.6.** *Termijärjestys on hyvä järjestys.*

*Todistus.* Ks. [3, s. 193].

Olkoon $S \subseteq \mathbb{N}^n$ epätyhjä osajoukko ja $\leq$ termijärjestys. Dicksonin lemman perusteella on olemassa äärellinen määrä alkioita $v_1, \ldots, v_r \in S$ siten, että

$$S \subseteq \{v_1 + \mathbb{N}^n\} \cup \cdots \cup \{v_r + \mathbb{N}^n\}.$$

Jos $v \in v_i + \mathbb{N}^n$, niin $v = v_i + w$ jollakin $w \in \mathbb{N}^n$. Tästä seuraa, että $v - v_i \in \mathbb{N}^n$. Koska termijärjestyksen määritelmän kohdan (ii) perusteella $v - v_i \geq 0$, seuraa tästä, että $v = (v - v_i) + v_i \geq v_i$ termijärjestyksen määritelmän kohdan (iii) perusteella. Tämän vuoksi alkioiden $v_i, \ldots, v_r$ pienin alkio on myös joukon $S$ pienin alkio, mistä huomataan, että $\leq$ on hyvä järjestys ja väite seuraa.

# 3 Polynomien jakoalgoritmi

Tässä luvussa esitellään usean muuttujan polynomien jakoalgoritmi, todistetaan sen toimivuus ja käydään läpi siihen liittyviä esimerkkejä. Tässä luvussa oletetaan, että $k$ on kunta.

**Lemma 3.1.** *Olkoot $S$ joukko, jossa on määritelty hyvä järjestys $\leq$ ja $F = \{s_1, s_2, \dots\}$ joukon $S$ osajoukko siten, että $s_1 \geq s_2 \geq s_3 \geq \dots$. Tällöin $F$ on äärellinen.*

*Todistus.* Ks. [3, s. 229].

Merkitään kirjaimella $s$ joukon $F$ pienintä alkiota. Koska $s \in F$, on oltava $s = s_N$ jollekin $N \in \mathbb{N}$. Koska $s_N \geq s_i$, kun $i \geq N$, seuraa tästä, että $s_N = s_i$, kun $i > N$, koska $s$ oli joukon $F$ pienin alkio. Tämän vuoksi $F$ on äärellinen ja väite seuraa.

**Määritelmä 3.1.** Olkoon

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v$$

polynomirenkaan $R[\mathbb{N}^n]$ nollasta eroava polynomi ja $\leq$ termijärjestys. Polynomin $f$ *johtava termi* järjestyksessä $\leq$ on

$$\mathrm{lt}_{\leq}(f) = a_w X^w,$$

missä $w = \max_{\leq} \{v \in \mathbb{N}^n \mid a_v \neq 0\}$. Lisäksi merkitään polynomin $f$ *johtavan termin eksponenttia*

$$\mathrm{lp}_{\leq}(f) = w,$$

missä $w = \max_{\leq} \{v \in \mathbb{N}^n \mid a_v \neq 0\}$ ja *johtavan termin kerrointa*

$$\mathrm{lc}_{\leq}(f) = a_w,$$

missä $w = \max_{\leq} \{v \in \mathbb{N}^n \mid a_v \neq 0\}$.

**Määritelmä 3.2.** Olkoon $R = k[X_1, \dots, X_n]$ polynomirengas, $\leq$ termijärjestys ja $f \in R$. Sanotaan, että polynomin $f$ *eksponenttien joukko* on

$$P(f) = \{v \mid f = \sum_{v \in \mathbb{N}^n} a_v X^v, a_v \neq 0\}.$$

**Lause 3.2.** *Olkoon $R$ kommutatiivinen rengas ja $f$, $g \in R[X_i, \dots, X_n] \setminus \{0\}$ sekä $\leq$ termijärjestys. Tällöin*

$$\mathrm{lt}_{\leq}(f+g) \leq \max(\mathrm{lt}_{\leq}(f), \mathrm{lt}_{\leq}(g)) \text{ ja}$$
$$\mathrm{lt}_{\leq}(fg) = \mathrm{lt}_{\leq}(f)\mathrm{lt}_{\leq}(g).$$

*Todistus.* Todistetaan ensin, että $\mathrm{lt}_{\leq}(f+g) \leq \max(\mathrm{lt}_{\leq}(f), \mathrm{lt}_{\leq}(g))$. Nyt $\mathrm{lt}_{\leq}(f)$ on eräs polynomin $f$ termi muotoa $a_v X^v$ ja $\mathrm{lt}_{\leq}(g)$ eräs polynomin $g$ termi muotoa $b_w X^w$. Nyt joko $v = w$, $v < w$ tai $v > w$. Oletetaan ensin, että $v \neq w$. Voidaan tällöin olettaa, että $v < w$. Tällöin polynomien yhteenlaskun määritelmän perusteella $\mathrm{lt}_{\leq}(f+g) = \mathrm{lt}_{\leq}(g)$, koska polynomi $f$ ei sisällä termiä, joka laskettaisiin yhteen termin $\mathrm{lt}_{\leq}(g)$ kanssa.

Jos $v = w$, on $\mathrm{lt}_{\leq}(f+g)$ polynomien yhteenlaskun määritelmän perusteella muotoa $(a_v + b_w)X^v$, jos $a_v + b_w \neq 0$. Tällöin $\mathrm{lp}_{\leq}(f+g) = \mathrm{lp}_{\leq}(f) = \mathrm{lp}_{\leq}(g)$. Koska termijärjestys $\leq$ vertailee ainoastaan polynomien eksponentteja, voidaan termijärjestyksen mielessä kirjoittaa $\mathrm{lt}_{\leq}(f+g) = \mathrm{lt}_{\leq}(f) = \mathrm{lt}_{\leq}(g)$. Jos $a_v + b_w = 0$, olisi $\mathrm{lt}_{\leq}(f+g) = \mathrm{lt}_{\leq}((f - \mathrm{lt}_{\leq}(f)) + (\mathrm{lt}_{\leq}(g - \mathrm{lt}_{\leq}(g))))$. Tällä tavalla voidaan tarvittaessa poistaa polynomien $f$ ja $g$ korkeimpia termejä, kunnes päästään tilanteeseen, jossa $\mathrm{lt}_{\leq}(f*) - \mathrm{lt}_{\leq}(g*) \neq 0$, kun $f*, g*$ ovat polynomeja, jotka saadaan poistamalla polynomien $f$ ja $g$ korkeimmat termit niin pitkään, kun ne ovat toistensa vasta-alkioita. Tämän jälkeen voidaan todeta, että $\mathrm{lt}_{\leq}(f+g) = \mathrm{lt}_{\leq}(f*)$ tai $\mathrm{lt}_{\leq}(f+g) = \mathrm{lt}_{\leq}(g*)$. Joka tapauksessa tällöin $\mathrm{lt}_{\leq}(f+g) < \mathrm{lt}_{\leq}(f)$ ja $\mathrm{lt}_{\leq}(g)$. On siis oltava $\mathrm{lt}_{\leq}(f+g) \leq \max(\mathrm{lt}_{\leq}(f), \mathrm{lt}_{\leq}(g))$.

Todistetaan sitten, että $\mathrm{lt}_{\leq}(fg) = \mathrm{lt}_{\leq}(f)\mathrm{lt}_{\leq}(g)$. Nyt $\mathrm{lt}_{\leq}(f)$ on muotoa $a_v X^v$ ja $\mathrm{lt}_{\leq}(g)$ on muotoa $a_w X^w$. Polynomien kertolaskun määritelmän perusteella tiedetään, että $a_v X^v a_w X^w = (a_v a_w) X^{v+w}$. Toisaalta $\mathrm{lt}_{\leq}(fg)$ on muotoa $(ab)X^{v_f + w_g}$, missä $v_f \in P(f)$ ja $w_g \in P(g)$. Nyt määritelmän perusteella $v$ on joukon $P(f)$ suurin alkio ja $w$ on joukon $P(g)$ suurin alkio. Toisaalta $v_f + w_g$ on joukon $P(f+g) = \{a + b \mid a \in P(f), b \in P(g)\}$ suurin alkio. Koska $\leq$ on termijärjestys, voidaan valita mitkä tahansa alkiot $x_g \in P(g), v_i \in P(f)$ ja huomataan, että $v_i + x_g \leq v + x_g$, joten selvästi $v = v_f$. Samoin voidaan valita mitkä tahansa alkiot $x_f \in P(f), w_i \in P(g)$ ja huomataan, että $x_f + w_i \leq x_f + w$, joten samoin $w = w_g$, eli $v + w$ on joukon $P(f+g)$ suurin alkio, joten $\mathrm{lt}_{\leq}(fg) = \mathrm{lt}_{\leq}(f)\mathrm{lt}_{\leq}(g)$ ja väite seuraa.

**Määritelmä 3.3.** Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys ja $f, g, h \in R$, missä $g \neq 0$. Sanotaan, että $f$ *supistuu polynomiin* $h$ modulo $g$ *yhden askeleen*, jos ja vain jos $\mathrm{lp}_{\leq}(g)$ jakaa jonkin $w \in P(f)$ ja

$$h = f - \frac{a_w X^w}{\mathrm{lt}_{\leq}(g)} g,$$

missä $A_w X^w$ on jokin polynomin $f$ termi. Supistumista merkitään

$$f \to_g h.$$

**Esimerkki 3.1.** Olkoot $f, g \in \mathbb{Q}[X, Y]$ ja $f = 6X^2Y - X + 4Y^3 - 1$, $g = 2XY + Y^3$ ja $\leq$ sanakirjajärjestys. Nyt $f \to_g h$, kun $h = -3XY^3 - X + 4Y^3 - 1$,

koska ensinnäkin $\mathrm{lp}_{\leq}(g) = XY$ jakaa alkion $X^2Y$ ja

$$\begin{aligned} h &= f - \frac{6X^2Y}{\mathrm{lt}_{\leq}(g)}g \\ &= 6X^2Y - X + 4Y^3 - 1 - \frac{6X^2Y}{2XY}(2XY + Y^3) \\ &= 6X^2Y - X + 4Y^3 - 1 - 3X(2XY + Y^3) \\ &= 6X^2Y - X + 4Y^3 - 1 - 6X^2Y - 3XY^3 \\ &= -3XY^3 - X + 4Y^3 - 1. \end{aligned}$$

**Määritelmä 3.4.** Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys ja
$f, h, f_1, \ldots, f_s \in R$, missä $f_i \neq 0 (1 \leq i \leq s)$ ja olkoon $F = \{f_1 \ldots, f_s\}$. Sanotaan, että $f$ *supistuu polynomiin* $h$ *modulo* $F$, jos ja vain jos on olemassa indeksit $i_1, i_2, \ldots i_t \in \{1, \ldots, s\}$ ja polynomit $h_1, \ldots, h_{t-1} \in R$, joille pätee

$$f \to_{f_{i_1}} h_1 \to_{f_{i_2}} h_2 \to_{f_{i_3}} \cdots \to_{f_{i_{t-1}}} h_{t-1} \to_{f_{i_t}} h.$$

Tätä merkitään

$$f \to_F h.$$

**Esimerkki 3.2.** Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys ja

$$\begin{aligned} f &= X^2Y^3 + XY^4 \\ f_1 &= X^2Y + X \\ f_2 &= X + Y \text{ ja} \\ f_3 &= X + Y^3 \end{aligned}$$

sekä $F = \{f_1, f_2, f_3\}$. Nyt $f \to_F 0$, koska

$$f \to_{f_1} XY^4 - XY^2 \to_{f_2} -XY^2 - Y^5 \to_{f_3} 0,$$

koska

$$\begin{aligned} & X^2Y^3 + XY^4 - \frac{X^2Y^3}{X^2Y}(X^2Y + X) \\ = {} & X^2Y^3 + XY^4 - Y^2(X^2Y + X) \\ = {} & XY^4 - XY^2, \end{aligned}$$

$$\begin{aligned} & XY^4 - XY^2 - \frac{XY^4}{X}(X + Y) \\ = {} & XY^4 - XY^2 - Y^4(X + Y) \\ = {} & -XY^2 - Y^5 \end{aligned}$$

ja

$$\begin{aligned} & -XY^2 - Y^5 - \frac{-XY^2}{X}(X + Y^3) \\ = & -XY^2 - Y^5 + Y^2(X + Y^3) \\ = & \ 0. \end{aligned}$$

**Määritelmä 3.5.** Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys ja $F = \{f_1, \ldots, f_s\} \subseteq R, f_i \neq 0, i = 1, \ldots, s$. Polynomia $r \in R$ sanotaan *supistetuksi polynomien $F$ suhteen* , jos $r = 0$, tai yksikään $w \in P(r)$ ei ole jaollinen yhdelläkään alkiolla $\mathrm{lp}_{\leq}(f_i), i = 1, \ldots, s$. Toisin sanoen $r$ ei supistu modulo $F$.

**Määritelmä 3.6.** Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys, $f, r \in R$ ja $F = \{f_1, \ldots, f_s\} \subseteq R, f_i \neq 0, i = 1, \ldots, s$. Jos $f \to_F r$ ja $r$ on supistunut polynomien $F$ suhteen, sanotaan, että $r$ on *polynomin $f$ jakojäännös* polynomien $F$ suhteen.

**Algorigmi 3.1.** (Jakoalgoritmi) Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas ja $\leq$ termijärjestys.

**INPUT:** $f, f_1, \ldots, f_s \in R$, missä $f_i \neq 0$ $(1 \leq i \leq s)$

**OUTPUT:** $u_1, \ldots, u_s, r \in R$, joille $f = u_1 f_1 + \cdots + u_s f_s + r$
ja $r$ on supistettu polynomien $\{f_1, \ldots, f_s\}$ suhteen ja
$max(\mathrm{lp}_{\leq}(u_1)\mathrm{lp}_{\leq}(f_1), \ldots, \mathrm{lp}_{\leq}(u_s)\mathrm{lp}_{\leq}(f_s), \mathrm{lp}_{\leq}(r)) = \mathrm{lp}_{\leq}(f)$

**INITIALIZATION** $u_1 := 0, u_2 := 0, \ldots, u_s := 0, r := 0, h := f$

**WHILE** $h \neq 0$ **DO**

**IF** on olemassa $i$, jolla $\mathrm{lp}_{\leq}(f_i)$ jakaa alkion $\mathrm{lp}_{\leq}(h)$, **THEN**
valitaan pienin sellainen $i$, jolla $\mathrm{lp}_{\leq}(f_i)$ jakaa alkion $\mathrm{lp}_{\leq}(h)$
$u_i := u_i + \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)}$
$h := h - \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)} f_i$

**ELSE**
$r := r + \mathrm{lt}_{\leq}(h)$
$h := h - \mathrm{lt}_{\leq}(h)$

**Lause 3.3.** *Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas, $\leq$ termijärjestys, $f \in R$ ja $F = \{f_1, \ldots, f_s\} \subseteq R, f_i \neq 0, i = 1, \ldots, s$. Jakoalgoritmi, algorigmi 3.1, tuottaa polynomit $u_1, \ldots, u_s, r \in R$, joille*

$$f = u_1 f_1 + \cdots + u_s f_s + r,$$

*missä $r$ on supistettu polynomien $F$ suhteen ja*

$$\mathrm{lp}_{\leq}(f) = \max(\max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)).$$

*Todistus.* Ks. [1, s. 31] Täytyy siis todistaa, että ensinnäkin algoritmi 3.1 päättyy. Lisäksi on todistettava, että algoritmi tuottaa väitteen mukaisen tuloksen. Lopuksi on todistettava, että $r$ supistuu polynomien $F$ suhteen ja että

$$\mathrm{lp}_{\leq}(f) = \max(\max_{1\leq i\leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)).$$

Todistetaan ensin, että algorigmin 3.1 suoritus päättyy. Huomataan ensin, että tämä vaatii sen, että päästään tilanteeseen, jossa $h = 0$. Kussakin vaiheessa algoritmin suoritusta polynomin $h$ johtava termi vähennetään, kunnes tätä ei voida enää tehdä. Jokaisessa algoritmin suorituskerrassa saadaan polynomi $h$ edellisen suorituskerran polynomista $h$. Jos kunkin suoritusvaiheen lukumäärää merkitään polynomin $h$ alaindeksinä, saadaan kutakin kertaa vastaava jono polynomeja $h_1, h_2, \ldots,$, missä polynomi $h_{i+1}$ saadaan polynomista $h_i$ vähentämällä $\mathrm{lt}_{\leq}(h_i)$, ja jos jokin $\mathrm{lp}_{\leq}(f_j)$ jakaa alkion $\mathrm{lp}_{\leq}(h_i)$, mahdollisesti alempia termejä, eli

$$h_{i+1} = h_i - \mathrm{lt}_{\leq}(h_i) + \text{alempia termejä},$$

joten jokaisella $i$ $\mathrm{lp}_{\leq}(h_{i+1}) < \mathrm{lp}_{\leq}(h_i)$. Koska lauseen 2.6 perusteella järjestys $\leq$ on hyvä järjestys, tiedetään, että jossain vaiheessa polynomien $h_i$ jono päättyy ja algoritmin suoritus on valmis.

Todistetaan sitten, että algoritmi 3.1 tuottaa halutun tuloksen. Algoritmin alkutilassa voidaan kirjoittaa $f = u_1f_1+u_2f_2+\cdots+u_sf_s+r+h$, koska $h = f$ ja kaikki muut termit ovat nollia. Kullakin suorituskerralla joko polynomi $\mathrm{lp}_{\leq}(f_i)$ jakaa tai ei jaa polynomia $\mathrm{lp}_{\leq}(h)$. Jos $\mathrm{lp}_{\leq}(f_i)$ jakaa polynomin $\mathrm{lp}_{\leq}(h)$ ja $i$ on pienin tällainen luku, tässä esitetty lauseke polynomille $f$ ei muutu, koska

$$u_i := u_i + \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)} \text{ ja}$$
$$h := h - \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)} f_i,$$

jolloin polynomin $f$ lauseke muuttuu muotoon

$$f = u_1f_1 + \cdots + (u_i + \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)})f_i + \ldots u_sf_s + r + (h - \frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)}f_i),$$

eli lausekkeeseen on lisätty ja siitä on vähennetty saman verran. Jos taas $\mathrm{lp}_{\leq}(f_i)$ ei jaa polynomia $\mathrm{lp}_{\leq}(h)$ millään $i$, niin polynomin $f$ lauseke muuttuu muotoon

$$f = u_1f_1 + u_2f_2 + \cdots + u_sf_s + (r + \mathrm{lt}_{\leq}(h)) + (h - \mathrm{lt}_{\leq}(h)),$$

eli lausekkeeseen on jälleen lisätty ja siitä on vähennetty saman verran. Algoritmi siis tuottaa väitteen mukaisen lausekkeen.

Huomataan, että $r$ on supistunut polynomien $F$ suhteen, koska joko $r = 0$ tai algoritmin 3.1 ehdoista seuraa suoraan, että yksikään $w \in P(r)$ ei ole jaollinen yhdelläkään alkiolla $\mathrm{lp}_{\leq}(f_i), i = 1, \ldots, s$, koska jokainen polynomin

$r$ termi on jokin termi $\mathrm{lt}_{\leq}(h_i)$ ja tiedetään, ettei mikään $\mathrm{lp}_{\leq}(h_i)$ ole jaollinen alkioilla $\mathrm{lp}_{\leq}(f_i), i = 1, \ldots, s$.

Lopuksi todistetaan, että

$$\mathrm{lp}_{\leq}(f) = \max(\max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)).$$

Huomataan, että koska algoritmin alkutilassa $h = f$, on algoritmin jokaisessa vaiheessa oltava $\mathrm{lp}_{\leq}(h) \leq \mathrm{lp}_{\leq}(f)$. Nyt jokaisella $i$ termi $u_i$ on joko nolla, tai se saadaan lisäämällä siihen

$$\frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)},$$

jolloin termi muuttuu muotoon

$$\frac{\mathrm{lt}_{\leq}(h)}{\mathrm{lt}_{\leq}(f_i)})f_i,$$

mistä huomataan, että tällöin $\mathrm{lt}_{\leq}(h)$ supistuu termistä aidosti pienemmäksi termiksi. On siis tällöin oltava $\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i) \leq \mathrm{lp}_{\leq}(f)$. Lisäksi termi $r$ muodostuu lisäämällä siihen termejä $\mathrm{lt}_{\leq}(h_i)$, joten $\mathrm{lp}_{\leq}(r) \leq \mathrm{lp}_{\leq}(f)$. On siis oltava

$$\mathrm{lp}_{\leq}(f) \geq \max(\max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)).$$

Toisaalta, koska $f = u_1 f_1 + \cdots + u_s f_s + r$, ei voi olla $\mathrm{lp}_{\leq}(f) > \mathrm{lp}_{\leq}(u_1 f_1 + \cdots + u_s f_s + r)$, joten on oltava

$$\mathrm{lp}_{\leq}(f) = \max(\max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)),$$

ja väite seuraa.

**Esimerkki 3.3.** Olkoon $R[X_1, \ldots, X_n] = \mathbb{Q}[X, Y]$ ja $\leq$ sanakirjajärjestys. Olkoot sitten $f = X^4 + Y^2$ sekä $f_1 = X^3 - Y$ ja $f_2 = Y^2 + XY$. Jaetaan polynomi $f$ polynomeilla $f_1$, $f_2$ käyttäen jakoalgoritmia.
INITIALIZATION: $u_1 := 0, u_2 := 0, r := 0, h := f = X^4 + Y^2$
Käydään läpi WHILE-silmukka ensimmäisen kerran:

$X^3 = \mathrm{lp}_{\leq}(f_1)$ jakaa alkion $X^4 = \mathrm{lp}_{\leq}(h)$

$u_1 := 0 + \frac{X^4}{X^3} = X$

$h := h - \frac{X^4}{X^3}(X^3 - Y) = X^4 + Y^2 - X^4 + XY = Y^2 + XY$

Koska $h \neq 0$, käydään läpi WHILE-silmukka toisen kerran:

$Y^2 = \mathrm{lp}_{\leq}(f_2)$ jakaa alkion $Y^2 = \mathrm{lp}_{\leq}(h)$

$u_2 := 0 + \frac{Y^2}{Y^2} = 1$

$h := h - \frac{Y^2}{Y^2}(Y^2 + XY) = Y^2 + XY - Y^2 - YX = 0$

Koska $h = 0$, on algoritmin suoritus valmis ja voidaan kirjoittaa

$$\begin{aligned} f &= u_1 f_1 + u_2 f_2 + r \\ &= X(X^3 - Y) + 1(Y^2 + XY). \end{aligned}$$

**Esimerkki 3.4.** Edellisen esimerkin jakolaskussa ei ole merkitystä sillä, missä järjestyksessä jakolaskun suorittaa. On kuitenkin helppo havaita, että tämä ei yleisesti pidä paikkaansa. Olkoot edelleen $R[X_1, \ldots, X_n] = \mathbb{Q}[X, Y]$ ja $\leq$ sanakirjajärjestys sekä $f = X^4 + Y^2$. Olkoot sitten $f_1 = X + Y$ ja $f_2 = X - Y$. Jaetaan polynomi $f$ polynomeilla $f_1$, $f_2$ käyttäen jakoalgorigmia:
INITIALIZATION: $u_1 := 0, u_2 := 0, r := 0, h := f = X^4 + Y^2$
Käydään läpi WHILE-silmukka ensimmäisen kerran:

$X = \mathrm{lp}_{\leq}(f_1) = X$ jakaa alkion $X^4 = \mathrm{lp}_{\leq}(h)$

$u_1 := 0 + \frac{X^4}{X} = X^3$

$h := h - \frac{X^4}{X}(X + Y) = X^4 + Y^2 - X^4 - X^3Y = -X^3Y + Y^2$

Koska $h \neq 0$, käydään läpi WHILE-silmukka toisen kerran:

$X = \mathrm{lp}_{\leq}(f_1) = X$ jakaa alkion $X^3Y = \mathrm{lp}_{\leq}(h)$

$u_1 := X^3 + \frac{-X^3Y}{X} = X^3 - X^2Y$

$h := h - \frac{-X^3Y}{X}(X + Y) = -X^3Y + Y^2 + X^3 + X^2Y = X^2Y^2 + Y^2$

Koska $h \neq 0$, käydään läpi WHILE-silmukkaa kolmannen kerran:

$X = \mathrm{lp}_{\leq}(f_1) = X$ jakaa alkion $X^2Y^2 = \mathrm{lp}_{\leq}(h)$

$u_1 := X^3 - X^2Y + \frac{X^2Y^2}{X} = X^3 - X^2Y + XY^2$

$h := h - \frac{X^2Y^2}{X}(X + Y) = X^2Y^2 + Y^2 - \frac{X^2Y^2}{X}(X + Y) = X^2Y^2 + Y^2 - X^2Y^2 - XY^3 = -XY^3 + Y^2$

Koska $h \neq 0$, käydään läpi WHILE-silmukkaa neljännen kerran:

$X = \mathrm{lp}_{\leq}(f_1) = X$ jakaa alkion $-XY^3 = \mathrm{lp}_{\leq}(h)$

$u_1 := X^3 - X^2Y + XY^2 + \frac{-XY^3}{X} = X^3 - X^2Y + XY^2 - Y^3$

$h := h - \frac{-XY^3}{X}(X + Y) = -XY^3 + Y^2 + XY^3 + Y^4 = Y^4 + Y^2$

Koska $h \neq 0$, käydään läpi WHILE-silmukkaa viidennen kerran:

$\mathrm{lp}_{\leq}(f_1)$ tai $\mathrm{lp}_{\leq}(f_2)$ ei jaa alkiota $Y^4 = \mathrm{lp}_{\leq}(h)$

$r := 0 + Y^4$

$h := Y^4 + Y^2 - Y^4 = Y^2$

Koska $h \neq 0$, käydään läpi WHILE-silmukkaa kuudennen kerran:

$\mathrm{lp}_{\leq}(f_1) = X$ tai $\mathrm{lp}_{\leq}(f_2) = X$ ei jaa alkiota $Y^2 = \mathrm{lp}_{\leq}(h)$

$r := Y^2 + Y^2$

$h := Y^2 - Y^2 = 0$

Koska $h = 0$, on algoritmin suoritus valmis ja voidaan kirjoittaa:

$$\begin{aligned} f &= (X^3 - X^2Y + XY^2 - Y^3)(X + Y) + 0(X - Y) + Y^4 + Y^2 \\ &= (X^3 - X^2YXY^2 - Y^3)(X + Y) + Y^4 + Y^2. \end{aligned}$$

Jos kuitenkin jaettavien järjestystä vaihdettaisiin, eli olisi $f_1 = X - Y$ ja $f_2 = X + Y$, niin vastaavalla jakoalgoritmin käytöllä saataisiin polynomi $f$ muotoon

$$f = (X^3 + X^2Y + XY^2 + Y^4)(X - Y) + Y^4 + Y^2.$$

**Korollaari 3.4.** *Olkoot $R = k[X_1, \ldots, X_n]$ polynomirengas, $f \in R$ ja $F = \{f_1, \ldots, f_s\} \subseteq R$. Jos $f \to_F 0$, niin*

$$\begin{aligned} &f = u_1 f_1 + \cdots + u_s f_s \text{ ja} \\ &\mathrm{lp}_{\leq}(f) = \max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)). \end{aligned}$$

*Todistus.* Jaetaan polynomi $f$ polynomeilla $F$ jakoalgoritmin avulla. Nyt on olemassa $h_1 \in R$, jolle $f \to_{f_1} h_1$. Tällöin tiedetään, että $\mathrm{lp}_{\leq}(f_1)$ jakaa termin $\mathrm{lp}_{\leq}(h) = \mathrm{lp}_{\leq}(f)$. Tällöin suoritettaessa jakoalgoritmin ensimmäistä askelta

$$\begin{aligned} h &:= f - \frac{\mathrm{lt}_{\leq}(f)}{\mathrm{lt}_{\leq}(f_1)} f_1 = h_1 \text{ ja} \\ u_1 &:= \frac{\mathrm{lt}_{\leq}(f)}{\mathrm{lt}_{\leq}(f_1)}. \end{aligned}$$

Samoin on olemassa $h_2 \in R$ ja tiedetään, että $h_1 \to_{f_2} h_2$ ja edellisen askeleen periaatteella voidaan jakoalgoritmin toisessa askeleessa suoraan kirjoittaa

$$\begin{aligned} h &= h_2 \text{ ja} \\ u_2 &:= \frac{\mathrm{lt}_{\leq}(h_1)}{\mathrm{lt}_{\leq}(f_2)}. \end{aligned}$$

Näin voidaan jatkaa koko algoritmi loppuun, ja koska $f \to_F 0$, löydetään jokaisella askeleella $i$ polynomi $f_i$, jonka korkein eksponentti jakaa kulloisenkin polynomin $h_i$ korkeimman eksponentin. Näin päästään lopulliseen tilanteeseen

$$f = u_1 f_1 + \cdots + u_s f_s.$$

Lisäksi lauseen 3.3 perusteella tiedetään, että on oltava

$$\begin{aligned} \mathrm{lp}_{\leq}(f) &= \max(\max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \mathrm{lp}_{\leq}(r)) \\ &= \max_{1 \leq i \leq s}(\mathrm{lp}_{\leq}(u_i)\mathrm{lp}_{\leq}(f_i)), \end{aligned}$$

mistä väite seuraa.

# 4 Gröbnerin kannat ja Hilbertin kantalause

Tässä luvussa esitellään tutkielman oleellisin käsite eli Gröbnerin kanta. Lisäksi todistetaan Hilbertin kantalause ja osoitetaan, että jokaisella ideaalilla on Gröbnerin kanta. Tässä luvussa oletetaan, että $k$ on kunta.

**Määritelmä 4.1.** Olkoon $\leq$ termijärjestys. Joukkoa nollasta eroavia polynomeja

$$F = \{f_1, \ldots, f_m\} \subseteq k[X_1, \ldots, X_n]$$

sanotaan *ideaalin $I$ Gröbnerin kannaksi* polynomirenkaassa $k[X_1, \ldots, X_n]$, jos $F \subseteq I$ ja kaikille $f \in I \setminus \{0\}$ pätee

$$\mathrm{lt}_{\leq}(f_i) \mid \mathrm{lt}_{\leq}(f)$$

joillakin $i = 1, \ldots, m$. Joukkoa $F$ kutsutaan *termijärjestyksen $\leq$ Gröbnerin kannaksi*, jos se on ideaalin $\langle f_1, \ldots f_m \rangle$ Gröbnerin kanta.

**Määritelmä 4.2.** Olkoon $S \subseteq k[X_1, \ldots, X_n]$ja $\leq$ termijärjestys. Joukon $S$ *johtavien termien virittämä ideaali* on joukko

$$LT_{\leq}(S) = \langle \mathrm{lt}_{\leq}(s) | s \in S \rangle .$$

**Lause 4.1.** *Olkoon $\leq$ termijärjestys, $I \neq \{0\}$ ideaali polynomirenkaassa $k[X_1, \ldots, X_n]$ ja $G = \{g_1, \ldots, g_m\} \subseteq I$ joukko nollasta eroavia polynomeja. Tällöin seuraavat väitteet ovat yhtäpitäviä:*

*(i)* $G$ *on ideaalin $I$ Gröbnerin kanta.*

*(ii)* $f \in I$, *jos ja vain jos* $f \to_G 0$.

*(iii)* $f \in I$, *jos ja vain jos* $f = \sum_{i=1}^{t} h_i g_i$, *missä*
$\mathrm{lp}_{\leq}(f) = \max_{1 \leq i \leq t}(\mathrm{lp}_{\leq}(h_i)\mathrm{lp}_{\leq}(g_i))$.

*(iv)* $\mathrm{LT}_{\leq}(G) = \mathrm{LT}_{\leq}(I)$.

*Todistus.* Ks. [1, s. 33] Oletetaan ensin, että kohta *(i)* pitää paikkansa. Olkoon tällöin $f \in k[X_1, \ldots, X_n]$. Tällöin Lauseen 3.3 (jakoalgoritmi) mukaan, kun $f$ jaetaan polynomeilla $G$, on olemassa supistunut $r \in k[X_1, \ldots, X_n]$ siten, että $f \to_G r$. Koska ideaalin ominaisuuksien perusteella $f - r \in I$, niin $f \in I$, jos ja vain jos $r \in I$. Selvästi jos $r = 0$, eli $f \to_G 0$, niin $f \in I$, mikä todistaa ekvivalenssin toisen suunnan. Jos taas $f \in I$ ja oletetaan vastoin alkuperäistä väitettä, että $r \neq 0$, niin $r \in I$ ja kohdan *(i)* perusteella on olemassa $i \in \{1, \ldots, t\}$ siten, että $\mathrm{lp}_{\leq}(g_i)$ jakaa termin $\mathrm{lp}_{\leq}(r)$. Tämä on ristiriita, koska $r$

on supistunut polynomien $G$ suhteen ja on siis oltava $r = 0$ ja $f \to_G 0$. On siis osoitettu, että kohdasta *(i)* seuraa kohta *(ii)*.

Oletetaan sitten, että kohta *(ii)* pitää paikkansa. Tällöin jos $f \in I$, on myös oltava $f \to_G 0$. Nyt korollaarista 3.4 seuraa välittömästi haluttu tulos, eli

$$f = \sum_{i=1}^{t} h_i g_i \text{ ja}$$
$$\mathrm{lp}_{\leq}(f) = \max_{1 \leq i \leq t}(\mathrm{lp}_{\leq}(h_i)\mathrm{lp}_{\leq}(g_i)).$$

On siis osoitettu, että kohdasta *(ii)* seuraa kohta *(iii)*.

Oletetaan sitten, että kohta *(iii)* pitää paikkansa. Tällöin, koska $G \subseteq I$, selvästi $\mathrm{LT}_{\leq}(G) \subseteq \mathrm{LT}_{\leq}(I)$. Toisen suunnan inkluusion osoittamiseksi riittää näyttää, että kaikille $f \in I$ $\mathrm{lt}_{\leq}(f) \in \mathrm{LT}_{\leq}(G)$, koska $\mathrm{LT}_{\leq}(I)$ koostuu kaikista termeistä $\mathrm{lt}_{\leq}(f)$. Kirjoittamalla $f$ kohdan *(iii)* mukaiseksi saadaan suoraan tulokseksi

$$\mathrm{lt}_{\leq}(f) = \sum_{i} \mathrm{lt}_{\leq}(h_i)\mathrm{lt}_{\leq}(g_i),$$

missä summa on yli kaikkien niiden lukujen $i$, joilla $\mathrm{lp}_{\leq}(f) = \mathrm{lp}_{\leq}(h_i)\mathrm{lp}_{\leq}(g_i)$, mistä seuraa suoraan ideaalin ominaisuuksien perusteella, että
$\mathrm{lt}_{\leq}(f) \in \mathrm{LT}_{\leq}(G)$. On siis osoitettu, että kohdasta *(iii)* seuraa kohta *(iv)*.

Oletetaan sitten, että kohta *(iv)* pitää paikkansa. Olkoon tällöin $f \in I$. Tällöin $\mathrm{lt}_{\leq}(f) \in \mathrm{LT}_{\leq}(G)$ ja siten

$$(*) \qquad \mathrm{lt}_{\leq}(f) = \sum_{i=1}^{t} h_i \mathrm{lt}_{\leq}(g_i)$$

jollakin $h_i \in k[X_1, \ldots, X_n]$. Jos yhtälön (*) oikeaa puolta lasketaan auki, huomataan, että jokainen termi on jaollinen jollakin termillä $\mathrm{lt}_{\leq}(g_i)$. Samoin yhtälön (*) vasemman puolen ainoa termi, $\mathrm{lt}_{\leq}(f)$, on jaollinen jollakin termillä $\mathrm{lt}_{\leq}(g_i)$, joten Gröbnerin kannan määritelmän mukaan $G$ on ideaalin $I$ Gröbnerin kanta. On siis osoitettu, että kohdasta *(iv)* seuraa kohta *(i)* ja väite seuraa.

*Merkintä.* Olkoon $f \in k[X_1, \ldots, X_N]$ polynomi ja $H \subseteq k[X_1, \ldots, X_N]$. Merkitään $f^H = r$, missä $r$ on jakojäännös, kun polynomi $f$ jaetaan polynomeilla $H$.

**Lause 4.2.** *Olkoon $\leq$ termijärjestys ja $G = \{f_1, \ldots, f_m\}$ ideaalin $I = \langle f_1, \ldots, f_m \rangle$ Gröbnerin kanta. Polynomille $f \in k[X_1, \ldots, X_n]$ pätee*

$$f \in I \Leftrightarrow f^G = 0.$$

*Todistus.* Ks. [3, s. 197]. Oletetaan ensin, että $f^G = 0$. Tällöin polynomien algoritmin 3.1, jakoalgoritmin, perusteella

$$f = a_1 f_1 + \cdots + a_m f_m$$

ja ideaalien ominaisuuksien perusteella

$$f \in I = \langle f_1, \ldots, f_m \rangle .$$

Oletetaan sitten, että $f \in I$. Jakoalgoritmin perusteella tiedetään, että $f$ voidaan esittää muodossa $f = a_1 f_1 + \cdots + a_m f_m + f^G$. Tästä saadaan

$$f^G = f - a_1 f_1 - \ldots a_m f_m \in I.$$

Jos $f^G \neq 0$, on olemassa jokin $\mathrm{lt}_{\leq}(f_i)$, joka jakaa termin $\mathrm{lt}_{\leq}(r)$, koska $\{f_1, \ldots, f_m\}$ on ideaalin $I$ Gröbnerin kanta. Tämä taas on ristiriidassa sen kanssa, että $f^G$ on jakojäännös, kun $f$ jaetaan polynomijoukolla $G$. Täten on oltava $f^G = 0$ ja väite seuraa.

**Korollaari 4.3.** *Olkoon $\leq$ termijärjestys ja $G = \{f_1, \ldots, f_m\} \subseteq R = k[X_1, \ldots, X_N]$ ideaalin $I \subseteq R$ Gröbnerin kanta. Tällöin $I = \langle f_1, \ldots, f_m \rangle$.*

*Todistus.* Ks. [3, s. 198]. Koska $f_1, \ldots, f_m \in I$, voidaan kirjoittaa $\langle f_1, \ldots, f_m \rangle \subseteq I$. Kuitenkin jos $f \in I$, on polynomien jakoalgoritmin sekä Lauseen 4.2 perusteella oltava $f^G = 0$ ja $f = a_1 f_1 + \cdots + a_m f_m$ sopivilla $a_1, \ldots, a_m \in k[X_1, \ldots, X_n]$. Tämä osoittaa, että $I \subseteq \langle f_1, \ldots, f_m \rangle$, ja väite seuraa.

**Lause 4.4.** *Olkoon $\leq$ termijärjestys ja $G = \{f_1, \ldots, f_m\} \subseteq k[X_1, \ldots, X_n]$ Gröbnerin kanta. Tällöin jakojäännös $r$ polynomien jakoalgoritmin, algoritmin 3.1, mukaisessa muodossa $f = a_1 f_1 + \cdots + a_m f_m$ on yksikäsitteinen jokaisella $f \in k[X_1, \ldots, X_n]$. Jakojäännös ei ole riippuvainen jakajien $f_1, \ldots, f_m$ järjestyksestä Gröbnerin kannassa $G$.*

*Todistus.* Ks. [3, s. 198]. Olkoon $f \in k[X_1, \ldots, X_n]$, ja oletetaan väitteen vastaisesti, että polynomille $f$ on olemassa kaksi eri jakoalgoritmin mukaista esitystä, eli $f = a_1 f_1 + \cdots + a_m f_m + r_1 = a_1' f_1 + \cdots + a_m' f_m + r_2$. Tällöin

$$r_2 - r_1 = (a_1 - a_1')f_1 + \cdots + (a_m - a_m')f_m.$$

Tällöin $r_2 - r_1 \in \langle f_1, \ldots f_m \rangle$. Jos $r_2 - r_1 \neq 0$, niin tällöin on olemessa sellainen $i$, että $\mathrm{lt}_{\leq}(f_i)$ jakaa termin $\mathrm{lt}_{\leq}(r_2 - r_1)$. Tästä seuraa, että $\mathrm{lt}_{\leq}(f_i)$ jakaa joko termin $r_1$ tai termin $r_2$, mikä on selvä ristiriita.

Joukon $G$ alkioiden permutaatio $G'$ tuottaa polynomille $f$ jakoalgoritmin mukaisen muodon $f = b_1 f_1 + \ldots b_m f_m + f^{G'}$. Tästä seuraa, että $f^{G'} = f^G$, sillä edellä osoitettiin, että jakojäännökset ovat samat, ja tästä väite seuraa.

**Lause 4.5.** *Olkoon $\leq$ termijärjestys ja $I \subseteq k[X_1, \ldots, X_n]$ ideaali. Tällöin ideaalilla $I$ on Gröbnerin kanta termijärjestyksessä $\leq$.*

*Todistus.* Ks. [3, s. 199] Olkoon

$$S = \{v \in \mathbb{N}^n \mid a_v X^v = \mathrm{lt}_{\leq}(f) \text{ jollakin } \ f \ \in \ I\} \ \subseteq \ \mathbb{N}^n.$$

Koska $S \subseteq \mathbb{N}^n$, tiedetään Dicksonin lemman perusteella, että on olemassa äärellinen määrä alkioita $f_1, \ldots, f_m \in I$, joille

$$S \subseteq \{v_1 + \mathbb{N}^n\} \cup \cdots \cup \{v_m + \mathbb{N}^n\},$$

missä $a_{v_i} X^{v_i} = \mathrm{lt}_{\leq}(f_i)$, kun $i = 1, \ldots, m$. Oletetaan sitten, että $aX^w = \mathrm{lt}_{\leq}(f)$, missä $f \in I$. Tällöin $w = v_j + v$ sopivalla $j = 1, \ldots, m$ ja $v \in \mathbb{N}^n$. Tämä todistaa sen, että $X^w = X^{v_j} X^v$, ja tämän seurauksena sen, että $\mathrm{lt}_{\leq}(f_j) \mid \mathrm{lt}_{\leq}(f)$, mikä on täsmälleen määritelmän mukaisesti vaadittava ehto sille, että $\{f_1, \ldots, f_m\}$ on ideaalin $I$ Gröbnerin kanta, ja väite seuraa.

**Lause 4.6.** *(Hilbertin kantalause) Olkoon $I$ mielivaltainen ideaali polynomirenkaassa $k[X_1, \ldots, X_n]$. Tällöin on olemassa äärellinen määrä polynomeja $f_1, \ldots, f_m \in I$ siten, että jokainen polynomi $f \in I$ voidaan kirjoittaa muodossa*

$$f = a_1 f_1 + \cdots + a_m f_m$$

*sopivilla $a_1, \ldots, a_m \in k[X_1, \ldots, X_n]$ ($I = \langle f_1, \ldots, f_m \rangle$).*

*Todistus.* Väite seuraa suoraan Lauseesta 4.5 ja Korollaarista 4.3.

**Korollaari 4.7.** *Olkoon $\leq$ termijärjestys, $I$ mielivaltainen ideaali polynomirenkaassa $k[X_1, \ldots, X_n]$ ja $G = \{g_1, \ldots, g_s\}$ sen Gröbnerin kanta. Tällöin*

$$\langle g_1, \ldots, g_s \rangle = I$$

*Todistus.* Ks. [2, s. 77] Olkoon $g_i \in G$. Tällöin ensinnäkin $g_i \in I$ ja toisaalta koska $I$ on ideaali, on oltava $hg_i \in I$ kaikilla $h \in k[X_1, \ldots, X_n]$. On siis oltava $\langle g_1, \ldots, g_s \rangle \subseteq I$.

Olkoon sitten $h \in I$. Jaetaan jakoalgoritmin avulla $f$ polynomeilla $\langle g_1, \ldots, g_s \rangle$. Tällöin saadaan

$$f = a_1 g_1 + \ldots, a_s g_s + r,$$

missä yksikään polynomin $r$ termeistä ei ole jaollinen termeillä $\mathrm{lt}_{\leq}(g_1), \ldots, \mathrm{lt}_{\leq}(g_s)$. Nyt riittää osoittaa, että $r = 0$, koska tällöin $\langle g_1, \ldots, g_s \rangle$ virittää minkä tahansa ideaalin $I$ polynomin. Huomataan ensin, että

$$r = f - a_i g_i - \cdots - a_s g_s \in I$$

ideaalien ominaisuuksien perusteella. Jos olisi $r \neq 0$, niin lauseen 4.1 kohdan (ii) perusteella tiedetään, että $r \to_G 0$, mikä tarkoittaa, että $r$ on jaollinen jollain polynomilla $\mathrm{lt}_{\leq}(g_i)$. Tämä on ristiriita sen tiedon kanssa, että $r$ on jakojäännös, ja on siis oltava $r = 0$ ja tällöin

$$f = a_1 g_1 + \cdots + a_s g_s \in \langle g_1, \ldots, g_s \rangle,$$

ja silloin on oltava $I \subseteq \langle g_1, \ldots, g_s \rangle$ ja täten $I = \langle g_1, \ldots, g_s \rangle$, ja väite seuraa.

# 5 S-polynomit ja Buchbergerin algoritmi

Edellä esitettiin Gröbnerin kannat ja todistettiin niiden olemassaolo. Ei kuitenkaan ole vielä selvää, miten Gröbnerin kantoja voi konkreettisesti löytää. Tähän kysymykseen pyritään antamaan vastaus tässä luvussa. Esitellään ensin S-polynomit, joita käytetään Buchbergerin algoritmissa, jonka avulla voidaan laskea minkä tahansa vähintään kahden polynomin virittämän ideaalin Gröbnerin kanta.

Tässä luvussa oletetaan, että $R = k[X_1, \ldots, X_n]$, missä $k$ on kunta. Lisäksi oletetaan, että $\leq$ on termijärjestys polynomirenkaassa $R$.

**Lemma 5.1.** *Olkoot $I = \langle f_1, \ldots, f_m \rangle \in R[X_1, \ldots X_n]$ ideaali, $F$ sen Gröbnerin kanta sekä*

$$f = a_1 f_1 + \cdots + a_m f_m \in \langle f_1, \ldots, f_m \rangle ,$$

*missä $a_1, \ldots, a_m \in R$. Jos $f \to_F 0$, niin termi $\mathrm{lt}_{\leq}(f)$ on jaollinen termillä $\mathrm{lt}_{\leq}(f_j)$ jollakin $f_j \in F$.*

*Todistus.* Ks. [3, s. 204] Olkoot $aX^v = \mathrm{lt}_{\leq}(f)$, $c_i X^{u_i} = \mathrm{lt}_{\leq}(a_i)$ ja $d_i X^{v_i} = \mathrm{lt}_{\leq}(f_i)$, kun $i = 1, \ldots, m$. Merkitään nyt

$$\delta = \max_{\leq} \{v_i + u_i \mid i = 1, \ldots, m\} .$$

Ei ole mahdollista, että $v > v_i + u_i$ kaikilla $i = 1, \ldots, m$, koska polynomin $f$ korkeimman termin täytyy olla k-lineaarinen kombinaatio korkeimmista termeistä $\mathrm{lt}_{\leq}(a_i f_i)$, kun $a_i f_i \neq 0$. Tämän vuoksi $v \leq \delta$. Koska $f \to_F 0$, on oltava $\mathrm{lt}_{\leq}(a_i f_i) \leq \mathrm{lt}_{\leq}(f)$. Tästä seuraa, että $\delta = v$. Tällöin voimme olettaa, että $\delta = v_1 + u_1 = \cdots = v_r + u_r$, missä $r \leq m$ ja $a_i f_i \neq 0$, kun $i = 1, \ldots, r$. Tällöin

$$aX^v = (c_1 d_1 + \cdots + c_r d_r) X^{u_1 + v_1}.$$

Tällöin $d_1 X^{v_1} = \mathrm{lt}_{\leq}(f_1)$ jakaa termin $aX^v = \mathrm{lt}_{\leq}(f)$ ja väite seuraa.

**Lause 5.2.** *Olkoon $F = \{f_1, \ldots, f_m\}$ ja $I = \langle f_1, \ldots, f_m \rangle$. Jos $f \to_F 0$ kaikilla $f \in I$, niin silloin $F$ on ideaalin $I$ Gröbnerin kanta. Jos $F$ on ideaalin $I$ Gröbnerin kanta, niin $f^F = 0$, jos ja vain jos $f \to_F 0$, kun $f \in I$.*

*Todistus.* Ks. [3, s. 205] Olkoon $f \in I \setminus \{0\}$. Tällöin lemman 5.1 mukaan jos $f \to_F 0$, niin termi $\mathrm{lt}_{\leq}(f)$ on jaollinen termillä $\mathrm{lt}_{\leq}(f_j)$ jollakin $f_j \in F$. Joten jos $f \to_F 0$ kaikilla $f \in I$, niin $F$ on ideaalin $I$ Gröbnerin kanta. Jakoalgoritmin (lause 3.3) perusteella seuraa suoraan, että jos $f^F = 0$, niin $f \to_F 0$. Jos $F$ on ideaalin $I$ Gröbnerin kanta ja $f \to_F 0$, niin lauseen 4.2 perusteella tiedetään, että koska $f \in I$, on oltava $f^F = 0$, ja väite seuraa.

**Määritelmä 5.1.** Olkoon $\leq$ termijärjestys ja $f, g \in R \setminus \{0\}$. Polynomien $f$ ja $g$ *suurin yhteinen tekijä* on polynomi $d \in R$, jolle pätee:

$(i)$ $d$ jakaa sekä polynomin $f$ että polynomin $g$,

$(ii)$ Jos polynomi $h \in R$ jakaa sekä polynomin $f$ että polynomin $g$, niin $h$ jakaa polynomin $d$ ja

$(iii)$ $\mathrm{lc}_{\leq}(d) = 1$.

Lisäksi polynomien $f$ ja $g$ *pienin yhteinen monikerta* on polynomi $\gamma \in R$, jolle pätee:

$(i)$ $f$ ja $g$ jakavat molemmat polynomin $\gamma$

$(ii)$ Jos $f$ ja $g$ molemmat jakavat polynomin $h \in R$, niin silloin $\gamma$ jakaa polynomin $h$.

$(iii)$ $\mathrm{lc}_{\leq}(\gamma) = \mathrm{lc}_{\leq}(f)\mathrm{lc}_{\leq}(g)$.

Merkitään polynomien suurinta yhteistä tekijää merkinnällä $\mathrm{syt}(f, g)$ ja pienintä yhteistä monikertaa merkinnällä $\mathrm{pym}(f, g)$.

**Määritelmä 5.2.** Olkoot $f$, $g \in R[X_1, \ldots, X_n]$.
Polynomien $f$ ja $g$ *S-polynomi* on

$$S(f, g) = \frac{\mathrm{pym}(\mathrm{lp}_{\leq}(f), \mathrm{lp}_{\leq}(g))}{\mathrm{lt}_{\leq}(f)} f - \frac{\mathrm{pym}(\mathrm{lp}_{\leq}(f), \mathrm{lp}_{\leq}(g))}{\mathrm{lt}_{\leq}(g)} g.$$

**Esimerkki 5.1.** Olkoon $k[X, Y, Z]$ polynomirengas, $\leq$ sanakirjajärjestys sekä $f = X^3 + 2X^2Y + 2$ ja $g = X^2YZ + XY^2 + Z$. Lasketaan polynomien $f$ ja $g$ S-polynomi. Huomataan, että $\mathrm{lp}_{\leq}(f) = X^3$, $\mathrm{lp}_{\leq}(g) = X^2YZ$, joten $\mathrm{pym}((\mathrm{lp}_{\leq}(f), \mathrm{lp}_{\leq}(g))) = X^3YZ$, eli voidaan kirjoittaa

$$\begin{aligned} S(f, g) &= \frac{X^3YZ}{X^3} f - \frac{X^3YZ}{X^2YZ} g \\ &= YZ(X^3 + 2X^2Y + 2) - X(X^2YZ + XY^2 + Z) \\ &= X^3YZ + 2X^2Y^2Z + 2YZ - X^3YZ - X^2Y^2 - XZ \\ &= 2X^2Y^2Z - X^2Y^2 - XZ + 2YZ. \end{aligned}$$

Huomataan, että polynomien $f$ ja $g$ S-polynomia laskettaessa polynomien $f$ ja $g$ korkeimmat termit supistuvat pois, ja tuloksena on polynomi, jonka korkein termi on pienempi kuin polynomien $f$ ja $g$ korkeimmat termit.

**Lemma 5.3.** *Olkoon $I = \langle f_1, \ldots, f_m \rangle$ ideaali ja $G$ sen Gröbnerin kanta. Nyt $f \in I$, jos ja vain jos*

$$f = \sum_{i=1}^{m} h_i g_i,$$

*missä* $\mathrm{lp}_{\leq}(f) = \max_{1 \leq i \leq m}(\mathrm{lp}_{\leq}(h_i)\mathrm{lp}_{\leq}(g_i))$.

*Todistus.* Ks. [1, s. 33] Koska $f \in I$, niin Lauseen 4.2 perusteella tiedetään, että $f^G = 0$. Tällöin haluttu tulos saadaan suoraan jakoalgoritmista, kun $f$ jaetaan Gröbnerin kannalla $G$, mistä väite seuraa.

**Lemma 5.4.** *Olkoot $f_1, \ldots, f_m \in R$ sellaisia polynomeja, joille $\mathrm{lp}_{\leq}(f_i) = M \neq 0$ kaikilla $i = 1, \ldots, m$. Olkoon lisäksi*

$$f = \sum_{i=1}^{m} c_i \, f_i,$$

*missä $c_i \in k$, $i = 1, \ldots, m$. Jos $\mathrm{lp}(f) < M$, niin $f$ on S-polynomin $S(f_i, f_j)$, $1 \leq i < j \leq m$ lineaarikombinaatio, jonka kertoimet ovat kunnassa $k$.*

*Todistus.* Ks. [1, s. 41] Kirjoitetaan $f_i = a_i M + C$, $a_i \in k$. Tässä $C$ sisältää polynomin $f_i$ kaikki alemmat termit. Nyt

$$\begin{aligned} f &= \sum_{i=1}^{m} c_i \, f_i \\ &= \sum_{i=1}^{m} c_i \, a_i (M + C) \\ &= \sum_{i=1}^{m} c_i \, a_i M + \sum_{i=1}^{m} C. \end{aligned}$$

Koska $c_i \in k$ kaikilla $i = 1, \ldots, m$ ja lisäksi oletuksen perusteella $\mathrm{lp}_{\leq}(f) < M$, on oltava

$$\sum_{i=1}^{m} c_i a_i = 0.$$

Nyt määritelmän perusteella

$$\begin{aligned} S(f_i, f_j) &= \frac{\mathrm{pym}(\mathrm{lp}_{\leq}(f_i), \ \mathrm{lp}_{\leq}(f_j)}{\mathrm{lt}_{\leq}(f_i)} f_i \ - \ \frac{\mathrm{pym}(\mathrm{lp}_{\leq}(f_i), \ \mathrm{lp}_{\leq}(f_j)}{\mathrm{lt}_{\leq}(f_j)} f_j \\ &= \frac{M}{M a_i} f_i \ - \ \frac{M}{M a_j} f_j \\ &= \frac{1}{a_i} f_i \ - \ \frac{1}{a_j} f_j, \end{aligned}$$

koska oletuksen perusteella $\mathrm{lp}_{\leq}(f_i) = \mathrm{lp}_{\leq}(f_j) = M$. Tästä seuraa, että

$$\begin{aligned}
f =& c_1 f_1 + \cdots + c_m f_m \\
=& c_1 a_1 (\frac{1}{a_1} f_1) + \cdots + c_m a_m (\frac{1}{a_m} f_m) \\
=& c_1 a_1 (\frac{1}{a_i} f_1 - \frac{1}{a_2} f_2) + (c_1 a_1 + c_2 a_2)(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3) \\
&+ \cdots + (c_1 a_1 + \cdots + c_{m-1} a_{m-1})(\frac{1}{a_{m-1}} f_{m-1} - \frac{1}{a_m} f_m) \\
&+ (c_1 a_1 + \cdots + c_m a_m) \frac{1}{a_m} f_m \\
=& c_1 a_1 S(f_1, f_2) + (c_1 a_1 + c_2 a_2) S(f_2, f_3) + \ldots \\
&+ (c_1 a_1 + \cdots + c_{m-1} a_{m-1}) S(f_{m-1}, f_m),
\end{aligned}$$

koska $c_1 a_1 + \cdots + c_m a_m = 0$, ja väite seuraa.

**Lause 5.5.** *(Buchbergerin S-kriteeri) Olkoon $G = \{g_1, \ldots, g_m\}$ joukko nollasta eroavia polynomeja polynomirenkaassa $R$. Nyt $G$ on ideaalin $I = \langle g_1, \ldots, g_m \rangle$ Gröbnerin kanta, jos ja vain jos kaikilla $i \neq j$*

$$S(g_i, g_j) \to_G 0.$$

*Todistus.* Ks. [1, s. 41] Oletetaan ensin, että $G$ on ideaalin $I$ Gröbnerin kanta. Tällöin lauseesta 4.1 seuraa suoraan, että $S(g_i, g_j) \to_G 0$ aina, kun $i \neq j$, koska ideaalien ominaisuuksien perusteella $S(g_i, g_j) \in I$.

Oletetaan sitten, että $S(g_i, g_j) \to_G 0$ kaikilla $i \neq j$. Käytetään Lauseen 4.1 kohtaa *(iii)* osoittamaan, että $G$ on ideaalin $I$ Gröbnerin kanta. Olkoon $f \in I$. Tällöin $f$ voidaan kirjoittaa usealla tavalla alkioiden $g_i$ lineaarikombinaationa. Merkitään

$$f = \sum_{i=1}^{m} h_i g_i,$$

missä

$$M = \max_{1 \leq i \leq t} (\mathrm{lp}(h_i)\mathrm{lp}(g_i))$$

on ensimmäinen termi. Näin voidaan tehdä, koska lauseen 2.6 perusteella termijärjestys on hyvä järjestys. Jos $M = \mathrm{lp}_{\leq}(f)$, väite seuraa. Oletetaan, että $M \neq \mathrm{lp}_{\leq}(f)$. Tällöin $M < \mathrm{lp}_{\leq}(f)$. Olkoon $S = \left\{ i \mid \mathrm{lp}_{\leq}(h_i)\mathrm{lp}(g_i) = M \right\}$. Kun $i \in S$, kirjoitetaan $h_i = c_i M_i +$ alempia termejä. Kirjoitetaan $g = \sum_{i \in S} c_i M_i g_i$. Tällöin $\mathrm{lp}_{\leq}(M_i g_i) = M$ kaikilla $i \in S$, mutta $\mathrm{lp}_{\leq}(g) < M$. Lemman 5.4 perusteella on olemassa $d_{ij} \in k$, jolle pätee

$$g = \sum_{i,j \in S, i \neq j} d_{ij} S(M_i g_i, M_j g_j).$$

Nyt $M = \text{pym}(\text{lp}_{\leq}((M_i g_i), (M_j g_j)))$, joten

$$\begin{aligned} S(M_i g_i, M_j, g_j) &= \frac{M}{\text{lt}_{\leq}(M_i g_i)} M_i g_i - \frac{M}{\text{lt}_{\leq}(M_j g_j)} M_j g_j \\ &= \frac{M}{\text{lt}_{\leq}(g_i)} g_i - \frac{M}{\text{lt}_{\leq}(g_j)} g_j = \frac{M}{M_{ij}} S(g_i, g_j), \end{aligned}$$

missä $M_{ij} = \text{pym}(\text{lp}_{\leq}(g_i), \text{lp}_{\leq}(g_j))$. Oletuksen perusteella $S(g_i, g_j) \to_G 0$ ja tällöin edellisen yhtälön perusteella $S(M_i g_i, M_j g_j) \to_G 0$. Tästä saadaan esitys

$$S(M_i g_i, M_j g_j) = \sum_{v=1}^{t} h_{ijv} g_v,$$

missä Lauseen 3.3 perusteella

$$\begin{aligned} \max_{1 \leq v \leq t}(\text{lp}_{\leq}(h_{ijv})\text{lp}_{\leq}(g_v)) &= \text{lp}_{\leq}(S(M_i g_i, M_j g_j)) \\ &< \max(\text{lp}_{\leq}(M_i g_i), \text{lp}_{\leq}(M_j g_j)) = M. \end{aligned}$$

Sijoittamalla nämä yhtälöt, saadaan $f = \sum_{i=1}^{t} h_i' g_i$, missä $\max_{1 \leq i \leq t}(\text{lp}_{\leq}(h_i')\text{lp}_{\leq}(g_i)) < M$, mikä on ristiriita ja väite seuraa.

**Korollaari 5.6.** *Olkoon $G = \{f_1, \ldots, f_m\} \in R$. Nyt $G$ on Gröbnerin kanta, jos ja vain jos $S(f_i, f_j)^F = 0$, kun $1 \leq i < j \leq m$.*

*Todistus.* Ks. [3, s. 208] Jos $S(f_i, f_j)^F = 0$, kun $1 \leq i < j \leq m$, niin $S(f_i, f_j) \to_F 0$ ja $G$ on Gröbnerin kanta lauseen 5.5 perusteella. Jos taas $G$ on Gröbnerin kanta, niin $S(f_i, f_j)^F = 0$ lauseen 4.2 perusteella, koska $S(f_i, f_j) \in \langle f_1, \ldots, f_m \rangle$, ja väite seuraa.

**Algorigmi 5.1. Buchbergerin algoritmi**

**INPUT:** $F = \{f_1, \ldots, f_s\} \subseteq R$, missä $f_i \neq 0 (1 \leq i \leq s)$

**OUTPUT:** Ideaalin $\langle f_1, \ldots, f_s \rangle$ Gröbnerin kanta $G = \{g_1, \ldots, g_t\}$

**INITIALIZATION** $G := F, \mathbf{G} := \{\{f_i, f_j\} \,|\, f_i \neq f_j \in G\}$

**WHILE** $\mathbf{G} \neq \emptyset$ **DO**

Valitaan mielivaltainen $\{f, g\} \in \mathbf{G}$

$\mathbf{G} := \mathbf{G} - \{\{f, g\}\}$

$S(f, g) \to_G h$, missä $h$ supistuu joukon $G$ suhteen

**IF** $h \neq 0$ **THEN**

$\mathbf{G} := \mathbf{G} \cup \{\{u, h\} \mid \text{kaikilla } u \in G\}$

$G := G \cup \{h\}$

**Lause 5.7.** *Olkoon $F = \{f_1, \ldots, f_s\} \subseteq R$, missä $f_i \neq 0 (1 \leq i \leq s)$. Buchbergerin algoritmi (5.1) tuottaa Gröbnerin kannan ideaalissa $I = \langle f_1, \ldots, f_s \rangle$.*

*Todistus.* Ks. [1, s. 42] Todistetaan ensin, että Algoritmi 5.1 päättyy. Tehdään vastaoletus, että algoritmin suoritus ei pääty. Konstruoidaan tällöin algoritmin joukosta $G$ kunkin suorituskerran jälkeen joukko $G_i$, missä $i$ on algoritmin joukko $G$ kunkin suorituskerran jälkeen. Nyt koska algoritmi ei pääty, $G_i$ on aidosti mahtavampi kuin $G_{i-1}$, ja saadaan kasvava ääretön jono joukkoja

$$G_1 \subset G_2 \subset G_3 \subset \dots.$$

Kukin $G_i$ saadaan lisäämällä joukkoon $G_{i-1}$ jokin $h \in I$, missä $h$ on nollasta eroava joukon $G_{i-1}$ supistus S-polynomilla, jonka osat ovat joukossa $G_{i-1}$. Koska $h$ on supistus joukossa $G_{i-1}$, tiedetään, että $lt(h) \notin Lt(G)_{i-1}$. Tällöin saadaan

$$LT(G_1) \subset LT(G_2) \subset LT(G_3) \subset \dots.$$

Tämä on aidosti suureneva ketju ideaaleja, mikä on ristiriita Lauseen 4.6 kanssa, koska lopulta päädyttäisiin tilanteeseen, jossa tarvittaisiin ääretön määrä polynomeja, joilla voitaisiin esittää mikä tahansa ideaalin polynomi näiden lineaarikombinaationa. Vastaoletus on siis väärä ja Algoritmin 5.1 suoritus loppuu.

Todistetaan sitten, että algoritmi 5.1 tuottaa Gröbnerin kannan. Nyt tiedetään, että algoritmin päättyessä $F \subseteq G \subseteq I$ ja täten lisäksi $I = \langle f_1, \dots, f_s \rangle \subseteq \langle g_1, \dots, g_t \rangle \subseteq I$. Tällöin siis $G$ virittää ideaalin $I$. Lisäksi jos $g_i, g_j$ ovat joukon $G$ polynomeja, niin $S(g_i, g_j) \to_G 0$ algoritmin konstruktiolla. Täten $G$ on ideaalin $I$ Gröbnerin kanta lauseen 5.5 perusteella, ja väite seuraa.

**Esimerkki 5.2.** Olkoon $f_1 = 2X - Y, f_2 = -X + 2Y \in \mathbb{Q}[X, Y]$ ja $\leq$ sanakirjajärjestys. Muodostetaan Gröbnerin kanta $G$ käyttäen Buchbergerin algoritmia.

INITIALIZATION: $G := F, \mathbf{G} = \{\{f_1, f_2\}\}$

Käydään läpi WHILE-silmukka ensimmäisen kerran:

$\mathbf{G} := \mathbf{G} - \{f_1, f_2\} = \emptyset$

$S(f_1, f_2) \to_G \frac{3}{2}Y = h$ (supistunut joukon $G$ suhteen). (1)

Koska $h \neq 0$, olkoon $f_3 := \frac{3}{2}Y$

$\mathbf{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Käydään läpi WHILE-silmukka toisen kerran:

$\mathbf{G} := \{\{f_2, f_3\}\}$

$S(f_1, f_3) \to_G 0$ (2)

Käydään läpi WHILE-silmukka kolmannen kerran:

$\mathbf{G} := \emptyset$

$S(f_2, f_3) \to_G 0$ (3)

Nyt

$$\begin{aligned} G &= \{f_1, f_2, f_3\} \\ &= \{2X - Y, -X + 2Y, \frac{3}{2}Y\} \end{aligned}$$

on ideaalin $\langle f_1, f_2 \rangle$ Gröbnerin kanta.

Esitetään vielä S-polynomien supistukset kohdissa (1), (2) ja (3):
Kohta (1):

$$\begin{aligned} S(f_1, f_2) &= \frac{X}{2X}(2X - Y) - \frac{X}{-X}(-X + 2Y) \\ &= -\frac{1}{2}Y + 2Y \\ &= \frac{3}{2}Y. \end{aligned}$$

Nyt polynomin $\frac{3}{2}Y$ ainoa termi ei ole jaollinen joukon
$G = \{f_1, f_2\} = \{2X - Y, -X + 2Y\}$ yhdenkään polynomin johtavalla termillä, joten voidaan suoraan kirjoittaa $S(f_1, f_2) \to_G \frac{3}{2}Y := f_3$.
Kohta (2):

$$\begin{aligned} S(f_1, f_3) &= \frac{XY}{2X}(2X - Y) - \frac{XY}{\frac{3}{2}Y}(\frac{3}{2}Y) \\ &= -\frac{1}{2}Y^2 \end{aligned}$$

Nyt

$$-\frac{1}{2}Y^2 - \frac{-\frac{1}{2}Y^2}{\frac{3}{2}Y}(\frac{3}{2}Y) = 0,$$

eli $S(f_1, f_3) \to_{f_3} 0$, joten voidaan kirjoittaa $S(f_1, f_3) \to_G 0$.
Kohta (3):

$$\begin{aligned} S(f_2, f_3) &= \frac{XY}{-X}(-X + 2Y) - \frac{XY}{\frac{3}{2}Y}(\frac{3}{2}Y) \\ &= -\frac{1}{2}Y^2 \end{aligned}$$

Nyt kohdan (2) perusteella tiedetään, että $S(f_2, f_3) = -\frac{1}{2}Y^2 \to_{f_3} 0$, joten voidaan kirjoittaa $S(f_2, f_3) \to_G 0$.

**Esimerkki 5.3.** Olkoon $f_1 = X^2Y + X, f_2 = X + Y \in \mathbb{Q}[X, Y]$ ja $\leq$ sanakirjajärjestys. Muodostetaan Gröbnerin kanta $G$ käyttäen Buchbergerin algoritmia.

INITIALIZATION: $G := F, \mathbf{G} = \{\{f_1, f_2\}\}$

Käydään läpi WHILE-silmukka ensimmäisen kerran:

$\mathbf{G} := \mathbf{G} - \{f_1, f_2\} = \emptyset$

$S(f_1, f_2) \to_G X + Y^3 = h$ (supistunut joukon $G$ suhteen). (1)

Koska $h \neq 0$, olkoon $f_3 := X + Y^3$

$\mathbf{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Käydään läpi WHILE-silmukka toisen kerran:

$\mathbf{G} := \{\{f_2, f_3\}\}$

$S(f_1, f_3) \to_G Y^5 - Y^3$ (2)

Koska $h \neq 0$, olkoon $f_4 = Y^5 - Y^3$

$\mathbf{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G := \{f_1, f_2, f_3, f_4\}$

Käydään läpi WHILE-silmukka kolmannen kerran:

$\mathbf{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_2, f_3) \to_G -Y^3 + Y = h$ (3)

Koska $h \neq 0$, olkoon $f_5 = -Y^3 + Y$

$\mathbf{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$G := \{f_1, f_2, f_3, f_4, f_5\}$

Käydään läpi WHILE-silmukka neljännen kerran:

$\mathbf{G} := \{\{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_1, f_4) \to_G 0 = h$ (4)

Käydään läpi WHILE-silmukka viidennen kerran:

$\mathbf{G} := \{\{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_2, f_4) \to_G 0 = h$ (5)

Käydään läpi WHILE-silmukka kuudennen kerran:

$\mathbf{G} := \{\{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_3, f_4) \to_G 0 = h$ (6)

Käydään läpi WHILE-silmukka 7. kerran:

$\mathbf{G} := \{\{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_1, f_5) \to_G 0 = h$ (7)

Käydään läpi WHILE-silmukka 8. kerran:

$\mathbf{G} := \{\{f_3, f_5\}, \{f_4, f_5\}\}$

$S(f_2, f_5) \to_G 0 = h$ (8)

Käydään läpi WHILE-silmukka 9. kerran:

$\mathbf{G} := \{\{f_4, f_5\}\}$

$S(f_3, f_5) \to_G 0 = h$ (9)

Käydään läpi WHILE-silmukka 10. kerran:

$\mathbf{G} := \emptyset$

$S(f_4, f_5) \to_G 0 = h$ (10)

WHILE-silmukka pysähtyy, koska $\mathbf{G} = \emptyset$. Nyt

$$\begin{aligned} G &= \{f_1, f_2, f_3, f_4, f_5\} \\ &= \{X^2Y + X, X + Y, X + Y^3 + Y^5 - Y^3, -Y^3 + Y\} \end{aligned}$$

on ideaalin $\langle f_1, f_2 \rangle$ Gröbnerin kanta.

Esitetään vielä S-polynomien supistukset kohdissa (1), (2), (3), (4), (5), (6), (7), (8), (9) ja (10):

On oleellista huomioida supistuksien laskemisessa, että joukko $G$ ei ole jokaisessa vaiheessa sama, vaan siihen lisätään alkioita sitä mukaa, kun algoritmin suoritus etenee.

Kohta (1):

$$\begin{aligned} S(f_1, f_2) &= \frac{X^2Y}{X^2Y}(X^2Y + X) - \frac{X^2Y}{X}(X + Y) \\ &= X^2Y + X - X^2Y - XY^2 \\ &= -XY^2 + X. \end{aligned}$$

Nyt

$$-XY^2 + X - \frac{X}{X}(X + Y) = X + Y^3$$

eli $S(f_1, f_2) \to_{f_2} X + Y^3$. Nyt polynomin $X + Y^3$ yksikään termi ei ole jaollinen joukon $G = \{f_1, f_2\}$ jäljellä olevien polynomien, eli polynomin $f_1$, korkeimman termin kanssa, joten voidaan kirjoittaa $S(f_1, f_2) \to_G X + Y^3 := f_3$ ja $G :=$

$\{f_1, f_2, f_3\}$.
Kohta (2):

$$\begin{aligned} S(f_1, f_3) &= \frac{X^2Y^2}{X^2Y}(X^2Y + X) - \frac{X^2Y^2}{X}(X + Y^3) \\ &= -XY^4 + X. \end{aligned}$$

Nyt

$$\begin{aligned} -XY^4 + X - \frac{-XY^4}{X}(X + Y) &= X + Y^5, \\ X + Y^5 - \frac{X}{X}(X + Y^3) &= Y^5 - Y^3, \end{aligned}$$

eli $S(f_1, f_3) \to_{f_2} X + Y^5 \to_{f_3} Y^5 - Y^3$. Polynomin $Y^5 - Y^3$ termit eivät ole jaollisia joukon $G$ jäljellä olevien polynomien johtavien termien kanssa, joten voidaan kirjoittaa $S(f_1, f_3) \to_G Y^5 - Y^3 = f_4$.
Kohta (3):

$$\begin{aligned} S(f_2, f_3) &= \frac{X}{X}(X + Y) - \frac{X}{X}(X + Y^3) \\ &= -Y^3 + Y. \end{aligned}$$

Nyt polynomin $-Y^3 + Y$ yksikään termi ei ole jaollinen joukon $G$ yhdenkään polynomin johtavalla termillä, joten voidaan suoraan kirjoittaa $S(f_2, f_3) \to_G -Y^3 + Y := f_5$.

Kohta (4):

$$\begin{aligned} S(f_1, f_4) &= \frac{X^2Y^5}{X^2Y}(X^2Y + X) - \frac{X^2Y^5}{Y^5}(Y^5 - Y^3) \\ &= X^2Y^3 + XY^4 \end{aligned}$$

Nyt

$$\begin{aligned} X^2Y^3 + XY^4 - \frac{X^2Y^3}{X^2Y}(X^2Y + X) &= XY^4 - XY^2, \\ XY^4 - XY^2 - \frac{XY^4}{X}(X + Y) &= -XY^2 - Y^5, \\ -XY^2 - Y^5 - \frac{-XY^2}{X}(X + Y^3) &= 0, \end{aligned}$$

eli $S(f_1, f_4) \to_{f_1} XY^4 + XY^2 \to_{f_2} XY^2 - Y^5 \to_{f_3} 0$, joten voidaan kirjoittaa $S(f_1, f_4) \to_G 0$.
Kohta (5):

$$\begin{aligned} S(f_2, f_4) &= \frac{XY^5}{X}(X + Y) - \frac{XY^5}{Y^5}(Y^5 - Y^3) \\ &= XY^3 + Y^6. \end{aligned}$$

Nyt

$$XY^3 + Y^6 - \frac{XY^3}{X}(X + Y^3) = Y^6 - Y^6 = 0,$$

eli $S(f_2, f_4) \to_{f_3} 0$, joten voidaan kirjoittaa $S(f_2, f_4) \to_G 0$.

Kohta (6):

$$\begin{aligned} S(f_3, f_4) &= \frac{XY^5}{X}(X + Y^3) - \frac{XY^5}{Y^5}(Y^5 - Y^3) \\ &= XY^3 + Y^8. \end{aligned}$$

Nyt

$$\begin{aligned} XY^3 + Y^8 - \frac{XY^3}{X}(X + Y^3) &= Y^8 - Y^6, \\ Y^8 - Y^6 - \frac{Y^8}{Y^5}(Y^5 - Y^3) &= 0, \end{aligned}$$

eli $S(f_3, f_4) \to_{f_3} Y^8 - Y^6 \to_{f_4} 0$, joten voidaan kirjoittaa $S(f_3, f_4) \to_G 0$.

Kohta (7):

$$\begin{aligned} S(f_1, f_5) &= \frac{X^2Y^3}{X^2Y}(X^2Y + X) - \frac{X^2Y^3}{-Y^3}(-Y^3 + Y) \\ &= X^2Y + XY^2. \end{aligned}$$

Nyt

$$\begin{aligned} XYX^2Y + XY^2 - \frac{X^2Y}{X^2Y}(X^2Y + X) &= XY^2 - X, \\ XY^2 - X - \frac{XY^2}{X}(X + Y) &= -X - Y^3, \\ -X - Y^3 - \frac{-X}{X}(x + Y^3) &= 0, \end{aligned}$$

eli $S(f_1, f_5) \to_{f_1} XY^2 - X \to_{f_2} -X - Y^3 \to_{f_3} 0$, joten voidaan kirjoittaa $S(f_1, f_5) \to_G 0$.

Kohta (8):

$$\begin{aligned} S(f_2, f_5) &= \frac{XY^3}{X}(X + Y) - \frac{XY^3}{-Y^3}(-Y^3 - Y) \\ &= -XY + Y^4. \end{aligned}$$

Nyt

$$\begin{aligned} -XY + Y^4 - \frac{-XY}{X}(X + Y) &= Y^4 + Y^2, \\ Y^4 + Y^2 - \frac{Y^4}{Y^3}(Y^3 + Y) &= 0, \end{aligned}$$

eli $S(f_2, f_5) \to_{f_2} Y^4 + Y^2 \to_{f_5} 0$, joten voidaan kirjoittaa $S(f_2, f_5) \to_G 0$.

Kohta (9):

$$\begin{aligned} S(f_3, f_5) &= \frac{XY^3}{X}(X + Y^3) - \frac{XY^3}{X}(-Y^3 + Y) \\ &= XY + Y^6. \end{aligned}$$

Nyt

$$\begin{aligned} XY + Y^6 - \frac{XY}{X}(X + Y) &= Y^6 - Y^2, \\ Y^6 - Y^2 - \frac{Y^6}{Y^5}(Y^5 - Y^3) &= Y^4 - Y^2, \\ Y^4 - Y^2 - \frac{Y^4}{Y^2}(Y^3 + Y) &= -2Y^2, \\ -2Y^2 - \frac{-2Y^2}{-2Y}(-2Y) &= 0, \end{aligned}$$

eli $S(f_3, f_5) \to_{f_2} Y^6 - Y^2 \to_{f_4} Y^4 - Y^2 \to_{f_5} -2Y^2 \to_{f_6} 0$, joten voidaan kirjoittaa $S(f_3, f_5) \to_G 0$.

Kohta (10):

$$\begin{aligned} S(f_4, f_5) &= \frac{Y^5}{Y^5}(Y^5 - Y^3) - \frac{Y^5}{-Y^3}(-Y^3 + Y) \\ &= -Y^3 + Y^3 = 0, \end{aligned}$$

eli voidaan suoraan kirjoittaa $S(f_4, f_5) \to_G 0$.

# 6 Redusoitu Gröbnerin kanta

Tässä luvussa oletetaan, että $k$ on kunta, $R = k[X_1, \dots X_n]$ ja $\leq$ termijärjestys.

**Esimerkki 6.1.** Olkoon $f \in I = \langle f_1, \dots, f_m \rangle \subseteq R$. Oletetaan, että $\{f_1, \dots, f_m\}$ on ideaalin $I$ Gröbnerin kanta. Nyt myös $\{f_1, \dots, f_m, f\}$ on ideaalin $I$ Gröbnerin kanta, sillä ensinnäkin selvästi $\{f_1, \dots, f_m, f\} \subseteq I$ ja toisaalta on olemassa $i \in 1, \dots, m$, jolle $\mathrm{lt}_{\leq}(f_i) \mid \mathrm{lt}_{\leq}(f)$ kaikilla $f \in I \backslash \{0\}$, koska tällainen $f_i$ löytyy jo Gröbnerin kannasta $\{f_1, \dots, f_m\}$, joka on joukon $\{f_1, \dots, f_m, f\}$ osajoukko.

Edellisestä esimerkistä voidaan huomata, että Gröbnerin kanta $G$ ideaalissa $I$ ei ole yksikäsitteinen. Tarvitaan siis tiukempia ehtoja, jotta yksikäsitteisyys toteutuu.

**Määritelmä 6.1.** *Minimaalinen Gröbnerin kanta* $\{f_1, \dots, f_m\} \in R$ on Gröbnerin kanta, jolle on voimassa seuraavat ehdot:

$$\begin{aligned} &\text{(i)}\mathrm{lt}_{\leq}(f_i) \text{ ei ole jaollinen termillä } \mathrm{lt}_{\leq}(f_j), \text{ kun } i \neq j, \\ &\text{(ii) } \mathrm{lc}_{\leq}(f_i) = 1 \end{aligned}$$

kaikilla $i, j \in \{1, \dots, m\}$.

**Määritelmä 6.2.** *Redusoitu Gröbnerin kanta* $\{f_1, \dots, f_m\} \in R$ on minimaalinen Gröbnerin kanta, jossa yksikään polynomin $f_i$ termi ei ole jaollinen termillä $\mathrm{lt}_{\leq}(f_j)$, kun $i \neq j$ kaikilla $i, j \in \{1, \dots, m\}$.

**Lause 6.1.** *Jokaisella ideaalilla $I \subseteq R$ on yksikäsitteinen redusoitu Gröbnerin kanta.*

*Todistus.* Ks. [3, s. 213] Todistetaan ensin redusoidun Gröbnerin kannan yksikäsitteisyys. Olkoot $\{f_1, \dots, f_m\} \in R$ ja $\{g_1, \dots, g_{m'}\} \in R$ redusoituja Gröbnerin kantoja ideaalissa $I \in R$. Nyt Gröbnerin kannan määritelmän perusteella tiedetään, että on olemassa sellainen $\mathrm{lt}_{\leq}(f_j)$, joka jakaa termin $\mathrm{lt}_{\leq}(g_1)$. Voimme tarvittaessa termejä järjestelemällä olettaa, että $j = 1$. Samoin tiedetään, että jokin $\mathrm{lt}_{\leq}(g_i)$ jakaa termin $\mathrm{lt}_{\leq}(f_1)$. Tässä tapauksessa $i = 1$, koska $\mathrm{lt}_{\leq}(g_1)$ on jaollinen termillä $\mathrm{lt}_{\leq}(g_i)$. Koska molemmat Gröbnerin kannat ovat redusoituja, ovat termien $\mathrm{lt}_{\leq}(f_1)$ ja $\mathrm{lt}_{\leq}(g_1)$ kertoimet molemmissa tapauksissa 1. Tällöin on oltava $\mathrm{lt}_{\leq}(f_1) = \mathrm{lt}_{\leq}(g_1)$. Samaa päättelyä voimme käyttää kaikkien muidenkin polynomien $f_2, \dots, f_m$ ja $g_2, \dots, g_m^{'}$ johtavien termien kohdalla ja tällöin $m = m^{'}$ sekä $\mathrm{lt}_{\leq}(f_i) = \mathrm{lt}_{\leq}(g_i)$ kaikilla $i \in \{1, \dots, m\}$.

Yksikäsitteisyyden osoittamiseksi täytyy vielä todistaa, että $f_1 = g_1, \dots, f_m = g_m$. Aloitetaan tämä lasketmalla $f_1 - g_1$. Koska korkeimmat termit ovat samoja, ne supistuvat laskussa pois. Redusoidun Gröbnerin kannan määritelmän perusteella yksikään polynomin $f_1 - g_1$ termi ei ole jaollinen

millään $\mathrm{lt}_{\leq}(f_1), \ldots, \mathrm{lt}_{\leq}(f_m)$. Tämä tarkoittaa, että jos polynomi $f_1 - g_1$ jaetaan polynomeilla $f_1, \ldots, f_m$, on tämän jakojäännös $f_1 - g_1$. Nyt täytyy olla $f_1 - g_1 = 0$, koska $f_1 - g_1 \in I$ ja lauseen 4.2 perusteella $(f_1 - g_1)^{\{f_1 \ldots, f_m\}} = 0$. Vastaava päättely pätee myös muille polynomeille $f_i, g_i$ kaikilla $i \in \{1, \ldots, m\}$, joten on siis oltava $\{f_1, \ldots, f_m\} = \{g_1, \ldots, g_{m'}\}$.

Todistetaan sitten redusoidun Gröbnerin kannan olemassaolo. Olkoon $\{f_1, \ldots, f_m\} \in R$ ideaalin $I \in R$ Gröbnerin kanta. Tavoitteena on päästä tilanteeseen, jossa yksikään johtava termi $\mathrm{lt}_{\leq}(f_i)$ ei ole jaollinen johtavalla termillä $\mathrm{lt}_{\leq}(f_j)$, kun $i \neq j$. Jos kuitenkin on olemassa johtava termi $\mathrm{lt}_{\leq}(f_i)$, joka on jaollinen jollakin $\mathrm{lt}_{\leq}(f_j)$, kun $i \neq j$, niin voidaan olettaa, että $i = 1$ ja poistaa tämä termi, minkä jälkeen saadaan muodostettua uusi Gröbnerin kanta $\{f_2, \ldots, f_m\} \in R$. Tämä on Gröbnerin kanta, koska

$$\mathrm{lt}_{\leq}(f_j) \mid \mathrm{lt}_{\leq}(f_1),$$

mikä täyttää määritelmän mukaisen ehdon Gröbnerin kannalle. Korollaarin 4.3 perusteella huomataan lisäksi, että $I = \langle f_2, \ldots, f_m \rangle$. Näin on osoitettu, että vastaavalla tavalla poistamalla Gröbnerin kannasta jokainen polynomi, jonka johtava termi on jaollinen kannan toisen polynomin johtavan termin kanssa, päästään tilanteeseen, jossa jäljellä on enää minimaalinen Gröbnerin kanta. On siis osoitettu, että ideaalilla $I$ on minimaalinen Gröbnerin kanta.

Olkoon sitten $\{f_1, \ldots, f_m\} \in R$ minimaalinen ideaalin $I \in R$ Gröbnerin kanta. Nyt jaetaan polynomi $f_1$ polynomeilla $f_2, \ldots f_m$ ja merkitään

$$r_1 = f_1^{f_2, \ldots, f_m}.$$

Jaetaan seuraavaksi $f_2$ polynomeilla $r_1, f_3, \ldots f_m$ ja merkitään

$$r_2 = f_2^{r_1, f_3, \ldots, f_m}.$$

Jatketaan tätä, kunnes jaetaan polynomi $f_m$ polynomeilla $r_1, \ldots, r_{m-1}$. Nyt meillä on uusi joukko $\{r_1, \ldots, r_m\}$. Minimaalisen Gröbnerin kannan polynomeja jakaessa jokaisen polynomin $f_1, \ldots, f_m$ korkeimmat termit eivät olleet jaollisia keskenään, joten $\mathrm{lt}_{\leq}(f_i) = \mathrm{lt}_{\leq}(r_i)$. Tämä tarkoittaa sitä, että johtava termi $\mathrm{lt}_{\leq}(r_i)$ ei ole jaollinen millään johtavalla termillä $\mathrm{lt}_{\leq}(r_j)$, kun $i \neq j$. Lisäksi kaikilla $f \in I \setminus \{0\}$

$$\mathrm{lt}_{\leq}(r_i) \mid \mathrm{lt}_{\leq}(f).$$

Huomataan siis, että $\{r_1, \ldots, r_m\}$ on minimaalinen Gröbnerin kanta. Lisäksi mikään polynomin $r_i$ termi ei ole jaollinen minkään polynomin $r_j$ termillä, kun $i \neq j$, koska kaikki termit ovat jakojäännöksiä keskinäisistä jakolaskuista. Näin redusoidun Gröbnerin kannan olemassaolo on saatu todistettua, ja väite seuraa.

**Esimerkki 6.2.** Esimerkissä 5.3 muodostettiin ideaalin $\langle f_1, f_2 \rangle$ Gröbnerin kanta

$$\begin{aligned} G &= \{f_1, f_2, f_3, f_4, f_5\} \\ &= \{X^2Y + X, X + Y, X + Y^3, Y^5 - Y^3, -Y^3 + Y\}. \end{aligned}$$

Muodostetaan ideaalin $\langle f_1, f_2\rangle$ redusoitu Gröbnerin kanta $\bar{G}$. Aloitetaan kirjoittamalla $\bar{G} := G$ ja sen jälkeen poistetaan sopivasti termejä, kunnes jäljellä on redusoitu Gröbnerin kanta. Käydään läpi niitä polynomeja, joiden johtavat termit ovat jaollisia kannan muiden johtavien termien kanssa. Näitä ovat $f_1, f_2, f_3$ ja $f_4$. Huomataan, että $\mathrm{lp}_{\leq}(f_2) = \mathrm{lp}_{\leq}(f_3) = X$, jolloin tarkastellaan näiden polynomien muita termejä ja huomataan, että polynomin $f_3$ termi $Y^3$ on jaollinen termillä $\mathrm{lp}_{\leq}(f_5) = -Y^3$. Poistetaan nyt termit $f_1$ ja $f_4$ ja myös termi $f_3$. Näin saadaan $\bar{G} := \{f_2, f_5\} = \{X + Y, -Y^3 + Y\}$, mikä on ideaalin $\langle f_1, f_2\rangle = \langle X^2Y + X, X + Y\rangle$ redusoitu Gröbnerin kanta.

$\bar{G}$ on selvästi Gröbnerin kanta, sillä esimerkiksi

$$\begin{aligned} S(f_2, f_5) &= \frac{XY^3}{X}(X + Y) - \frac{XY^3}{-Y^3}(-Y^3 - Y) \\ &= -XY + Y^4 \end{aligned}$$

ja

$$\begin{aligned} -XY + Y^4 - \frac{-XY}{X}(X + Y) &= Y^4 + Y^2, \\ Y^4 + Y^2 - \frac{Y^4}{Y^3}(Y^3 + Y) &= 0, \end{aligned}$$

eli $S(f_2, f_5) \to_{f_2} Y^4 + Y^2 \to_{f_5} 0$, siis $S(f_2, f_5) \to_{\bar{G}} 0$, mikä on lauseen 5.5 perusteella riittävä ehto sille, että $\bar{G}$ on ideaalin $\langle f_1, f_2\rangle$ Gröbnerin kanta.

Tässä esimerkissä jokaisella $i \in \{1, 2, 3, 4, 5\}$ $\mathrm{lc}_{\leq}(f_i) = 1$. Jos kuitenkin olisi ollut jollakin $i$ tilanne, missä $\mathrm{lc}_{\leq}(f_i) = a \neq 1$, pitäisi vielä jakaa tämä polynomi luvulla $a$, jonka jälkeen tuloksena olisi redusoitu Gröbnerin kanta.

# 7 Sovelluksia: Eliminointi ja yhtälöryhmien ratkaiseminen

Gröbnerin kannoille on olemassa lukuisia sovelluksia. Tässä luvussa esitetään niistä kaksi: eliminointi ja polynomiyhtälöryhmien ratkaiseminen. Useissa sovelluksissa käydään läpi jotakin polynomijoukkoon liittyvää ongelmaa, jonka ratkaiseminen on helpompaa, kun on ensin laskettu tämän polynomijoukon virittämän ideaalin Gröbnerin kanta. Käytännössä tämä on hyödyllistä etenkin siksi, että sekä polynomien jakoalgoritmilla että Buchbergerin algoritmilla ei ole eksponentiaalista aikavaatimusta, joten näitä Gröbnerin kantoja voidaan suhteellisen nopeasti ja tehokkaasti laskea tietokoneen avulla.

Tässä luvussa oletetaan, että $k$ on kunta.

## 7.1 Eliminointi

**Määritelmä 7.1.** Olkoot $v_1$ ja $v_2 \in \mathbb{N}^n$, $w_1$ ja $w_2 \in \mathbb{N}^m$ sekä $\leq_X$ termijärjestys joukossa $\mathbb{N}^n$ ja $\leq_Y$ termijärjestys joukossa $\mathbb{N}^m$. Määritellään joukossa $\mathbb{N}^{n+m}$ järjestys $\leq_E$ seuraavasti:

$$v_1 w_1 \leq_E v_2 w_2 \iff \begin{cases} v_1 <_X v_2 \\ \text{tai} \\ v_1 = v_2 \text{ ja } w_1 <_Y w_2 \\ \text{tai} \\ v_1 = v_2 \text{ ja } w_1 = w_2, \end{cases}$$

missä $v_i w_i := (v_{i_1}, v_{i_2} \ldots, v_{i_n}, w_{i_1}, \ldots, w_{i_m}) \in \mathbb{N}^{n+m}$. Järjestystä $\leq_E$ sanotaan *eliminointijärjestykseksi*. Jos $R = k[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$, voidaan sanoa, että järjestys $\leq_E$ on eliminointijärjestys, missä X-muuttujat ovat suurempia kuin Y-muuttujat.

**Lause 7.1.** *Edellisen määritelmän mukainen eliminointijärjestys $\leq_E$ on termijärjestys.*

*Todistus.* On siis osoitettava, että $\leq_E$ toteuttaa kaikki termijärjestyksen ehdot, eli

$$\begin{aligned} &(i) \leq_E \text{ on täydellinen järjestys,} \\ &(ii)\ 0 \leq_E v_i w_i \text{ ja} \\ &(iii)\ v_1 w_1 \leq_E v_2 w_2 \Rightarrow v_1 w_1 + v_i w_i \leq_E v_2 w_2 + v_i w_i \end{aligned}$$

kaikilla $v_1, v_2, v_i \in \mathbb{N}^n$ ja $w_1, w_2, w_i \in \mathbb{N}^m$.

Osoitetaan ensin, että $\leq_E$ on termijärjestys. Olkoon $v_1, w_1 \in \mathbb{N}^n$ ja $v_2, w_2 \in \mathbb{N}^m$ sekä $\leq_X$ termijärjestys joukossa $\mathbb{N}^n$ ja $\leq_Y$ termijärjestys joukossa

$\mathbb{N}^m$. Koska $\leq_X$ on termijärjestys, on se myös täydellinen järjestys, ja tällöin on oltava $v_1 <_X v_2$, $v_2 <_X v_1$ tai $v_1 = v_2$. Samoin koska $\leq_Y$ on termijärjestys ja täten täydellinen järjestys, on oltava $w_1 <_Y w_2$, $w_2 <_Y w_1$ tai $w_1 = w_2$.

- Jos $v_1 <_X v_2$, on määritelmän perusteella $v_1 w_1 \leq_E v_2 w_2$.
- Jos $v_2 <_X v_1$, on määritelmän perusteella $v_2 w_2 \leq_E v_1 w_1$.
- Jos $v_1 = v_2$ ja $w_1 <_Y w_2$, on määritelmän perusteella $v_1 w_1 \leq_E v_2 w_2$.
- Jos $v_1 = v_2$ ja $w_2 <_Y w_1$, on määritelmän perusteella $v_2 w_2 <_E v_1 w_1$.
- Jos $v_1 = v_2$ ja $w_2 = w_1$, on määritelmän perusteella $v_1 w_1 \leq_E v_2 w_2$.

On siis kaikissa mahdollisissa tapauksissa oltava $v_1 w_1 \leq_E v_2 w_2$ tai $v_2 w_2 \leq_E v_1 w_1$, eli $\leq_E$ on täydellinen järjestys.

Osoitetaan sitten, että $0 \leq_E v_i w_i$ kaikilla $v_i \in \mathbb{N}^n$ ja $w_i \in \mathbb{N}^m$. Merkitään $0_n = (0, \ldots, 0) \in \mathbb{N}^n, 0_m = (0, \ldots, 0) \in \mathbb{N}^m$ ja $0_{n+m} = (0, \ldots, 0) \in \mathbb{N}^{n+m}$. Koska $\leq_X$ on termijärjestys, on oltava $0_N \leq_X v_i$, ja koska $\leq_Y$ on termijärjestys, on oltava $0_m \leq_Y w_i$.

- Jos $0_n <_X v_i$, on määritelmän perusteella $0_{m+n} \leq_E v_i w_i$.
- Jos $0_n = v_i$ ja $0_m <_Y w_i$, on määritelmän perusteella $0_{n+m} \leq_E v_i w_i$.
- Jos $0_n = v_i$ ja $0_m = w_i$, on määritelmän perusteella $0_{n+m} \leq_E v_i w_i$.

On siis kaikissa mahdollisissa tapauksissa oltava $0 \leq_E v_i w_i$ kaikilla $v_i \in \mathbb{N}^n$ ja $w_i \in \mathbb{N}^m$.

Osoitetaan sitten, että $v_1 w_1 \leq_E v_2 w_2 \Rightarrow v_1 w_1 + v_i w_i \leq_E v_2 w_2 + v_i w_i$. Olkoon $v_1 w_1 \leq_E v_2 w_2$ sekä $v_i \in \mathbb{N}^n$ ja $w_i \in \mathbb{N}^m$. Nyt

$$
\begin{aligned}
&v_1 w_1 + v_i w_i \\
&= (v_{1_1} + v_{i_1}, \ldots, v_{1_n} + v_{i_n}, w_{1_1} + w_{i_1}, \ldots, w_{1_m} + w_{i_m}) \\
&\text{ja} \\
&v_2 w_2 + v_i w_i \\
&= (v_{2_1} + v_{i_1}, \ldots, v_{2_n} + v_{i_n}, w_{2_1} + w_{i_1}, \ldots, w_{2_m} + w_{i_m}).
\end{aligned}
$$

Tästä huomataan, että

$$
\begin{aligned}
v_1 v_i &= (v_{1_1} + v_{i_1}, \ldots, v_{1_n} + v_{i_n}) \\
v_2 v_i &= (v_{2_1} + v_{i_1}, \ldots, v_{2_n} + v_{i_n}) \\
w_1 w_i &= (w_{1_1} + w_{i_1}, \ldots, w_{1_m} + w_{i_m}) \\
w_2 w_i &= (w_{2_1} + w_{i_1}, \ldots, w_{2_m} + w_{i_m}).
\end{aligned}
$$

Nyt koska $\leq_X$ ja $\leq_Y$ ovat termijärjestyksiä, on oltava $v_1 v_i <_X w_1 w_i$ tai $v_1 v_i = w_1 w_i$ sekä $v_2 v_i <_Y w_2 w_i$ tai $v_2 v_i = w_2 w_i$.

- Jos $v_1 v_i <_X w_1 w_i$, on määritelmän perusteella $v_1 w_1 + v_i w_i \leq_E v_2 w_2 + v_i w_i$.

- Jos $v_1v_i = w_1w_i$ ja $v_2v_i <_Y w_2w_i$, on määritelmän perusteella $v_1w_1 + v_iw_i \leq_E v_2w_2 + v_iw_i$.
- Jos $v_1v_i = w_1w_i$ ja $v_2v_i = w_2w_i$, on määritelmän perusteella $v_1w_1 + v_iw_i \leq_E v_2w_2 + v_iw_i$.

Huomataan siis, että kaikissa tapauksissa $v_1w_1 + v_iw_i \leq_E v_2w_2 + v_iw_i$, joten järjestys $\leq_E$ täyttää kaikki termijärjestyksen ehdot ja väite seuraa.

**Lause 7.2.** *Olkoon $I \neq \{0\}$ ideaali polynomirenkaassa $k[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$ ja $\leq_E$ eliminointijärjestys joukossa $\mathbb{N}^{n+m}$, missä X-muuttujat ovat suurempia kuin Y-muuttujat. Olkoon $G = \{g_1, \ldots, g_t\}$ ideaalin $I$ Gröbnerin kanta. Tällöin $G \cap k[Y_1, \ldots, Y_m]$ on ideaalin $I \cap k[Y_1, \ldots, Y_m]$ Gröbnerin kanta.*

*Todistus.* Ks. [1, s. 70] Todistetaan ensin, että $I \cap k[Y_1, \ldots, Y_m]$ on ideaali polynomirenkaassa $k[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$. Valitaan mielivaltaiset $f \in I \cap k[Y_1, \ldots, Y_m]$ ja $\lambda \in k[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$. Nyt polynomirenkaan määritelmän perusteella

$$\lambda f = (\lambda f)(v) = \sum_{v_1+v_2=v} \lambda(v_1)f(v_2),$$

missä $v_1, v_2 \in \mathbb{N}^{n+m}$. Nyt kuitenkin $v_2 = (a_1, \ldots, a_m, 0, \ldots, 0)$, joten

$$\lambda(v_1)f(v_2) = 0,$$

kun vektorin $v_2$ indeksi on suurempi kuin $m$, joten voidaan kirjoittaa $v_1, v_2 \in \mathbb{N}^m$, eli polynomien määritelmän perusteella $\lambda f \in I \cap k[Y_1, \ldots, Y_m]$, eli $I \cap k[Y_1, \ldots, Y_m]$ on ideaali polynomirenkaassa $k[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$ ideaalin määritelmän perusteella.

Todistetaan sitten, että $G \cap k[Y_1, \ldots, Y_m]$ on ideaalin $I \cap k[Y_1, \ldots, Y_m]$ Gröbnerin kanta. Voidaan aluksi todeta, että selvästi $G \cap k[Y_1, \ldots, Y_m]$ kuuluu joukkoon $I \cap k[Y_1, \ldots, Y_m]$. Olkoon nyt $0 \neq f \in I \cap k[Y_1, \ldots, Y_m]$. Koska $G$ on ideaalin $I$ Gröbnerin kanta, on olemassa sellainen $i$, jolla $\mathrm{lp}_{\leq_E}(g_i)$ jakaa termin $\mathrm{lp}_{\leq_E}(f)$. Lisäksi koska polynomilla $f$ on vain Y-muuttujia, on myös termillä $\mathrm{lp}_{\leq_E}(g_i)$ oltava vain Y-muuttujia, joten lauseen 7.1 perusteella jokainen polynomin $g_i$ termi sisältää vain Y-muuttujia, koska järjestyksessä $\leq_E$ X-muuttujat ovat suurempia kuin Y-muuttujat, ja tällöin jos polynomilla $g_i$ olisi X-muuttujia sisältäviä termejä, $\mathrm{lp}_{\leq_E}(g_i)$ sisältäisi X-muuttujia . Siispä $g_i \in G \cap k[Y_1, \ldots, Y_m]$. Täten jokaiselle $f \in I \cap k[Y_1, \ldots, Y_m]$ on olemassa $g_i \in G \cap k[Y_1, \ldots, Y_m]$, jolla $\mathrm{lp}_{\leq_E}(g_i)$ jakaa termin $\mathrm{lp}_{\leq_E}(f)$, ja täten $G \cap k[Y_1, \ldots, Y_m]$ on määritelmän perusteella ideaalin $I \cap k[Y_1, \ldots, Y_m]$ Gröbnerin kanta, ja väite seuraa.

**Määritelmä 7.2.** Lauseen 7.2 Mukaista ideaalia $I \cap k[Y, 1, \ldots, Y_m]$ sanotaan *eliminointi-ideaaliksi.*

**Lause 7.3.** *Olkoot $I, J$ ideaaleja polynomirenkaassa $k[X_1, \ldots, X_n]$ ja olkoon $w$ uusi muuttuja. Tällöin polynomirenkaan $k[X_1, \ldots, X_n, w]$ ideaalin $\langle wI, (1-w)J\rangle$ avulla voidaan laskea leikkaus $I \cap J$ eliminointi-ideaalina:*

$$I \cap J = \langle wI, (1-w)J\rangle \cap k[X_1, \ldots, X_n].$$

*Huomautus.* Jos $I = \langle f_1, \ldots, f_s\rangle$ ja
$J = \left\langle f_1^{'}, \ldots, f_p^{'}\right\rangle$, niin ideaalin $\langle wI, (1-w)J\rangle$ virittävä joukko on
$\left\{wf_1, \ldots, wf_s, (1-w)f_1{'}, \ldots, (1-w)f_p^{'}\right\}$.

*Todistus.* Ks. [1, s. 70] Olkoon $f \in I \cap J$. Koska

$$f = wf + (1-w)f,$$

on oltava $f \in \langle wI, (1-w)J\rangle \cap k[X_1, \ldots, X_n]$. Tällöin siis
$I \cap J \subseteq \langle wI, (1-w)J\rangle \cap k[X_1, \ldots, X_n]$.

Kääntäen, oletetaan, että $f \in \langle wI, (1-w)J\rangle \cap k[X_1, \ldots, X_n]$. Tällöin koska $f \in \langle wI, (1-w)J\rangle \cap k[X_1, \ldots, X_n]$, saadaan

$$\begin{aligned} f(x_1, \ldots, x_n) = &\sum_{i=1}^{s} wf_i(x_1, \ldots, x_n)h_i(x_1, \ldots, x_n, w) \\ &+ \sum_{j=1}^{p}(1-w)f_j^{'}(x_1, \ldots, x_n)h_j^{'}(x_1, \ldots, x_n, w). \end{aligned}$$

Koska $w$ ei esiinny arvossa $f(x_1, \ldots, x_n)$, voimme asettaa $w = 1$, ja saadaan

$$\begin{aligned} f(x_1, \ldots, x_n) = &\sum_{i=1}^{s} 1f_i(x_1, \ldots, x_n)h_i(x_1, \ldots, x_n, w) \\ &+ \sum_{j=1}^{p}(1-1)f_j^{'}(x_1, \ldots, x_n)h_j^{'}(x_1, \ldots, x_n, w) \\ = &\sum_{i=1}^{s} f_i(x_1, \ldots, x_n)h_i(x_1, \ldots, x_n), \end{aligned}$$

eli $f \in I$. Tämän jälkeen voimme asettaa $w = 0$, ja saadaan

$$\begin{aligned} f(x_1, \ldots, x_n) = &\sum_{i=1}^{s} 0f_i(x_1, \ldots, x_n)h_i(x_1, \ldots, x_n, w) \\ &+ \sum_{j=1}^{p}(1-0)f_j^{'}(x_1, \ldots, x_n)h_j^{'}(x_1, \ldots, x_n, w) \\ = &\sum_{j=1}^{p} f_j^{'}(x_1, \ldots, x_n)h_j^{'}(x_1, \ldots, x_n), \end{aligned}$$

eli $f \in J$, eli $f \in I \cap J$, ja väite seuraa.

**Lemma 7.4.** *Olkoot $f, g \in k[X_1, \ldots, X_n]$ nollasta eroavia polynomeja. Tällöin*

$$\langle f \rangle \cap \langle g \rangle = \langle \mathrm{pym}(f, g) \rangle .$$

*Todistus.* Ks. [1, s. 71] Olkoon ensin $\gamma = \mathrm{pym}(f, g)$. Tällöin $\gamma \in \langle f \rangle \cap \langle g \rangle$ pienimmän yhteisen monikerran määritelmän perusteella. Olkoon sitten $h \in \langle f \rangle \cap \langle g \rangle$. Tällöin $h = af = bg$ joillekin $a, b \in k[X_1, \ldots, X_n]$. Koska $f$ jakaa polynomin $h$ ja $g$ jakaa polynomin $h$ ja koska $\gamma$ jakaa polynomin $h$ pienimmän yhteisen monikerran määritelmän perusteella, on oltava $h \in \langle \gamma \rangle$, ja väite seuraa.

Lemman 7.4 avulla voimme laskea polynomirenkaassa $k[X_1, \ldots, X_n]$ kahden nollasta eroavan polynomin $f$ ja $g$ pienimmän yhteisen monikerran ja suurimman yhteisen tekijän. Lasketaan ensin redusoitu ideaalin $\langle wf, (1-w)g \rangle$ Gröbnerin kanta käyttäen eliminointijärjestystä $\leq_E$, missä $X_1, \ldots, X_n$ -muuttujat ovat pienempiä kuin muuttuja $w$. Tällöin $\mathrm{pym}(f, g)$ on polynomi Gröbnerin kannassa $G$, missä muuttuja $w$ ei esiinny. Suurin yhteinen tekijä voidaan laskea algoritmin 3.1, jakoalgoritmin, avulla ja saadaan $\mathrm{syt}(f, g) = \frac{fg}{\mathrm{pym}(f,g)}$. Laskettaessa pienintä yhteistä monikertaa ja suurinta yhteistä tekijää useammalle kuin kahdelle polynomille voidaan käyttää useita kertoja peräkkäin tätä metodia sekä sitä tietoa, että

$$\begin{aligned} &\mathrm{pym}(f_1, f_2, f_3) = \mathrm{pym}(f_1, \mathrm{pym}(f_2, f_3)) \text{ ja} \\ &\mathrm{syt}(f_1, f_2, f_3) = \mathrm{syt}(f_1, \mathrm{syt}(f_2, f_3)). \end{aligned}$$

**Esimerkki 7.1.** Olkoon $f = X^2Y - 2XY + Y$ ja $g = 3X^2 + 2XY - 3X - 2Y - 1$ polynomirenkaan $\mathbb{Q}[X, Y]$ polynomeja ja $\leq$ sanakirjajärjestys. Lasketaan $\mathrm{pym}(f, g)$ ja $\mathrm{syt}(f, g)$. Aloitetaan laskemalla redusoitu Gröbnerin kanta $G$ ideaalissa $\langle Wf, (1-W)g \rangle = \langle W(X^2Y - 2XY + Y), (1-W)(3X^2 + 2XY - 3X - 2Y - 1) \rangle \subseteq \mathbb{Q}[X, Y, W]$. Käyttämällä Sage-ohjelmaa, ks. [4], saadaan laskettua redusoiduksi Gröbnerin kannaksi

$$\begin{aligned} G = \{ & WX^2 - WX - 1/3W - 2X^3Y - 4/3X^2Y^2 + 4X^2Y - X^2 + 8/3XY^2 \\ & - 2XY + X - 4/3Y^2 + 1/3, WY + 6X^3Y^2 + 9X^3Y + 4X^2Y^3 \\ & - 6X^2Y^2 - 15X^2Y - 8XY^3 - 6XY^2 + 3XY + 4Y^3 + 6Y^2 + 2Y, \\ & X^4Y + 2/3X^3Y^2 - 3X^3Y - 2X^2Y^2 + 8/3X^2Y + \\ & 2XY^2 - 1/3XY - 2/3Y^2 - 1/3Y \}. \end{aligned}$$

Tällöin

$$\begin{aligned} \mathrm{pym}(f, g) = & X^4Y + 2/3X^3Y^2 - 3X^3Y - 2X^2Y^2 + 8/3X^2Y + 2XY^2 \\ & - 1/3XY - 2/3Y^2 - 1/3Y. \end{aligned}$$

Jaettaessa polynomi $fg$ polynomilla $\mathrm{pym}(f, g)$ käyttäen Sage-ohjelmaa, saadaan $\mathrm{syt}(f, g) = 3$.

Sage-ohjelman syötteet ja tulosteet on esitetty Liitteessä.

**Määritelmä 7.3.** Olkoot $I$ ja $J$ polynomirenkaan $R = k[X_1, \ldots, X_n]$ ideaaleja. Määritellään

$$J : I := \{g \in R | gI \subseteq j\}.$$

Ideaalia $J : I$ sanotaan *jäännösideaaliksi.*

**Lause 7.5.** *Olkoot $I = \langle f_1, \ldots, f_s \rangle$ ja $J$ ideaaleja polynomirenkaassa $R = k[X_1, \ldots, X_n]$. Tällöin*

$$J : I = \bigcap_{i=1}^{s} J : \langle f_i \rangle.$$

*Todistus.* Ks. [1, s. 72] Olkoon ensin $g \in J : I$. Tällöin $gI \subseteq J$, joten erityisesti $gf_i \in J$, kun $i = 1, \ldots, s$ ja tällöin

$$g \in \bigcap_{i=1}^{s} J : \langle f_i \rangle, \text{ eli}$$
$$J : I \subseteq \bigcap_{i=1}^{s} J : \langle f_i \rangle.$$

Olkoon sitten

$$g \in \bigcap_{i=1}^{s} J : \langle f_i \rangle.$$

Tällöin $g\langle f_i \rangle \subseteq J$, kun $i = 1, \ldots, s$ ja täten $gI \subseteq J$, joten $g \in J : I$, eli

$$\bigcap_{i=1}^{s} J : \langle f_i \rangle \subseteq I : J,$$

ja väite seuraa.

Edellä on esitetty tapa laskea ideaalien leikkauksia. Lauseen 7.5 avulla voidaan jäännösideaaleja $J : I$ laskettaessa keskittyä laskemaan yksittäisiä ideaalien leikkauksia $J : \langle f \rangle$, kun $f \in I$.

**Lause 7.6.** *Olkoon $R = k[X_1, \ldots, X_n]$ polynomirengas ja $J$ sen ideaali sekä $f \in R$, $f \neq 0$. Tällöin*

$$J : \langle f \rangle = \frac{1}{f}(J \cap \langle f \rangle).$$

*Todistus.* Ks. [1, s. 73] Olkoon ensin $g \in \frac{1}{f}(J \cap \langle f \rangle)$. Tällöin $gf \in J$, ja täten $g \in J\langle f \rangle$, eli $\frac{1}{f}(J \cap \langle f \rangle) \subseteq J\langle f \rangle$.

Olkoon sitten $g \in J\langle f \rangle$. Tällöin $gf \in J$, ja täten $gf \in J \cap \langle f \rangle$, joten $g \in \frac{1}{f}(J \cap \langle f \rangle)$, eli $J\langle f \rangle \subseteq \frac{1}{f}(J \cap \langle f \rangle)$, ja väite seuraa.

**Esimerkki 7.2.** Olkoot $g_1 = X^2 + Y, g_2 = -Y^2, f_1 = X^2$ ja $f_2 = X - Y$ polynomirenkaan $\mathbb{Q}[X, Y]$ polynomeja ja $\leq$ sanakirjajarjestys. Merkitään $I = \langle f_1, f_2 \rangle$ ja $J = \langle g_1, g_2 \rangle$. Lasketaan $J : I$. Lauseen 7.5 perusteella tiedetään, että

$$J : I = (J : \langle f_1 \rangle) \cap (J : \langle f_2 \rangle)$$

ja lauseen 7.6 perusteella taas

$$J : I = \frac{1}{f_1}(J \cap \langle f_1 \rangle) \cap \frac{1}{f_2}(J \cap \langle f_2 \rangle).$$

Ensin lasketaan $J \cap \langle f_1 \rangle$ laskemalla Gröbnerin kanta $G_1$ ideaalille $\langle Wg_1,\ Wg_2,\ (1 - W)f_1 \rangle \subseteq \mathbb{Q}[X,\ Y,\ W]$. Tästä saadaan Sage-ohjelmaa käyttämällä, ks. [4] Gröbnerin kannaksi

$$G_1 = \{WX^2 - X^2, WY + X^2, X^4, X^2Y\},$$

ja tästä saadaan

$$\begin{aligned}\frac{1}{f_1}(J \cap \langle f_1 \rangle) &= \langle \frac{1}{X^2}(X^4), \frac{1}{X^2}(X^2Y) \rangle \\ &= \langle X^2, Y \rangle.\end{aligned}$$

Seuraavaksi lasketaan $J \cap \langle f_2 \rangle$ laskemalla Gröbnerin kanta $G_2$ ideaalille $\langle Wg_1,\ Wg_2,\ (1 - W)f_2 \rangle \subseteq \mathbb{Q}[X,\ Y,\ W]$ käyttäen samaa metodia kuin edellä. Tästä saadaan

$$\begin{aligned}G_2 = \{&WX + X^2 - X - Y^2 + Y, WY + X^2 - Y^2, X^3 + XY - Y^3 - Y^2, \\ &X^2Y - Y^3, XY^2 - Y^3\},\end{aligned}$$

ja tästä saadaan

$$\begin{aligned}\frac{1}{f_2}(J \cap \langle f_2 \rangle) =& \langle \frac{1}{X - Y}(X^3 + XY - Y^3 - Y^2), \frac{1}{X - Y}(X^2Y - Y^3), \\ & \frac{1}{X - Y}(XY^2 - Y^3) \\ =& \langle X^2 + XY + Y^2 + Y, XY + Y^2, Y^2 \rangle.\end{aligned}$$

Nyt voidaan laskea

$$\langle X^2, Y \rangle \cap \langle X^2 + XY + Y^2 + Y, XY + Y^2, Y^2 \rangle$$

laskemalla Gröbnerin kanta $G$ ideaalissa

$$\begin{aligned}&\langle WX^2, WY, (1 - W)(X^2 + XY + Y^2 + Y), (1 - W)(XY + Y^2), (1 - W)Y^2 \rangle \\ &\subseteq \mathbb{Q}[W, X, Y],\end{aligned}$$

mistä saadaan Sage-ohjelmaa käyttäen

$$G = \{WY, X^2 + Y, XY, Y^2\},$$

joten $J : I = \langle X^2 + Y, XY, Y^2 \rangle$.

Sage-ohjelman syötteet ja tulosteet ovat nähtävissä Liitteessä.

## 7.2 Polynomiyhtälöryhmien ratkaiseminen

Yksi hyödyllinen ja käytetty Gröbnerin kantojen sovellus on polynomiyhtälöryhmien ratkaisu. Tässä luvussa osoitetaan, että mikä tahansa polynomiyhtälöryhmä voidaan esittää näitä yhtälöitä vastaavien polynomien virittämän ideaalin Gröbnerin kantana siten, että niiden juuret ovat samat. Tämän jälkeen voidaan tästä yhtälöryhmästä eliminoida muuttujia, jolloin yhtälöryhmän ratkaiseminen koulumatematiikasta tutuilla metodeilla, kuten Euklideen algoritmin avulla, on mahdollista.

Aikaisemmissa luvuissa on osoitettu, että Gröbnerin kantoja voidaan konstruoida algoritmisesti. Täten myös polynomiyhtälöryhmän ratkaiseminen voidaan tehdä algoritmisesti, joten kyseessä on varsin houkutteleva mahdollisuus soveltaa metodia polynomiyhtälöryhmien ratkaisemiseen tietokoneen avulla.

**Määritelmä 7.4.** Olkoon $R = k[X_1, \ldots, x_n]$ ja $f_1, \ldots, f_m \in R$. Määritellään *affiini varisto* $V(f_1, \ldots, f_m)$ seuraavasti:

$$V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in k^n | f_i(a_1, \ldots, a_n) = 0 \text{ kaikilla } i = 1, \ldots, m\}.$$

**Lause 7.7.** *Olkoon* $f_1, \ldots, f_m \in R = k[X_1, \ldots, X_n]$ *ja* $I = \langle f_1, \ldots, f_m \rangle$. *Nyt*

$$V(f_1, \ldots, f_m) = V(I).$$

*Todistus.* Ks. [2, s. 80] Olkoon $(a_1, \ldots, a_n) \in V(I)$. Nyt siis $g(a_1, \ldots, a_n) = 0$ aina, kun $g \in I$. Koska kuitenkin $I = \langle f_1, \ldots, f_m \rangle$ ja tämän vuoksi $f_1, \ldots, f_m \in I$, on oltava myös $f_i(a_1, \ldots, a_n) = 0$ kaikilla $i = 1, \ldots, m$ ja täten $V(I) \subseteq V(f_1, \ldots, f_m)$.

Olkoot sitten $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_m)$ ja $g \in I$. Koska $I = \langle f_1, \ldots, f_m \rangle$, voidaan $g$ kirjoittaa muotoon

$$g = \sum_{i=1}^{s} h_i f_i$$

joillakin $h_i \in R$. Tällöin kuitenkin

$$\begin{aligned} g(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 \\ &= 0. \end{aligned}$$

On siis oltava $(a_1, \ldots, a_n) \in V(I)$ ja $V(f_1, \ldots, f_m) \subseteq V(I)$, ja väite seuraa.

**Lause 7.8.** *Olkoon* $\langle f_1, \ldots, f_m \rangle = I \in k[X_1, \ldots, X_n]$ *ideaali ja* $G = \{g_1, \ldots, g_s\}$ *sen Gröbnerin kanta. Nyt*

$$V(f_1, \ldots, f_m) = V(g_1, \ldots, g_s).$$

*Todistus.* Väite seuraa suoraan Lauseesta 7.7 ja korollaarista 4.7.

Huomataan siis, että laskettaessa polynomijoukon affiinia varistoa, eli koulumatematiikan tapauksessa polynomiyhtälöryhmää, riittää laskea näiden polynomien virittämän ideaalin Gröbnerin kannan affiininen varisto. Tämä taas on yleensä selvästi helpompi tehtävä, koska Gröbnerin kannassa voidaan eliminoida muuttujia, ja näin yhtälöryhmä voidaan ratkaista muuttuja kerrallaan.

**Esimerkki 7.3.** Ratkaistaan kompleksinen yhtälöryhmä

$$\begin{cases} V + X - Y - Z = 1 \\ V + X + Y^3 - Z = 1 \\ V - X - Y^2 + Z = 1 \\ V + X - Y - Z^2 = 1. \end{cases}$$

Muodostetaan polynomirenkaassa $\mathbb{C}[V, X, Y, Z]$ ideaali $I$ seuraavasti:

$$\begin{aligned} I = &\langle V + X - Y - Z - 1, V + X + Y^3 - Z - 1, V - X - Y^2 + Z - 1, \\ &V + X - Y - Z^2 - 1\rangle. \end{aligned}$$

Olkoon $\leq$ sanakirjajärjestys. Muodostamalla ideaalin $I$ redusoitu Gröbnerin kanta $G$ järjestyksessä $\leq$ käyttämällä Sage-ohjelmaa, ks. [4], saadaan $G = \{g_1, g_2, g_3, g_4\}$, missä

$$\begin{aligned} g_1 &= V - \frac{1}{2}Y^2 - \frac{1}{2}Y - 1 \\ g_2 &= X + \frac{1}{2}Y^2 - \frac{1}{2}Y - Z \\ g_3 &= Y^3 + Y \\ g_4 &= Z^2 - Z. \end{aligned}$$

Nyt $g_4 = Z^2 - Z$, mistä huomataan, että mahdolliset Z-muuttujan nollakohdat ovat 0 ja 1. Lisäksi $g_3 = Y^3 + Y$, mistä huomataan, että mahdolliset Y-muuttujan nollakohdat ovat $0, i$ ja $-i$. Sijoittamalla nämä arvot polynomeihin $g_1$ ja $g_2$ saadaan laskettua X- ja V-muuttujien nollakohdat, ja lopulta

$$\begin{aligned} V(G) = \{&(1,0,0,0), (1,1,0,1), (-\frac{1}{2}i + \frac{1}{2}, -\frac{1}{2}i + \frac{3}{2}, -i, 1), \\ &(-\frac{1}{2}i + \frac{1}{2}, -\frac{1}{2}i + \frac{1}{2}, -i, 0), (\frac{1}{2}i + \frac{1}{2}, \frac{1}{2}i + \frac{3}{2}, i, 1), \\ &(\frac{1}{2}i + \frac{1}{2}, \frac{1}{2}i + \frac{1}{2}, i, 0)\}. \end{aligned}$$

Aikaisemman perusteella tiedetään ja laskemalla voidaan tarkistaa, että $V(G)$ on alkuperäisen yhtälöryhmän ratkaisujoukko.

Lauseen 7.2 avulla voidaan muodostaa ideaalin $I$ eliminointi-ideaali $I_1 = I \cap \mathbb{C}[X, Y, Z]$ ja tästä taas uusi eliminointi-ideaali $I_2 = (I \cap \mathbb{C}[X, Y, Z]) \cap \mathbb{C}[Y, Z]$. Tällöin

$$\begin{aligned} I_1 &= \langle X + \frac{1}{2}Y^2 - \frac{1}{2}Y - Z, Y^3 + Y, Z^2 - Z \rangle \\ &= \langle g_2, g_3, g_4 \rangle \text{ ja} \\ I_2 &= \langle Y^3 + Y, Z^2 - Z \rangle \\ &= \langle g_3, g_4 \rangle. \end{aligned}$$

Eliminointi-ideaalin avulla voidaan siis eliminoida täsmälleen haluttu määrä muuttujia, kunnes ideaalissa on jäljellä vähintään kaksi virittäjää. Oleelliseksi ongelmaksi yhtälöryhmien ratkaisemisessa muodostuukin näin sopivan termijärjestyksen valinta, jotta polynomiyhtälöryhmästä muodostetun ideaalin Gröbnerin kanta olisi mahdollisimman sopiva.

Liitteessä on esitetty Sage-ohjelman syötteet ja tulosteet sekä Gröbnerin kannan laskussa että yhtälöryhmän ratkaisussa.

# Lähteet


[1] William W. Adams, Philippe Loustaunau: *An introduction to Gröbner bases*. The American Mathematical Society, 1994

[2] David Cox, John Little, Donal O'Shea: *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*. New York: Springer, cop. 2007

[3] Lauritzen, Niels: *Concrete Abstract Algebra*. Cambridge University Press, 2003

[4] http://www.sagemath.org/

# Liite

Tässä liitteessä esitetään niiden tutkielman esimerkkien Gröbnerin kantojen laskeminen, jotka on laskettu tietokoneen avulla. Tässä tapauksessa on käytetty Sage-ohjelmaa, Ks. [4]. Ohjelma on tekstisyöttöön perustuva avoimen lähdekoodin matemaattinen ohjelmisto. Ensimmäisessä kuvassa esitetään esimerkin 7.1 Gröbnerin kannan ja pienimmän yhteisen tekijän laskeminen. Sage antaa komennon Groebnerbasis avulla tulosteena redusoidun Gröbnerin kannan. Toisessa kuvasssa esitetään esimerkin 7.2 Gröbnerin kantojen laskeminen sekä joidenkin monimutkaisempien polynomien jakolaskujen laskeminen Sage-ohjelmalla. Kolmannessa kuvassa esitetään esimerkin 7.3 Gröbnerin kannan laskenta sekä tästä kannasta muodostetun polynomiyhtälöryhmän että myös alkuperäisen yhtälöryhmän ratkaisu Sage-ohjelman solve-komennon avulla ratkaistuna.

## Esimerkki 6.1.

```
sage: P.<W,X,Y> = PolynomialRing(QQ,3,order='lex')
sage: I = ideal((W*(X^2*Y-2*X*Y+Y)), ((W-1)*(3*X^2+2*X*Y-3*X-2*Y-1)))
sage: B = I.groebner_basis()
sage: print(B)
```

```
[W*X^2 - W*X - 1/3*W - 2*X^3*Y - 4/3*X^2*Y^2 + 4*X^2*Y - X^2 +
8/3*X*Y^2 - 2*X*Y + X - 4/3*Y^2 + 1/3, W*Y + 6*X^3*Y^2 + 9*X^3*Y +
4*X^2*Y^3 - 6*X^2*Y^2 - 15*X^2*Y - 8*X*Y^3 - 6*X*Y^2 + 3*X*Y + 4*Y^3
+ 6*Y^2 + 2*Y, X^4*Y + 2/3*X^3*Y^2 - 3*X^3*Y - 2*X^2*Y^2 + 8/3*X^2*Y
+ 2*X*Y^2 - 1/3*X*Y - 2/3*Y^2 - 1/3*Y]
```

```
((X^2*Y-2*X*Y+Y)*(3*X^2+2*X*Y-3*X-2*Y-1))/(X^4*Y+2/3*X^3*Y^2-3*X^3*Y-
2*X^2*Y^2+8/3*X^2*Y+2*X*Y^2-1/3*X*Y-2/3*Y^2-1/3*Y)
```

```
3
```

## Esimerkki 6.2.

```
sage: P.<W,X,Y> = PolynomialRing(QQ,3,order='lex')
sage: I = ideal((W*(X^2+Y)), (W*(-Y^2)), ((1-W)*(X^2)))
sage: B = I.groebner_basis()
sage: print(B)
```

```
[W*X^2 - X^2, W*Y + X^2, X^4, X^2*Y]
```

```
sage: P.<W,X,Y> = PolynomialRing(QQ,3,order='lex')
sage: I = ideal((W*(X^2+Y)), (W*(-Y^2)), ((1-W)*(X-Y)))
sage: B = I.groebner_basis()
sage: print(B)
```

```
[W*X + X^2 - X - Y^2 + Y, W*Y + X^2 - Y^2, X^3 + X*Y - Y^3 - Y^2,
X^2*Y - Y^3, X*Y^2 - Y^3]
```

```
sage: (X^3+X*Y-Y^3-Y^2)/(X-Y)
```

```
X^2 + X*Y + Y^2 + Y
```

```
sage: (X^2*Y-Y^3)/(X-Y)
```

```
X*Y + Y^2
```

```
(X*Y^2-Y^3)/(X-Y)
```

```
Y^2
```

```
sage: P.<W,X,Y> = PolynomialRing(QQ,3,order='lex')
sage: I = ideal((W*X^2), (W*Y), ((1-W)*(X^2+X*Y+Y^2+Y)), ((1-W)*(X*Y+Y^2)),
((1-W)*Y^2))
sage: B = I.groebner_basis()
sage: print(B)
```

```
[W*Y, X^2 + Y, X*Y, Y^2]
```

## Esimerkki 6.3.

```
sage: P.<V, X, Y, Z> = PolynomialRing(QQ,4,order='lex')
sage: I = ideal((V+X-Y-Z-1), (V+X+Y^3-Z-1), (V-X-Y^2+Z-1), (V+X-Y-Z^2-1))
sage: B = I.groebner_basis()
sage: print(B)
```

```
[V - 1/2*Y^2 - 1/2*Y - 1, X + 1/2*Y^2 - 1/2*Y - Z, Y^3 + Y, Z^2 - Z]
```

```
sage: V, X, Y, Z = var('V, X, Y, Z')
sage: solve([V-(1/2)*Y^2-1/2*Y==1, X+1/2*Y^2-(1/2)*Y-Z==0, Y^3+Y==0,
Z^2-Z==0], V, X, Y, Z)
```

```
[[V == 1, X == 0, Y == 0, Z == 0], [V == (-1/2*I + 1/2), X ==
(-1/2*I + 1/2), Y == -I, Z == 0], [V == (1/2*I + 1/2), X == (1/2*I +
1/2), Y == I, Z == 0], [V == 1, X == 1, Y == 0, Z == 1], [V ==
(-1/2*I + 1/2), X == (-1/2*I + 3/2), Y == -I, Z == 1], [V == (1/2*I
+ 1/2), X == (1/2*I + 3/2), Y == I, Z == 1]]
```

```
sage: V, X, Y, Z = var('V, X, Y, Z')
sage: solve([V+X-Y-Z==1, V+X+Y^3-Z==1, V-X-Y^2+Z==1, V+X-Y-Z^2==1], V, X, Y,
Z)
```

```
[[V == (-1/2*I + 1/2), X == (-1/2*I + 3/2), Y == -I, Z == 1], [V ==
(1/2*I + 1/2), X == (1/2*I + 3/2), Y == I, Z == 1], [V == (-1/2*I +
1/2), X == (-1/2*I + 1/2), Y == -I, Z == 0], [V == (1/2*I + 1/2), X
== (1/2*I + 1/2), Y == I, Z == 0], [V == 1, X == 1, Y == 0, Z == 1],
[V == 1, X == 0, Y == 0, Z == 0]]
```