Polynomialgebra 2007

Samuli Piipponen
Joensuun yliopisto

Sisältö

1 yksi

2 Polynomialgebra

2.1 Monomijärjestykset ja jakoalgoritmi

Joukossa $\mathbb{N}$ on luonnollinen järjestysrelaatio $<$ esim. $2 < 3$. Tämä indusoi yhden yhden muuttujan polynomien monomeille järjestyksen $x^k < x^n \Leftrightarrow k < n$. Tarkastellaan sitten usean muuttujan tapausta.

- $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ on *moni-indeksi*
- $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ on *monomi*
- $a_\alpha x^\alpha$, $a_\alpha \in \mathbb{K}$ on *termi*
- $\mathbb{K}[x_1, \ldots, x_n]$ on *polynomirengas*

Määritelmä 2.1.1. Relaatio $<$ on *lineaarinen järjestys* joukossa S, jos $\forall\ x, y \in S$ joko $x < y$, $x = y$ tai $y < x$.

Esimerkki 2.1.2. *a.*) $S = \mathbb{N}^2$. Määritellään $\alpha \leq \beta$ jos $[\alpha_1 \leq \beta_1,\ \alpha_2 \leq \beta_2]$. Nyt esimerkiksi alkioita $\alpha = (2, 3) \in \mathbb{N}^2$ ja $\beta = (3, 2) \in \mathbb{N}^2$ ei voi verrata kyseisellä relaatiolla, sillä $\alpha_1 \leq \beta_1$, mutta $\beta_2 \leq \alpha_2$. Näin ollen $\leq$ ei ole lineaarinen järjestys.

b.) $S = \mathbb{N}^2$. Määritellään $\alpha < \beta$ jos $\alpha_1 < \beta_1$ tai $\alpha_1 = \beta_1$ ja $\alpha_2 < \beta_2$. Kyseinen järjestys on lineaarinen järjestys.

Usein halutaan lisäki implikaation

$$\alpha < \beta \ \Rightarrow\ \alpha + \gamma < \beta + \gamma$$

olevan voimassa. Monomeiden tapauksessa

$$x^\alpha < x^\beta \ \Rightarrow\ x^\alpha x^\gamma < x^\beta x^\gamma.$$

Määritelmä 2.1.3. Oletetaan, että joukossa S on annettu lineaarinen järjestys $<$. Joukon S sanotaan olevan *hyvinjärjestetty*, jos $\forall\ B \subset S\ \exists\ a \in B$ siten, että $a \leq c \quad \forall\ c \in B$. Järjestyksen $<$ sanotaan tällöin olevan *hyvinjärjestys*.

Esimerkki 2.1.4.

1. $\mathbb{N}$ on hyvinjärjestetty.
2. Joukkoa $S = [0,1] \subset \mathbb{R}$ ei ole hyvinjärjestetty sillä esim. joukkolla

$$B = \left\{ \frac{1}{n+1} \mid n \in \mathbb{N} \right\}$$

ei ole pienintä alkiota, sillä $\inf(B) = 0 \notin B$.

Todistetaan, että esimerkissä 4.0.2(b) määritelty järjestys $<$ on hyvinjärjestys. Olkoon

$$a_1 = \min\{\alpha_1 \in \mathbb{N} \mid \alpha = (\alpha_1, \alpha_2) \in B\}.$$

Minimi on olemassa, sillä $\mathbb{N}$ on hyvinjärjestetty. Olkoon

$$\widetilde{B} = \{\alpha \in B \mid \alpha_1 = a_1\},$$

ja olkoon

$$a_2 = \min\{\alpha_2 \in \mathbb{N} \mid \alpha = (a_1, \alpha_2) \in \widetilde{B}\}.$$

Minimi on jälleen olemassa, ja $a = (a_1, a_2) = \min(B)$

Lemma 2.1.5. *Olkoon joukossa $\mathbb{N}^n$ annettu järjestys $<$ siten, että*

1. *$<$ on lineaarinen järjestys*
2. *$\alpha < \beta \;\Rightarrow\; \alpha + \gamma < \beta + \gamma$.*

Tällöin $<$ on hyvinjärjestys jos ja vain jos $\alpha \geq 0 \quad \forall\ \alpha \in \mathbb{N}^n$.

Määritelmä 2.1.6. $<$ On *monomijärjestys* joukossa $\mathbb{N}^n$, jos

1. $<$ on lineaarinen järjestys
2. Implikaatio $\alpha < \beta \;\Rightarrow\; \alpha + \gamma < \beta + \gamma$ on voimassa.
3. $\alpha \geq 0 = (0, \ldots, 0)$.

Määritelmä 2.1.7 (Aakkosjärjestys)**.** Olkoon $\alpha, \beta \in \mathbb{N}^n$, tällöin $\alpha >_{lex} \beta$, jos $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$, ja $\alpha_{k+1} > \beta_{k+1}$.

Esimerkki 2.1.8.

1. Esimerkissä 4.0.2(b) esitetty järjestys on aakkosjärjestys.

2. Olkoon $\alpha = (2, 5, 0, 3)$ ja $\beta = (2, 2, 9, 1)$ tällöin $\alpha >_{lex} \beta$. Monomien avulla kirjoitettuna $m_1 = x_1^2 x_2^5 x_4^3 >_{lex} x_1^2 x_2^2 x_3^9 x_4 = m_2$. Kuitenkin $deg(m_1) = 10 < deg(m_2) = 14$.

3. Joukossa $\mathbb{N}^4$ saadaan $(1, 0, 0, 0) >_{lex} (0, 1, 0, 0) >_{lex}$, joten $x_1 >_{lex} x_2 >_{lex} x_3 >_{lex} x_4$. Permutoimalla muuttujia x_1, x_2, x_3, x_4 saadaan $4! = 24$ aakkosjärjestystä.

Määritelmä 2.1.9.
a.)
Määritellään järjestys $>_{grlex}$ joukossa $\mathbb{N}^n$. $\alpha >_{grlex} \beta$, jos $|\alpha| > |\beta|$ tai $|\alpha| = |\beta|$, $\alpha >_{lex} \beta$. Järjestystä $>_{grlex}$ sanotaan *porrastetuksi aakkosjärjestykseksi*

b.)
Määritellään järjestys $>_{grevlex}$ joukossa $\mathbb{N}^n$. $\alpha >_{grevlex} \beta$ jos $|\alpha| > |\beta|$ tai $|\alpha| = |\beta|$ ja $\alpha_n = \beta_n, \ldots, \alpha_{n-i+1} = \beta_{n-i+1}$, $\alpha_{n-i} < \beta_{n-i}$.

Esimerkki 2.1.10. Oletetaan $x > y > z$. Järjestetään polynomin f termit (suurin vasemmalla) eri monomijärjestyksien avulla

1. lex: $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$

2. grlex: $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$

3. grevlex: $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$.

Määritelmä 2.1.11. Olkoon $f \in \mathbb{K}[x_1, \ldots, x_n]$ polynomi

$$f = \sum_{\alpha} a_\alpha x^\alpha.$$

Polynomin f *monomiaste* on

$$mdeg(f) = \max\{\alpha \mid a_\alpha \neq 0\}$$

Polynomin f *isoin monomi* on

$$LM(f) = x^{mdeg(f)}.$$

Polynomin f *isoin kerroin* on

$$LC(f) = a_{mdeg}(f)$$

Polynomin f *isoin termi* on

$$LT(f) = LC(f)LM(f).$$

Yhden muuttujan tapauksessa saatiin tulos: Jos $f_1, \ldots, f_s \in \mathbb{K}[x]$ ja $g = syt(f_1, \ldots, f_s)$, niin

$$I = \langle f_1, \ldots, f_s \rangle = \langle g \rangle.$$

Jos on annettu $f \in \mathbb{K}[x]$, niin jakolaskualgoritmin avulla $f = hg + r$, ja jos $r = 0$ niin tämä on yhtäpitävää sen kanssa, että $f \in I$. Usean muuttujan tapauksessa voidaan kysyä: Jos on annettu $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ ja $I = \langle f_1, \ldots, f_s \rangle$, niin koska $f \in I$ ja onko olemassa algoritmia, jonka avulla saadaan esitys

$$f = a_1 f_1 + \ldots + a_s f_s + r.$$

Tarkastellaan sitten mahdollista jakolaskualgoritmia

Esimerkki 2.1.12. Käytetään aakkosjärjestystä $x > y$, ja olkoon

$$\begin{aligned} f &= xy^2 + 1 \\ f_1 &= xy + 1 \\ f_2 &= y + 1 \end{aligned}$$

Halutaan siis esitys

$$f = a_1 f_1 + a_2 f_2 + r, \quad a_1, a_2 \in \mathbb{K}[x, y].$$

Nyt $LT(f_1) = xy$, $LT(f_2) = y$, joten $y * LT(f_1) = xy^2 = LT(f)$ ja $x^2 * LT(f_2) = x^2 y$, joten sekä $LT(f_1)$, että $LT(f_2)$ jakaa termin $LT(f)$. Asetetaan sitten $a_1 = a_2 = 0$ ja $r = f$. Tämän jälkeen edetään

$$\begin{aligned} a_1 &:= a_1 + \frac{LT(r)}{LT(f_1)} = y \\ r &:= r - \frac{LT(r)}{LT(f_1)} f_1 = -y + 1 \end{aligned}$$

Nyt $LT(f_1)$ ei enää jaa termiä $LT(r) = -y$, joten siirrytään käyttämään termiä $LT(f_2) = y$. Tästä saadaan

$$\begin{aligned} a_2 &:= a_2 + \frac{LT(r)}{LT(f_2)} = -1 \\ r &:= r - \frac{LT(r)}{LT(f_2)} f_2 = 2. \end{aligned}$$

Näin ollen saatiin esitys

$$x^2 y + 1 = y(xy + 1) + (-1)(y + 1) + 2.$$

Tarkastellaan sitten seuraavaa esimerkkiä

$$\begin{aligned} f &= x^2y + xy^2 + y^2 \\ f_1 &= xy - 1 \\ f_2 &= y^2 - 1. \end{aligned}$$

Nyt $LT(f_1)$ jakaa termin $LT(p) = LT(f) = x^2y$. Tästä saadaan

$$\begin{aligned} a_1 &:= x \\ p &:= p - xf_1 = xy^2 + x + y^2. \end{aligned}$$

Edelleen $LT(f_1)$ jakaa termin $LT(p) = xy^2$ ja $LT(p)/LT(f) = y$, joten

$$\begin{aligned} a_1 &:= a_1 + y = x + y \\ p &:= p - yf_1 = x + y^2 + y. \end{aligned}$$

Nyt kumpikaan termeistä $LT(f_1), LT(f_2)$ ei jaa termiä $LT(p) = x$, joten se siirretään jakojäännökseen, ja näin ollen

$$\begin{aligned} r &:= x \\ p &:= y^2 + y. \end{aligned}$$

Nyt $LT(f_2) = y^2$ jakaa termin $LT(p) = y^2$ ja algoritmiä voidaan jatkaa

$$\begin{aligned} a_2 &:= 1 \\ p &:= p - 1 * f_2 = y + 1. \end{aligned}$$

Nyt kumpikaan termeistä $LT(f_1), LT(f_2)$ ei enää jaa termiä $LT(p) = y$, eikä termiä 1 joten loppu siirretään jakojäännökseen, ja näin ollen

$$f = a_1f_1 + a_2f_2 + r = (x + y) * f_1 + 1 * f_2 + x + y + 1.$$

Lause 2.1.13. *Olkoon $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Edellinen algoritmi antaa polynomit $a_1, \ldots, a_s, r$ siten, että*

$$f = a_1f_1 + \ldots + a_sf_s + r,$$

missä

1. *$LT(f_i)$ ei jaa mitään polynomin r termeistä*
2. *$mdeg(f) \geq mdeg(a_if_i)$.*

Todistus. Koska algoritmi antaa selvästi polynomit $a_1, \ldots, a_n, r$ siten, että

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

riittää todistaa että algoritmi päättyy äärellisen askelmäärän jälkeen. Algoritmi päättyy, kun $p := 0$. Alussa $p := f$ ja jokaisella kierroksella, joko

1. $p = p - \frac{LT(p)}{LT(f_i)} f_i$, tai
2. $p := p - LT(p)$.

Nyt

$$LT\Big(\frac{LT(p)}{LT(f_i)}\Big) f_i = LT(p)$$

Siis molemmissa tapauksissa

$$mdeg(p_{uusi}) < mdeg(p).$$

Koska monomijärjestys on hyvinjärjestys polynomin p monomiaste voi vähentyä vain äärellisen monta kertaa, joten algoritmi päättyy äärellisen askelmäärän jälkeen.

2.2 Hilbertin kantalause ja Gröbner kannat

Määritelmä 2.2.1. Ideaali $I \subset \mathbb{K}$ on *monomi-ideaali*, jos on olemassa $A \subset \mathbb{N}^n$ siten, että jokainen polynomi $f \in I$ on muotoa

$$f = \sum_{\alpha \in A} p_\alpha x^\alpha, \qquad p_\alpha \in \mathbb{K}[x_1, \ldots, x_n].$$

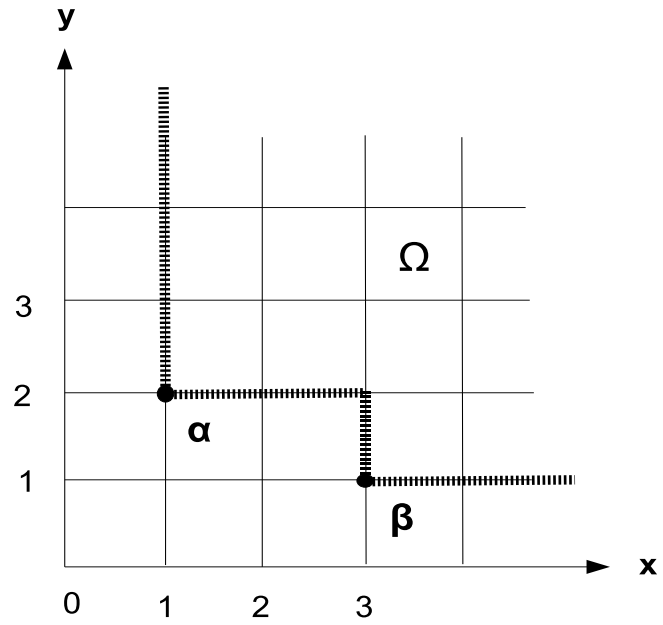
Merkitään tällöin

$$I = \langle x^\alpha,\ \alpha \in A \rangle.$$

Esimerkki 2.2.2. Olkoon esimerkiksi

$$I = \langle x^3y, xy^2 \rangle$$

monomi-ideaali. Seuraavassa kuvassa on havainnollistettu mitkä monomit voivat kuulua monomi-ideaalin I polynomien monomeihin.



Kuva 1: Mahdolliset monomi-ideaaliin kuuluvien polynomien monomit alueessa Ω.

Lemma 2.2.3. *Olkoon $I = \langle x^\alpha,\ \alpha \in A \rangle$ monomi-ideaali, ja olkoon x^β monomi. Tällöin seuraava ekvivalenssi on voimassa*

$$x^\beta \in I \quad \Leftrightarrow \quad x^\beta = x^\gamma x^\alpha \quad \textit{jollakin } \alpha \in A.$$

Ts. x^α jakaa monomin x^β jollakin $\alpha \in A$.

Todistus. ($\Leftarrow$)
Jos x^α jakaa monomin x^β, niin $x^\beta = x^\gamma x^\alpha \in I$.
($\Rightarrow$)

$$x^\beta \in I \quad \Rightarrow \quad x^\beta = \sum_{i=1}^{k} p_i x^{\alpha_i}, \quad p_i \in \mathbb{K}[x_1, \ldots, x_n]$$

Oikean puolen jokainen termi on jaollinen *jollain* monomilla x^{α^l}, joten sama pätee myös vasemmalle puolelle (vaikka vasemmalla puolella on vain yksi termi!).

Lause 2.2.4 (Dicksonin lemma)**.** *Olkoon* $I = \langle x^\alpha \mid \alpha \in A \rangle$*. Tällöin on olemassa multi-indeksit* $\alpha^1, \ldots, \alpha^s \in A$ *siten, että*

$$I = \langle x^{\alpha^1}, \ldots, x^{\alpha^s} \rangle.$$

Toisin sanoen jokainen monomi-ideaali on äärellisesti generoitu.

Lemma 2.2.5. *Olkoon* $I = \langle x^{\alpha^1}, \ldots, x^{\alpha^s} \rangle$ *ja* $f \in \mathbb{K}[x_1, \ldots, x_n]$*. Tällöin on voimassa ekvivalenssi*

$$f \in I \quad \Leftrightarrow \quad \textit{jakojäännös } r = 0.$$

Todistus. ($\Leftarrow$)
Jos $r = 0$, niin määritelmän mukaan $f \in I$.
($\Rightarrow$)
Jos $f \in I$, niin

$$f = \sum_{i=1}^{k} p_i x^{\alpha^i}.$$

Tällöin polynomin f *jokainen* termi on jaollinen jollain x^{α^l} ja näin ollen jakolaskualgoritmissa $r = 0$.

Esimerkki 2.2.6. Olkoon $I = \langle x^2y, xy^2 \rangle$ ja

$$f = x^4y^2 + x^3y^2 + x^3y + xy^3.$$

Aluksi $p := f$. Koska x^2y jakaa termin $LT(f) = x^4y^2$, niin

$$\begin{aligned} a_1 &:= x^2y \\ p &:= x^3y^2 + x^3y + xy^3 \end{aligned}$$

Koska jälleen x^2y jakaa termin $LT(p) = x^3y^2$ saadaan

$$\begin{aligned} a_1 &:= x^2y + xy \\ p &:= x^3y + xy^3. \end{aligned}$$

Edelleen x^2y jakaa termin $LT(p) = x^3y$ ja

$$\begin{aligned} a_1 &:= x^2y + xy + x \\ p &:= xy^3 \end{aligned}$$

Termiä $p := xy^3$ ei termi x^2y enää jaa mutta termi xy^2 jakaa

$$\begin{aligned} a_2 &:= y \\ p &:= 0 \end{aligned}$$

Näin ollen

$$f := (x^2y + xy + x) * x^2y + y * xy^2 = x^4y^2 + x^3y^2 + x^3y + xy^3.$$

Todistus. [Dickson] Todistetaan lause induktiolla muuttujien lukumäärän suhteen.
1.
Tapauksessa $n = 1$ $\langle 1 \rangle$ matala-asteisin monomi $\alpha_1 \in A$, $m = x^{\alpha_1}$ virittää loput ideaalin monomit, joten tapaus $n = 1$ on O.K.
2.
Oletetaan, että väite pätee kun muuttujia on $n - 1$ kappaletta ja todistetaan että tästä seuraa, että se pätee myös kun muuttujia on n kappaletta. Merkitään

$$B = \mathbb{K}[x_1, \ldots, x_{n-1}, y]$$

Olkoon $I \subset B$ sitten monomi-ideaali,

$$I = \langle x^\alpha y^m \mid (\alpha, m) \in A \rangle, \quad \alpha \in \mathbb{N}^{n-1}.$$

Olkoon

$$J = \langle x^\alpha \mid (\alpha, m) \in A \text{ jollekkin } m \rangle \subset \mathbb{K}[x_1, \ldots, x_{n-1}].$$

Induktio-oletuksen mukaan on olemassa moni-indeksit $\alpha^1, \ldots, \alpha^s$ siten, että

$$J = \langle x^{\alpha^1}, \ldots, x^{\alpha^s} \rangle.$$

Siis $(\alpha^i, m_i) \in A$ jollekkin m_i. Olkoon sitten

$$m = \max(m_i).$$

Olkoon $J_k \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$

$$J_k = \langle x^\beta \mid x^\beta y^k \in \rangle, \quad 0 \leq k < m.$$

Nyt $J = J_m$, ja kaikki idaalit J_k ovat monomi-ideaaleja ja induktio-oletuksen perusteella niillä on äärellinen kanta

$$J_k = \langle x^{\alpha^{1,k}}, \ldots, x^{\alpha^{s_k,k}} \rangle.$$

Nyt väitetään, että ideaalin I virittää monomit

$$\begin{aligned} J_0 &= x^{\alpha^{1,0}}, \ldots, x^{\alpha^{s_0,0}} \\ &\vdots \\ J_{m-1} &= x^{\alpha^{1,m-1}} y^{m-1}, \ldots, x^{\alpha^{s_{m-1},m-1}} y^{m-1} \\ J_m &= x^{\alpha^1} y^m, \ldots, x^{\alpha^s,m} y^m \end{aligned}$$

Lemman 2.2.3 perusteella $x^\alpha y^p \in I \Leftrightarrow x^\alpha y^p$ on jaollinen jollain ideaalin I monomeista. Saadaan kaksi tapausta. Olkoon $x^\alpha y^p \in I$

1. Jos $p \geq m \Rightarrow$ ideaalin I konstruktion perusteella on olemassa monomi $x^{\alpha^i} y^m$ joka jakaa monomin $x^\alpha y^p$
2. Jos $p < m \Rightarrow$ ideaalien J_k konstruktion perusteella on olemassa $l, \alpha^{i,l}$ siten, että monomi $x^\alpha y^\alpha$ on jaollinen monomilla $x^{\alpha^{i,l}}$.

Esimerkki 2.2.7. Olkoon $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$. Tällöin

$$\begin{aligned} J_5 &= \langle x^k \mid x^k y^m \in I \rangle = \langle x^2 \rangle = J \\ J_0 &= \langle x^k \mid x^k \in I \rangle = \{0\} \\ J_1 &= \langle x^k \mid x^k y \in I \rangle = \{0\} \\ J_2 &= \langle x^k \mid x^k y^2 \in I \rangle = \{x^4\} \\ J_3 &= \langle x^k \mid x^k y^3 \in I \rangle = \{x^4\} \\ J_4 &= \langle x^k \mid x^k y^3 \in I \rangle = \{x^3\}, \end{aligned}$$

joten

$$I = \langle x^4y^2, x^4y^3, x^3y^4, x^2y^5 \rangle.$$

Määritelmä 2.2.8. Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali. Valitaan monomijärjestys $<$, ja olkoon

$$LT(I) = \{cx^\alpha \mid \exists\ f \in I \ s.e\ LT(f) = cx^\alpha\}.$$

Tällöin ideaalin I polynomien *johtavien monomien virittämä monomi-ideaali* on $\langle LT(I) \rangle$.

Lemma 2.2.9. *Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Koska $\langle LT(I) \rangle$ on monomi-ideaali suoraan Dicksonin lemmasta seuraa, että on olemassa polynomit $g_1, \ldots, g_t \in I$ siten, että*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Olkoon sitten $I = \langle f_1, \ldots, f_s \rangle$ aina on voimassa

$$\langle LT(f_1), \ldots, LT(f_s) \rangle \subset \langle LT(I) \rangle,$$

mutta käänteinen inkluusio ei ole välttämättä voimassa, kuten seuraava esimerkki osoittaa

Esimerkki 2.2.10. Olkoon

$$f_1 = x^3 - 2xy$$
$$f_2 = x^2y - 2y^2 + x.$$

Tällöin $\langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle$. Kuitenkin $f_3 = xf_2 - yf_1 = x^2 \in I$ ja

$$LT(f_3) = x^2 \notin \langle x^3, x^2y \rangle,$$

mutta $x^2 \in \langle LT(I) \rangle$, joten välttämättä *ei ole voimassa* $LT(I) \subset \langle LT(f_1), \ldots, LT(f_s) \rangle$.

Lause 2.2.11 (Hilbertin kantalause)**.** *Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali, tällöin on olemassa polynomit $g_1, \ldots, g_t$ siten, että*

$$I = \langle g_1, \ldots, g_t \rangle.$$

Toisinsanoen jokainen *ideaali on äärellisesti generoitu.*

Todistus. Jos $I = \{0\}$, niin $I = \langle 0 \rangle$. Oleteaan sitten, että $I \neq \{0\}$. Lemman 2.2.9 nojalla on olemassa monomit siten, että

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Väitämme, että

$$\widetilde{I} = \langle g_1, \ldots, g_t \rangle = I.$$

Selvästi $\widetilde{I} \subset I$, koska $g_i \in I \quad \forall\, 1 \leq i \leq t$. Olkoon $f \in I$, tällöin jakolaskualgoritmi antaa

$$f = a_1g_1 + \ldots + a_tg_t + r,$$

joten

$$r = f - (a_1g_1 + \ldots + a_tg_t) \in I$$

Näin ollen $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$, joten lemman 2.2.3 nojalla on olemassa sellainen $k, \;\; 1 \leq k \leq t$ että termi $LT(g_k)$ jakaa termin $LT(r)$. Tämä on ristiriita jakolaskualgoritmin kanssa koska minkään termin $LT(g_i)$ ei pidä jakaa mitään jakojäännöksen r termiä. Näin ollen $r = 0$, joten $f \in \widetilde{I}$.

Määritelmä 2.2.12 (Gröbner kanta)**.** Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Tällöin joukkoa

$$G = \{g_1, \ldots, g_t\} \subset I$$

sanotaan ideaalin I *Gröbner kannaksi*, jos

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Hilbertin kantalauseen perusteella saadaan lemma

Lemma 2.2.13. *Kaikille ideaaleille $I \subset \mathbb{K}[x_1, \ldots, x_n]$ on olemassa Gröbner kanta $G = \{g_1, \ldots, g_t\}$,*

$$\langle G \rangle = I.$$

Lause 2.2.14. *Olkoon $I = \langle g_1, \ldots, g_t \rangle$, missä $G = \{g_1, \ldots, g_t\}$ on ideaalin I Gröbner kanta ja olkoon $f \in \mathbb{K}[x_1, \ldots, x_n]$. Tällöin on olemassa 1-käsitteinen jakojäännös r siten, että*

1. *$LT(g_i)$ ei jaa mitään jakojäännöksen r termiä*
2. *On olemassa $g \in I$ siten, että $f = g + r$.*

Todistus. 1. ja 2. kohta seuraa suoraan jakolaskualgoritmistä. Tämän perusteella saadaan esitys

$$f = a_1 g_1 + \ldots + a_t g_t + r,$$

ja jakolaskualgoritmin perusteella $LT(g_i)$ ei jaa mitään polynomin r termiä, ja polynomiksi g voidaan valita $g = a_1 g_1 + \ldots + a_t g_t \in I$. Todistetaan sitten jakojäännöksen r yksikäsitteisyys. Tehdään vastaoletus: Oletetaan, että on olemassa kaksi jakojäännöstä r_1 ja r_2 siten, että

$$f = h_1 + r_1 = h_2 + r_2.$$

Näin ollen

$$r_1 - r_2 = h_2 - h_1 \in I.$$

Toisaalta

$$LT(r_1 - r_2) \in LT(I) = \langle LT(g_1), \ldots, LT(g_t) \rangle,$$

joten jokin polynomin r_1 tai r_2 termi on jaollinen jollain termillä $LT(g_i)$. Tämä on ristiriita, sillä r_1 ja r_2 ovat jakojäännöksiä.

Seuraus 2.2.15. *Olkoon G ideaalin I Gröbner kanta. Tällöin on voimassa ekvivalenssi $f \in I \quad \Leftrightarrow$ jakojäännös $r = 0$.*

Todistus.
($\Leftarrow$)
Jos $r = 0$, niin $f \in I$ (pätee aina)
($\Rightarrow$)
Edellisen lauseen kohdan 2. nojalla $f = g + r = g + 0 = g \in I$, joten $f \in I$.

Lemma 2.2.16. *Jos on annettu kaksi ideaalia $I_1 = \langle f_1, \ldots, f_s \rangle$ ja $I_2 = \langle g_1, \ldots, g_t \rangle$, niin on voimassa ekvivalenssi*

$$I_1 \subset I_2 \quad \Leftrightarrow \quad f_i \in I_2 \quad \forall\ 1 \leq i \leq s.$$

Gröbner kannan määrittelemisen jälkeen voidaan kysyä kaksi peruskysymystä:

1. Jos on annettu $I = \langle f_1, \ldots, f_s \rangle$ onko $\{f_1, \ldots, f_s\}$ ideaalin I gröbner kanta ?

2. Jos on annettu ideaali $I = \langle f_1, \ldots, f_s \rangle$, kuinka sille konstruoidaan Gröbner kanta ?

2.3 Eräitä sovelluksia

Esimerkki 2.3.1. Olkoon

$$\begin{aligned} f_1 &= (x-1)^2 + y^2 - 1 \\ f_2 &= 4(x-1)^2 + y^2 + xy - 2, \quad f_1, f_2 \in \mathbb{K}[x, y], \end{aligned}$$

ja $I = \langle f_1, f_2 \rangle$. Valitaan monomijärjestys *lex* ja $y > x$. Tällöin Gröbner kannan polynomit ovat

$$\begin{aligned} g_1 &= y - 5x^3 + 19x^2 - 21x + 6 \\ g_2 &= 5x^4 - 19x^3 + 24x^2 - 12x + 2. \end{aligned}$$

Koska $\mathbf{V}(I) = \mathbf{V}(\langle G \rangle)$, niin $\mathbf{V}(I)$ sisältää korkeintaan 4 pistettä. Polynomin g_2 nollakohdat a_i ovat

$$a_1 = 1, \quad a_2 \approx 0.35, \quad a_3 \approx 0.63, \quad a_4 \approx 1.85.$$

Esimerkki 2.3.2. Maksiomoidaan/minimoidaan funktiota $f = x^2 + y^2 + xy$ joukossa $g = x^2 + 2y^2 - 1 = 0$. Lokaalissa maksimissa/minimissä $\nabla f \| \nabla g$ joten maksimi/minimi pisteissä pn voimassa

$$\begin{aligned} \nabla f + \lambda \nabla g &= 0 \\ g &= 0, \end{aligned}$$

eli

$$\begin{aligned} g_1 &= 2x + y + 2\lambda x = 0 \\ g_2 &= 2y + x + 4\lambda y = 0 \\ g &= x^2 + 2y^2 - 1 = 0. \end{aligned}$$

Min/Max tehtävän Lagrangen funktio on $L = f + \lambda g$, ja

$$g = \frac{\partial L}{\partial \lambda}, \quad g_1 = \frac{\partial L}{\partial x}, \quad g_2 = \frac{\partial L}{\partial y}.$$

Olkoon sitten $I = \langle g_1, g_2, g \rangle$. Ideaalin I Gröbner kannan polynomit p_i järjestyksen lex, $\lambda > y > x$ suhteen ovat

$$\begin{aligned} p_1 &= \lambda + y^2 + yx + x^2 \\ p_2 &= y - 3x^2 + 2x \\ p_3 &= 6x^4 - 6x^2 + 1. \end{aligned}$$

$\mathbf{V}(I)$ sisältää tällöin korkeintaan 4 pistettä

$$x = \pm \sqrt{\frac{1}{2} \pm \frac{\sqrt{3}}{6}},$$

jolloin funktion f arvot ovat

$$f = 0.32, \ f = 0.32, \ f = 1.18, \ f = 1.18.$$

Esimerkki 2.3.3. Olkoon $c : \mathbb{R} \mapsto \mathbb{R}^2$, $c(t) = (c_1(t), c_2(t))$ funktio, ja

$$C = \{c(t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$$

käyrä. Toisaalta jos $f : \mathbb{R}^2 \mapsto \mathbb{R}$, missä f on polynomifunktio, niin käyrä voidaan esittää myös muodossa $\mathbf{V}(f)$. Tarkastellaan esimerkiksi käyrää jonka parametriesitys on

$$c(t) = (t^2 - 3t + 4, -t^3 + 2t - 1),$$

ja asetetaan

$$f_1 = x - t^2 + 3t - 4$$
$$f_2 = y + t^3 - 2t + 1.$$

Olkoon sitten $I = \langle f_1, f_2 \rangle$. Ideaalin I Gröbner kannan ensimmäiseksi polynomiksi g_1 saadaan järjestyksessä lex, $t > y > x$

$$g_1 = y^2 + xy - 13y - x^3 + 16x^2 - 57x + 58.$$

Nyt saatiin käyrä $\mathbf{V}(g_1)$. Toisaalta $\mathbf{V}(I)$ on käyrä avaruudessa $\mathbb{R}^3$. Määrittelemällä projektiokuvaus $\pi : \mathbb{R}^3 \mapsto \mathbb{R}^2$, $\pi(t, x, y) = (x, y)$ saadaan

$$\pi(\mathbf{V}(I)) = \mathbf{V}(g_1).$$

Esimerkki 2.3.4 (Kardioidi)**.** Kardioidi on tasokäyrä C , jonka yhtälö on napakoordinaateissa $r = 2 + 2\cos(\theta)$, jolloin sen parametriesitys $c : [0, 2\pi[\mapsto \mathbb{R}^2$ on

$$c(\theta) = (2(1 + \cos(\theta))\cos(\theta), 2(1 + \cos(\theta))\sin(\theta)).$$

Asetetaan sitten

$$c = \cos(\theta)$$
$$s = \cos(\theta),$$

jolloin $c^2 + s^2 - 1 = 0$. Olkoon sitten $I = \langle f_1, f_2, f_3 \rangle$, missä

$$f_1 = x - 2(1 + c)c$$
$$f_2 = y - 2(1 + c)s$$
$$f_3 = c^2 + s^2 - 1.$$

Ideaalin I Gröbner kannassa on järjestyksessä lex, $c > s > y > x$ 5 polynomia g_i, joista yksi g_1 sisältää vain muuttujia x, y,

$$g = (x^2 + y^2)^2 - 4x(x^2 + y^2) - y^2,$$

ja nyt $C = \mathbf{V}(g)$.

Määritelmä 2.3.5 (Käyrän singulaariset pisteet)**.** Olkoon $f : \mathbb{R}^2 \mapsto \mathbb{R}$ funktio, ja $\mathbf{V}(f)$ käyrä. Implisiittifunktiolauseen nojalla piste $p \in \mathbf{V}(f)$ on *säännöllinen*, jos $\nabla f(p) \neq 0$. Piste $p \in \mathbf{V}(f)$ on *singulaarinen*, jos $\nabla f(p) = 0$. Singulaaristen pisteiden varieteetti on siis

$$S(f) = \mathbf{V}\Big(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\Big) \subset \mathbf{V}(f).$$

Esimerkki 2.3.6. Olkoon $f = x^2 + y^2 - 1$. Tällöin singulaarisen varieteetin määräävät polynomiyhtälöt

$$\begin{aligned} x^2 + y^2 - 1 &= 0 \\ 2x &= 0 \\ 2y &= 0, \end{aligned}$$

jolloin $S(f) = \emptyset$. Tämä on yhtäpitävää sen kanssa, että $I(S(f)) = \langle 1 \rangle = \mathbb{K}[x, y]$. Nyt esimerkiksi

$$1 = (-1)f + (x/2)x + (y/2)y$$

Esimerkki 2.3.7. Tarkastellaan kardioidin singulaarista varieteettia. Olkoon $I = \langle g, g_x, g_y \rangle$. Ideaalin Gröbner kannan polynomit järjestyksessä lex $y > x$ laskettuna ovat

$$\begin{aligned} g_1 &= y \\ g_2 &= x^2 + y^2. \end{aligned}$$

Näin ollen kardioidin singulaarinen varieteetti on yksi piste $S(g) = \{(0, 0)\}$.

Esimerkki 2.3.8 (Scarabee)**.** Scarabee on tasokäyrä, joka on annettu polynomin

$$f = (x^2 + y^2 + ax)^2(x^2 + y^2) - b(x^2 - y^2)^2, \quad f \in \mathbb{K}[x, y],\ \mathbb{K} = \mathbb{Q}(a, b)$$

varieteettina $\mathbf{V}(f)$. Olkoon sitten jälleen

$$I = \langle f_1, f_2, f_3 \rangle = \langle f, f_x, f_y \rangle,$$

ja $S(f) = \mathbf{V}(I)$. Jos ideaalin I Gröbner kanta lasketaan järjestyksessä lex, $x > y$ se sisältää polynomin

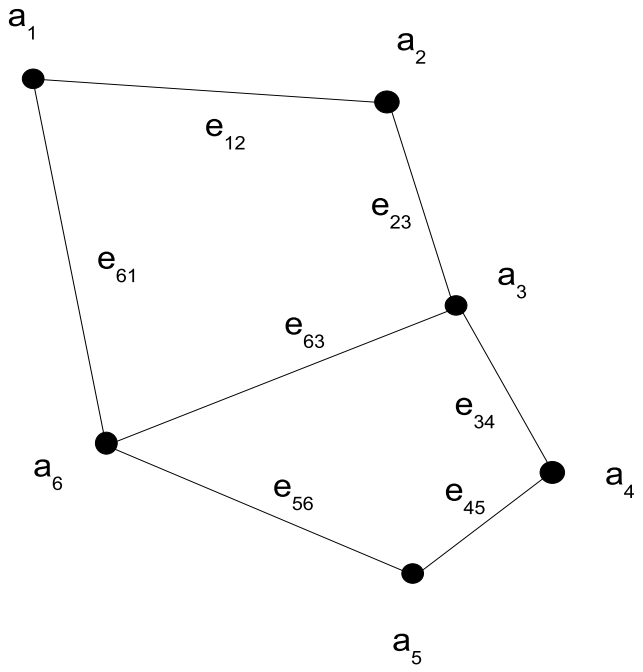
$$g = 4y^2 - a^2y^5.$$

Näin ollen singulaarisessa varieteetissa $y = 0$ tai $y = \pm a/2$. Scarabeen singulaarinen varieteetti on siis tason pistejoukko

$$S(f) = \{(0, 0), (a/2, a/2), (a/2, -a/2)\}.$$

Esimerkki 2.3.9 (3-väri ongelma)**.** Graafi G on järjestetty pari $G = (V, E)$, joka koostuu graafin solmupisteistä $V = \{a_1, \ldots, a_n\}$, sekä niitä yhditävistä janoista $E = \{e_{12}, e_{23}, e_{34}, e_{41}, \ldots\}$. 3-Väri ongelmassa kysytään voidaanko löytää graafin solmupisteiden väritys kolmella eri värillä siten, että vierekkäiset janoilla yhdistetyt solmupisteet eivät tule väritetyiksi samoilla väreillä ? Tarkastellaan esimerkissä kuvan 2 mukaista graafia

$$V = \{a_1, \ldots, a_6\}$$
$$E = \{e_{12}, e_{23}, e_{34}, e_{45}, e_{56}, e_{61}, e_{63}\}.$$



Kuva 2: Graafi $G = (V, E)$

Tarkastellaan miten ongelmaa voidaan lähestyä algebrallisen geometrian menetelmin. Asetetaan

$$p_i = x_i^3 - 1 = (x_i - 1)(x_i^2 + x + 1)$$

polynomin p_i varieteetti on

$$\mathbf{V}(p_i) = \{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\} = \{v_1, v_2, v_3\}.$$

Kolmiväriongelma voidaan nyt muotoilla seuraavasti: Vastatkoon jokaista pistettä a_i polynomi p_i, jos vierekkäisille polynomeille p_i ja p_j voidaan löytää eri ratkaisut v_i ja v_j, niin graafi voidaan kolmella eri värillä v_i. Koska kuitenkin

$$x_i^3 = x_j^3 \quad \Leftrightarrow \quad (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0,$$

ja kahdella vierekkäisellä pisteellä ei saa olla samaa väritystä $v_j \neq v_i$ niin tällöin täytyy olla

$$x_i^2 + x_i x_j + x_j^2 = 0.$$

Kuvan 2 graafille löytyy siis väritys, jos polynomiyhtälöillä

$$\begin{aligned} p_1 &= x_1^3 - 1 = 0 \\ &\vdots \\ p_6 &= x_6^3 - 1 = 0 \\ q_1 &= x_1^2 + x_1 x_2 + x_2^2 = 0 \\ &\vdots \\ q_6 &= x_1^2 + x_1 x_6 + x_6^2 = 0 \\ q_7 &= x_3^2 + x_3 x_6 + x_6^2 = 0 \end{aligned}$$

on ratkaisu. Jos merkitään $I = \langle p_1, \ldots, p_6, q_1, \ldots, q_7 \rangle$, niin tämä on yhtäpitävää sen kanssa, että $\mathbf{V}(I) \neq \emptyset$.

2.4 Buchenbergerin algoritmi

Olkoon

$$I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n].$$

Aikaisemmin kysyttiin

1. Onko $f_1, \ldots, f_s$ Gröbner kanta?
2. Miten Gröbner kannan voi laskea?

Jos $G = \{g_1, \ldots, g_t\}$ on Gröbner kanta, niin

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Jos G ei ole Gröbner kanta, niin $\exists\ f \in I$ siten, että

$$LT(f) \notin \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Määritelmä 2.4.1. Olkoon f ja g polynomeja missä $LM(f) = x^\alpha$ ja $LM(g) = x^\beta$. Määritellään monomien x^α ja x^β pienin yhteinen jaettava

$$x^\gamma = pyj\{x^\alpha, x^\beta\},$$

missä γ on *pienin* moni-indeksi, siten että x^α ja x^β jakavat monomin x^γ.

Määritelmä 2.4.2. Määritellään kahden polynomin $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *S-polynomi*

$$S(f,g) = \frac{x^\gamma}{LT(f)}f - \frac{x^\gamma}{LT(g)}g,$$

missä

$$x^\gamma = pyj(LM(f), LM(g)).$$

Esimerkki 2.4.3. Olkoon $I = \langle f_1, f_2 \rangle$, missä

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y + 2y^2 + x. \end{aligned}$$

Nyt saadaan

$$x^\gamma = pyj(LT(f_1), LT(f_2)) = pyj(x^3, x^2y) = x^3y.$$

Polynomien f_1 ja f_2 S-polynomi on siis

$$S(f_1, f_2) = yf_1 - xf_2 = -x^2 = -x^2 - 4xy^2.$$

Nyt huomataan

$$LT(S(f_1, f_2)) = -x^2 \notin \langle x^3, x^2y \rangle.$$

Olkoon sitten $F = \{f_1, \ldots, f_s\}$ polynomijoukko ja f annettu polynomi

$$f, f_i \in \mathbb{K}[x_1, \ldots, x_n]$$

Jakolaskualgoritmi antaa

$$f = a_1f_1 + \ldots + a_sf_s + r.$$

Määritelmä 2.4.4. Sanotaan, että polynomi f *redusoituu* polynomiksi r polynomijoukon $F = \{f_1, \ldots, f_s\}$ suhteen ja merkitään

$$f \to^F r$$

Jos r on jakolaskualgoritmin antama jakojäännös jaettaessa polynomijoukolla F.

Lause 2.4.5 (Buchenbergerin kriteeri)**.** *Olkoon G polynomijoukko*

$$G = \{g_1, \ldots, g_t\},$$

ja

$$I = \langle g_1, \ldots, g_t \rangle = \langle G \rangle.$$

Tällöin G on ideaalin I Gröbner kanta jos ja vain jos

$$S(g_i, g_j) \to^G 0 \quad \forall\ 1 \leq i, j \leq t.$$

Todistus. [Buchenbergerin kriteeri] Todistetaan ensin vain " $\Rightarrow$ ". Oletetaan, että G on Gröbner kanta. Koska $g_i, g_j \in I$ tällöin $S(g_i, g_j) \in I$ ja seurauksen 2.2.15 perusteella

$$S(g_i, g_j) \to^G 0.$$

Esitetään sitten todistuksen $\Leftarrow$ idea ja oletetaan kaikki S polynomit redusoituvat nollaksi. Olkoon $f \in I$ tällöin täytyy osoittaa

$$LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$$

ja

$$f = \sum_{i=1}^{t} a_i g_i.$$

Aina on voimassa

$$mdeg(f) \leq \max\{mdeg(a_i g_i)\},$$

mutta nyt voidaan osoittaa, että polynomit a_i voidaan valita siten, että

$$mdeg(f) = \max\{mdeg(a_i g_i)\}.$$

Tästä seuraa, että polynomin f johtava termi $LT(f)$ on jaollinen jollakin polynomin $g_i,\ 1 \leq i \leq t$ johtavalla johtavalla termillä $LT(g_i)$, $LT(g_i) | LT(f)$. Tästä seuraa

$$LT(f) = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Esimerkki 2.4.6. Jatkoa esimerkistä 2.4.3. Asetetaan $f_3 = S(f_1, f_2)$, ja

$$F_1 = \{f_1, f_2, f_3\}.$$

Nyt saadaan

$$S(f_1, f_2) \to^{F_1} 0,$$

mutta $S(f_1, f_3) = -2xy$, ja

$$S(f_1, f_3) \to^{F_1} -2xy.$$

Asetetaan sitten $f_4 = -2xy$ ja

$$F_2 = \{f_1, f_2, f_3, f_4\}.$$

Nyt $S(f_1, f_4) = -2xy^2$ ja

$$S(f_1, f_4) \to^{F_2} 0,$$

mutta $S(f_2, f_3) = -2y^2 + x$ ja

$$S(f_2, f_3) \to^{F_2} -2y^2 + x.$$

Asetetaan sitten $f_5 = -2y^2 + x$, ja

$$F_3 = \{f_1, f_2, f_3, f_4, f_5\}.$$

Nyt saadaan

$$S(f_i, f_j) \to^{F_3} 0 \quad \forall\ 1 \leq i, j \leq 5,$$

joten F_3 on ideaalin $I = \langle f_1, f_2 \rangle$ Gröbner kanta.

Lause 2.4.7 (Buchbergerin algoritmi)**.** *Buchbergerin algoritmi antaa Gröbner kannan äärellisen askelmäärän jälkeen.*

Määritelmä 2.4.8. Olkoon $I_k \subset \mathbb{K}[x_1, \ldots, x_n], \quad k \in \mathbb{N}$. Ideaalit I_k muodostavat *laajenevan jonon ideaaleja* (ascending chain), jos

$$I_1 \subset I_2 \subset \ldots \subset I_k \subset I_{k+1} \subset \ldots$$

Lause 2.4.9. *Olkoon $I_1, I_2, \ldots$ laajeneva jono ideaaleja, tällöin on olemassa $m \in \mathbb{N}$ siten, että*

$$I_m = I_{m+1} = I_{m+2} = \ldots$$

Toisin sanoen laajeneva jono ideaaleja stabiloituu jonkun indeksin m jälkeen.

Todistus. Olkoon

$$I = \bigcup_{k=1}^{\infty} I_k.$$

Todetaan ensin, että I on ideaali, sillä

1. $0 \in I$
2. $f, g \in I \Rightarrow \exists\, k_1, k_2$ s.e $f \in I_{k_1}$ ja $g \in I_{k_2}$. Jos valitaan $k = \max\{k_1, k_2\}$, niin tällöin $f + g \in I_k$, joten $f + g \in I$.
3. $f \in I \Rightarrow \exists\, k$ s.e $f \in I_k$ tällöin $hf \in I_k \subset I$, $h \in \mathbb{K}[x_1, \ldots, x_n]$.

Koska 1, 2 ja 3 ovat voimassa I on ideaali. Hilbertin lauseen nojalla ideaalilla I on olemassa äärellinen kanta siten, että $I = \langle g_1, \ldots, g_t \rangle$. Nyt jokaista indeksiä $1 \leq i \leq t$ kohti on olemassa indeksi k_i siten, että $g_i \in I_{k_i}$. Olkoon sitten $m = \max\{k_i\}$. Tällöin

$$I = \langle g_1, \ldots, g_t \rangle \subset I_m \subset I_{m+1} \subset \ldots \subset I,$$

joten

$$I_m = I_{m+1} = I_{m+2} = \ldots$$

Todistus. [Buchbergerin algoritmi]

1. Algoritmin lopussa $I = \langle F \rangle = \langle G \rangle$.
2. Jos algoritmi päättyy Buchbergerin kriteeri on voimassa, joten algoritmi antaa Gröbner kannan.

Jää todistettavaksi vain kohta 3: Todistetaan, että algoritmi päättyy äärellisen toistomäärän jälkeen.
Jos $GV \neq G$ niin $GV \subset G$ ja $\langle GV \rangle = \langle G \rangle$, joten $\langle LT(GV) \rangle \subset \langle LT(G) \rangle$. Pitää osoittaa, että itseasiassa

$$\langle LT(GV) \rangle \subsetneq \langle LT(G) \rangle.$$

Algoritmissa

$$\begin{aligned} GV &= \{g_1, \ldots, g_t\} \\ G &= \{g_1, \ldots, g_t, r\}, \end{aligned}$$

missä $S(g_i, g_j) \to^{GV} r$ joillekkin $1 \leq i, j \leq t$. Näin ollen kaikilla $g_i \in G$ on voimassa

$$LT(g_i) \nmid LT(r),$$

joten $LT(r) \notin \langle LT(GV)\rangle$. Toisaalta $LT(r) \in \langle LT(G)\rangle$, joten $\langle LT(GV)\rangle \subsetneq \langle LT(G)\rangle$. Koska $\langle LT(G_1)\rangle \subsetneq \langle LT(G_2)\rangle \subsetneq \ldots$ on laajeneva jono ideaaleja sen täytyy stabiloitua äärellisen askelmäärän jälkeen lauseen 2.4.9 perusteella, joten

$$G_{m+1} = G_m$$

jollekkin $m \in \mathbb{N}$, joten algoritmi päättyy.

Esimerkki 2.4.10. Aikaisemmassa esimerkissä tarkasteltiin ideaalia $I = \langle f_1, f_2\rangle$

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x. \end{aligned}$$

Buchenbergerin algoritmi antoi ideaalille Gröbner kannan

$$G = \{f_1, f_2, -x^2, -2xy, -2y^2 + x\}.$$

Nyt voidaan kysyä: Voisiko Gröbner kantaa jotenkin yksinkertaistaa siten, että siinä olisi vähemmän polynomeja mutta se edelleen olisi ideaalin Gröbner kanta?

Lemma 2.4.11. *Olkoon G ideaalin I Gröbner kanta. Jos on olemassa $p \in G$ siten, että*

$$LT(p) \in \langle LT(G \setminus \{p\})\rangle,$$

niin $G \setminus \{p\}$ on myös ideaalin I Gröbner kanta.

Todistus. Oletetaan, että $LT(p) \in \langle LT(G \setminus \{p\})\rangle$, tällöin

$$\langle LT(G \setminus \{p\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle.$$

Tällöin Hilbertin kantalauseen todistuksen perusteella

$$\langle G \setminus \{p\}\rangle = I,$$

joten $G \setminus \{p\}$ on ideaalin I Gröbner kanta.

Esimerkki 2.4.12. Tarkastellaan jälleen tapausta $I = \langle f_1, f_2 \rangle$,

$$G = \{f_1, f_2, -x^2, -2xy, -2y^2 + x\} = \{f_1, \ldots, f_5\}.$$

Nyt

$$LT(f_3)|LT(f_1)$$
$$LT(f_4)|LT(f_2),$$

joten polynomit f_1 ja f_2 voidaan poistaa joukosta G ja näin saatu uusi joukko

$$\widetilde{G} = \{f_3, f_4, f_5\}$$

on edelleen ideaalin I Gröbner kanta. Nyt enää mikään jäljellä olevisen polynomien johtavista termeistä ei jaa minkään toisen jäljellä olevan polynomin johtavaa termiä.
Kuitenkin voidaan edelleen kysyä: Voitaisiinko jäljellä olevia polynomeja yksinkertaistaa (poistaa termejä), siten että jäljelle jäävien polynomien joukko olisi edelleen ideaalin I Gröbner kanta?

Määritelmä 2.4.13. Joukko G on ideaalin I *minimi Gröbner kanta*, jos se on Gröbner kanta ja

$$\forall\ p \in G,\ LT(p) \notin \langle LT(G \setminus \{p\}) \rangle.$$

Toisinsanoen mikään Gröbnerkannan polynomien johtavista termeistä ei jaa kannan toisen polynomin johtavaa termiä.

Määritelmä 2.4.14. Joukko G on ideaalin I *redusoitu Gröbner kanta*, jos se on Gröbner kanta ja

1. $LC(p) = 1, \quad \forall\ p \in G$
2. Mikään polynomin $p \in G$ termi ei kuulu ideaaliin$\langle LT(G \setminus \{p\}) \rangle$.

Lause 2.4.15. *Olkoon*

$$F = \{f_1, \ldots, f_s\}$$
$$G = \{g_1, \ldots, g_t\},$$

ja $I = \langle F \rangle = \langle G \rangle$. *Jos* F *ja* G *ovat ideaalin* I *minimi Gröbner kantoja, niin*

1. $s = t$
2. $LM(f_i) = LM(g_i)$.

Jos F ja G ovat ideaalin I redusoituja Gröbner kantoja, niin $F = G$.

Lause 2.4.16 (Ideaalien yhtäsuuruus)**.** *Olkoon $I_1 \subset \mathbb{K}[x_1, \ldots, x_n]$ ja $I_2 \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaaleja*

$$I_1 = \langle f_1, \ldots, f_s \rangle$$
$$I_2 = \langle g_1, \ldots, g_t \rangle.$$

Tällöin $I_1 = I_2$ jos ja vain jos

1. *$f_i \in I_2 \ \ \forall\ 1 \leq i \leq s$ ja $g_j \in I_1 \ \ \forall\ 1 \leq j \leq t$*
2. *Jos G_i on ideaalin I_i redusoitu Gröbner kanta, niin $G_1 = G_2$.*

Esimerkki 2.4.17. Olkoon

$$f_1 = y^2 + yx + x^2$$
$$f_2 = y + x$$
$$f_3 = y,$$

$I = \langle f_1, f_2, f_3 \rangle$ ja käyteyään järjestystä lex, $y > x$. Olkoon sitten $\mathcal{F} = \{f_1, f_2, f_3\}$. Tällöin

$$S(f_1, f_2) = x^2 \rightarrow^{\mathcal{F}} x^2 = f_4$$
$$S(f_2, f_3) = x \rightarrow^{\mathcal{F}} x = f_5.$$

Nyt kaikki joukon $G = \{f_1, \ldots, f_5\}$ S-polynomit redusoituvat nollaksi joukon G suhteen, joten se on ideaalin I Gröbner kanta. Nyt kuitenkin

$$LT(f_5) | LT(f_4)$$
$$LT(f_3) | LT(f_1),$$

joten polynomit f_1 ja f_4 voidaan poistaa. Lisäksi

$$LM(f_2) = LM(f_3),$$

joten *jompikumpi* voidaan poistaa. Näin saadaan Gröbner kannat

$$G_1 = \{y + x, x\}$$
$$G_2 = \{y, x\}.$$

Koska $LT(G_1(2)) | x$ kanta G_1 ei ole redusoitu Gröbner kanta. Kanta G_2 taas on.

Lause 2.4.18. *Olkoon $G = \{g_1, \ldots, g_t\}$ ideaalin I Gröbner kanta. Tällöin seuraavat väittämät ovat yhtäpitäviä*

1. $\langle LT(G)\rangle = \langle LT(I)\rangle$
2. $\forall\ f \in I\ \exists\ i$ *siten, että* $LT(g_i)|LT(f)$.
3. $f \in I \ \Leftrightarrow\ f \to^G 0$
4. $f \to^G r$ *on yksikäsitteinen. Toisinsanoen se on riippumaton polynomien* g_i *järjestyksestä jaossa* $f \to^G r$.
5. $S(g_i, g_j) \to^G 0 \quad \forall\ 1 \leq i, j \leq t$.

2.5 Eliminointiteoria

Määritelmä 2.5.1. Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Ideaalin I *eliminaatio ideaali* I_k on

$$I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

Lemma 2.5.2. *I_k on ideaali. Tod H.T*

Lause 2.5.3. *Olkoon G ideaalin I Gröbner kanta järjestyksessä lex, $x_1 > \ldots > x_n$, tällöin joukko G_k*

$$G_k = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$$

on eliminointi-ideaalin I_k Gröbner kanta.

Todistus. Olkoon $G = \{g_1, \ldots, g_t\}$ ja $G_k = \{g_1, \ldots, g_m\}$ tällöin selvästi $G_k \subset I_k$, joten $\langle G_k\rangle \subset I_k$. Pitää osoittaa

1. $\langle G_k\rangle = I_k$
2. Joukko G_k on ideaalin I_k Gröbner kanta.

Olkoon $f \in I_k \subset I$. Tällöin jakolaskualgoitmi antaa

$$f = a_1 g_1 + \ldots + a_t g_t.$$

Jakojäännös $r = 0$, koska G on Gröbner kanta. Jos käytetään järjestystä lex, niin jokainen termi $LT(g_{m+1}), \ldots, LT(g_t)$ on suurempi polynomin f jokainen

termi. Tällöin polynomit $g_{m+1}, \ldots, g_t$ eivät voi jakaa polynomia f. Näin ollen $a_{n+1} = \ldots = a_t = 0$, joten

$$f = a_1 g_1 + \ldots + a_m g_m.$$

Tästä seuraa $f \in \langle G_k \rangle$, joten $\langle G_k \rangle = I_k$. Lauseen 2.4.18 kohdan 3 perusteella $f \in I \;\Leftrightarrow\; f \to^G 0$. Äsken saatiin

$$f \in I_k \quad \Rightarrow \quad f \to^{G_k} 0$$

ja implikaatio toiseen suuntaan on selvä, joten G_k on ideaalin I_k Gröbner kanta.

Määritelmä 2.5.4 (Tulojärjestys)**.** Merkitään

$$\begin{aligned} \mathbb{A} &= \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m] \\ \mathbb{A}_x &= \mathbb{K}[x_1, \ldots, x_n] \\ \mathbb{A}_y &= \mathbb{K}[y_1, \ldots, y_m]. \end{aligned}$$

Olkoon renkaassa $\mathbb{A}_x$ määritelty monomijärjestys $>_x$ ja renkaassa $\mathbb{A}_y$ monomijärjestys $>_y$. Määritellään renkaassa $\mathbb{A}$ *tulojärjestys* $>$, $x^{\alpha_1} y^{\beta_1} > x^{\alpha_2} y^{\beta_2}$, jos

$$\begin{aligned} &x^{\alpha_1} > x^{\alpha_2}, \quad \text{tai} \\ &x^{\alpha_1} = x^{\alpha_2} \quad \text{ja} \\ &y^{\beta_1} > y^{\beta_2}. \end{aligned}$$

Lemma 2.5.5. *Tulojärjestys on monomijärjestys.*

Lause 2.5.6. *Olkoon $I \subset \mathbb{A} = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ ideaali ja oletetaan, että G on ideaalin I Gröbner kanta, ja olkoon*

$$I_n = I \cap \mathbb{A}_y.$$

Jos G on tulojärjestyksellä saatu Gröbner kanta niin joukko G_n,

$$G_n = G \cap \mathbb{A}_y$$

on ideaalin I_n Gröbner kanta.

Tarkastellaan sitten tilannetta, missä kaikki eliminaatio ideaalin varieteetin pisteet eivät laajennu alkuperäisen varieteetin pisteiksi.

Esimerkki 2.5.7. Olkoon esimerkiksi

$$f_1 = xy - 1$$
$$f_2 = xz - 1$$

Valitaan järjestys lex, $x > y > z$ ja lasketaan Gröber kanta. Tällöin saadaan

$$I_1 = \langle y - z \rangle = \langle g \rangle,$$

ja

$$\mathbf{V}(g) = \{(a, a) \in \mathbb{R}^2 \mid a \in \mathbb{R}\} \subset \mathbb{R}^2,$$

mutta

$$\mathbf{V}(f_1, f_2) = \left\{ \left(\frac{1}{a}, a, a \right) \in \mathbb{R}^3 \mid a \neq 0 \right\} \subset \mathbb{R}^3.$$

Esimerkki 2.5.8. Olkoon sitten

$$f_1 = x^2 - y$$
$$f_2 = x^2 - z$$

ja $I = \langle f_1, f_2 \rangle$. Valitaan järjestys lex, $x > y > z$. Tässä järjestyksessä lasketusta Gröbner kannasta saadaan ensimmäinen eliminointi-ideaali $I_1 = \langle y - z \rangle = \langle g \rangle$ ja

$$\mathbf{V}(g) = \{(a, a) \mid a \in \mathbb{K}\} \subset \mathbb{K}^2.$$

Jos $\mathbb{K} = \mathbb{R}$ niin ja koska $f_2 = x^2 - z$, niin ratkaisut laajenevat jos $a \geq 0$.
Jos $\mathbb{K} = \mathbb{C}$, niin ratkaisut laajenevat kaikilla $a \in \mathbb{C}$.

Lause 2.5.9 (Laajennus teoreema)**.** *Olkoon $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ ideaali ja I_1 sen ensimmäinen eliminaatioideaali*

$$I_1 = I \cap \mathbb{C}[x_2, \ldots, x_n].$$

Esitetetään polynomit f_i muodossa $f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \ldots$, missä N_i on suurin potenssi muuttujan x_1 suhteen.
Olkoon sitten $\widetilde{c} = (c_2, \ldots, c_n) \in \mathbb{C}^{n-1}$, $\widetilde{c} \in \mathbf{V}(I_1)$. Jos $\widetilde{c} \notin \mathbf{V}(\langle g_1, \ldots, g_s \rangle)$, niin on olemassa $c_1 \in \mathbb{C}$ siten, että $(c_1, \widetilde{c}) \in \mathbf{V}(I)$.

Esimerkki 2.5.10. Jos tarkastellaan jälleen esimerkin 2.5.7 tapausta, niin saadaan laajennus teoreemaa vastaaviksi polynomeiksi g_i

$$g_1 = y$$
$$g_2 = z.$$

Näin ollen $\mathbf{V}(g_1, g_2) = \{(0, 0)\}$, josta voidaan päätellä että ratkaisut

$$\mathbf{V}(I_1) = \{(a, a) \mid a \in \mathbb{C}\}$$

laajenevat koko systeemin ratkaisuiksi jos $a \neq 0$.

Esimerkki 2.5.11. Olkoon $f_1 = x^2+y^2+z^2-1$, $f_2 = xyz-1$ ja $I = \langle f_1, f_2\rangle$. Jos ideaalin I Gröbner kanta lasketaan järjestyksessä lex, $x > y > z$ niin saadaan $G = \{g_1, g_2\}$,

$$g_1 = x + y^3z + yz^3 - yz$$
$$g_2 = y^4z^2 + y^2z^4 - y^2z^2 + 1.$$

Tästä saadaan

$$I_1 = I \cap \mathbb{C}[y, z] = \langle g_2\rangle$$
$$I_2 = I \cap \mathbb{C}[z] = 0.$$

Koska $I_2 = 0$, niin $\mathbf{V}(I_2) = \mathbb{C}$. Jos g_2 esitetään sitten laajennus teoreeman muodssa

$$g_2 = \underbrace{z^2}_{=h} y^4 + \dots$$

niin huomataan kaikki arvot $z \neq 0$ laajentuvat polynomin $g_2 = 0$ ratkaisuiksi. Siis jos $c \neq 0$ on olemassa $b \in \mathbb{C}$ siten, että $(b, c) \in \mathbf{V}(I_1) = \mathbf{V}(g_2)$. Koska polynomi g_1 esittettynä laajennus teoreeman muodossa on

$$g_1 = \underbrace{1}_{=\widetilde{h}} * x + \dots$$

ja $\mathbf{V}(\widetilde{h}) = 0$, niin jos $c \neq 0$ on olemassa luvut $a, b \in \mathbb{C}$ siten, että

$$(a, b, c) \in \mathbf{V}(I).$$

Lemma 2.5.12. *Olkoon $f, g \in \mathbb{K}[x]$ tällöin seuraavat väitteet ovat ekvivalentteja.*

1. *Polynomeilla f ja g on yhteinen tekijä.*
2. *On olemassa $A, B \in \mathbb{K}[x]$ siten, että*
   - *A ja B eivät ole molemmat nollia.*
   - *$deg(A) \leq deg(g) - 1$ ja $deg(B) \leq deg(f) - 1$*
   - *$Af + Bg = 0$.*

Todistus. (1) $\Rightarrow$ (2) Jos polynomeilla f ja g on yhteinen tekijä $f = hf_1$ ja $g = hg_1$. Jos valitaan $A = g_1$ ja $B = -f_1$, niin saadaan $Af + Bg = g_1f - f_1g = h(g_1f_1 - f_1g_1) = 0$ ja selvästi polynomit A ja B toteuttavat kaksi ensimmäistä ehtoa. Todistetaan sitten implikaatio (2) $\Rightarrow$ (1). Oletetaan esimerkiksi, että $B \neq 0$ ja tehdään vastaoletus. Oletetaan, että suurin yhteinen tekijä on

$$syt(f, g) = 1.$$

Koska $1 \in \langle f, g \rangle = \langle syt(f, g) \rangle$, niin on olemassa h_1 ja h_2 siten, että

$$h_1f + h_2g = 1.$$

Kun yhtälö kerrotaan puolittain polynomilla $B \neq 0$ saadaan

$$Bh_1f + Bh_2g = B,$$

ja koska $-Af = Bg$ saadaan

$$B = (Bh_1 - Ah_2)f,$$

joten $deg(B) \geq deg(f)$ mikä on ristiriita.

Määritelmä 2.5.13 (Resultantti)**.** Olkoon $A, B, f, g \in \mathbb{K}[x]$ ja

$$\begin{aligned} f &= a_l x^l + \ldots + a_0 \\ g &= b_m x^m + \ldots + b_0 \\ A &= c_{m-1} x^{m-1} + \ldots + c_0 \\ B &= d_{l-1} x^{l-1} + \ldots + d_0. \end{aligned}$$

Olkoon sitten

$$p = Af + Bg = \sum_{j=0}^{l+m-1} e_j x^j.$$

Tällöin $p = 0 \;\Leftrightarrow\; e_j = 0 \;\forall\; 0 \leq j \leq l + m - 1$. Tämä on yhtäpitävää matriisiyhtälön

$$Ax = 0$$

kanssa, missä $x = (c_{m-1}, \ldots, c_0, d_{l-1}, \ldots, d_0)$ ja A on Sylvesterin matriisi. Polynomien f ja g *resultantti* on tällöin polynomi

$$res(f, g, x) = \det(A) := \det(syl(f, g, x)).$$

Seuraus 2.5.14. *Polynomeilla $f, g \in \mathbb{K}[x]$ on yhteinen tekijä, jos*

$$res(f, g, x) = 0.$$

Määritelmä 2.5.15. Olkoon $f \in \mathbb{K}[x]$. Polynomin f *Diskriminantti* on

$$\mathcal{D}(f) = \frac{(-1)^{l(l-1)/2}}{a_l} res(f, f', x).$$

Lause 2.5.16. *Polynomilla f on moninkertaisia tekijöitä, jos ja vain jos*

$$\mathcal{D}(f) = 0.$$

Jos $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, $f = a_l(x_2, \ldots, x_n)x_1^l + \ldots$ niin $res(f, g, x_1) \in \mathbb{K}[x_2, \ldots, x_n]$.

Lemma 2.5.17. *Olkoon $I = \langle f, g \rangle$ tällöin*

$$res(f, g, x_1) \in I_1 = I \cap \mathbb{K}[x_2, \ldots, x_n].$$

Todistus. Pitää osoittaa, että $Af + Bg = res(f, g, x)$. Todistus on samanlainen kuin yhden muuttujan tapauksessa.

Lemma 2.5.18. *Olkoon $\widetilde{c} \in \mathbb{K}^{n-1}$ kiinnitetty. Määritellään tällöin funktio $\varphi : \mathbb{K}[x_1, \ldots, x_n] \mapsto \mathbb{K}[x_1]$,*

$$\varphi(f(x_1, \ldots, x_n)) = f(x_1, \widetilde{c}).$$

Jos $I \subset \mathbb{K}[x_1, \ldots, x_n]$ on ideaali, niin

$$\varphi(I) \subset \mathbb{K}[x_1]$$

on ideaali.

Lemma 2.5.19. *Olkoon $\widetilde{c} \in \mathbb{K}^{n-1}$ ja $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Oletetaan lisäksi, että*

1. *$deg(f) = l$, $deg(g) = m$*
2. *$deg(\varphi(f)) = l$, $deg(\varphi(g)) = p \leq m$*
3. *$h = res(f, g, x_1)$*

Tällöin

$$\varphi(h) = a_l(\widetilde{c})^{m-p} res(\varphi(f), \varphi(g), x_1)$$

Todistus. Seuraa suoraan sylvesterin matriisista.

Todistus. [Laajennus teoreema]
Olkoon $\widetilde{c} \in \mathbb{K}^{n-1}$, tällöin

$$\widetilde{I} = \{f(x_1, \widetilde{c}) \mid f \in I\} = \varphi(I).$$

Tällöin on olemassa $u \in \mathbb{K}[x_1]$ siten, että $\widetilde{I} = \langle u \rangle$. On kolme mahdollisuutta:
1. $u = 0 \ \Rightarrow \ f(c_1, \widetilde{c}) = 0 \ \ \forall \ f \in I$, joten $(c_1, \widetilde{c}) \in \mathbf{V}(I) \ \ \forall \ c_1 \in \mathbb{C}$.
2. $deg(u) > 0$, jolloin on olemassa c_1 siten, että $u(c_1) = 0$, mistä seuraa

$$f(c_1, \widetilde{c}) = 0 \ \forall \ f \in I,$$

joten $(c_1, \widetilde{c}) \in x^2 - yz(I)$.
3. $u = vakio = u_0 \neq 0$. Tällöin on olemassa $f \in I$ siten, että $f(x_1, \widetilde{c}) = u_0$ ja $\widetilde{c} \notin \mathbf{V}(g_1, \ldots, g_s)$. Näin ollen on olemassa g_i siten, että $h = res(f, f_i, x_1)$

$$f_i = g_i x_1^{N_i} + \ldots$$

Koska $f_i, f \in I$ niin $h \in I_1 \subset I$ ja näin ollen $h(\widetilde{c}) = 0$. Toisaalta

$$res(\varphi(f_i), \varphi(f), x) = u_0^{N_i}.$$

Tällöin edellisen lemman perusteella

$$h(\widetilde{c}) = \varphi(h) = g_i(\widetilde{c})^{deg(f)} u_0^{N_i} \neq 0,$$

mikä on ristiriita, joten osittaisratkaisu

Määritelmä 2.5.20 (Projektiokuvaus)**.** Määritellään *projektiokuvaus* $\pi_k : \mathbb{K}^n \mapsto \mathbb{K}^{n-k}$,

$$\pi(a_1, \ldots, a_n) = (a_{k+1}, \ldots, a_n).$$

Projektiokuvausta voidaan tarkastella myös sen rajoittumana varieteettiin $\mathbf{V} \subset \mathbb{K}^n$, $\pi : \mathbf{V} \mapsto \mathbb{K}^{n-k}$.

Voidaan kysyä mikä on eliminaatioideaalien varieteettien ja alkuperäisestä varieteetista projisoimalla saadun joukon yhteys?

Jos $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, niin $\mathbf{V}(I) \subset \mathbb{K}^n$. Ideaalin I eliminaatioideaali I_k on $I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$. Nyt $\mathbf{V}(I_k) \subset \mathbb{K}^{n-k}$ ja tietenkin myös $\pi_k(\mathbf{V}(I)) \subset \mathbb{K}^{n-k}$

Esimerkki 2.5.21. Olkoon $I = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$. Tällöin $\mathbf{V}(I) \subset \mathbb{R}^2$ on yksikkökehä. Toisaalta nyt ensimmäinen eliminaatioideaali on $I_1 = \langle 0 \rangle$, joten $\mathbf{V}(I_1) = \mathbb{R}$. Jos sitten tarkastellaan projektiokuvausta $\pi_1(x, y) = y$ niin saadaan $\pi_1(\mathbf{V}(I)) = [-1, 1]$. Näin ollen siis

$$\pi_1(\mathbf{V}(I)) \subsetneqq \mathbf{V}(I_1).$$

Jos taas tarkastellaan ideaalia $I = x^2 + y^2 - 1 \in \mathbb{C}[x, y]$ ja sen varieteettia $\mathbf{V}(I) \subset \mathbb{C}^2$, niin saadaan jälleen $\mathbf{V}(I_1) = \mathbb{C}$, mutta nyt laajennusteoreeman nojalla kaikki pisteet $y \in \mathbb{C}$ laajentuvat varieteetin $\mathbf{V}(I)$ pisteiksi. Näin ollen

$$\pi_1(\mathbf{V}(I)) = \mathbf{V}(I_1).$$

Esimerkki 2.5.22. Tarkastellaan aikaisemman esimerkin ideaalia $I = \langle xy - 1, xz - 1 \rangle$ ja sen varieteettia

$$\mathbf{V}(I) = \left\{ \left(\frac{1}{a}, a, a \right) \mid a \neq 0 \right) \right\}.$$

Aikaisemmin todettiin

$$\mathbf{V}(I_1) = \{(a, a) \mid a \in \mathbb{K}\},$$

mutta nyt oli $\mathbb{K}$ mikä hyvänsä kunta

$$\pi_1(\mathbf{V}(I)) = \{(a, a) \mid a \neq 0\}$$

Lemma 2.5.23. *Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali ja I_k sen eliminaatioideaali*

$$I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

Tällöin

$$\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$$

Todistus. Eliminaatioideaalin I_k varieteetti on

$$\mathbf{V}(I_k) = \{(a_{k+1}, \ldots, a_n) \in \ \mathbb{K}^{n-k} |\ f(a_{k+1}, \ldots, a_n) = 0 \ \ \forall\ f \in I_k)\} \subset \mathbb{K}^{n-k}.$$

Olkoon sitten $f \in I_k$ mielivaltainen. Pitää osoittaa

$$f(b) = 0 \quad \forall\ b \in \pi_k(\mathbf{V}(I)).$$

Olkoon $\widetilde{a} = (a_{k+1}, \ldots, a_n) \in \mathbf{V}(I_k)$. Koska $f \in I_k \subset I$, niin
$f(a_1, \ldots, a_n, \widetilde{a}) = 0 \quad \forall\ a_1, \ldots, a_k$. Näin ollen

$$0 = f(a) = f(\pi_k(a)), \quad a \in \mathbf{V}(I).$$

joten $\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$.

Lause 2.5.24. $\mathbf{V}(I_k)$ *on pienin varieteetti joka sisältää joukon* $\pi_k(\mathbf{V}(I))$, $\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$.

Tarkastellaan sitten (hyper) pintaa $P \subset \mathbb{K}^n$, jonka parametriesitys $f : \mathbb{K}^m \mapsto \mathbb{K}^n,\ n > m$ on

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m). \end{aligned}$$

Funktion f *graafi* F on funktio $F : \mathbb{K}^m \mapsto \mathbb{K}^m \times \mathbb{K}^n \simeq \mathbb{K}^{m+n}$,

$$F(t_1, \ldots, t_m) = (t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Tällöin seuraava diagrammi kommutoi

$$\begin{aligned} &\mathbb{K}^m \to^f \mathbb{K}^n \\ &\mathbb{K}^m \to^F \mathbb{K}^{m+n} \to^{\pi_m} \mathbb{K}^n \end{aligned}$$

Jos määritellään polynomit

$$h_i = x_i - f_i \in \mathbb{K}[t_1, \ldots, t_m, x_1, \ldots, x_n]$$

ja ideaali $I = \langle h_1, \ldots, h_n \rangle$, niin $\mathbf{V}(I) \subset \mathbb{K}^{n+m}$. Tällöin on voimassa

Lemma 2.5.25.

$$\pi_m(\mathbf{V}(I)) \subset \mathbf{V}(I_m)$$

Siis $\mathbf{V}(I_m)$ *on pienin varieteetti, joka sisältää pinnan* $P = f(\mathbb{K}^m) \subset \mathbb{K}^n$.

Esimerkki 2.5.26. Tarkastellaan käyrää, jonka parametriesitys $\varphi : \mathbb{R} \mapsto \mathbb{R}^3$ on

$$\begin{aligned} x_1 &= t_1 \\ x_2 &= t_1^2 \\ x_3 &= t_1^3 \end{aligned}$$

Käyrän tangentti vektori pisteessä t_1 on $\varphi'(t_1) = (1, 2t_1, 3t_1^2)$ ja koska $\varphi'(t_1) \neq 0$, niin se on hyvin määritelty kaikilla $t_1 \in \mathbb{R}$. Käyrän φ *tangenttipinnan* $S \subset \mathbb{R}^3$ parametriesitys $f : \mathbb{R}^2 \mapsto \mathbb{R}^3$ on

$$f(t_1, t_2) = \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \end{pmatrix} + t_2 \begin{pmatrix} 1 \\ 2t_1 \\ 3t_1^2 \end{pmatrix}.$$

Muodostetaan sitten tangettipinnan koordinaattien esityksistä polynomit

$$\begin{aligned} h_1 &= x_1 - t_1 - t_2 \\ h_2 &= x_2 - t_1^2 - 2t_1 t_2 \\ h_3 &= x_3 - t_1^3 - 3t_1^2 t_2. \end{aligned}$$

Muodostetaan polynomeista ideaali $I = \langle h_1, h_2, h_3 \rangle$. Laskemalla Gröbner kanta esim. järjestyksessä *lex*, $t_1 > t_2 > x_1 > x_2 > x_3$ saadaan

$$I_2 = \langle g \rangle,$$

missä

$$g = x_1^3 x_3 - \frac{3}{4} x_1^2 x_2^2 - \frac{3}{2} x_1 x_2 x_3 + x_2^2 + \frac{1}{4} x_3^2.$$

Tässä tapauksessa on voimassa $Im(f) = \mathbf{V}(I_2) = \mathbf{V}(g)$.

Esimerkki 2.5.27 (Whitneyn sateenvarjo)**.** Whiteneyn sateenvarjon parametrisointi $s : \mathbb{K}^2 \mapsto \mathbb{K}^3$ on

$$\begin{aligned} x_1 &= t_1 t_2 \\ x_2 &= t_2 \\ x_3 &= t_1^2. \end{aligned}$$

Eliminointi-ideaaliksi I_2 saadaan $I_2 = f = x_1^2 - x_2^2 x_3$. Yhtälö $f = x_1^2 - x_2^2 x_3 = 0$ toteutuu esimerkiksi kun $x_2 = 0$ ja $x_1 = 0$. Näin ollen koko x_3-akseli kuuluu varieteettiin $\mathbf{V}(I_2)$. Jos asetetaan $\mathbb{K} = \mathbb{R}$, niin $(0, 0, a) \notin Im(f)$, jos $a < 0$.

Näin ollen $Im(f) \subsetneqq \mathbf{V}(I_2)$. Jos tarkastellaan pinnan singulaarista varieteettia saadaan ensinnäkin $df = (2x_1, -2x_1x_2, -x_2^2)$, joten singulaarinen varieteetti on

$$S(f) = \mathbf{V}(\langle f, df \rangle) = \mathbf{V}(\langle x_1, x_2 \rangle).$$

Pinnan singulaarinen varieteetti on siis koko x_3-akseli.

Tarkastellaan sitten (hyper) pinnan rationaalista parametrisointia

$$\begin{aligned} x_1 &= \frac{f_1}{g_1} \\ &\vdots \\ x_n &= \frac{f_n}{g_n}, \end{aligned}$$

missä $f_i, g_i \in \mathbb{K}[t_1, \ldots, t_m]$ ja $n > m$. Aikaisemmassa esimerkissä todettiin, että yksikkö voidaan parametrisoida rationaalisesti lukuunottamatta pistettä $(-1, 0)$. Parametrisointi oli

$$\begin{aligned} x &= \frac{1 - t^2}{t^2 + 1} \\ y &= \frac{2t}{1 + t^2}. \end{aligned}$$

Rationaalisesta parametrioinnista voidaan muodostaa polynomit

$$h_i = g_i x_i - f_i,$$

kun $g_i \neq 0$, ja näistä edelleen ideaali $I = \langle h_1, \ldots, h_n \rangle$.

Esimerkki 2.5.28. Tarkastellaan pintaa jonka koordinaatit on parametrisoitu

$$\begin{aligned} x_1 &= \frac{t_1^2}{t_2} \\ x_2 &= \frac{t_2^2}{t_1} \\ x_3 &= t_1. \end{aligned}$$

Parametrioinnista muodostetut polynomit h_i ovat

$$\begin{aligned} h_1 &= t_2 x_1 - t_1^2 \\ h_2 &= t_1 x_2 - t_2^2 \\ h_3 &= x_3 - t_1, \end{aligned}$$

ja ideaali I on $I = \langle h_1, h_2, h_3 \rangle$. Laskemalla eliminaatio ideaali $I_2 = I \cap \mathbb{K}[x_1, x_2, x_3]$ saadaan

$$I_2 = \langle g \rangle = \langle x_3(x_1^2 x_2 - x_3^3) \rangle.$$

Näin ollen

$$\mathbf{V}(I_2) = \mathbf{V}(x_3) \cup \mathbf{V}(x_1^2 x_2 - x_3^3),$$

mutta $Im(f) \subset \mathbf{V}(x_1^2 x_2 - x_3^3)$.

Määritellään sitten kuvaus

$$\varphi = \Big(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\Big).$$

Nyt

$$\mathbf{V}(g_1) \cup \ldots \cup \mathbf{V}(g_n) = \mathbf{V}\Big(\prod_{i=1}^{n} g_i\Big) = W.$$

Nyt saadaan jälleen diagrammi

$$\varphi : \mathbb{K}^m \setminus W \to^{\varphi} \mathbb{K}^n$$
$$\varphi : \mathbb{K}^m \setminus W \to^{\phi} \mathbb{K}^{m+n} \to^{\pi_m} \mathbb{K}^n$$

Asetetaan jälleen

$$p_i = g_i x_i - f_i.$$

$$Im(\phi) \subset \mathbf{V}(I),$$

mutta ongelma on, että $\mathbf{V}(I)$ voi olla liian iso.

Esimerkki 2.5.29. Jatkoa edellsiestä esimerkistä. Nyt $g_1 = t_2$, $g_2 = t_1$ ja $g_3 = 1$ ja $W = \mathbf{V}(t_1 t_2) = \mathbf{V}(t_1) \cup \mathbf{V}(t_2)$.

Olkoon sitten $p_0 = 1 - gy$, missä

$$g = \prod_{i=1}^{n} g_i,$$

ja

$$I = \langle p_0, p_1, \ldots, p_n \rangle \subset \mathbb{K}[y, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

Nyt

$$\mathbf{V}(I) \subset \mathbb{K}^{n+m+1}$$

ja jos $b \in \mathbf{V}$, niin $g(b) \neq 0$. Nyt seuraava diagrammi kommutoi

$$\varphi : \mathbb{K}^m \setminus W \to^{\varphi} \mathbb{K}^n$$
$$\varphi : \mathbb{K}^m \setminus W \to^{\widetilde{\phi}} \mathbb{K}^{m+n+1} \setminus W \to^{\pi_m} \mathbb{K}^n,$$

missä

$$\widetilde{\phi} = \Big(\frac{1}{g}, t_1, \ldots, t_m, \frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\Big).$$

Nyt on voimassa

$$\mathbf{V}(\widetilde{\phi}) = \mathbf{V}(I),$$

ja toisaalta

$$Im(\varphi) = Im(\pi_{m+1} \circ \widetilde{\varphi}).$$

Lause 2.5.30. *Olkoon I_{m+1} ideaalin $I = \langle p_0, p_1, \ldots, p_n\rangle \subset \mathbb{K}[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ esliminointi-ideaali. Tällöin $\mathbf{V}(I_{m+1})$ on pienin varieteetti, joka sisältää joukon $Im(\varphi)$.*

Todistus. Koska

$$I_{m+1} = I \cap \mathbb{K}[x_1, \ldots, x_n],$$

niin lauseen 2.5.24 perusteella $\mathbf{V}(I_{m+1})$ on pienin varieteetti siten, että

$$\pi_{m+1}(\mathbf{V}(I)) \subset \mathbf{V}(I_{m+1}).$$

Toisaalta koska

$$Im(\varphi) = Im(\pi_{m+1} \circ \widetilde{\varphi}),$$

niin lause on todistettu.

Esimerkki 2.5.31. Jatkoa edellisestä esimerkistä.

$$p_0 = t_1 t_2$$
$$p_1 = t_2 x_1 - t_1^2$$
$$p_2 = t_1 x_2 - t_2^2$$
$$p_3 = x_3 - t_1.$$

Kun nyt asetetaan $I = \langle p_0, p_1, p_2, p_3\rangle$ niin $J_3 = \langle x_1^2 x_2 - x_3^3\rangle$.

Esimerkki 2.5.32 (Verhokäyrä)**.** Olkoon $f_t = (x - t)^2 + y^2 - 1$, tällöin $\mathbf{V}(f_t)$ on käyräparvi joka koostuu 1 säteisistä ympyröistä joiden keskipiste on x-akselilla. Käyräparven $\mathbf{V}(f_t)$ *verhokäyrä* on käyrä joka sivuaa kaikkia käyräparven pisteitä.

Tarkastellaan sitten, miten annetun käyräparven verhokäyrä voitaisiin muodostaa. Olkoon $f_t(x,y) = f(t,x,y)$ ja merkitään vastaavaa käyräparvea $\mathbf{V}_t = \mathbf{V}(f_t(x,y)) \subset \mathbb{R}^2$. Olkoon sitten $c : \mathbb{R} \mapsto \mathbb{R}^2$, $c(t) = (x(t), y(t))$ verhokäyrän parametriesitys. Käyräparven $\mathbf{V}_t$ normaalit ovat vektoreita

$$\nabla f_t = \Big(\frac{\partial f_t}{\partial x}, \frac{\partial f_t}{\partial y}\Big)$$

on käyräparven $\mathbf{V}_t$ normaali. Nyt täytyy olla voimassa

$$\begin{aligned} f(x(t), y(t), t) &= 0 \\ \langle c'(t), \nabla f_t \rangle &= 0 \end{aligned}$$

Jälkimmäisestä yhtälöstä saadaan

$$\frac{\partial f}{\partial x}x' + \frac{\partial f}{\partial y}y' = 0.$$

Derivoimalla ensimmäistä yhtälöä muuttujan t suhteen saadaan

$$\frac{d}{dt}f(x(t), y(t), t) = \frac{\partial f}{\partial x}x' + \frac{\partial f}{\partial y}y' + \frac{\partial f}{\partial t} = 0.$$

Näin ollen verhokäyrä toteuttaa yhtälöt

$$\begin{aligned} f(x,y,t) &= 0 \\ f_t(x,y,t) &= 0. \end{aligned}$$

Määritelmä 2.5.33. Käyräparven $\mathbf{V}(f(t,x,y)) = \mathbf{V}_t$ verhokäyrä on $\mathbf{V}(I_1)$, missä

$$I = \langle f, f_t \rangle$$

ja

$$I_1 = I \cap \mathbb{K}[x,y].$$

Esimerkki 2.5.34. Jos tarkastellaan jälleen käyräparvea $\mathbf{V}(f(t,x,y)) = \mathbf{V}_t$, missä $f = (x-t)^2 + y^2 - 1$ saadaan

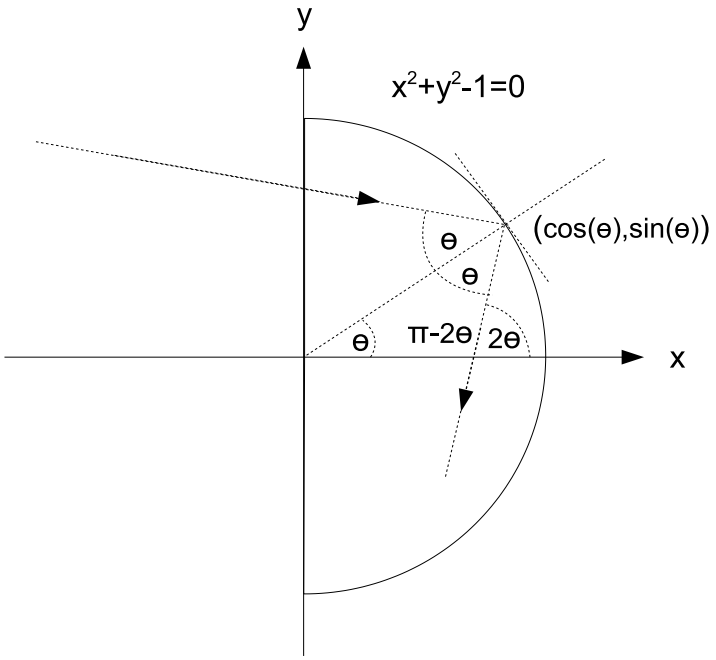
$$I = \langle f(t,x,y), f_t(t,x,y) \rangle = \langle (x-t)^2 + y^2 - 1, -2(x-t) \rangle.$$

Edelleen

$$\mathbf{V}(I_1) = \mathbf{V}(\langle y^2 - 1 \rangle) = \{(x,y) \in \mathbb{R}^2 \mid x \in \mathbb{R},\ y = \pm 1\},$$

mikä oli arvattavissa.

Esimerkki 2.5.35 (Caustic)**.** Lasketaan puoliympyrän muotoisesta peilistä heijastunneittein valonsäteiden verhokäyrä kun peilin ajatellaan rajoittuneen alueeseen $x \geq 0$. Heijastuneiden säteiden yhtälö voidaan muodostaa kuvasta



Kuva 3: Puoliympyrän muotoisesta peilistä heijastunut valonsäde

Heijastunutta sädettä esittävän suoran yhtälöksi saadaan

$$y - \sin(\theta) = \tan(2\theta)(x - \cos(\theta)).$$

Verhokäyrän yhtälöiksi saadaan

$$f(\theta, x, y) = y - \sin(\theta) - \tan(2\theta)(x - \cos(\theta)) = 0$$
$$f_\theta(\theta, x, y) = \cos(\theta) + 2(1 + \tan^2(\theta))(x - \cos(\theta)) + \tan(2\theta)\sin(\theta) = 0.$$

Asettamalla $c = \cos(\theta)$, $s = \sin(\theta)$ ja yhtälöstä

$$\tan(2\theta) = \frac{\sin(2\theta)}{\cos(2\theta)}$$

saadaan verhokäyrälle jälleen esitys algebrallisena varieteettina. Nyt $I = \langle f, f_\theta, c^2 + s^2 - 1 \rangle$ ja vehokäyrä on $\mathbf{V}(I_2)$.

2.6 Varieteettien ja ideaalien yhteys

Olkoon

$$I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n].$$

Ideaalia vastaava varieteetti on

$$\mathbf{V}(I) = \{a \in \mathbb{K}^n \mid f(a) = 0 \ \forall \ f \in I\}.$$

Tästä saadaan funktio/kuvaus ideaalien ja varieteettien välille.

$$\text{Ideaalit} \rightarrow \text{Varieteetit}$$

Esimerkki 2.6.1. Olkoon $I_1 = \langle 1 \rangle = \mathbb{K}[x]$ ja $I_2 = \langle 1 + x^2 \rangle \subsetneqq \mathbb{K}[x]$. Nyt jos

1. Jos $\mathbb{K} = \mathbb{R}$, niin $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \emptyset$
2. Jos taas $\mathbb{K} = \mathbb{C}$, niin $\mathbf{V}(I_1) = \emptyset$, mutta $\mathbf{V}(I_2) = \{\pm i\}$.

Lemma 2.6.2. *Olkoon $S \subset \mathbb{K}^n$ varieteetti ja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali. Tällöin*

1. $S = \mathbf{V}(J(S))$
2. $I \subset I(\mathbf{V}(I))$

Todistus. Koska $J(S)$ on ideaali sillä on äärellinen määrä virittäjiä

$$J(S) = \langle g_1, \ldots, g_t \rangle.$$

Nyt

1. $g_i(a) = 0 \quad \forall \ a \in S$
2. $\mathbf{V}(I(S)) = \{a \in \mathbb{K}^n \mid g_i(a) = 0\}$,

joten $S \subset \mathbf{V}(I(S))$. Koska S on varieteetti

$$S = \mathbf{V}(f_1, \ldots, f_s)$$
$$I = \langle f_1, \ldots, f_s \rangle.$$

Mutta toisaalta $J \subset I(S)$, joten $\mathbf{V}(I(S)) \subset \mathbf{V}(J) = S$.
Todistetaan toinen kohta. Olkoon $J = \langle f_1, \ldots, f_s \rangle$. Tällöin $f_i(a) = 0 \quad \forall \ a \in \mathbf{V}(J)$. Näin ollen $f_i \in I\mathbf{V}(J))$, joten $J \subset I(\mathbf{V}(J))$.

Esimerkki 2.6.3. Jatkoa edellisestä esimerkistä. Nyt $J = \langle x^2 \rangle$, joten $\mathbf{V}(J) = \{0\}$. Näin ollen $I(\mathbf{V}(J)) = \langle x \rangle \supsetneqq J$. Yleisesti jos $f^k \in I(\mathbf{V})$, niin $f \in I(\mathbf{V})$.

Määritelmä 2.6.4 (Radikaali-ideaali)**.** Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali. Tällöin ideaalin I *radikaali* $\sqrt{I}$ on

$$\sqrt{I} = \{f \mid f^k \in I, \text{ jollakin } k \geq 1\}.$$

Ideaali I on radikaali-ideaali, jos $\sqrt{I} = I$

Lemma 2.6.5. *Ideaalin I radikaali $\sqrt{I}$ on ideaali.*

Todistus. 1. Koska $0 \in I$ ja $I \subset \sqrt{I}$, niin $0 \in \sqrt{I}$
2. Jos $f, g \in \sqrt{I}$ tällöin $f^k \in I$ ja $f^m \in I$, $k, m \in \mathbb{N}$. tarkastellaan sitten plynomia $(f+g)^{k+m}$ binomikehitelmän perusteella polynomin $f+g$, $k+m$ kertaisen tulon yleinen monomi on

$$f^{k+m-j} g^j.$$

Nyt jos $j \geq m$, niin $g_j \in I$ jos taas $j < m$, niin $f^{k+m-j} \in I$. Näin ollen $(f+g)^{k+m} \in I$, joten $f+g \in I$.
3. Jos $f \in \sqrt{I}$ ja $h \in \mathbb{K}[x_1, \ldots, x_n]$, niin $f^k \in I$. Tällöin $h^k f^k = (hk)^k \in I$, joten $hf \in \sqrt{I}$

Lemma 2.6.6. *Jos $I \subset \mathbb{C}[x]$, niin*

$$\mathbf{V}(I) \neq \emptyset \;\Leftrightarrow\; I \neq \mathbb{C}[x].$$

Todistus. Olkoon $g \in \mathbb{C}[x]$ s.e $I = \langle g \rangle$. Algebran peruslauseen nojalla

$$\mathbf{V}(g) \neq \emptyset \;\Leftrightarrow\; g \neq \text{ vakio} \neq 0.$$

Lause 2.6.7. *Olkoon $I \subset \mathbb{C}[x_1, \ldots, x_n]$. Tällöin on voimassa*

$$\mathbf{V}(I) \neq \emptyset \;\Leftrightarrow\; I \neq \mathbb{C}[x_1, \ldots, x_n].$$

Todistus. " $\Leftarrow$ " Koska esimerkiksi $1 \in \mathbb{C}[x_1, \ldots, x_n]$, niin $V(I) = \emptyset$.
" $\Rightarrow$ " Todistus nojaa heikkoon nollakohtalauseeseen. Todistetaan väite induktiolla muuttujien x_i lukumäärän suhteen. Tapaus $n = 1$ seuraa edellisestä lauseesta. Oletetaan sitten, että väite pätee arvolla $n-1$. Olkoon sitten $I = \langle f_1, \ldots, f_s \rangle \in \mathbb{C}[x_1, \ldots, x_n]$, $\mathbf{V}(I) = \emptyset$ ja $\deg(f_1) \geq 1$. Yleisyyttä rajoittamatta voidaan olettaa, että

$$f_1 = C x_1^N + \ldots$$

missä f_1 on kirjoitettu siinä muodossa, että N on korkein muuttujaa x_1 vastaava potenssi ja $C = vakio$. Tämä saadaan aikaan lineaarisella muuttujan

vaihdolla $(\widetilde{x}_1, \ldots, \widetilde{x}_n) = \widetilde{x} = Ax$, $x = (x_1, \ldots, x_n)$. Täytyy osoittaa, että $1 \in I$. Ensimmäinen eliminaatioideaali on

$$I_1 = I \cap \mathbb{K}[x_2, \ldots, x_n]$$

Koska $C = vakio$ kaikki osaratkaisut laajenevat, eli

$$\mathbf{V}(I_1) = \pi_1(\mathbf{V}(I)).$$

Koska $\mathbf{V}(I) = \emptyset$, niin $\mathbf{V}(I_1) = \emptyset$, näin ollen induktio-oletuksen nojalla

$$I_1 = \mathbb{K}[x_2, \ldots, x_n].$$

Koska $1 \in I_1 \subset I$, niin $I = \mathbb{C}[x_1, \ldots, x_n]$.

Seuraus 2.6.8. *Olkoon G ideaalin I minimi Gröbner kanta. Tällöin*

$$I = \mathbb{K}[x_1, \ldots, x_n] \;\Leftrightarrow\; G = \{1\}.$$

Todistus. " $\Leftarrow$ " on selvä. Todistetaan " $\Rightarrow$ ". Olkoon

$$1 = LT(1) \in \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Tällöin $LT(g_i)|1$ jollekkin $1 \leq i \leq t$. Näin ollen $LT(g_i) = vakio$, joten g_i on vakio, siis $\langle G \rangle = \langle g_i \rangle$, joten G ei ole minimi Gröbner kanta, mutta $\{g_i\}$ on minimi Gröbner kanta.

Lause 2.6.9 (Nullstellensatz)**.** *Olkoo $I \subset \mathbb{C}[x_1, \ldots, x_n]$ ideaali tällöin*

$$\sqrt{J} = I(\mathbf{V}(J)).$$

Tästä saadaan bijektiivinen kuvaus Kompleksisten varieteettien ja radikaali-ideaalien välille

$$\sqrt{J} \to^{\mathbf{V}} \mathbf{V}(J)$$
$$\mathbf{V}(J) \to^{I} \sqrt{J}$$

Todistus. " $\subset$ " Koska $J \subset I(\mathbf{V}(J))$ ja $I(\mathbf{V}(J))$ on radikaali-ideaali, niin

$$\sqrt{J} \subset I(\mathbf{V}(J)).$$

" $\supset$ " Olkoon sitten $J = \langle f_1, \ldots, f_s \rangle$ ja $f \in I(\mathbf{V}(J))$. Tällöin täytyy osoittaa, että $f \in \sqrt{J}$ eli on olemassa $m \in \mathbb{N}$ siten, että $f^m \in \sqrt{J}$. Toisinsanoen on olemassa $m \in \mathbb{N}$ ja polynomit a_i siten, että

$$f^m = a_1 f_1 + \ldots + a_s f_s.$$

Olkoon sitten

$$\widetilde{J} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbb{C}[x_1, \ldots, x_n, y].$$

Väite: $\mathbf{V}(J) = \emptyset$. Todistetaan väite. Olkoon $(b_1, \ldots, b_{n+1}) \in \mathbb{C}^{n+1}$ tällöin on kaksi mahdollisuutta

1. $(b_1, \ldots, b_n) \in \mathbf{V}(J)$
2. $(b_1, \ldots, b_n) \notin \mathbf{V}(J)$.

Tapaus (1) $f(c) = 0$ aina kun $f_i(c) = 0 \quad \forall\, i$. Tästä seuraa

$$1 - yf(b_1, \ldots, b_n) = 1 \neq 0.$$

Näin ollen $b_1, \ldots, b_n, b_{n+1} \notin \mathbf{V}(\widetilde{J})$. Tapaus 2 $(b_1, \ldots, b_n) \notin \mathbf{V}(J)$. Tästä seuraa, että on olemassa l siten, että

$$f_l(b_1, \ldots, b_n) \neq 0.$$

Tästä seuraa $(b_1, \ldots, b_n, b_{n+1}) \notin \mathbf{V}(\widetilde{J})$. Nyt kohdista 1 ja 2 seuraa $\mathbf{V}(\widetilde{J}) = \emptyset$. Näin ollen $1 \in \widetilde{J}$, ja

$$1 = p_1 f_1 + \ldots + p_s f_s + p_{s+1}(1 - yf).$$

Asetetaan sitten

$$y = \frac{1}{f},$$

jolloin

$$1 = p_1(x_1, \ldots, x_n, \frac{1}{f}) f_1 + \ldots + p_s f_s.$$

Kerrotaan puolittain tarpeeksi korkealla potenssilla polynomin f potenssilla f^m, niin saadaan

$$f^m = a_1(x_1, \ldots, x_n) f_1 + \ldots + a_s(x_1, \ldots, x_n) f_s,$$

joten $f \in \sqrt{J}$.

Esimerkki 2.6.10. Olkoon $f \in \mathbb{C}[x]$ tällöin

$$f = a_n(x - c_1)^{r_1} \cdots (x - c_k)^{r_k}$$
$$f_r = (x - c_1) \cdots (x - c_k)$$

Aikaisemmin saatiin tulos

$$f_r = \frac{f}{syt(f, f')}.$$

Nyt $\langle f_r \rangle = \sqrt{\langle f \rangle}$.

Lemma 2.6.11. *Olkoon* $f_i \in \mathbb{K}[x_1, \ldots, x_n]$,

$$f = f_1^{r_1} \cdots f_k^{r_k},$$

ja

$$I = \langle f \rangle.$$

Oletetaan, että $syt(f_i, f_j) = 1 \quad \forall\ i \neq j$ *tällöin*

$$\sqrt{I} = \langle f_1 \cdot f_k \rangle.$$

Lause 2.6.12. *Olkoon* $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ *ja*

$$I = \langle f_1, \ldots, f_s \rangle.$$

Tällöin on voimassa ekvivalenssi

$$f \in \sqrt{I} \ \Leftrightarrow\ 1 \in \widetilde{I}$$

Todistus. " $\Leftarrow$ " Koska $1 \in \widetilde{I}$, niin

$$1 = \sum_{i=1}^{s} a_i f_i + b(1 - yf)$$

Sijoitetaan $y = 1/f$. Kerrotaan polynomilla f^m missä m on tarpeeksi korkea potenssi. Tällöin

$$f^m = \sum_{i=1}^{s} p_i f_i \in I,$$

joten $f \in \sqrt{I}$.
" $\Rightarrow$ " Jos $f \in \sqrt{I}$, niin $f^m \in I \subset \widetilde{I}$. Toisaalta $1 - yf \in \widetilde{I}$. Näin ollen

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \ldots + y^{m-1} f^{m-1}) \in$$
$$widetildeI.$$

Esimerkki 2.6.13. Olkoon $I = \langle f_1, f_2 \rangle$, missä

$$f_1 = x_1 x_2^2 + 2x_2^2$$
$$f_2 = x_1^4 - 2x_1^2 + 1$$
$$f = x_2 - x_1^2 + 1.$$

Nyt

$$\widetilde{I} = \langle f_1, f_2, 1 - y(x_2 - x_1 + 1)\rangle$$

Kun lasketaan ideaalin $\widetilde{I}$ minimi Gröbner kanta saadaan $G = \{1\}$. Näin ollen $f \in \sqrt{I}$. Ideaalin I minimi Gröbner kanta on

$$G = \{x_1^4 - 2x_1^2 + 1, x_2^2\}.$$

Nyt saadaan

$$\begin{aligned} f &\to^G f \\ f^2 &\to^G -2x_1^2x_2 + 2x_2 \\ f^3 &\to^G 0, \end{aligned}$$

joten $f^3 \in I$.

2.7 Operaatiot ideaaleilla ja varieteteilla

(1) Varieteettien leikkaus. Olkoon $I_1 = \langle f_1, \ldots, f_s\rangle$ ja $I_2 = \langle g_1, \ldots, g_t\rangle$ ideaaleja. Onko

$$\mathbf{V}(I_1) \cap \mathbf{V}(I_2)$$

varieteetti? Olkoon sitten $a \in \mathbf{V}(I_1) \cap (\mathbf{V}(I_2))$. Tällöin

$$\begin{aligned} f_i(a) &= 0 \quad \forall\ i \\ g_i(a) &= 0 \quad \forall\ j. \end{aligned}$$

Olkoon sitten

$$I_3 = \langle f_1, \ldots, f_s, g_1, \ldots, g_t\rangle.$$

Tällöin

$$\mathbf{V}(I_3) = \mathbf{V}(I_1) \cap \mathbf{V}(I_2)$$

Määritelmä 2.7.1 (Ideaalien summa)**.** Olkoon I_1 ja I_2 ideaaleja. Määritellään

$$I_1 + I_2 = \{h \in \mathbb{K}[x_1, \ldots, x_n] \mid h = f + g,\ f \in I_1,\ g \in I_2\}$$

Lause 2.7.2. *Ideaalien summa $I_1 + I_2$ on ideaali.*

Lemma 2.7.3.

$$\mathbf{V}(I_1 + I_2) = \mathbf{V}(I_1) \cap \mathbf{V}(I_2).$$

Esimerkki 2.7.4. Olkoon

$$f_1 = x^2 + y^2 - 4$$
$$f_2 = x - y$$

Tällöin

$$\mathbf{V}(\langle f_1 \rangle) \cap \mathbf{V}(\langle f_2 \rangle) = \mathbf{V}(\langle f_1, f_2 \rangle) = \{p, -p\}.$$

Määritelmä 2.7.5 (Ideaalien tulo)**.** Olkoon I_1 ja I_2 ideaaleja. Tällöin ideaalien I_1 ja I_2 tulo määritellään

$$I_1 I_2 = \langle \{h \mid h = fg,\ f \in I_1,\ g \in I_2\} \rangle.$$

Lemma 2.7.6. *Olkoon*

$$I_1 = \langle f_1, \ldots, f_s \rangle$$
$$I_2 = \langle g_1, \ldots, g_t \rangle$$

Tällöin ideaali $I_1 I_2$ on

$$I_1 I_2 = \langle f_1 g_1, \ldots, f_1 g_t, f_2 g_1, \ldots f_2 g_t, \ldots, f_s g_1, \ldots, f_s g_t \rangle$$

Todistus. HT

Lemma 2.7.7.

$$\mathbf{V}(I_1 I_2) = \mathbf{V}(I_1) \cup \mathbf{V}(I_2).$$

Todistus. ” $\subset$ ” Olkoon $a \in \mathbf{V}(I_1 I_2)$ tällöin $f(a)f(g) = 0 \quad \forall\ f \in I_1,\ g \in I_2$. Jos $g(a) \neq 0$, niin $a \in \mathbf{V}(I_1)$. Jos on olemassa f siten, että $f(a) \neq 0$, niin $g(a) = 0 \quad \forall\ g \in I_2$ joten $a \in \mathbf{V}(I_1)$.
” $\supset$ ” Olkoon $a \in \mathbf{V}(I_1) \cup \mathbf{V}(I_2)$. Tällöin

$$f(a) = 0 \quad \forall\ f \in I_1$$

tai

$$g(a) = 0 \quad \forall\ g \in I_2.$$

Näin ollen

$$f(a)g(a) = 0,$$

kun $f \in I_1,\ g \in I_2$, joten $h(a) = 0 \quad \forall\ h \in I_1 I_2$, joten $a \in \mathbf{V}(I_1 I_2)$.

Lemma 2.7.8. *Jos I_1 ja I_2 ovat ideaaleja, niin $I_1 \cap I_2$ on ideaali.*

Todistus. H.T
Osoitetaan, että $I_1 I_2 \subset I_1 \cap I_2$. Olkoon $p \in I_1 I_2$, ja

$$I_1 = \langle f_1, \ldots, f_s \rangle$$
$$I_2 = \langle g_1, \ldots, g_t \rangle.$$

Nyt polynomi p on muotoa

$$p = a_1 f_1 g_1 + a_2 f_1 g_2 + \ldots + a_{st} f_s g_t$$

Koska $f_i g_j \in I_1 \cap I_2 \quad \forall\, i, j$, niin $a_l f_i g_j \in I_1 \cap I_2$, joten $p \in I_1 \cap I_2$.

Esimerkki 2.7.9. Olkoon $I_1 = I_2 = \langle x \rangle$, nyt

$$I_1 I_2 = \langle x^2 \rangle \subsetneqq \langle x \rangle = I_1 \cap I_2.$$

Lause 2.7.10. *Olkoon I_1 ja I_2 ideaaleja*

$$I_1 = \langle f_1, \ldots, f_s \rangle$$
$$I_2 = \langle g_1, \ldots, g_r \rangle.$$

Olkoon J ideaali

$$J = \langle t f_1, \ldots, t f_s, (1-t) g_1, \ldots, (1-t) g_r \rangle \subset \mathbb{K}[t, x_1, \ldots, x_n].$$

Tällöin

$$I_1 \cap I_2 = J_1 = J \cap \mathbb{K}[x_1, \ldots, x_n].$$

Todistus. " $\subset$ " Olkoon $p \in I_1 \cap I_2$. Tällöin p on muotoa

$$p = a_1 f_1 + \ldots + a_s f_s = b_1 g_1 + \ldots + b_r g_r.$$

Näin ollen

$$\begin{aligned} p &= t(a_1 f_1 + \ldots + a_s f_s) + (1-t)(b_1 g_1 + \ldots + b_r g_r) \\ &= a_1 t f_1 + \ldots + a_s t f_s + b_1 (1-t) g_1 + \ldots b_r (1-t) g_r \in J. \end{aligned}$$

Toisaalta p *ei* riipu muuttujasta t, joten $p \in J_1$.
" $\supset$ " Olkoon sitten $p \in J_1 \subset J$. Tällöin

$$p = a_1 t f_1 + \ldots + a_s t f_s + b_1 (1-t) g_1 + \ldots + b_r (1-t) g_r.$$

Nyt

$$p|_{t=0} = b_1 g_1 + \ldots + b_r g_r \in I_2$$
$$p|_{t=1} = a_1 f_1 + \ldots + a_s f_s \in I_1.$$

Koska $p \in J_1$, niin

$$p = p|_{t=0} = p|_{t=1} \in I_1 \cap I_2.$$

Esimerkki 2.7.11. Olkoon

$$I_1 = \langle x^2 y \rangle$$
$$I_2 = \langle xy^2 \rangle$$

Nyt ideaali J on

$$J = \langle tx^2 y, (1-t)xy^2 \rangle$$

Laskemalla ideaaliun J Gröbner kanta järjestyksessä lex, $t > x > y$ saadaan

$$J = \langle tx^2 y, (1-t)xy^2, x^2 y^2 \rangle.$$

Tästä saadaan

$$I_1 \cap I_2 = \langle x^2 y^2 \rangle$$

Huomataan

$$I_1 I_2 = \langle x^3 y^3 \rangle \subsetneqq I_1 \cap I_2,$$

mutta

$$\sqrt{I_1 I_2} = \langle xy \rangle = \sqrt{I_1 \cap I_2}.$$

Lause 2.7.12.

$$\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2}.$$

Todistus. " $\subset$ " Olkoon $p \in \sqrt{I_1 I_2}$, tällöin $p^m \in I_1 I_2$ ja näin ollen $P^m \in I_1 \cap I_2$, joten $p \in \sqrt{I_1 \cap I_2}$. " $\supset$ " Olkoon $p \in \sqrt{I_1 \cap I_2}$, jolloin $p^m \in I_1 \cap I_2$. Tästä seuraa

$$p^m = a_1 f_1 + \ldots + a_s f_s = b_1 g_1 + \ldots + b_r g_r.$$

Lasketeaan sitten tulo

$$p^{2m} = p * p = a_1 b_1 f_1 g_1 + a_2 b_1 f_2 g_1 + \ldots + a_s b_r f_s g_r \in I_1 I_2.$$

Näin ollen $p \in \sqrt{I_1 I_2}$.

Seuraus 2.7.13.

$$\mathbf{V}(I_1 I_2) = \mathbf{V}(I_1 \cap I_2) = \mathbf{V}(I_1) \cup \mathbf{V}(I_2).$$

Lause 2.7.14.

$$\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}.$$

Todistus. H.T

Seuraus 2.7.15. *Jos I_1 ja I_2 ovat radikaali-ideaaleja, niin myös $I_1 \cap I_2$ on radikaali-ideaali.*

Määritelmä 2.7.16 (Zariski-sulkeuma)**.** Olkoon $S \subset \mathbb{K}^n$. Joukon S *Zariski-sulkeuma* $\overline{S}$ on pienin varieteetti joka sisältää joukon S.

Jos joukot $\mathbf{V}_i,\ i \in I$ ovat varieteetteja niiden yhdiste ei välttämättä ole jos I on ääretön indeksijoukko.

Esimerkki 2.7.17. Olkoon $\mathbf{V}_i = \{i\} \subset \mathbb{R}$, tällöin $\cup_{i\in\mathbb{Z}} = \mathbb{Z} \subset \mathbb{R}$, mutta $\mathbb{Z}$ *ei* ole varieteetti.

Lemma 2.7.18. *Olkoon $\{\mathbf{V}_\alpha\},\ \alpha \in I$ kokoelma varieteetteja. Tällöin*

$$\bigcap_{\alpha\in I} \mathbf{V}_\alpha$$

on varieteetti.

Todistus. Olkoon $\mathbf{V}_\alpha = \mathbf{V}(I_\alpha)$. Tällöin

$$\begin{aligned}\bigcap_{\alpha\in I} \mathbf{V}_\alpha &= \bigcap_{\alpha\in I} \mathbf{V}(I_\alpha) \\ &= \mathbf{V}\Big(\sum_{\alpha\in I} I_\alpha\Big) = J.\end{aligned}$$

Hilbertin kantalauseen perusteella

$$J = \langle f_1, \ldots, f_s \rangle,$$

joten

$$\bigcap_{\alpha\in I} \mathbf{V}_\alpha = \mathbf{V}(J).$$

Esimerkki 2.7.19. Jos $A, B \in \tau_{zar}$, $\tau_{zar} \subset P(\mathbb{R})$, niin A ja B ovat varieteettien kompementteja. Nyt on voimassa: Jos $A \neq \emptyset \neq B$, niin $A \cap B \neq \emptyset$, joten $(\mathbb{R}, \tau_{zar})$ ei ole Hausdorff avaruus.

Esimerkki 2.7.20. Olkoon $I = \langle zx, zy \rangle = \langle z \rangle \langle x, y \rangle$. Tällöin Ideaalin I varieteetti on yhdiste (x, y)-tasosta ja suorasta z-akselista, $\mathbf{V}(I) = \mathbf{V}(\langle z \rangle) \cup \mathbf{V}(\langle x, y \rangle)$. Nyt $\mathbf{V}(\langle x, y \rangle) - \mathbf{V}(z) = \{z - akseli\} - \{0\}$. Nyt

$$\overline{\mathbf{V}(\langle x, y \rangle) - \mathbf{V}(z)} = \overline{\{z - akseli\} - \{0\}} = \{z - akseli\}.$$

Olkoon sitten $\pi : \mathbb{K}^n \mapsto \mathbb{K}^k,\ k < n$ ja $\mathbf{V} \subset \mathbb{K}^n$, tällöin yleensä $\pi(\mathbf{V}) \subset \mathbb{K}^k$ *ei* ole varieteetti.
Olkoon sitten $W = V_1 - V_2 = \{p \in V_1, p \notin V_2\}$ myöskään W ei yleensä ole varieteetti. Nyt minkä tahansa joukon A Zariski-sulkeuma on pienin varieteetti, joka sisältää annetun joukon.

Määritelmä 2.7.21 (Jakoideaali)**.** Olkoon $I_1, I_2 \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaaleja. Ideaalien I_1 ja I_2 *jakoideaali* on

$$I_1 : I_2 = \{p \mid pf \in I_1, \quad \forall f \in I_2\}.$$

Esimerkki 2.7.22.

1. Jos $I_1 = \langle x^2 \rangle$ ja $I_2 = \langle x \rangle$, niin

$$\begin{aligned} I_1 : I_2 &= \{p \mid pf \in \langle x^2 \rangle,\ \forall\ f \in \langle x \rangle\} \\ &= \{p \mid px \in I_1\} \\ &= \langle x \rangle. \end{aligned}$$

2. $I_1 \cup I_1 : I_2$, tai yhtäpitävästi $\mathbf{V}(I_1) \cap \mathbf{V}(I_1 : I_2)$.

3. $I_1 : \mathbb{K}[x_1, \ldots, x_n] = I_1$.

4. Jos $I_2 \subset I_1$, niin

$$I_1 : I_2 = \mathbb{K}[x_1, \ldots, x_n].$$

Lemma 2.7.23. *$I_1 : I_2$ on ideaali*

Todistus. H.T
Tiedetään, että $I_2 \subset I_1 \ \Leftrightarrow\ \mathbf{V}(I_1) \subset \mathbf{V}(I_2)$. Toisaalta, jos $I_2 \subset I_1$, niin $\mathbf{V}(I_1 : I_2) = \emptyset$.

Lause 2.7.24. *Olkoon $I_1, I_2 \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaaleja tällöin on voimassa*

1. $\overline{\mathbf{V}(I_1) - \mathbf{V}(I_2)} \subset \mathbf{V}(I_1 : I_2)$

2. Jos $\mathbb{K} = \mathbb{C}$ ja I_1 on radikaali-ideaali, niin

$$\overline{\mathbf{V}(I_1) - \mathbf{V}(I_2)} = \mathbf{V}(I_1 : I_2)$$

Esimerkki 2.7.25. Tarkastellaan edellisen esimerkin tapausta $I_1 = \langle x^2 \rangle$ ja $I_2 = \langle x \rangle$. Nyt $\mathbf{V}(I_1) - \mathbf{V}(I_2) = \emptyset = \overline{\mathbf{V}(I_1) - \mathbf{V}(I_2)} \subsetneqq \mathbf{V}(I_1 : I_2) = \{0\}$, mutta I_1 *ei* ole radikaali-ideaali.

Esimerkki 2.7.26. Olkoon

$$I_1 = \langle x^2 + y^2 \rangle$$
$$I_2 = \langle y \rangle.$$

Nyt I_1 on radikaali-ideaali ja $I_1 : I_2 = I_1$.

1. Jos $\mathbb{K} = \mathbb{R}$, niin $\mathbf{V}(I_1) = \{0\}$, jolloin $\overline{\mathbf{V}(I_1) - \mathbf{V}(I_2)} = \emptyset \subsetneqq \mathbf{V}(I_1 : I_2) = \{0\}$
2. Jos $\mathbb{K} = \mathbb{C}$, niin

$$\mathbf{V}(I_1) = \{(a, ia) \mid a \in \mathbb{C}\}$$
$$\mathbf{V}(I_2) = \{(b, 0) \mid b \in \mathbb{C}\}.$$

Nyt

$$\mathbf{V}(I_1) - \mathbf{V}(I_2) = \{(a, ia) \mid a \neq 0\} = \overline{\mathbf{V}(I_1) - \mathbf{V}(I_2)} = \mathbf{V}(I_1) = \mathbf{V}(I_1 : I_2).$$

Todistus. [Lause 2.7.24] Ensimmäisessä kohdassa täytyy osoittaa

$$I_1 : I_2 \subset I(\mathbf{V}(I_1) - \mathbf{V}(I_2)).$$

Olkoon $f \in I_1 : I_2$ ja $x \in \mathbf{V}(I_1) - \mathbf{V}(I_2)$. Jos $fg \in I_1$, niin $f(x)g(x) = 0$. Jos $x \notin \mathbf{V}(I_2)$, niin on olemassa $\widetilde{g} \in I_2$ siten, että $\widetilde{g}(x) \neq 0$, joten $f(x) = 0 \quad \forall\, x \in \mathbf{V}(I_1) - \mathbf{V}(I_2)$, joten $f \in I(\mathbf{V}(I_1) - \mathbf{V}(I_2)) = I_3$.
Toisessa kohdassa täytyy vielä osoittaa $I_3 \subset I_1 : I_2$. Jos $h \in I_3$ ja $g \in I_2$, niin $h(x)g(x) = 0 \; \forall\, x \in \mathbf{V}(I_1)$. Nollakohtalauseen perusteella

$$hg \in \sqrt{I_1} = I(\mathbf{V}(I_1)),$$

joten $hg \in I_1 \; \forall\, g \in I_2$. Näin ollen $h \in I_1 : I_2$.

Lemma 2.7.27. *Olkoon $I_1, I_2, I_3 \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaaleja, tällöin on voimassa ekvivalenssi*

$$I_1 I_2 \subset I_3 \;\Leftrightarrow\; I_1 \subset I_3 : I_2.$$

Todistus. Varieteettien avulla saadaan

$$\mathbf{V}(I_1) \supset \mathbf{V}(I_3 : I_2) \supset \mathbf{V}(I_3) - \mathbf{V}(I_2).$$

Lemma 2.7.28.

$$I_1 : (I_2 + I_3) = (I_1 : I_2) \cap (I_1 : I_3).$$

Todistus. Olkoon $p \in I_1 : (I_2 + I_3)$ ja

$$\begin{aligned} I_1 &= \langle f_1, \ldots, f_s \rangle \\ I_2 &= \langle g_1, \ldots, g_t \rangle \\ I_3 &= \langle h_1, \ldots, h_r \rangle. \end{aligned}$$

Nyt kaikkia kertoimia b_i, c_j vastaa kertoimet a_k siten, että

$$p(b_1 g_1 + \ldots + b_t g_t + c_1 h_1 + \ldots + c_r h_r) = a_1 f_1 + \ldots + a_s f_s.$$

Jos asetetaan $c_i = 0, \ \forall \ i$, niin $p \in I_1 : I_2$. Jos asetetaan $b_i = 0 \ \forall$, niin $p \in I_1 : I_3$, joten $I_1 : (I_2 + I_3) \subset (I_1 : I_2) \cap (I_1 : I_3)$. Oletaan sitten, että $p \in (I_1 : I_2) \cap (I_1 : I_3)$. Tällöin kaikkia kertoimia b_i kohti on olemassa kertoimet a_j siten, että

$$p(b_1 g_1 + \ldots + b_t g_t) = a_1 f_1 + \ldots + a_s f_s.$$

Lisäksi kaikkia kertoimia c_i kohti on olemassa kertoimet $\widetilde{a_i}$ siten, että

$$p(c_1 h_1 + \ldots + c_r g_r) = \widetilde{a}_1 f_1 + \ldots + \widetilde{a}_s f_s$$

Laskemalla edelliset yhtälöt yhteen saadaan $p \in I_1 : (I_2 + I_3)$, joten $(I_1 : I_2) \cap (I_1 : I_3) \subset I_1 : (I_2 + I_3)$, ja näin ollen $I_1 : (I_2 + I_3) = (I_1 : I_2) \cap (I_1 : I_3)$.

Seuraus 2.7.29. *Olkoon $I_2 = \langle f_1, \ldots, f_s \rangle$, tällöin*

$$I_1 : I_2 = \bigcap_{i=1}^{s} I_1 : \langle f_i \rangle.$$

Lause 2.7.30. *Olkoon $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideaali ja $g \in \mathbb{K}[x_1, \ldots, x_n]$ polynomi. Olkoon sitten*

$$I \cap \langle g \rangle = \langle h_1, \ldots, h_s \rangle.$$

Tällöin on voimassa

$$I_1 : \langle g \rangle = \langle \frac{h_1}{g}, \ldots, \frac{h_s}{g} \rangle.$$

Todistus. Todistetaan " $\supset$ ". Oletetaan, että

$$f \in \langle \frac{h_1}{g}, \ldots, \frac{h_s}{g} \rangle.$$

Pitää osoittaa, että $pf \in I \ \forall \ p \in \langle g \rangle$. Jos $p \in \langle g \rangle$, niin pf on

$$\begin{aligned} pf = agf &= ag\Big(b_1 \frac{h_1}{g} + \ldots + b_s \frac{h_s}{g}\Big) \\ &= a(b_1 h_1 + \ldots + b_s h_s) \subset I \cap \langle g \rangle \subset I. \end{aligned}$$

Todistetaan " $\subset$ ". Oletetaan, että $f \in I : \langle g \rangle$. Tällöin $fg \in I$, joten $fg \in I \cap \langle g \rangle$. Näin ollen

$$fg = a_1 h_1 + \ldots + a_s h_s, \quad h_i \in \langle g \rangle.$$

Näin ollen h_i/g on polynomi jolloin

$$f = a_1 \frac{h_1}{g} + \ldots + a_s \frac{h_s}{g}.$$

Esimerkki 2.7.31. Olkoon $I_1 = \langle xz - y^2, x^3 - yz \rangle$. Nyt $\{z - akseli\} \subset \mathbf{V}(I_1)$. Toisaalta $\{z - akseli\} = \mathbf{V}(\langle x, y \rangle) = \mathbf{V}(I_2)$. Ideaalien I_1 ja I_2 jakoideaali on

$$I_1 : I_2 = I_1 : \langle x, y \rangle = (I_1 : \langle x \rangle) \cap (I_2 : \langle y \rangle).$$

Laskemalla $I_1 \cap \langle x \rangle$ saadaan

$$I_1 \cap \langle x \rangle = \langle x^2 z - xy^2, x^4 - xyz, x^3 y - xz^2 \rangle,$$

joten

$$I_1 : \langle x \rangle = I_1 + \langle x^2 y - z^2 \rangle.$$

Lisäksi $I_1 : \langle y \rangle = I_1 : \langle x \rangle$, joten

$$I_1 : I_2 = I_1 + \langle x^2 y - z^2 \rangle.$$

Ideaalin $I_1 : I_2$ varieteetti voidaan parametrisoida

$$\mathbf{V}(I_1 : I_2) \simeq (t^3, t^4, t^5).$$

Määritelmä 2.7.32 (Osittumaton varieteetti)**.** Varieteettia $\mathbf{V} \subset \mathbb{K}^n$ sanotaan osittumattomaksi jos implikaatio

$$\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2 \ \Rightarrow \ \mathbf{V} = \mathbf{V}_1 \text{ tai } \mathbf{V} = \mathbf{V}_2$$

on voimassa.

Määritelmä 2.7.33 (Alkuideaali)**.** Ideaalia $I \subset \mathcal{R}$ sanotaan alkuideaaliksi, jos implikaatio

$$fg \in I \;\Rightarrow\; f \in I \text{ tai } g \in I$$

on voimassa.

Esimerkki 2.7.34. Olkoon $I \subset \mathbb{Z}$, tällöin on olemassa m siten, että $I = \langle m \rangle$. Jos m *ei* ole alkuluku, niin on olemassa $a, b \in \mathbb{Z}$ siten, että $m = ab$ ja $1 < a, b < m$. Tällöin $ab \in I$, mutta $a \notin I$ ja $b \notin I$. Näin ollen I ei ole alkuideaali. Siis on voimassa ekvivalenssi

$$I \text{ on alkuideaali } \Leftrightarrow\; m \text{ on alkuluku.}$$

Lause 2.7.35. *Olkoon $\mathbf{V} \subset \mathbb{K}^n$ osittumaton varieteetti, tällöin on voimassa ekvivalenssi*

$$\mathbf{V} \textit{ on osittumaton varieteetti } \Leftrightarrow\; I(\mathbf{V}) \textit{ on alkuideaali.}$$

Todistus. ” $\Rightarrow$ ” Olkoon $fg \in I(\mathbf{V})$ ja

$$\mathbf{V}_1 = \mathbf{V} \cap \mathbf{V}(f)$$
$$\mathbf{V}_2 = \mathbf{V} \cap \mathbf{V}(g).$$

Tällöin $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$. Koska $\mathbf{V}$ on osittumaton, niin joko $\mathbf{V} = \mathbf{V}_1$ tai $\mathbf{V} = \mathbf{V}_2$. Olkoon esimerkiksi $\mathbf{V} = \mathbf{V}_1 = \mathbf{V} \cap \mathbf{V}(f)$, tällöin $f \in I(\mathbf{V})$ jos taas $\mathbf{V} = \mathbf{V}_2$, niin $g \in I(\mathbf{V})$.
” $\Leftarrow$ ” Olkoon $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$ ja $\mathbf{V} \neq \mathbf{V}_1$. Osoitetaan, että $I(\mathbf{V}_2) = I(\mathbf{V})$. Koska $\mathbf{V}_2 \subset \mathbf{V}$, niin $I(\mathbf{V}) \subset I(\mathbf{V}_2)$. Täytyy siis osoittaa $I(\mathbf{V}_2) \subset I(\mathbf{V})$. Koska $\mathbf{V}_1 \subsetneq \mathbf{V}$, niin $I(\mathbf{V}) \subsetneq I(\mathbf{V}_1)$. Olkoon sitten $f \in I(\mathbf{V}_1) - I(\mathbf{V}_2)$, $g \in I(\mathbf{V}_2)$. Nyt $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$, joten $fg \in I(\mathbf{V})$. Koska $I(\mathbf{V})$ on alkuideaali, niin $g \in I(\mathbf{V})$, joten $I(\mathbf{V}_2) \subset I(\mathbf{V})$.

Esimerkki 2.7.36.

1. Olkoon $I = \langle x^2 - 2 \rangle$, tällöin I on alkuideaali renkaassa $\mathbb{Q}[x]$, mutta ei renkaassa $\mathbb{R}[x]$, sillä $I = \langle x - \sqrt{2} \rangle \cap \langle x + \sqrt{2} \rangle$

2. Jos taas $I = \langle x^2 - 2y^2 \rangle$, niin I on alkuideaali renkaassa $\mathbb{Q}[x, y]$, mutta ei renkaassa $\mathbb{R}[x, y]$. Ideaali $J = \langle x^2 - 2y^2 + c \rangle$ taas on alkuideaali myös renkaassa $\mathbb{R}[x, y]$.

3. Olkoon sitten $I = \langle x^2 + 1 \rangle$, tällöin I on alkuideaali renkaassa $\mathbb{R}[x]$, mutta ei renkaassa $\mathbb{C}[x]$, sillä $I = \langle x + i \rangle \cap \langle x - i \rangle \subset \mathbb{C}[x]$.

Lause 2.7.37.

1. *Olkoon* $\mathbf{V}$ *varieteetti. Tällöin on olemassa* 1*-käsitteinen minimihajotelma*

$$\mathbf{V} = \mathbf{V}_1 \cup \ldots \cup \mathbf{V}_2,$$

missä varieteetit $\mathbf{V}_i$ *ovat osittumattomia.*

2. *Olkoon* I *ideaali. Tällöin ideaalin* I *radikaalilla* $\sqrt{I}$ *on olemassa* 1*-käsitteinen minimihajotelma*

$$\sqrt{I} = P_1 \cap \ldots \cap P_r,$$

missä ideaalit $P_i \nsubseteq P_j$ *ovat alkuideaaleja.*

Lause 2.7.38. *Olkoon* $(\mathbf{V}_i)_{i\in\mathbb{N}}$ *jono varieteettejä siten, että*

$$\mathbf{V}_1 \supset \mathbf{V}_2 \supset \mathbf{V}_3 \supset \ldots$$

Tällöin on olemassa $N \in \mathbb{N}$ *siten, että indeksistä* N *alkaen*

$$\mathbf{V}_N = \mathbf{V}_{N+1} = \mathbf{V}_{N+2} = \ldots.$$

Todistus. Jos varieteetit toteuttavat lauseen ehdon, niin tällöin

$$I(\mathbf{V}_1) \subset I(\mathbf{V}_2) \subset I(\mathbf{V}_3) \subset \ldots$$

ja tällöin laajenevan jonon periaatteen nojalla on olemassa $N \in \mathbb{N}$ siten, että $I(\mathbf{V}_N) = I(\mathbf{V}_{N+1}) = \ldots$, joten $\mathbf{V}_N = \mathbf{V}_{N+1} = \ldots$

Lause 2.7.39. *Jokainen varieteetti* $\mathbf{V}$ *voidaan esittää muodossa*

$$\mathbf{V} = \mathbf{V}_1 \cup \ldots \cup \mathbf{V}_r,$$

missä varieteetit $\mathbf{V}_i$ *ovat osittumattomia.*

Todistus. Vastaoletus: Oletetaan, että edellisen lauseen hajotelma ei ole mahdollinen. Olkoon sitten $\mathbf{V} = \mathbf{V}_1 \cup \widetilde{\mathbf{V}}$. Tällöin hajotelma esim. verieteetille $\mathbf{V}_1$ ei ole mahdollinen. Olkoon sitten taas $\mathbf{V}_1 = \mathbf{V}_2 \cup \widetilde{\mathbf{V}}_2$. Jälleen esim. varieteetille $\mathbf{V}_2$ ei ole lauseen mukaista esitystä. Tällöin

$$\mathbf{V} \supsetneq \mathbf{V}_1 \supsetneq \mathbf{V}_2 \supsetneq \ldots$$

mikä on ristiriita lauseen 2.7.38 kanssa.

Todistus. [lause 2.7.37] Olkoon

$$\mathbf{V} = \mathbf{V}_1 \cup \ldots \cup \mathbf{V}_r.$$

Jos jokin $\mathbf{V}_i \subset \mathbf{V}_j$, niin poistetaan $\mathbf{V}_i$. Olkoon sitten

$$\mathbf{V} = \mathbf{V}_1 \cup \ldots \cup \mathbf{V}_r = \widetilde{\mathbf{V}}_1 \cup \ldots \cup \widetilde{\mathbf{V}}_m.$$

Nyt

$$\begin{aligned}\mathbf{V}_i &= \mathbf{V}_i \cap \mathbf{V} \\ &= \mathbf{V}_i \cap (\widetilde{\mathbf{V}}_1 \cup \ldots \cup \widetilde{\mathbf{V}}_m) \\ &= (\mathbf{V}_i \cap \widetilde{\mathbf{V}}_1) \cup \ldots \cup (\mathbf{V}_i \cap \widetilde{\mathbf{V}}_m).\end{aligned}$$

Koska $\mathbf{V}_i$ on osittumaton on olemassa indeksi l siten, että $\mathbf{V}_i = \mathbf{V}_i \cap \mathbf{V}_l \subset \widetilde{\mathbf{V}}_l$. Samoin on olemassa indeksi k siten, että

$$\widetilde{\mathbf{V}}_l = \widetilde{\mathbf{V}}_l \cap \mathbf{V}_k \subset \mathbf{V}_k,$$

joten

$$\mathbf{V}_i \subset \widetilde{\mathbf{V}}_l \subset \mathbf{V}_k.$$

Koska kyseessä on minimihajotelma, niin tapauksessa $i = k$ saadaan $\mathbf{V}_i = \mathbf{V}_l$, joten hajotelmissa on samat varieteetit.

Lemma 2.7.40. *Olkoon I_1 alkuideaali. Tällöin joko $I_1 : I_2 = I_1$ tai $I_1 : I_2 = \mathbb{K}[x_1, \ldots, x_n]$.*

Todistus. Olkoon $I_2 = \langle g_1, \ldots, g_t \rangle$, tällöin

$$I_1 : I_2 = I_1 : \langle g_1 \rangle \cap \ldots \cap I_1 : \langle g_t \rangle.$$

Riittää siis osoittaa $I_1 : \langle g \rangle = I_1$ tai $I_1 : \langle g \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Jos $g \in I_1$, niin aikaisemmin todetun perusteella $I_1 : \langle g \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Oletetaan sittem, että $g \notin I_1$. Tällöin

$$I_1 : \langle g \rangle = \{p \mid pg \in I_1\}.$$

Koska I_1 on alkuideaali ja $g \notin I_1$, niin $p \in I_1$.

Määritelmä 2.7.41 (Maksimi-ideaali)**.** Olkoon $I \subsetneqq \mathbb{K}[x_1, \ldots, x_n]$. I on maksimi-ideaali jos ei ole olemassa ideaalia J siten, että

$$I \subsetneqq J \subsetneqq \mathbb{K}[x_1, \ldots, x_n].$$

Lemma 2.7.42. *Olkoon* $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$. *Tällöin* I *on maksimi-ideaali.*

Todistus. 1.) Selvästi $I \neq \mathbb{K}[x_1, \ldots, x_n]$, koska I:n polynomit ovat minimi Gröbner kanta, ja $1 \notin I$.
2.) Olkoon $I \subsetneqq J$ ja olkoon $f \in J - I$. Jakolaskualgoritmi antaa tällöin

$$f = b_1(x_1 - a_1) + \ldots + b_n(x_n - a_n) + r.$$

Koska $0 \neq r \in \mathbb{K}$, ja koska $\deg(r) < 1$, niin $r = vakio$. Tästä saadaan

$$r = f - b_1(x_1 - a_1) - \ldots - b_n(x_n - a_n) \in J.$$

Näin ollen $1 \in J$, joten $J = \mathbb{K}[x_1, \ldots, x_n]$.

Lemma 2.7.43. *Olkoon* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *ideaali, tällöin on voimassa implikaatiot*

$$I \text{ on maksimi-ideaali } \Rightarrow \ I \text{ on alkuideaali } \Rightarrow \ I \text{ on radikaali-ideaali.}$$

Todistus. H.T

Lemma 2.7.44. *Olkoon* $I \subset \mathbb{C}[x_1, \ldots, x_n]$. *Tällöin on voimassa implikaatio*

$$I \text{ on maksimi-ideaali } \Rightarrow \ I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Todistus. Olkoon $I \subsetneqq \mathbb{C}[x_1, \ldots, x_n]$, tällöin heikon nollakohtalauseen perusteella $\mathbf{V}(I) \neq \emptyset$. Olkoon sitten $a \in \mathbf{V}(I)$. Tällöin $f(a) = 0 \ \forall \ f \in I$, joten

$$f \in I(\{a\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

joten $I \subset I(\{a\})$. Koska I on maksimi-ideaali, niin $I = I(\{a\})$.

Edellisen tuloken perusteella voidaan päätellä, että maksimi-ideaalit ovat isomorfisia avaruuden $\mathbb{C}^n$ kanssa. Maksimi-ideaalit $\simeq \mathbb{C}^n$.

2.8 Sovelluksia

Lause 2.8.1. *Olkoon* $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ *tällöin seuraavat väittämät ovat ekvivalentteja*

1. $\mathbf{V}(I)$ *on äärellinen joukko.*
2. $I \cap \mathbb{C}[x_i] \neq 0$
3. *On olemassa vain äärellinen määrä monomeja* x^α *siten, että* $x^\alpha \notin \langle LT(I) \rangle$
4. $\forall\ i\ \exists\ N_i$ *siten, että* $x_i^{N_i} \in \langle LT(I) \rangle$

Määritelmä 2.8.2. Ideaali $I \subset \mathbb{K}[x_1, \ldots, x_n]$ on nollaulotteinen, jos $I \cap \mathbb{K}[x_i] \neq \{0\}\ \ \forall\ 1 \leq i \leq n$.

Todistus. Todistetaan (1) $\Rightarrow$ (2). Olkoon $\mathbf{V}(I) = \{a^1, \ldots, a^l\}$ ja

$$f_i = (x_i - a_i^1) \cdots (x_i - a_i^l).$$

Tällöin $f_i(a^j) = 0 \qquad 1 \leq j \leq l$. Näin ollen

$$f_i \in I(\mathbf{V}(I)) = \sqrt{I},$$

joten on olemassa $m \in \mathbb{N}$ siten, että $f_i^m \in I$ ja näin ollen $f_i^m \in I \cap \mathbb{C}[x_i]$.
(2) $\Rightarrow$ (4) Olkoon $p \in I \cap \mathbb{C}[x_i]$. Tällöin

$$LM(p) = x_i^N \in \langle LT(I) \rangle.$$

(4) $\Rightarrow$ (3) Olkoon

$$I_M = \langle x_1^{N_1}, \ldots, x_n^N \rangle \subset LT(I).$$

Nyt nähdään, että jos $x^\alpha \notin I_M$, niin $\alpha_i < N_i$. On siis olemassa $N_1 \cdots N_n$ kappaletta monomeja siten, että $x^\alpha \notin LT(I)$. Siis on olemassa äärellinen määrä monomeja $x^\alpha \notin LT(I)$.
(3) $\Rightarrow$ (2) Olkoon

$$p_i = \sum_{k=0}^{N} c_{k_i} x_i^k.$$

Koska on olemassa vain äärellinen määrä monomeja $x^\alpha \notin \langle LT(I) \rangle$, niin $LT(p_i) \in \langle LT(I) \rangle$, kun N on riittävän iso. Valitaan sitten monomijärjestys *lex*, ja x_i on pienin muuttuja. Olkoon G ideaalin I Gröbner kanta. Tällöin

$$LT(p_i) \in \langle LT(g_1), \ldots, LT(g_s) \rangle.$$

Nyt $LT(g_i)|LT(p_i)$, joten $g_i \in I \cap \mathbb{C}[x_i]$.
(2) $\Rightarrow$ (1) Olkoon $g_i \in I \cap \mathbb{C}[x_i]$. Tällöin i-koordinaatilla on korkeintaan $\deg(g_i)$ arvoa, joten

$$\#\mathbf{V}(I) \leq \deg(g_1) \cdots \deg(g_n).$$

Määritelmä 2.8.3. Määritellään vektoriavaruus L_I,

$$L_I := \{x^\alpha \mid x^\alpha \notin \langle LT(I) \rangle\}.$$

Tällöin $\dim(L_I)$ on

$$\dim(L_I) = \#\{x^\alpha \mid x^\alpha \notin \langle LT(I) \rangle\}.$$

Lause 2.8.4. *Oleteaan, että ideaali I on nollaulotteinen. Tällöin*

$$\#\mathbf{V}(I) \leq \dim(L_I).$$

Lause 2.8.5. *Oletetaan, että I on nollaulotteinen radikaali-ideaali. Tällöin*

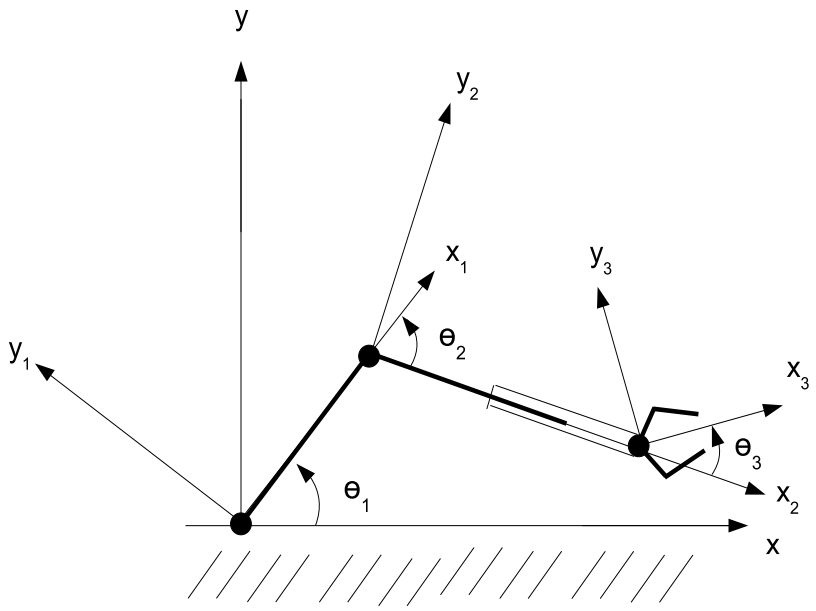
$$\#\mathbf{V}(I) = \dim(L_I).$$

Huomautus 2.1. Reaalisessa tapauksessa saadaan tietenkin vain epäyhtälö

$$\#\mathbf{V}(I) \leq \dim(L_I),$$

2.9 Robotit

Tarkastellaan robottia tasossa $\mathbb{R}^2$. Tarkstellaan esimerkiksi robottia, jossa on kaksi vartta kiinnitetty toisiinsa sarananivelellä, kolmas varsi joka on kiinnitetty toiseen varteen translaationivelellä ja koura joka on kiinnitetty kolmanteen varteen sarananivelellä. Oletaan lisäksi, että jokaisen varren lokaali koordinaatisto on kiinnitetty varren päähän. Robotin konfiguraatioavaruus



Kuva 4: Robotti

on

$$T = S^1 \times S^1 \times S^1 \times I.$$

Robotin mahdolliset liikkeet tapahtuvat avaruudessa $\mathbb{R}^2 \times S^1$ mikä ottaa huomioon kouran paikan globaalissa koordinaatistossa, sekä sen orientaation globaaliin koordinaatistoon nähden. Funktio f kuvaa kouran aseman konfiguraatio avaruudelta avaruudelle $\mathbb{R}^2 \times S^1$,

$$f : T \mapsto C = U \times S^1 \subset \mathbb{R}^2 \times S^1,$$

missä $U \subset \mathbb{R}^2$ on kouran kaikkien mahdollisten paikkavektoreiden joukko.

Nyt voidaan kysyä

1. Mikä on kuvaus $f : T \mapsto C$?
2. Mikä on U ?
3. Mikä on $f^{-1}(p)$?

Olkoon

$$A_i = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}.$$

Nyt kuvaus φ_i, joka kuvaa koordinaatit (a_{i+1}, b_{i+1}) $i+1$ koordinaatistossa koordinaatteihin (a_i, b_i), i koordinaatistossa on

$$\varphi(a_{i+1}, b_{i+1}) = \begin{pmatrix} a_i \\ b_i \end{pmatrix} = A_i \begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} + \begin{pmatrix} l_{i-1} \\ 0 \end{pmatrix}.$$

Affiini kuvaus φ_i voidaan esittää ekvivalentisti lineaarikuvausena

$$\varphi(a_{i+1}, b_{i+1}) = \begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix} = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) & l_{i-1} \\ \sin(\theta_i) & \cos(\theta_i) & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{pmatrix}$$

Kuvaukset φ_i kuuluvat erikoiseen affiiniin ryhmään

$$\mathbb{SE}(2) = \{f : \mathbb{R}^2 \mapsto \mathbb{R}^2 \mid f(x) = Ax + b,\ A \in \mathbb{SO}(2)\},$$

$\varphi_i \in \mathbb{SE}(2)$. Olkoon sitten

$$B_1 = \begin{pmatrix} \cos(\theta_1) & -\sin(\theta_1) & 0 \\ \sin(\theta_1) & \cos(\theta_1) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$B_2 = \begin{pmatrix} \cos(\theta_2) & -\sin(\theta_2) & l_1 \\ \sin(\theta_2) & \cos(\theta_2) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Tällöin

$$B_1 B_2 = \begin{pmatrix} \cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) & l_1 \\ \sin(\theta_1 + \theta_2) & \cos(\theta_1 + \theta_2) & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nyt funktio f voidaan esittää kuvauksena $f \simeq B_1B_2B_3B_4$,

$$f(\theta_1, \theta_2, \theta_3, l_2) = \begin{pmatrix} l_2\cos(\theta_1+\theta_2) + l_1\cos(\theta_1) \\ l_2\sin(\theta_1+\theta_2) + l_1\sin(\theta_1) \\ \theta_1+\theta_2+\theta_3 \end{pmatrix} \simeq B_1B_2B_3B_4 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Olkoon sitten (a, b) piste globaalissa koordinaatistossa, ja merkitään

$$\begin{aligned} c_i &= \cos(\theta_i) \\ s_i &= \sin(\theta_i). \end{aligned}$$

Jotta saataisiin selville millä kulman arvoilla kyseiseen pisteeseen (a, b) päästään täytyy tutkia ideaalin $I = \langle f_1, f_2, f_3, f_4 \rangle$ varieteettia, missä

$$\begin{aligned} f_1 &= l_2c_1c_2 - l_2s_1s_2 + l_1c_1 - a \\ f_2 &= l_2c_1s_2 + l_2c_1s_2 + l_1s_1 - b \\ f_3 &= c_1^2 + s_1^2 - 1 \\ f_4 &= c_2^2 + s_2^2 - 1. \end{aligned}$$

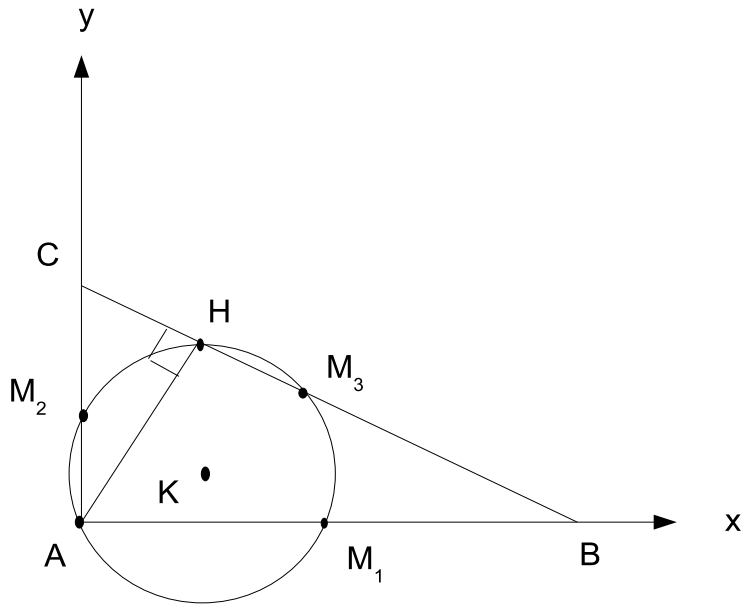
Paras rengas analyysiin on

$$\mathbb{Q}(a, b, l_1, l_2)[c_1, s_1, c_2, s_2]$$

järjestyksenä lex, $c_2 > s_2 > c_1 > s_1$.

2.10 Geometrian lauseiden todistaminen

Todistetaan algebrallisen geometrian keinoin Apolloniuksen lause.



Kuva 5: Suorakulmainen kolmio

$$
\begin{aligned}
A &= (0,0)\\
B &= (u_1,0)\\
C &= ((1/2)u_1,0)\\
M_1 &= (0,(1/2)u_2)\\
M_2 &= (0,(1/2)u_2)\\
M_3 &= ((1/2)u_1,(1/2)u_2)\\
H &= (x_1,x_2)\\
K &= (x_3,x_4).
\end{aligned}
$$

Ehto (1) sanoo $AH \perp BC$, joten

$$
\begin{aligned}
f_1 &= (x_1,x_2)\cdot(u_1,-u_2)\\
&= x_1u_1 - x_2u_2\\
&= 0.
\end{aligned}
$$

Ehto (2) sanoo $CH \| CB$, joten on olemassa λ siten, että

$$\underbrace{(x_1, x_2 - u_2)}_{CH:nsuunta} = \lambda(u_1, -u_2).$$

Tästä saadaan yhtälöt

$$\begin{aligned} x_1 &= \lambda u_1 \\ x_2 - u_2 &= -\lambda u_2. \end{aligned}$$

Näistä saadaan λ eliminoitua jolloin

$$f_2 = x_1 u_2 + x_2 u_1 - u_1 u_2 = 0.$$

Ehto (3) sanoo

$$|KM_1| = |KM_2| = |KM_3|.$$

Ehdosta $|KM_1| = |KM_2|$ saadaan yhtälö

$$f_3 = (x_3 - (1/2)u_1)^2 + x_4^2 - x_3^2 - (x_4 - (1/2)u_2)^2 = 0.$$

Ehdosta $|KM_1| = |KM_3|$ saadaan yhtälö

$$f_4 = (x_3 - (1/2)u_1)^2 + x_4^2 - (x_3 - (1/2)u_1)^2 - (x_4 - (1/2)u_2)^2 = 0.$$

Hypoteeseista saadaan ideaali $I = \langle f_1, f_2, f_3, f_4 \rangle$. Väite oli $|KM_1| = |KH|$, joka voidaan esittää yhtälönä

$$f = (x_3 - (1/2)u_1)^2 + x_4^2 - (x_3 - x_1)^2 - (x_1 - x_2)^2.$$

Nollakohtalauseen perusteella, jos $\mathbb{K} = \mathbb{C}$ $\sqrt{I} = I(\mathbf{V}(I))$. Reaalisessakin tapauksessa on voimassa

$$\sqrt{I} \subset I(\mathbf{V}(I)).$$

Siis jos $f \in \sqrt{I}$ Apolloniuksen lause on voimassa. Miten sitten valita rengas?

1. Jos $\mathbb{A} = \mathbb{Q}[u_1, u_2, x_1, x_2, x_3, x_4]$, niin $f \notin \sqrt{I} \subset \mathbb{A}$
2. Jos taas $\mathbb{A} = \mathbb{Q}(u_1, u_2)[x_1, x_2, x_3, x_4]$, niin $f \to^G 0$, joten $f \in I$.

Hakemisto