TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Riikka Salo

Varistoista ja ideaaleista

Luonnontieteiden laitos
Matematiikka
2018

Sisältö

1 Johdanto

Tässä työssä tutustutaan algebralliseen geometriaan ja erityisesti Hilbertin nollakohtalauseeseen. Algebrallinen geometria tutkii geometriaa abstraktin algebran avulla. Työssä käydään läpi yksi todistus Hilbertin nollakohtalauseelle.
Luvuissa 2 ja 3 esitellään Gröbnerin kanta, Hilbertin kantalause, resultantit polynomirenkaassa ja eliminaatio- ja laajennuslauseet, joita tarvitaan nollakohtalauseen todistuksessa.
Nollakohtalauseesta todistetaan edelleen vahva nollakohtalause ja tarkastellaan radikaaleja ideaaleja sekä varistojen ja ideaalien yhteyttä. Nollakohtalauseen merkittävin seuraus on ns. Hilbertin vastaavuus, minkä merkitykseen tutustutaan hieman luvun lopussa.
Luvussa 8 tarkastellaan ideaaliteoriaa polynomirenkaassa, eli laskutoimituksia ideaaleilla, sekä erilaisten ideaali- ja varistotyyppien yhteyksiä.

Lukijalta edellytetään joidenkin algebran peruskäsitteiden tuntemista, mutta kaikkein olennaisimpia peruskäsitteitä käydään läpi työn aluksi. Myös joitain kommutatiivisen algebran, eli vaihdannaisia renkaita tutkivan algebran, peruskäsitteitä tarvitaan, sillä algebrallinen geometria perustuu pitkälti siihen.

Pääasiallinen lähdeteos on ollut Coxin, Littlen ja O'Shean teosta *Ideals, Varieties, and Algorithms*.

2 Tärkeitä käsitteitä

2.1 Polynomi

Määritelmä 2.1 (**Kunta**). (Ks. [s. 5][7].) Vaihdannaista rengasta $(k, +, \cdot)$ nimitetään *kunnaksi* jos $0 \neq 1$ ja pari $(k \setminus \{0\}, \cdot)$ muodostaa vaihdannaisen ryhmän.

Algebran käsitteet rengas ja kunta ovat tärkeitä algebrallisessa geometriassa. Kunta on tärkeä mm. sen vuoksi, että lineaarialgebran perustulokset pätevät minkä tahansa kunnan yli (Ks. [1, s. 1]). Tässä työssä rengas on polynomirengas.

Määritelmä 2.2. Polynomit ovat äärellisiä jonoja $f\colon \mathbb{Z}^n_{\geq 0} \to k$, jotka voidaan tulkita formaaleina summina, missä monomin x^α potenssi ilmaisee kertoimen a_α paikan jonossa f. Merkitään polynomien joukkoa

$$k[x_1, \ldots, x_n] = \left\{ \sum_\alpha a_\alpha x^\alpha | a_\alpha \in k, \alpha \in \mathbb{Z}^n_{\geq 0} \right\}.$$

Koska jonot ovat äärellisiä jokaista polynomia $p \in k[x_1, \ldots, x_n]$ vastaa tietenkin N, siten että $a_\alpha = 0$, kun $|\alpha| > N$. Varustettuna polynomien normaaleilla yhteen- ja kertolaskuilla $k[x_1, \ldots, x_n]$ muodostaa polynomirenkaan, jolle käytetään jatkossa samaa merkintää $k[x_1, \ldots, x_n]$.

Määritelmä 2.3. (Ks. [1, s. 3].) Polynomi $f = x^\alpha \in k[x_1, \ldots, x_n]$, joka on muotoa

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

missä $\alpha \in \mathbb{Z}^n_{\geq 0}$ sanotaan *monomiksi*.

Huomautus 2.4. (Ks.[1, s. 2].) Olkoon $f = \sum_\alpha a_\alpha x^\alpha, \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ polynomi renkaassa $k[x_1, \ldots, x_n]$.

(i) Monomin x^α vakiokerroin on $a_\alpha \in k$.

(ii) Jos $a_\alpha \neq 0$, niin polynomin f indeksiin α liittyvä termi on $a_\alpha x^\alpha$.

(iii) Polynomin $p \in k[x_1, \ldots, x_n]$ aste on suurin luku $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$, jolla $a_\alpha \neq 0$.

Huomataan, että useampi termi voi olla asteeltaan suurin, minkä vuoksi myöhemmin määritellään monomien suuruusjärjestys.

Esimerkki 2.5. Esimerkiksi polynomi $p = 2xy + 5y^2$ on polynomi $p\colon \mathbb{Z}^2_{\geq 0} \to \mathbb{R}$ jolle $p(1, 1) = 2, p(0, 2) = 5$ ja $p(i, j) = 0$ muulloin.

Tässä jonomerkinnässä muuttuja/monomi $x = x^1y^0$ on $f(1,0) = 1$ ja muuttuja $y = x^0y^1$ on $f(0,1) = 1$.

Tästä lähtien polynomit kirjoitetaan aina formaaleina summina $f = \sum_\alpha a_\alpha x^\alpha$, missä monomin x potenssi ilmaisee polynomin/jonon arvon indeksillä α.

Sanotaan, että kunta k on algebrallisesti suljettu, jos jokaisella polynomilla $f \in k[x]$, joka ei ole vakiopolynomi, on juuri kunnassa k. Tässä työssä käsittelemme polynomeja yli äärettömien kuntien.

Lause 2.6. *Olkoon k algebrallisesti suljettu kunta, tällöin kunta k on ääretön.*

Todistus. Tehdään vastaoletus, eli oletetaan, että F on äärellinen ja olkoon $F = \{a_1, \ldots, a_p\}$. Määritelmän 2.1 mukaan sen täytyy olla muotoa $k = \{0, 1, \ldots, a_p\}$, sillä kuntaan täytyy aina kuulua 0 ja 1-alkiot.

Olkoon $f(x) = 1 + x(x-1) \cdot \ldots \cdot (x - a_p)$. Tällä ei ole juuria joukossa F, joten F ei voi olla suljettu. □

2.2 Ideaalit

Määritelmä 2.7. (Ks. [1, s. 30].)

Polynomirenkaan $k[x_1, \ldots, x_n]$ osajoukko $I \subset k[x_1, \ldots, x_n]$ on *ideaali*, kun

(1) $0 \in I$.

(2) Kaikilla $f, g \in I$ pätee $f + g \in I$ ja

(3) kaikilla $f \in I$ ja $h \in k[x_1, \ldots, x_n]$ pätee $fh \in I$.

Esimerkki 2.8. (Vrt. [6, s. 127].) Olkoon rengas kokonaislukujen joukko $\mathbb{Z}$. Sen ideaaleja ovat esimerkiksi parilliset kokonaisluvut, joukko $2\mathbb{Z}$, sillä

(1) $0 \in 2\mathbb{Z}$.

(2) Jos $a \in 2\mathbb{Z}$ ja $b \in 2\mathbb{Z}$, niin $a + b \in 2\mathbb{Z}$, sillä parillisten lukujen summa on aina parillinen.

(3) Jos $a \in 2\mathbb{Z}$ ja $h \in \mathbb{Z}$, niin $a = 2k$, jolloin $ah = 2kh$ kaikilla $h \in \mathbb{Z}$.

Tämä sama pätee myös kaikilla muillakin kokonaisluvuilla n: joukko $n\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali, samoin perustein.

Määritelmä 2.9. (Ks. [1, s. 30].) Olkoon $f_1, \ldots, f_s$ polynomeja renkaassa $k[x_1, \ldots, x_n]$. Tällöin joukkoa

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \colon h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}$$

sanotaan polynomien f_i generoimaksi ideaaliksi.

Tärkein seuraus tästä on, että $\langle f_1, \ldots, f_s \rangle$ on ideaali.

Lause 2.10. *(Vrt. [1, s. 30].) Jos* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, *niin* $\langle f_1, \ldots, f_s \rangle$ *on ideaali renkaassa* $k[x_1, \ldots, x_n]$.

Todistus. Koska $0 = \sum_{i=1}^{s} 0 \cdot f_i = 0$, niin $0 \in \langle f_1, \ldots, f_s \rangle$. Olkoon nyt $f = \sum_{i=1}^{s} p_i f_i \in \langle f_1, \ldots, f_s \rangle$ ja $g = \sum_{i=1}^{s} q_j f_i \in \langle f_1, \ldots, f_s \rangle$ ja olkoon $h \in k[x_1, \ldots, x_n]$. Nyt nähdään, että

$$f + g = \sum_{i=1}^{s} (p_i + q_j) f_i$$

ja

$$hf = \sum_{i=1}^{s} (hp_i) f_i.$$

Määritelmän 2.7 nojalla $\langle f_1, \ldots, f_s \rangle$ on siis ideaali. □

Lause 2.11. *(Vrt. [1, s. 36].) Olkoon* $I \subset k[x_1, \ldots, x_n]$ *ideaali ja olkoon* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. *Tällöin seuraavat väittämät ovat yhtäpitäviä*

(i) $f_1, \ldots, f_s \in I$

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

Todistus. Oletetaan ensin, että $f_1, \ldots, f_s \in I$. Tällöin polynomit generoivat määritelmän 2.9 ideaalin $\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \colon h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}$, joillain $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$. Määritelmän 2.7 nojalla tämä summa sisältyy myös ideaaliin, eli toinen osa seuraa ensimmäisestä. Oletetaan sitten, että $\langle f_1, \ldots, f_s \rangle \subset I$. Tällöin määritelmän 2.9 oletusten nojalla polynomit $f_1, \ldots, f_s \in I$, joten toisesta väittämästä seuraa ensimmäinen. □

Edellistä lausetta voidaan hyödyntää, kun osoitetaan että jokin ideaali sisältyy toiseen ja että ideaalit ovat samat, vaikka niitä generoivat eri polynomit.

Esimerkki 2.12. (a.) Osoitetaan, että $\langle x + y, x - y \rangle = \langle x, y \rangle$ pätee joukossa $\mathbb{R}^2$.

Osoitetaan ensin, että $\langle x, y \rangle \subset \langle x+y, x-y \rangle$, eli että polynomit $x, y \in \langle x+y, x-y \rangle$.

Valitaan, että $h_1 = h_2 = \frac{1}{2}$, jolloin $h_1(x + y) + h_2(x - y) = x$. Jos valitaan, että $h_1 = \frac{1}{2}$ ja $h_2 = -\frac{1}{2}$, niin $h_1(x + y) + h_2(x - y) = y$. Tällöin edellisen lauseen perusteella, koska polynomit sisältyvät oikeanpuoleiseen ideaaliin, niin myös niiden generoima ideaali sisältyy toiseen ideaaliin.

Osoitetaan toiseen suuntaan, eli että $\langle x + y, x - y \rangle \subset \langle x, y \rangle$. Tällöin siis

$$h_1 x + h_2 y = x + y,$$

kun valitaan $h_1 = 1 = h_2$, joten $x + y \subset \langle x, y \rangle$. Jos valitaan $h_1 = 1$ ja $h_2 = -1$, niin

$$h_1 x + h_2 y = x - y,$$

joten $x - y \subset \langle x, y \rangle$. Näin ollen siis ideaalit ovat samat.

(b.) Osoitetaan, että $\langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle$. Osoitetaan ensin, että $\langle x + xy, y + xy, x^2, y^2\rangle \subset \langle x, y\rangle$. Huomataan ensin, että $h_1x + h_2y = x + xy$, kun $h_1 = 1$ ja $h_2 = x$. Jos valitaan $h_1 = x, h_2 = 0$, niin $h_1x + h_2y = x^2$. Jos $h_1 = 0, h_2 = y$ on $h_1x + h_2y = y^2$ ja vastaavasti kun $h_1 = y, h_2 = 1$, niin $y \cdot x + 1 \cdot y = xy + y$, joten polynomit $x + xy, y + xy, x^2, y^2 \subset \langle x, y\rangle$.

Osoitetaan sitten, että $\langle x, y\rangle \subset \langle x + xy, y + xy, x^2, y^2\rangle$. Nyt voidaan valita $h_1(x+xy)+h_2(y+xy)+h_3x^2+h_4y^2 = -1(x+xy)+1(y+xy)+\frac{1}{x}x^2+0\cdot y^2 = x$, kun $h_1 = -1, h_2 = 1, h_3 = \frac{1}{x}, h_4 = 0$ ja jos valitaan $h_1 = -1, h_2 = 1, h_3 = 0, h_4 = \frac{1}{y}$ niin $h_1(x+xy)+h_2(y+xy)+h_3x^2+h_4y^2 = -1(x+xy)+1(y+xy)+0\cdot x^2+\frac{1}{y}\cdot y^2 = y$. Nyt siis lauseen 2.11 nojalla ideaalit ovat samat.

(c.) Osoitetaan vielä $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle = \langle x^2 - 4, y^2 - 1\rangle$. Osoitetaan ensin, että $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle \subset \langle x^2 - 4, y^2 - 1\rangle$. Jos $h_1 = 2$ ja $h_2 = 3$, niin

$$2(x^2 - 4) + 3(y^2 - 1) = 2x^2 + 3y^2 - 11.$$

Asettamalla $h_1 = 1$ ja $h_2 = -1$ saadaan

$$1(x^2 - 4) + (-1)(y^2 - 1) = x^2 - y^2 - 3.$$

Osoitetaan sitten samalla tavalla, että $\langle x^2-4, y^2-1\rangle \subset \langle 2x^2+3y^2-11, x^2-y^2-3\rangle$.

$$\frac{1}{5}(2x^2 + 3y^2 - 11) + \frac{3}{5}(x^2 - y^2 - 3) = x^2 - 4.$$

Jos taas $h_1 = \frac{1}{5}$ ja $h_2 = -\frac{2}{5}$, niin

$$\frac{1}{5}(2x^2 + 3y^2 - 11) + -\frac{2}{5}(x^2 - y^2 - 3) = y^2 - 1,$$

eli väite pätee.

2.3 Affiinit varistot

Algebrallisessa geometriassa tarkastellaan affiineja varistoja, tai lyhyemmin vain varistoja, mitkä ovat esimerkiksi kaaria, pintoja tai useampiulotteisia objekteja, jotka voidaan määritellä polynomien nollakohtien joukkona.

Määritelmä 2.13. Olkoon $p \in k[x_1, \ldots, x_n]$ polynomi ja $c \in k^n$. *Sijoitushomomorfismi* on rengashomomorfismi

$$s\colon k[x_1, \ldots, x_n] \to k, s(p) = \sum_{\alpha} a_\alpha c^\alpha$$

joka toteuttaa luonnollisesti rengashomomorfismilta vaaditut ominaisuudet, $s(p + g) = s(p) + s(g)$, $s(pg) = s(p)s(g)$ ja $s(1) = 1$.

Huomautus 2.14. Jos esimerkiksi $k = \mathbb{R}$ tai $k = \mathbb{C}$ niin sijoitushomomorfismi määrittelee näin analyysistä tutun polynomifunktion

$$p\colon k^n \to k, p(c) = \sum_{\alpha} a_\alpha c^\alpha, c \in k^n.$$

Polynomifunktioiden yhteiset nollakohdat määritellään myöhemmin määritelmässä 2.18 affiinina varistona, mikä on tämän työn tärkeimpiä käsitteitä. Edelleen lauseessa 2.17 osoitetaan, että äärettömissä kunnissa polynomit $f, g \in k[x_1, \ldots, x_n]$ ovat samat jos ja vain jos niiden määräämät polynomifunktiot $f\colon k^n \to k$ ja $g\colon k^n \to k$ ovat samat.

Määritelmä 2.15. (Ks. [1, s. 3].) Määritellään n-ulotteinen *affiini avaruus* yli kunnan k joukkona

$$k^n = \{(a_1, \ldots, a_n)\colon a_1, \ldots, a_n \in k\},$$

missä $n \in \mathbb{Z}_{\geq 0}$.

Lause 2.16. *(Ks.[1, s. 3].) Olkoon k ääretön kunta ja olkoon $f \in k[x_1, \ldots, x_n]$. Tällöin $f = 0$ renkaassa $k[x_1, \ldots, x_n]$ jos ja vain jos $f\colon k^n \longrightarrow k$ on nollafunktio.*

Todistus. On siis osoitettava, että nollapolynomi vastaa nollafunktiota äärettömässä kunnassa. Nollapolynomin $\sum_n a_n x^n$ kaikki kertoimet a ovat nollia. Tällöin myös $f(a_1, \ldots, a_n) = 0$.
Olkoon sitten f nollafunktio, eli $f(a_1, \ldots, a_n) = 0$ kaikilla $(a_1, \ldots, a_n) \in k^n$. Todistetaan tämä induktiolla, missä n on muuttujien määrä. Kun $n = 1$, niin nollasta poikkeavalla, m-asteisella funktiolla on korkeintaan m juurta. Kuitenkin nollafunktio $f(a) = 0$ kaikilla $a \in k$ ja k on oletusten mukaan ääretön kunta, eli siinä on äärettömän monta alkiota, joten f:llä on äärettömän monta juurta, eli sen täytyy olla nollapolynomi. Oletetaan nyt väite todistetuksi $n - 1$:lle muuttujalle ja olkoon f polynomi, joka saa arvon nolla kaikilla $(a_1, \ldots, a_n) \in k^n$. Järjestelemällä termejä x_n potenssien mukaan voidaan f kirjoittaa muotoon

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

missä $g_i \in k[x_1, \ldots, x_{n-1}]$. Osoitetaan, että jokainen g_i on nollapolynomi, kun muuttujia on $n-1$ kappaletta, jolloin myös f on nollapolynomi renkaassa $k[x_1, \ldots, x_n]$. Pisteellä $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ polynomi f on muotoa $f = f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$. Oletuksen nojalla tämä polynomi on nolla kaikilla $a_n \in k$. Jos sijoitetaan ylläoleva summamuoto nyt tähän polynomin f muotoon, niin että yksittäinen
$g_i(a_1, \ldots, a_{n-1}) = f(a_1, \ldots, a_{n-1}, x_n)$ huomataan, että jokainen $g_i = 0$.
Koska $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ voi olla mikä tahansa piste menevät kaikki polynomit g_i nolliksi ja koska ne ovat induktio-oletuksen mukaan nollapolynomeja on myös f nollapolynomi, mikä todistaa väitteen. □

Ylläolevat lauseet perustelevat sitä, että voimme tarkastella polynomeja polynomifunktioina. Jatkossa polynomeja tarkastellaan nimenomaan yli äärettömien kuntien.

Lause 2.17. *(Ks. [1, s. 4].) Olkoon k ääretön kunta ja olkoon $f, g \in k[x_1, \ldots, x_n]$. Tällöin $f = g$ renkaassa $k[x_1, \ldots, x_n]$ jos ja vain jos funktiot $f\colon k^n \to k$ ja $g\colon k^n \to k$ ovat samoja.*

Todistus. Oletetaan ensin, että polynomit $f, g \in k[x_1, \ldots, x_n]$ määräävät samat funktiot avaruudessa k^n. Oletuksen nojalla polynomi $f - g$ katoaa kaikissa avaruuden k^n pisteissä. Lauseen 2.16 nojalla $f - g$ on nollapolynomi, joten $f = g$ renkaassa $k[x_1, \ldots, x_n]$. Oletetaan sitten, että $f = g \in k[x_1, \ldots, x_n]$. Nyt polynomi f määrää funktion $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$. □

Määritelmä 2.18. (Ks. [1, s. 5].) Olkoon k kunta ja $f_1, \cdots, f_s$ polynomeja renkaassa $k[x_1, \cdots, x_n]$. Tällöin joukko

$$\mathbb{V}(f_1, \cdots, f_s) = \{(a_1, \cdots, a_n) \in k^n\colon f_i(a_1, \cdots, a_n) = 0, \text{ kaikilla } 1 \leq i \leq s\}$$

on polynomien $f_1, \cdots, f_s$ määrittelemä *affiini varisto* eli *varisto*.

Varisto on siis ratkaisujen joukko yhtälöille

$$f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0.$$

Jos $(a_1, \ldots, a_n) \in V$, niin sanotaan, että f *häviää* tai katoaa pisteessä $(a_1, \ldots, a_n)$.

Esimerkki 2.19. .

(i) Koko affiini avaruus on polynomin $p = 0$ varisto $\mathbb{V}(p) = k^n$.

(ii) Tyhjä joukko on vakiopolynomien $p = a, a \neq 0$ varisto $\mathbb{V}(a) = \emptyset$.

(iii) Yhden pisteen joukot ovat affiineja varistoja $\mathbb{V}(x_1 - a_1, \ldots, x_n - a_n) = \{a\}$. Eli jokainen k^n:n yksittäinen piste on varisto, sillä $x_i - a_i = 0$, kun $x_i = a_i$, kaikilla $0 \leq i \leq n$.

Esimerkki 2.20. Tarkastellaan, onko joukko S varisto, kun

1. $S_1 = \{(\cos t, \sin t) \mid t \in [0, 2\pi]\} \subset \mathbb{R}^2$,
2. $S_2 = \{(x, y) \mid f(x, y) = y - \sin(x) = 0\} \subset \mathbb{R}^2$.

Joukko S_1 on yksikköympyrä, eli varisto $\mathbb{V}(x^2 + y^2 + 1)$, sillä merkitsemällä $x = \cos(t)$ ja $y = \sin(t)$ yksikköympyrä voidaan parametrisoida sini- ja kosinimuodossa ja ympyrän pisteet toteuttavat yhtälön $x^2 + y^2 = 1$.

Joukon $S_2 = \{(x, y) \mid f(x, y) = y - \sin(x) = 0\}$ määritelmässä $f(x, y) = 0$ on transkendenttinen yhtälö, eikä sitä voi muuttaa polynomiyhtälöiksi, joten S_2 ei ole varisto.

Esimerkki 2.21. Tason $x = 0$ ja x-akselin yhdiste on varisto $\mathbb{V}(xy, xz) = \mathbb{V}(x) \cup \mathbb{V}(y, z)$, missä $xy = xz = 0$ määrittää (y, z)-tason ja polynomi $y = z = 0$ x-akselin.

Esimerkki 2.22. Kokonaislukujen joukko $\mathbb{Z} \subset \mathbb{R}$ ei ole varisto, sillä ainoa polynomifunktio, joka katoaa kaikilla kokonaisluvuilla on nollapolynomi ja sen varisto on koko $\mathbb{R}$.

Esimerkki 2.23. Polynomifunktioiden kuvaajat $y = f(x)$ muodostavat variston $V(y - f(x))$. Esimerkiksi paraabelin kuvaaja $y = x^2$ on varisto $\mathbb{V}(y - x^2)$.

Seurauslause 2.24. *(Ks. [1, s. 11].) Jos V ja W ovat varistoja, niin myös $V \cup W$ ja $V \cap W$ ovat varistoja.*

Todistus. Olkoon $V = \mathbb{V}(f_1, \ldots, f_s)$ ja $W = \mathbb{V}(g_1, \ldots, g_t)$. Tällöin väitetään, että

(i) $V \cap W = \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$

(ii) $V \cup W = \mathbb{V}(f_i g_j \colon 1 \leq i \leq s, 1 \leq j \leq t)$.

Ensimmäisen osan todistamiseksi oletetaan, että jos piste $(a_1, \ldots, a_n) \in \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$, niin tällöin f katoaa kaikissa varistojen V ja W pisteissä, joten se katoaa myös niiden yhteisissä pisteissä, eli $(a_1, \ldots, a_n) \in V \cap W$. Oletetaan sitten, että $(a_1, \ldots, a_n) \in V \cap W$. Tällöin $(a_1, \ldots, a_n) \in V$ ja $(a_1, \ldots, a_n) \in W$ joillakin indekseillä a_i, joten $(a_1, \ldots, a_n) \in \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$.

Toinen puoli todistuksesta: Jos $(a_1, \ldots, a_n) \in V$, niin kaikki polynomit f_i katoavat tässä pisteessä, eli ovat arvoltaan nollia tässä pisteessä, mistä seuraa, että kaikki termit $f_i g_j$ katoavat myös pisteessä $(a_1, \ldots, a_n)$. Siten molemmat $V \subset \mathbb{V}(f_i g_j)$ ja $W \subset \mathbb{V}(f_i g_j)$ pätevät yhtälailla, mikä osoittaa, että $V \cup W \subset \mathbb{V}(f_i g_j)$.

Todistetaan inkluusio toiseen suuntaan valitsemalla ensin $(a_1, \ldots, a_n) \in \mathbb{V}(f_i g_j)$. Jos tämä piste sisältyy varistoon V, väite pätee ja ellei sisälly, niin $f_{i_0}(a_1, \ldots, a_n) \neq 0$ jollain i_0. Koska $f_i g_j$ häviää pisteessä $(a_1, \ldots, a_n)$ kaikilla j:n arvoilla, täytyy kaikkien polynomien g_j hävitä tässä pisteessä, mistä seuraa, että $(a_1, \ldots, a_n) \in W$. Näin ollen $\mathbb{V}(f_i g_j) \subset V \cup W$. □

Tällaisesta yhdisteestä jo mainittiin yksi esimerkki $V(x) \cup V(y, z) = \mathbb{V}(xy, xz)$. Seurauslauseesta voidaan todistaa edelleen, että äärelliset leikkaukset ja yhdistelmät ovat myös varistoja.

Esimerkki 2.25. Varistojen V_i äärelliset leikkaukset ja yhdisteet ovat varistoja.

Todistus. (1) Olkoon $V_1, V_2, \ldots, V_s$ varistoja. Yhdiste $V_1 \cup V_2$ on lauseen 2.24 nojalla varisto.

(2) Tehdään induktio-oletus, että yhdiste $\bigcup_{i=s}^{s} V_i$ on varisto.

(3) Nyt yhdiste

$$\bigcup_{i=s}^{s+1} V_i = \bigcup_{i=s}^{s} V_i \cup V_{s+1}.$$

Induktio-oletuksen ja lauseen 2.24 nojalla tämäkin on kahden variston yhdiste, eli varisto, joten väite pätee.
Sama päättely voidaan tehdä samalla tavalla äärellisille leikkauksille, jolloin

$$\bigcap_{i=s}^{s+1} V_i = \bigcap_{i-s}^{s} V_i \cap V_{s+1}$$

on myös varisto. □

Esimerkki 2.26. Olkoon V ja W varistoja. Varistojen erotus, $V - W$, ei välttämättä ole varisto.

Todistus. Olkoon $V = \mathbb{R}$ ja $W = 0$. Tällöin $\mathbb{V}(V - W) = \{a \in \mathbb{R} \colon a \neq 0\}$. Tämä on ääretön joukko ja kaikilla muilla polynomeilla on äärellinen määrä ratkaisuja, paitsi nollapolynomilla, joten joukko ei voi olla varisto. □

Esimerkki 2.27. Varistojen karteesinen tulo on varisto.

Todistus. Olkoon $V \subset k^n = \mathbb{V}(f_1, \ldots, f_s)$ ja $W \subset k^m = \mathbb{V}(g_1, \ldots, g_t)$, missä $g_i, g_i \in k[x_1, \ldots, x_n], 1 \leq i, j \leq s, t$. Olkoon nyt $y_1, \ldots, y_n \in k[x_1, \ldots, x_m]$ uusia muuttujia ja $\hat{g} = g_j[y_1, \ldots, y_m]$. Nyt on osoitettava, että

$$V \times W = \mathbb{V}(f_1, \ldots, f_s, \hat{g}_1, \ldots, \hat{g}_t) \subset k^{n+m}.$$

Olkoon $(a, b) \in V \times W$, jolloin $f(a, b) = f_i(a) = 0$ ja $\hat{g}_j(a, b) = \hat{g}_j(b) = 0$, sillä $a \in V$ ja $b \in W$. Näin ollen siis $(a, b) \in \mathbb{V}(f_1, \ldots, f_s, \hat{g}_1, \ldots, \hat{g}_t)$.
Oletetaan sitten, että $(a, b) \in \mathbb{V}(f_1, \ldots, f_s, \hat{g}_1, \ldots, \hat{g}_t)$. Tällöin $f_i(a) = 0$, kun $1 \leq i \leq s$ ja $g_j(b) = 0$, kun $1 \leq j \leq t$, joten $a \in V$ ja $b \in W$, mikä todistaa väitteen. □

2.4 Varistojen parametrisoinnista

Varisto $\mathbb{V}(f_1, \ldots, f_n)$ on polynomien $f_1 = \cdots = f_n = 0$ ratkaisujen joukko. Esimerkiksi yhtälöryhmä

$$\begin{aligned} x + y + z &= 1, \\ x + 2y - z &= 3, \end{aligned} \tag{2.1}$$

on geometrisesti avaruuden $\mathbb{R}^3$ suora, joka on tasojen $x + y + z = 1$ ja $x + 2y - z = 3$ leikkaus. Ratkaisujen joukon määrittämiseksi voidaan alkuperäisistä yhtälöistä muokata 2.1 matriisien rivioperaatioilla yhtälöt

$$\begin{aligned} x + 3z &= -1, \\ y - 2z &= 2. \end{aligned} \tag{2.2}$$

Kun nyt merkitään $z = t$, niin yhtälöiden 2.1 ratkaisut saadaan yhtälöistä

$$\begin{aligned} x &= -1 - 3t, \\ y &= 2 + 2t, \\ z &= t, \end{aligned} \tag{2.3}$$

missä $t \in \mathbb{R}$. Muuttuja t on nyt parametri, jonka avulla yhtälöt 2.1 on parametrisoitu. Yksikköympyrä $x^2 + y^2 = 1$ voidaan parametrisoida trigonometrisilla funktioilla

$$\begin{aligned} x &= \cos(t), \\ y &= \sin(t). \end{aligned} \tag{2.4}$$

Esimerkki 2.28. (Ks. [1, s. 18].) Yksikköympyrä, eli varisto $\mathbb{V}(x^2 + y^2 - 1)$, voidaan määritellä myös geometriaa apuna käyttäen. Yksikköympyrän kehän pisteestä $(-1, 0)$ voidaan piirtää suora jokaiseen kehän pisteeseen x, y. Kehän pisteet voidaan määritellä pisteinä, missä suora leikkaa pisteen $x^2 + y^2 - 1$. Jokainen näistä suorista leikkaa y-akselin pisteessä $(0, t)$. Näillä suorilla on äärellinen kulmakerroin, joka voidaan määrittää kahdella tavalla; pisteen $(-1, 0)$ ja kehän pisteen (x, y) suhteen, tai pisteiden $(-1, 0)$ ja $(0, t)$ suhteen. Parametrisaatio saadaan, kun t käy läpi kaikki y- akselin arvot. Muodostetaan yhtälöt kirjoittamalla edellä kuvatun suoran kulmakerroin kahdella tavalla. Saadaan yhtälö

$$\frac{t - 0}{0 - (-1)} = \frac{y - 0}{x - (-1)},$$

mikä sieventyy muotoon

$$t = \frac{y}{x + 1}.$$

Samoin voidaan tehdä, kun $y = t(x + 1)$. Sijoitetaan tämä yksikköympyrän yhtälöön ja saadaan $x^2 + t^2(x + 1)^2 = 1$. Kun yhdistetään termit muuttujan x^2 suhteen saadaan toisen asteen yhtälö

$$(1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0.$$

Tämän yhtälön avulla voidaan selvittää, missä suora leikkaa ympyrän. Niillä on kaksi leikkauspistettä, joista toinen on -1, joten $x+1$ on yhtälön toinen tekijä. Toinen tekijä on koordinaatti $x = \frac{1-t^2}{1+t^2}$. Nyt yhtälö voidaan täydentää muotoon

$$(x + 1)((1 + t^2)x - (1 - t^2)) = 0.$$

Sijoittamalla koordinaatti $x = \dfrac{1 - t^2}{1 + t^2}$ yhtälöön $y = t(x+1)$ saadaan $y = \dfrac{2t}{1 + t^2}$. Nämä koordinaatit ovat siis yksikköympyrän, poislukien pisteen $(-1, 0)$, parametrisaatio.

3 Hilbertin kantalause ja Gröbnerin kanta

Määritelmä 3.1 (Monomijärjestys)**.** (Ks. [4, s.11].) Renkaassa $k[x_1, \ldots, x_n]$ voidaan määritellä ***monomijärjestys*** $>$, eli monomit ovat hyvin järjestetty, kun seuraavat ehdot täyttyvät.
1. Jos $x^\alpha > x^\beta$ niin silloin kaikilla α, β, γ pätee $x^{\alpha\gamma} > x^{\beta\gamma}$, missä $\gamma \in \mathbb{Z}^n_{\geq 0}$
2. Satunnaisessa monomijoukossa

$$\{x^\alpha\}_{\alpha \in \mathbb{Z}^n_{\geq 0}}$$

on pienin alkio monomijärjestyksen suhteen.

Tässä työssä käytetään aakkosellista monomijärjestystä, joka määritellään seuraavasti.

Määritelmä 3.2. (Ks. [1, s. 56].) Olkoon $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Merkitään $\alpha > \beta$, jos vektorierotuksen $\alpha - \beta \in \mathbb{Z}^n$ ensimmäinen nollasta poikkeava tulos on positiivinen. Merkitään $x^\alpha > x^\beta$, jos $\alpha > \beta$.

Muuttujat $x_1, \ldots, x_n$ järjestetään yleensä $x_1 > x_2 > \ldots > x_n$. Kun muuttujia on vähemmän merkitään yleensä $x > y > z$. Tällöin suuruusjärjestys on aakkosellinen ja samoin määritelty kuin edellä.

Lause 3.3. *(Ks. [1, s. 41].) Jos k on kunta, niin jokainen ideaali renkaassa $k[x]$ voidaan kirjoittaa muotoon $\langle f \rangle$ jollain $f \in k[x]$.*

Todistus. (Vrt. [1, s. 41].) Olkoon $I \subset k[x]$ ideaali. Jos $I = \{0\}$, niin väite pätee, sillä $I = \langle 0 \rangle$. Oletetaan sitten, että ideaaliin kuuluu polynomi $f \neq 0$, jonka aste on pienin mahdollinen ideaalissa I. Väite voidaan nyt kirjoittaa muotoon $I = \langle f \rangle$. Ideaalin määritelmän nojalla $\langle f \rangle \subset I$.
Todistetaan sitten, että $I \subset \langle f \rangle$. Olkoon $g \in I$. Myöhemmin, lauseessa 3.13 osoitetaan, että polynomit voidaan kirjoittaa $g = qf + r$, missä joko $r = 0$ tai $deg(r) < deg(f)$. Ideaalin määritelmän nojalla $qf \in I$ ja siis $r = g - qf \in I$. Jos r ei ole nolla, niin $deg(r) < deg(f)$, mikä on ristiriidassa f:n oletusten kanssa. Jos $r = 0$, niin $g = qf \in \langle f \rangle$, mikä todistaa, että $I = \langle f \rangle$. □

Yhden alkion generoimia ideaaleja sanotaan *pääideaaleiksi* tai alkuideaaleiksi. Edellisen lauseen nojalla $k[x]$ on pääideaalialue (engl. *principal ideal domain*).

Määritelmä 3.4. (Ks. [1, s. 41].) Polynomien $f, g \in k[x]$ suurin yhteinen tekijä, lyhennetään GCD (engl. *greatest common divisor*), h on polynomi, jolle pätee seuraavat väitteet.

(i) Polynomi h on polynomien $(f_1, \ldots, f_s) \in k[x]$ tekijä,

(ii) ja jos polynomi p on polynomien $(f_1, \ldots, f_s) \in k[x]$ tekijä, niin p on h:n tekijä.

Määritelmä 3.5. Rengas on *Noetherin rengas*, eli lyhyemmin vain *Noether*, jos sen kaikki jonot toisiinsa sisältyviä ideaaleja

$$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots$$

stabiloituvat, eli jollain $n_0 \in \mathbb{Z}_{\geq 0}$ pätee $I_{n_0+k} = I_{n_0}$ kaikilla $k \geq 0$.

Lause 3.6. *Toinen tapa määritellä Noetherin rengas on todeta, että sen kaikki ideaalit ovat äärellisesti generoituja (ks. [8, s.19].)*

Todistus. (Ks. [4, s. 20].) Osoitetaan, että määritelmät ovat yhtenevät. Oletetaan, että renkaan jokainen ideaali on äärellisesti generoitu ja olkoon $I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_i \subset \cdots$ jono toisiinsa sisältyviä ideaaleja ja määritellään

$$I_\infty = \bigcup_i^\infty I_i.$$

Osoitetaan ensin, että I_∞ on ideaali.

1. koska $0 \in I_i \; \forall \; i \in \mathbb{Z}_{\geq 0}$ niin $0 \in I_\infty$

2. Olkoon sitten $f, g \in I_\infty$ eli $f \in I_i$ ja $g \in I_j$ joillekin $i, j \in \mathbb{Z}_{\geq 0}$. Oletetaan sitten, että $i \leq j$ jolloin $I_i \subset I_j \subset I_\infty$, mistä seuraa $f+g \in I_j \subset I_\infty$ eli $f+g \in I_\infty$.

3. Jos sitten $h \in k[x_1, \ldots, x_n]$ ja $g \in I_\infty$ niin $g \in I_i$ jollakin $i \in \mathbb{Z}_{\geq 0}$ jolloin $hg \in I_i \subset I_\infty$ eli $hg \in I_\infty$.

Kohtien (1) - (3) perusteella I_∞ on siis ideaali.

Olkoon $g_1, \ldots, g_r \in I_\infty$ generaattoreita, joista jokainen $g_i \in I_{n_i}$ vastaa jotain n_i. Jos $N = \max(n_1, \ldots, n_r)$, niin $I_\infty = I_N$.

Oletetaan sitten, että jokainen nouseva ideaaliketju stabiloituu. Olkoon I ideaali ja merkitään

$$I = \langle f_\alpha \rangle, \alpha \in A.$$

Tehdään vastaoletus, että I ei ole generoitu äärellisellä määrällä α. Tällöin muodostuu ääretön jono $f_{\alpha(1)}, f_{\alpha(2)}, \cdots$, jolle

$$I_r = \langle f_{\alpha(1)}, \ldots, f_{\alpha(r)} \rangle \subsetneq I_{r+1} = \langle f_{\alpha(1)}, \ldots, f_{\alpha(r+1)} \rangle$$

jokaisella r, mikä on ristiriita.

□

Määritelmä 3.7. (Ks.[1, s. 75].) Olkoon $I \subset k[x_1, \ldots, x_n]$ ideaali, joka ei ole nollaideaali.

(i) Määritellään $LT(I)$ johtavien termien joukoksi ideaalissa I. Eli

$$LT(I) = \{cx^\alpha : \text{ löytyy sellainen} f \in I, \text{ jolla } LT(f) = cx^\alpha\}.$$

(ii) Merkitään $\langle LT(I)\rangle$:llä ideaalin I johtavien termien generoimaa ideaalia.

Lause 3.8. *(Ks. [1, s. 75].) Olkoon $I \subset k[x_1, \ldots, x_n]$ ideaali.*

(i) $\langle LT(I)\rangle$ on monomiaalinen ideaali.

(ii) Voidaan löytää polynomit $g_1, \ldots, g_t \in I$, joilla $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t).\rangle$

Todistus. Ohitetaan, ei ole työn pääasiallista aluetta, Ks. [1, s. 75]. □

Lause 3.9 (Hilbertin kantalause)**.** *(Ks. [1, s. 76].) Jokainen ideaali $I \subset k[x_1, \ldots, x_n]$ on äärellisesti generoitu, eli $I = \langle g_1, \ldots, g_t\rangle$, joillain $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$.*

Todistus. (Ks. [1, s. 76].) Jos ideaali on nollaideaali, niin generoiva joukko on $\{0\}$, joka on äärellinen. Lauseen 3.8 mukaan voidaan löytää polynomit $g_1, \ldots, g_t \in I$, joilla $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Väitetään, että $I = \langle g_1, \ldots, g_t\rangle$.

oletusten nojalla $g_i \in I$, joten $\langle g_1, \ldots, g_t\rangle \subset I$.
Olkoon $f \in I$ mielivaltainen polynomi. Jaollisuuslauseen, eli lause 3.13, nojalla voidaan jakaa f polynomeilla $g_1, \ldots, g_t$, jolloin saadaan

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

missä r ei ole jaollinen millään $LT(g_1), \ldots, LT(g_t)$. Väitetään nyt, että $r = 0$. Huomataan, että edellisestä yhtälöstä saadaan

$$r = f - a_1 g_1 - \ldots - a_t g_t \in I.$$

Jos $r \neq 0$, niin lauseen 3.11 nojalla sen johtava termi $LT(r)$ on jaollinen jollain $LT(g_i)$, mikä taas on ristiriita jakojäännöksen määritelmän nojalla, joten $r = 0$. Nyt siis

$$f = a_1 g_1 + \ldots + a_t g_t + 0 \in \langle g_1, \ldots g_t\rangle,$$

jolloin $I \subset \langle g_1, \ldots g_t\rangle$, mikä todistaa väitteen. □

3.1 Gröbnerin kanta

Määritelmä 3.10. (Ks. [1, s. 70].) Ideaali I on *monomiaalinen-ideaali*, kun se on monomien generoima. Tällöin on joukko $A \subset \mathbb{Z}^n_{\geqslant 0}$, jolla I sisältää kaikki polynomit, jotka ovat äärellisiä summia, muotoa $\sum_{\alpha \in A} h_\alpha x^\alpha$, missä $h_\alpha \in k[x_1, \ldots, x_n]$. Merkitään $I = \langle x^\alpha : \alpha \in A\rangle$.

Lause 3.11. *(Ks. [1, s. 70].) Olkoon $I = \langle x^\alpha : \alpha \in A\rangle$ monomiaalinen ideaali. Monomi x^β sisältyy ideaaliin I jos ja vain jos x^β on jaollinen termillä x^α, jollain $\alpha \in A$.*

Todistus. Jos x^β on moninkerta monomista x^α, jollain α, niin $x^\beta \in I$ ideaalin määritelmän nojalla. Toisaalta, jos $x^\beta \in I$, niin $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, missä $h_i \in k[x_1, \ldots, x_n]$ ja $\alpha(i) \in A$. Jos jokainen h_i jaetaan monomien lineaarikombinaatioiksi, nähdään että oikean puolen jokainen termi on jaollinen jollain termillä $x^{\alpha(i)}$. Näin ollen vasemman puolen termillä x^β täytyy olla tämä sama ominaisuus. □

Määritelmä 3.12. (Ks. [1, s. 77]) Määritellään jokin monomijärjestys. Nyt ideaalin I äärellinen osajoukko $G = \{g_1, \ldots, g_t\}$ on ideaalin Gröbnerin kanta, jos

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

Gröbnerin kannalla on käyttökelpoisia, toivottavia ominaisuuksia, mitä kaikilla kannoilla ei ole. Voidaan osoittaa, että kaikilla ideaaleilla, jotka eivät ole nollaideaaleja on Gröbnerin kanta. Gröbnerin kanta ei kuitenkaan ole yksikäsitteinen. Seuraavan lauseen mukaan jakojäännös on yksikäsitteisesti määritelty, kun jaetaan Gröbnerin kannalla. Muilla kannoilla jakamalla näin ei välttämättä ole.

Lause 3.13 (Jaollisuuslause polynomirenkaassa)**.** *(Ks. [1, s. 64].) Valitaan jokin monomijärjestys $>$ ja olkoon $F = (f_1, \ldots, f_s)$ järjestetty joukko polynomirenkaasta $k[x_1, \ldots, x_n]$. Tällöin jokainen $f \in k[x_1, \ldots, x_n]$ voidaan kirjoittaa muotoon*

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

missä $a_i, r \in k[x_1, \ldots, x_n]$ ja joko $r = 0$ tai r on sellaisten monomien lineaarikombinaatio kunnassa k, joista mikään ei ole jaollinen millään termillä $LT(f_1), \ldots, LT(f_s)$.

Todistus. Ohitetaan, ei ole työn pääasiallista sisältöä. (Ks. [1, s. 64].) □

Lause 3.14. *(Ks. [1, s. 82].) Olkoon $G = \{g_1, \ldots, g_t\}$ Gröbnerin kanta ideaalille $I \subset k[x_1, \ldots, x_n]$ ja olkoon $f \in k[x_1, \ldots, x_n]$. Tällöin on olemassa yksikäsitteinen jakojäännös $r \in k[x_1, \ldots, x_n]$, jolla on seuraavat kaksi ominaisuutta.*

(i) Mikään r:n termi ei ole jaollinen millään termeillä $LT(g_1), \ldots, LT(g_t)$.

(ii) On sellainen funktio $g \in I$, jolla $f = g + r$.

Erityisesti r on polynomien f jakojäännös, kun jaetaan joukolla G olipa G:n alkiot järjestetty miten hyvänsä.

Todistus. Lauseen 3.13 mukaan $f = a_1 g_1 + \ldots + a_t g_t + r$, missä r toteuttaa ehdon (i). Myös kohta (ii) todistetaan sillä, kun valitaan, että $g = a_1 g_1 + \ldots + a_t g_t$, jolloin on todistettu, että r on olemassa. Todistetaan yksikäsitteisyys olettamalla, että $f = g + r = g' + r'$ toteuttaa kohdat (i) ja (ii). Tällöin $r - r' = g - g' \in I$, joten jos $r \neq r'$, niin tällöin $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Monomi-ideaaleja koskevan lauseen nojalla (Ks. [1, s. 70]) monomi kuuluu ideaaliin, jos ja vain jos se on jaollinen jollain ideaalin termillä, joten $LT(r - r')$ on oltava jaollinen jollain $LT(g_i)$. Tämä on ristiriita, sillä kumpikaan jakojäännöksistä r, r' ei ole jaollinen termeillä $LT(g_i)$. Siispä jakojäännöksen on oltava yksikäsitteinen $r = r'$. □

Seuraavaa lausetta voidaan pitää myös Gröbnerin kannan määritelmänä.

Lause 3.15. *(Ks.[1, s. 82].) Olkoon $G = \langle g_1, \ldots, g_t\rangle$ Gröbnerin kanta ideaalille $I \subset k[x_1, \ldots, x_n]$ ja olkoon $f \in k[x_1, \ldots, x_n]$. Tällöin $f \in I$ jos ja vain jos f:n jakojäännös G:llä jaettuna on nolla.*

Todistus. Seuraa lauseesta 3.14 ja erityisesti sen todistuksen loppuosasta. □

Määritelmä 3.16. (Ks. [1, s. 83].) Merkitään polynomin f jakojäännöstä $\bar{f}^F$, kun se jaetaan järjestetyllä joukolla $F = (f_1, \ldots, f_s)$. Jos F on Gröbnerin kanta polynomeille $\langle f_1, \ldots, f_s \rangle$, niin lauseen 3.14 nojalla joukon F järjestyksellä ei ole väliä.

Gröbnerin kantoja ideaaleille voidaan määrittää laskemalla ideaalin generaattoreille S-polynomit.

Määritelmä 3.17. (Ks. [1, s. 59].) Olkoon $f = \sum_\alpha a_\alpha x^\alpha$ polynomi, jolle $f \neq 0$ ja $f \in k[x_1, \ldots, x_n]$ ja olkoon $>$ monomijärjestys. Polynomin f

(i) multideg$(f) = \max(\alpha \in \mathbb{Z}^n_{\geq} | a_\alpha \neq 0)$,

(ii) johtava kerroin $LC(f) = a_{multideg(f)} \in k$ ja

(iii) johtava monomi $LM(f) = x^{multideg(f)}$.

Määritelmä 3.18. (Ks. [1, s. 83].) Olkoon $f, g \in k[x_1, \ldots, x_n]$ polynomeja ja $f, g \neq 0$.

(i) Olkoon polynomien $multideg(f) = \alpha$ ja $multideg(g) = \beta$. Olkoon tällöin $\gamma = \gamma_1, \ldots, \gamma_n$, missä $\gamma_i = \max(\alpha, \beta)$ kaikilla i ja $LM(f)$:n ja $LM(g)$:n pienin yhteinen jaettava $LCM(LM(f), LM(g)) = x^\gamma$.

(ii) Polynomien f ja g *S-polynomi* on

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

Lause 3.19 (Buchbergerin kriteerilause)**.** *(Ks. [1, s. 85].) Olkoon I polynomi-ideaali. Tällöin ideaalin I kanta $G = \{g_1, \ldots, g_t\}$ on Gröbnerin kanta ideaalille I jos ja vain jos kaikilla indeksipareilla $i \neq j$ pätee, että $S(g_i, g_j)$ jaettuna G:llä, jonkin monomijärjestyksen suhteen, jakojäännös on nolla.*

Todistus. Todistus ohitetaan, ei työn pääasiallista sisältöä. (Ks.[1, s. 85].) □

Seurauslause 3.20. *(Ks. [1, s. 91].) Olkoon G Gröbnerin kanta polynomi-ideaalille I. Olkoon $p \in G$ sellainen polynomi, jolla $LT(p) \in \langle LT(G - \{p\}) \rangle$. Tällöin myös $G - \{p\}$ on Gröbnerin kanta.*

Todistus. Gröbnerin kannan määritelmän nojalla $\langle LT(G) \rangle = \langle LT(I) \rangle$. Jos $LT(p) \in \langle LT(G - \{p\}) \rangle$, niin tällöin pätee $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$. Määritelmästä seuraa, että tällöin $G - \{p\}$ on Gröbnerin kanta. □

Useimmiten Buchbergin algoritmin avulla määritellyt Gröbnerin kannat ovat laajempia, kuin on tarpeen, eli sisältävät ylimääräisiä polynomeja. Ylimääräisiä generaattoreita voidaan vähentää edellisen seurauslauseen tiedon avulla. Saadaan minimaalinen Gröbnerin kanta.

Määritelmä 3.21. (Ks. [1, s. 91].) *Minimaalinen Gröbnerin kanta* polynomi-ideaalille I on Gröbnerin kanta $G \in I$, jolle pätee:

(i) $LC(P) = 1$ kaikilla $p \in G$.

(ii) Kaikilla $p \in G, LT(p) \notin \langle (G - \{p\}) \rangle$.

Määritelmä 3.22. (Ks. [1, s. 92].) *Redusoitu Gröbnerin kanta* polynomi-ideaalille I on sellainen Gröbnerin kanta $G \in I$, jolla

(i) $LC(p) = 1$, kaikilla $p \in G$.

(ii) Kaikilla $p \in G$ pätee, ettei mikään p:n monomi sisälly ideaaliin $\langle LT(G - \{p\}) \rangle$.

Redusoidulla Gröbnerin kannalla on seuraava, tärkeä ominaisuus.

Lause 3.23. *(Ks. [1, s. 92].)*
Olkoon $I \neq 0$ polynomi-ideaali. Tällöin, annetulla monomijärjestyksellä, ideaalilla I on yksikäsitteinen redusoitu Gröbnerin kanta.

Todistus. Ohitetaan, ei ole työn pääasiallista sisältöä. Ks. [1, s. 92]. □

4 Variston ideaali

Määritelmä 4.1. (Ks. [1, s. 32].) Olkoon $V \subset k^n$ affiini varisto. Merkitään

$$\mathbb{I}(V) = \{f \in k[x_1, \ldots, x_n] \colon f(a_1, \ldots, a_n) = 0 \text{ kaikilla } (a_1, \ldots, a_n) \in V\}.$$

Huomataan, että $\mathbb{I}(V)$ on ideaali.

Seurauslause 4.2. *(Ks. [1, s. 32].) Jos $V \subset k^n$ on affiini varisto, niin $\mathbb{I}(V) \subset k[x_1, \ldots, x_n]$ on ideaali. Tällöin $\mathbb{I}(V)$ on variston V ideaali.*

Todistus. Ensinnäkin $0 \in \mathbb{I}(V)$ pätee kaikkialla joukossa k^n ja niin myös joukossa V. Oletetaan sitten, että $f, g \in \mathbb{I}(V)$ ja $h \in k[x_1, \ldots, x_n]$. Olkoon $(a_1, \ldots, a_n)$ mikä tahansa piste varistossa V. Tällöin

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$

$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0,$$

joten määritelmän 2.7 nojalla $\mathbb{I}(V)$ on ideaali. □

Esimerkki 4.3. (Ks. [1, s. 11].) Tarkastellaan varistoa $\{(0, 0)\}$, eli joukon $\mathbb{R}^2$ origoa esimerkkinä variston ideaalista. Origon ideaali $I(\{(0, 0)\})$ koostuu polynomeista, jotka katoavat origossa. Väitetään nyt siis, että

$$\mathbb{I}(\{(0, 0)\}) = \langle x, y \rangle.$$

Kaikki $A(x, y)x + B(x, y)y$ muotoiset polynomit ovat origossa nollia, joten $\langle x, y \rangle \subset \mathbb{I}(\{(0, 0)\})$.

Todistetaan sitten, että $\mathbb{I}(\{(0, 0)\}) \subset \langle x, y \rangle$. Oletetaan, että $f = \sum_{i,j} a_{ij} x^i y^j$ on nolla origossa. Tällöin $a_{00} = f(0, 0) = 0$. Tästä seuraa, että

$$f = a_{00} + \sum_{i,j \neq 0,0} a_{ij} x^i y^j = 0 + \left(\sum_{i,j>0} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{i,j>0} a_{0j} x^i y^{j-1} \right) y \in \langle x, y \rangle,$$

mikä todistaa väitteen.

Esimerkki 4.4. Olkoon varisto nyt $V = k^n$, eli koko affiini avaruus. Tällöin sen ideaali $\mathbb{I}(k^n)$ sisältää ne polynomit, jotka katoavat kaikkialla. Kun k on ääretön, niin lauseen 2.16 nojalla $\mathbb{I}(k^n) = \{0\}$.

Esimerkki 4.5. (Ks. [1, s. 12]) Olkoon $V \subset \mathbb{R}^3$ kaari, joka on parametrisoitu muotoon $c(t) = (t, t^2, t^4)$. Jos tällöin $x = t$, niin $y - x^2 = z - x^4 = 0$, joten $V = \mathbb{V}(y - x^2, z - x^4)$. Sen ideaali on $\mathbb{I}(V) = \langle y - x^2, z - x^4 \rangle$. Todistetaan tämä.

Oletetaan ensin, että $f = x^\alpha y^\beta z^\gamma$, eli monomimuotoinen. Tällöin binomilauseen nojalla

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + (y - x^2))^\beta (x^3 + (z - x^3))^\gamma \\ &= x^\alpha (x^{2\beta} + \text{ termit, joissa tekijöinä } y - x^2)(x^{3\gamma} + \text{ termit, joissa } z - x^3). \end{aligned}$$

Kertomalla auki yhtälö voidaan saattaa muotoon

$$x^\alpha y^\beta z^\gamma = h_1(y - x^2) + h_2(z - x^3) + x^{\alpha+2\beta+3\gamma}$$

joillain polynomeilla $h_1, h_2 \in \mathbb{R}[x, y, z]$. Nyt polynomi f voidaan kirjoittaa muotoon

$$f = h_1(y - x^2) + h_2(z - x^4) + r,$$

missä $h_1, h_2 \in \mathbb{R}[x, y, z]$ ja r riippuvat vain muuttujasta x. Koska mikä tahansa polynomi voidaan kirjoittaa monomimuodossa väite pätee kaikille $f \in \mathbb{R}[x, y, z]$.

Nyt koska polynomit $y - x^2, z - x^4$ muodostavat variston $V(y - x^2, z - x^4)$, niin $y-x^2, z-x^4 \in \mathbb{I}(V)$ ja ideaalin määritelmän nojalla myös $h_1(y-x^2)+h_2(z-x^4) \in \mathbb{I}(V)$. Näin ollen $\langle y-x^2, z-x^4\rangle \subset \mathbb{I}(V)$. Väitteen todistamiseksi toiseen suuntaan oletetaan, että $f \in \mathbb{I}(V)$ ja

$$f = h_1(y - x^2) + h_2(z - x^4) + r.$$

Polynomi oli parametrisoitu muotoon $c(t) = (t, t^2, t^4)$. Koska f on nolla joukossa V, saadaan

$$0 = f(t, t^2, t^4) = 0 + 0 + r(t).$$

Tällöin lauseen 2.16 nojalla $r \in \mathbb{R}[x]$ täytyy olla nollapolynomi. Näin on osoitettu, että $\mathbb{I}(V) = \langle y - x^2, z - x^4\rangle$.

Lause 4.6. *(Ks. [1, s. 34].) Jos polynomit $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, niin $\langle f_1, \ldots, f_s\rangle \subset \mathbb{I}(V(f_1, \ldots, f_s))$.*

Todistus. Olkoon $f \in \langle f_1, \ldots, f_s\rangle$, eli se on muotoa $f = \sum_{i=1}^s h_i f_i$, joillain $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$. Koska polynomit $f_1, \ldots, f_s$ katoavat joukossa $V(f_1, \ldots, f_s)$, niin myös $f = \sum_{i=1}^s h_i f_i$. Koska f katoaa joukossa $V(f_1, \ldots, f_s)$ tarkoittaa se, että $f \in \mathbb{I}(V(f_1, \ldots, f_s))$. □

Esimerkki 4.7. (Ks. [1, s. 35].) Edellistä lausetta ei voida kirjoittaa muodossa $\langle f_1, \ldots, f_s\rangle = \mathbb{I}(V(f_1, \ldots, f_s))$, sillä

$$\langle x^2, y^2\rangle \subset \mathbb{I}(V(x^2, y^2))$$

ei päde toiseen suuntaan. Määritetään ensin $\mathbb{I}(V(x^2, y^2))$. Yhtälöstä $x^2 = y^2 = 0$ seuraa, että $V(x^2, y^2) = \{(0, 0)\}$. Esimerkissä 4.3 on kuitenkin todettu, että joukon $\{(0, 0)\}$ ideaali on $\langle x, y\rangle$, joten $\mathbb{I}(V(x^2, y^2)) = \langle x, y\rangle$. Tämä joukko on suurempi, kuin $\langle x^2, y^2\rangle$. Joukon $\langle x^2, y^2\rangle$ polynomien aste on vähintään kaksi ja sen polynomit ovat muotoa $h_1x^2 + h_2y^2$, joten esimerkiksi $x \notin \langle x^2, y^2\rangle$, sillä $x \neq h_1x^2 + h_2y^2$.

Lause 4.8. *(Ks. [1, s. 35].) Olkoon V ja W affiineja varistoja renkaassa k^n. Tällöin:*

(i) $V \subset W$ jos ja vain jos $\mathbb{I}(W) \subset \mathbb{I}(V)$.

(ii) $V = W$ jos ja vain jos $\mathbb{I}(V) = \mathbb{I}(W)$.

Todistus. (Vrt. [1, s. 35, 37].) Oletetaan ensin, että $V \subset W$. Tällöin mikä tahansa polynomi, joka katoaa varistossa W katoaa myös varistossa V. Tästä seuraa että $\mathbb{I}(W) \subset \mathbb{I}(V)$.
Oletetaan sitten, että $\mathbb{I}(W) \subset \mathbb{I}(V)$. Tiedetään, että W on joidenkin polynomien $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ määrittelemä, eli $g_1, \ldots, g_t \in \mathbb{I}(W) \subset \mathbb{I}(V)$ eli kaikki polynomit g_i, $1 \leq i \leq t$, katoavat varistossa V. Koska varistossa W ovat polynomien g_i kaikki yhteiset nollakohdat, niin $V \subset W$.

Todistetaan kohta (ii) samoin, kuin kohta (i), mutta vaihdetaan varistojen V ja W paikkaa. Osoitetaan että joukot ovat molemmat toistensa osajoukkoja, jolloin niiden täytyy olla yhtä suuret. Oletetaan ensin, että $W \subset V$, jolloin jos $f \in V$, niin f katoaa myös joukossa W, eli $\mathbb{I}(V) \subset \mathbb{I}(W)$. Oletetaan sitten, että $\mathbb{I}(V) \subset \mathbb{I}(W)$. Nyt V on polynomien $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ määrittelemä, eli $g_1, \ldots, g_t \in \mathbb{I}(W) \subset \mathbb{I}(V)$. Nyt kaikki polynomit g_i katoavat varistossa V. Varistojen V ja W yhteiset nollakohdat sisältyvät siten varistoon W eli $V \subset W$.

□

4.1 Ideaalin varisto

Määritelmä 4.9. (Ks. [1, s. 79].) Olkoon I ideaali. Merkitään $\mathbb{V}(I)$ joukkoa

$$\mathbb{V}(I) = \{(a_1, \ldots, a_n) \in k^n \colon f(a_1, \ldots, a_n) = 0, \ \forall\ f \in I\}.$$

Vaikka nollasta poikkeava ideaali sisältää aina äärettömän monta polynomia joukko $\mathbb{V}(I)$ voidaan määrittää äärellisellä joukolla polynomeja.

Lause 4.10. *(Ks. [1, s. 79])* $\mathbb{V}(I)$ *on affiini varisto. Erityisesti, jos* $I = \langle f_1, \ldots f_s \rangle$, *niin* $\mathbb{V}(I) = V(f_1, \ldots, f_s)$.

Todistus. Osoitetaan ensin, että $\mathbb{V}(I) \subset V(f_1, \ldots, f_s)$. Nyt Hilbertin kantalauseen, eli lauseen 3.9, nojalla jollain äärellisesti generoidulla joukolla $I = \langle f_1, \ldots, f_s \rangle$. Väitetään siis, että $\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s)$. Huomataan ensin, että $f_i \in \mathbb{I}$, jos $f(a_1, \ldots, a_n) = 0$ kaikilla $f \in \mathbb{I}$, niin $f_i(a_1, \ldots, a_n) = 0$, joten $\mathbb{V}(I) \subset \mathbb{V}(f_1, \ldots, f_s)$.

Toisaalta olkoon $(a_1, \ldots, a_n) \in \mathbb{V}(f_1, \ldots, f_s)$ ja olkoon $f \in I$. Koska $I = \langle f_1, \ldots, f_s \rangle$ voidaan kirjoittaa

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

jollain $h_i \in k[x_1, \ldots, x_n]$. Jolloin pätee, että

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0.$$

Joten myös $\mathbb{V}(f_1, \ldots, f_s) \subset \mathbb{V}(I)$, eli väite pätee. □

Tärkein seuraus tälle lauseelle on, että varistot voidaan määritellä ideaalien avulla.

Lause 4.11. *(Ks.[1, s. 32].) Jos $f_1, \ldots, f_s$ ja $g_1, \ldots, g_t$ ovat saman ideaalin kantoja, niin että $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, niin tällöin myös $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t.)$*

Todistus. (Vrt. [1, s.36].) Seuraa suoraan lauseen 4.10 jälkimmäisestä osasta. Jos $I = \langle f_1 \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, niin $\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t)$. □

Esimerkki 4.12. Tarkastellaan esimerkiksi varistoa $V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$. Esimerkissä 2.12 on osoitettu, että $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$. Edellisen lauseen nojalla siis

$$\mathbb{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbb{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}.$$

Näin siis myös $\mathbb{V}(x - xy, y - xy, x^2, y^2) = \mathbb{V}(\langle x + y, x - y \rangle) = \mathbb{V}(x, y) = \{(0, 0)\}$.

Esimerkki 4.13. Osoitetaan, että $\mathbb{V}(\mathbb{I}(V)) = V$. Olkoon ensin $(a_1, \ldots, a_n) \in \mathbb{V}(\mathbb{I}(V))$, jolloin kaikilla $f \in \mathbb{I}(V)$ pätee, että $f(a_1, \ldots, a_n) = 0$. Variston ideaalin määritelmän nojalla $f(a_1, \ldots, a_n) = 0$ kaikilla $(a_1, \ldots, a_n) \in V$, joten $(a_1, \ldots, a_n) \in V$, eli $\mathbb{V}(\mathbb{I}(V)) \subset V$.

Olkoon sitten $(a_1, \ldots, a_n) \in V$. Nyt $\mathbb{I}(V) = \langle f_1, \ldots, f_s \rangle$ ja $f_i(a_1, \ldots, a_n) = 0$, kun $1 \leq i \leq s$. Tämän ideaalin varisto on joukko pisteitä, joilla $f_1 = f_2 = \cdots = f_s = 0$ ja valittu piste $(a_1, \ldots, a_n)$ on sellainen, joten $V \subset \mathbb{V}(\mathbb{I}(V))$, mikä todistaa väitteen.

5 Eliminaatio- ja laajennuslause

Yhtälöryhmiä ratkaistessa kahden, kolmen tai neljän muuttujan tapauksissa on voidaan yrittää eliminoida jokin muuttuja ja sijoittaa saatu ratkaisu toisiin yhtälöihin. Tämä voidaan yleistää tomivaksi myös n:n muuttujan yhtälöryhmissä, kun hyödynnetään ideaaleja ja Gröbnerin kantoja.

Määritelmä 5.1. (Ks. [1, s. 116].) Ideaalin $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ l:s *eliminaatioideaali* renkaassa $k[x_1, \ldots, x_n]$ määritellään

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

Eli eliminaatioideaali I_l sisältää ideaalin I polynomit, jotka riippuvat vain muuttujista $x_{l+1}, \ldots, x_n$. Eliminaatioideaali siis muuttuu riippuen siitä, onko polynomit aakkosjärjestyksessä, eli $x > y > z$, tai jossain muussa järjestyksessä. Tässä työssä muuttujat järjestetään $x_1 > x_2 > \ldots > x_n$. Pisteitä, jotka ovat varistossa $V(I_l)$ kutsutaan *osittaisiksi ratkaisuiksi.* (Ks. [1, s. 123].)

Lause 5.2 (Eliminaatiolause.)**.** *(Vrt. [1, s. 116].) Olkoon $I \subset k[x_1, \ldots, x_n]$ ideaali ja olkoon G ideaalin I Gröbnerin kanta monomijärjestyksen $x_1 > x_2 > \ldots > x_n$ mukaan. Tällöin jokaisella indeksillä $0 \leq l \leq n$, joukko*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

on Gröbnerin kanta l:nnelle eliminaatioideaalille I_l.

Todistus. Olkoon $0 \leq l \leq n$. Gröbnerin kannan määritelmän (määritelmä 3.12) nojalla riittää osoittaa, että

$$\langle LT(I_{G_l}) \rangle = \langle LT(I_l) \rangle.$$

Koska $G_l \subset I_l$, niin myös $\langle LT(I_{G_l}) \rangle \subset \langle LT(I_l) \rangle$. Lauseen 3.15 nojalla väitteen toiseen suuntaan todistamiseksi riittää osoittaa, että ensimmäinen termi $LT(f)$ on jaollinen termillä $LT(g)$, jollain $g \in G$. Huomataan, että myös funktio f sisältyy ideaaliin I, mistä seuraa, että $LT(f)$ on jaollinen jollain termillä $LT(g)$, jollain polynomilla g, sillä G on ideaalin I Gröbnerin kanta. Huomataan vielä, että koska $f \in I_l$ on termissä $LT(g)$ vain muuttujat $x_{l+1}, \ldots, x_n$. Käytetään aakkosellista monomijärjestystä, jossa $x_1 > \cdots > x_n$, joten mikä tahansa monomi, jossa on muuttujia $x_1, \ldots, x_l$ on suurempi kuin kaikki monomit, jotka ovat renkaassa $k[x_{l+1}, \ldots, x_n]$. Siispä, koska $LT(g) \in [x_{l+1}, \ldots, x_n]$, niin $g \in k[x_{l+1}, \ldots, x_n]$. Tästä seuraa, että $g \in G_l$, mikä todistaa väitteen.

□

Eliminaatiolauseen avulla voidaan eliminoida muuttujia ottamalla Gröbnerin kanta jonkin monomijärjestyksen avulla.

Esimerkki 5.3. Olkoon $I \subset k[x_1, \ldots, x_n]$ ideaali. Osoitetaan, että $I_l = I \cap k[x_{l+1}, \ldots, x_n]$ on ideaali renkaassa $k[x_{l+1}, \ldots, x_n]$.

(1) Koska $0 \in I$ ja $0 \in k[x_{l+1}, \ldots, x_n]$, niin $0 \in I \cap k[x_{l+1}, \ldots, x_n]$.

(2) Jos $f \in I \cap k[x_{l+1}, \ldots, x_n]$, niin $f \in I$ ja $f \in k[x_{l+1}, \ldots, x_n]$. Samoin, jos $g \in I \cap k[x_{l+1}, \ldots, x_n]$, niin $g \in I$ ja $g \in k[x_{l+1}, \ldots, x_n]$. Nyt siis $f \in I$ ja $g \in I$, joten ideaalin määritelmän nojalla myös $f+g \in I$ ja koska $f+g \in k[x_{l+1}, \ldots, x_n]$, niin myös $f+g \in I \cap k[x_{l+1}, \ldots, x_n]$, eli ideaalin määritelmän toinen osa toteutuu.

(3) Olkoon $f \in I \cap k[x_{l+1}, \ldots, x_n]$. Jos $h \in k[x_{l+1}, \ldots, x_n]$, niin $hf \in I$ ideaalin määritelmän nojalla ja koska $hf \in k[x_{l+1}, \ldots, x_n]$, niin $hf \in I \cap k[x_{l+1}, \ldots, x_n]$, eli kolmaskin ideaalin määritelmän osa toteutuu joten $I_l = I \cap k[x_{l+1}, \ldots, x_n]$ on ideaali.

Kaikista osittaisista ratkaisuista ei kuitenkaan saada laajennettua ratkaisujen joukkoa. Laajennuslauseen avulla voidaan selvittää, milloin näin voidaan tehdä.

5.1 Resultantit ja laajennuslause

5.1.1 Polynomien jaottomuudesta

Määritelmä 5.4. (Ks. [1, s. 150].) Olkoon k kunta. Polynomi $f \in k[x_1, \ldots, x_n]$ on *jaoton kunnassa* k, jos f ei ole vakiopolynomi, eikä se ole minkään renkaan $k[x_1, \ldots, x_n]$ vakioista poikkeavien polynomien tulo.

Lause 5.5. *(Ks. [1, s. 151].) Olkoon $f \in k[x_1, \ldots, x_n]$ jaoton kunnassa k ja oletetaan, että f jakaa tulon gh, missä $g, h \in k[x_1, \ldots, x_n]$. Tällöin f jakaa joko g:n tai h:n.*

Todistus. Voidaan todistaa induktiolla; ensin yhdelle muuttujalle suurimman yhteisen tekijän avulla ja useammalle muuttujalle rationaalipolynomirenkaassa renkaan $k(x_2, \ldots, x_n)[x_1]$ avulla. Ks. [1, s. 151].

□

Lause 5.6. *(Ks. [1, s. 152].) Oletetaan, että molempien polynomien $f, g \in k[x_1, \ldots, x_n]$ muuttujan x_1 aste* $\deg(x_1) > 0$. *Polynomeilla f ja g on yhteinen tekijä renkaassa $k[x_1, \ldots, x_n]$ jos ja vain jos niillä on yhteinen tekijä renkaassa $k(x_2, \ldots, x_n)[x_1]$.*

Todistus. Jos polynomeilla f ja g, joiden termin x_1 aste > 0, on yhteinen tekijä h renkaassa $k[x_1, \ldots, x_n]$, niin niillä on myös yhteinen tekijä suuremmassa polynomirenkaassa $k(x_2, \ldots, x_n)[x_1]$. Toisaalta, jos polynomeilla f ja g on yhteinen tekijä $h \in k(x_2, \ldots, x_n)[x_1]$, niin

$$f = \hat{h}\hat{f}_1, \hat{f}_1 \in k(x_2, \ldots, x_n)[x_1].$$
$$g = \hat{h}\hat{g}_1, \hat{g}_1 \in k(x_2, \ldots, x_n)[x_1].$$

Nyt polynomeilla $\hat{h}$, $\hat{f}_1$ ja $\hat{g}_1$ voi olla nimittäjiä, jotka ovat polynomeja renkaasta $k[x_2, \ldots, x_n]$. Olkoon $d \in k[x_2, \ldots, x_n]$ yhteinen osamäärän nimittäjä. Tällöin $h =$

$d\hat{h}$, $f_1 = d\hat{f}_1$ ja $g_1 = d\hat{g}_1$ renkaassa $k[x_1, \ldots, x_n]$. Jos kerrotaan f ja g, niin kuin ne on edellä kirjoitettu nimittäjän toisella potenssilla d^2 saadaan

$$d^2 f = hf_1,$$
$$d^2 g = hg_1$$

renkaassa $k[x_1, \ldots, x_n]$. Olkoon nyt h_1 jaoton h:n tekijä, kun polynomien aste on positiivinen muuttujan x_1 suhteen. Koska $\hat{h} = h/d$:n aste on positiivinen muuttujassa x_1, niin sellaisen tekijän h_1 tulee olla olemassa, että h_1 jakaa tekijän $d^2 f$. Se siis jakaa joko tekijän d^2 tai f (Ks. [1, s. 151]). Ensimmäinen vaihtoehto on mahdoton, sillä $d^2 \in k[x_2, \ldots, x_n]$, eli f on jaollinen tekijällä h_1 renkaassa $k[x_1, \ldots, x_n]$. Samoin g on jaollinen tekijällä h_1, joten h_1 on polynomien f ja g yhteinen tekijä. □

5.1.2 Resultantin ominaisuuksia

Polynomien resultantteja voidaan käyttää selvittämään, onko polynomeilla yhteisiä tekijöitä polynomirenkaassa laskematta jakolaskuja. Tässä työssä resultantteja tarvitaan laajennuslauseen todistamiseen.

Lause 5.7. *(Ks. [1, s. 154].) Olkoon $f, g \in k[x]$ polynomeja, joiden asteet ovat $l > 0$ ja $m > 0$. Tällöin polynomeilla on yhteinen tekijä jos ja vain jos on polynomit $A, B \in k[x]$, joille pätee:*

(i) molemmat A ja B eivät ole nollia.

(ii) $\deg(A) \leq m - 1$ *ja* $\deg(B) \leq l - 1$.

(iii) $Af + Bg = 0$.

Todistus. Oletetaan ensin, että polynomeilla f ja g on yhteinen tekijä $h \in k[x]$, jolloin $f = hf_1$ ja $g = hg_1$, missä $f_1, g_1 \in k[x]$. Koska f:n aste on l, niin f_1:n aste on korkeintaan $l - 1$ ja g_1:n aste on korkeintaan $m - 1$. Nyt siis

$$g_1 \cdot f + (-f_1) \cdot g = g_1 \cdot hf_1 + (-f_1) \cdot hg_1 = 0,$$

joten polynomeilla $A = g_1$ ja $B = -f_1$ on halutut ominaisuudet.
Oletetaan sitten, että on sellaiset polynomit A ja B, joilla on yllä luetellut ominaisuudet. Olkoon $B \neq 0$. Jos oletaan, ettei polynomeilla g ja f ole yhteistä tekijää, niin niiden $GCD(f, g) = 1$. Tällöin on olemassa sellaiset polynomit $\hat{A}$ ja $\hat{B}$, joilla $\hat{A}f + \hat{B}g = 1$. Kerrotaan tämä yhtälö puolittain polynomilla B ja sijoitetaan oletuksen mukainen $Bg = -Af$, jolloin

$$B = (\hat{A}f + \hat{B}g)B = \hat{A}Bf + \hat{B}Bg = \hat{A}Bf - \hat{B}Af = (\hat{A}B - \hat{B}A)f.$$

Tällöin B:n aste olisi vähintään $deg(f) = l$, mikä on ristiriidassa oletusten kanssa, joten A:lla ja B:llä on oltava yhteinen tekijä. □

Kun halutaan selvittää, onko tällaisia polynomeja A ja B olemassa voidaan hyödyntää lineaarialgebran tuloksia kirjoittamalla $Af + Bg = 0$ lineaariseksi yhtälöryhmäksi. Nyt

$$A = c_0 x^{m-1} + \cdots + c^{m-1}, \tag{5.1}$$

$$B = d_0 x^{l-1} + \cdots + d_{l-1}. \tag{5.2}$$

Tahdotaan määrittää $c_i, d_i \in k$, jotka eivät kaikki ole nollia, niin että yhtälö

$$Af + Bg = 0$$

pätee. Tällöin saadaan polynomit A ja B, jotka täyttävät lauseen 5.7 ehdot. Yhtälöryhmämuotoon saattamiseksi kirjoitetaan polynomit f ja g seuraavasti

$$\begin{aligned} f &= a_0 x^l + \cdots + a_l, a_0 \neq 0, \\ g &= b_0 x^m + \cdots + b_m, b_0 \neq 0, \end{aligned}$$

missä $a_i, b_i \in k$. Eli nyt $Af + Bg = c_0 a_0 x^{m-1} x^l + \cdots + d_0 b_0 x^{l-1} x^m + d_0 b_0 x^{l-1} x^m \cdots + d_{l-1} b_m = 0$. Sijoitetaan nämä haluttuun muotoon, jolloin saadaan lineaarinen yhtälöryhmä, minkä muuttujat ovat c_i, d_i ja kertoimet ovat $a_i, b_i \in k$:

$$\begin{cases} a_0 c_0 + b_0 d_0 = 0, & \text{muuttujat } x^{l+m-1}\text{:stä} \\ a_0 c_0 + a_1 c_1 + b_0 d_0 + b_1 d_1 = 0, & \text{muuttujat } x^{l+m-2}\text{:stä} \\ \vdots & \vdots \\ a_l c_{m-1} + b_m d_{l-1} = 0, & \text{muuttujat } x^0\text{:sta.} \end{cases}$$

Koska nyt lineaarisia yhtälöitä on $l + m$ ja muuttujia $l + m$ kappaletta, tiedetään lineaarialgebrasta, että yhtälöryhmällä on nollasta poikkeava ratkaisu jos ja vain jos sen matriisin determinantti on nolla. Kyseistä matriisia sanotaan Sylvesterin matriisiksi.

Määritelmä 5.8 (Sylvesterin matriisi)**.** (Ks. [1, s. 155].) Kirjoitetaan kiinnitetyt polynomit $f, g \in k[x]$, joiden aste on positiivinen, muotoon

$$\begin{aligned} f &= a_0 x^l + \cdots + a_l, a_0 \neq 0, \\ g &= b_0 x^m + \cdots + b_m, b_0 \neq 0. \end{aligned}$$

Tällöin polynomien f ja g *Sylvesterin matriisi*, muutujan x suhteen, merkitään $\mathrm{Syl}(f, g, x)$ on kerroinmatriisi, joka muodostetaan yhtälöistä, joiden muuttujat ovat

c_i, d_i. Tällöin $\mathrm{Syl}(f, g, x)$ on seuraavanlainen $(l + m) \times (l + m)$ matriisi:

$$\mathrm{Syl}(f, g, x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix},$$

missä tyhjät kohdat ovat nollia. Nyt polynomien f ja g *resultantti* muuttujan x suhteen, on Sylvesterin matriisin determinantti ja merkitään

$$\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x)).$$

Määritelmästä seuraa resultantin ominaisuudet, kuten esimerkiksi seuraava mielenkiintoinen ominaisuus.

Lause 5.9. *(Ks. [1, s. 156, 511].) Kun kiinnitettyjen polynomien $f, g \in k[x]$ aste on positiivinen niin niiden resultantti $\mathrm{Res}(f, g, x)$ on kokonaislukupolynomi, eli antaa kokonaislukuarvoilla vastaukseksi kokonaislukuja ja polynomeilla f ja g on yhteinen tekijä renkaassa $k[x]$ jos ja vain jos resultantti $\mathrm{Res}(f, g, x) = 0$.*

Todistus. Ensimmäisen osan todistus seuraa $n \times n$ matriisin $A = (a_{ij})_{l<i,j<s}$ determinantin määritelmästä

$$det(A) = \sum_s \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{s\sigma(s)},$$

missä $\mathrm{sgn}(\sigma)$ on permutaatioiden merkki ja $\sigma \in S_n$, missä S_n on permutaatioryhmä. Tästä nähdään, että determinantti on kokonaislukupolynomi, jonka kertoimet ovat 1 tai -1.

Toinen osa seuraa siitä, että jos resultantti on nolla on se yhtäpitävää sen kanssa, että yhtälöryhmän kerroinmatriisin determinantti on nolla, mikä on taas yhtäpitävää sen kanssa, että yhtälöryhmällä on nollasta poikkeava ratkaisu. Tämä todettiin lauseen 5.7 todistuksessa. □

5.2 Resultantit polynomirenkaassa

Koska halutaan todistaa laajennuslause, niin tarvitaan resultantteja polynomirenkaassa, kun muuttujia on n kappaletta. Olkoon $f, g \in k[x_1, \ldots, x_n]$ polynomeja, joiden muuttujan x_1 aste on positiivinen. Nyt polynomien f ja g resultantti, muuttujan x_1 suhteen, on seuraavan matriisin determinantti:

$$\mathrm{Res}(f,g,x_1) = \det \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix},$$

missä tyhjät kohdat ovat nollia. Määritellään resultanttien ominaisuudet polynomirenkaassa.

Lause 5.10. *(Ks. [1, s. 163].) Olkoon $f, g \in k[x_1, \ldots, x_n]$ polynomeja, joiden muuttujan x_1 aste on positiivinen. Tällöin:*

(i) $Res(f, g, x_1)$ sisältyy ensimmäiseen eliminaatioideaaliin $\langle f, g\rangle \cap k[x_2, \ldots, x_n]$.

(ii) $Res(f, g, x_1) = 0$ jos ja vain jos polynomeilla f ja g on yhteinen tekijä renkaassa $k[x_1, \ldots, x_n]$, jonka muuttujan x_1 aste on positiivinen.

Todistus. Kun polynomi kirjoitetaan muuttujan x_1 suhteen, sen kertoimet a_i, b_i ovat renkaasta $k[x_2, \ldots, x_n]$. Lauseen 5.9 mukaan resultantti on kertoimien a_i, b_i kokonaislukupolynomi, joten $\mathrm{Res}(f, g, x_1) \in k[x_2, \ldots, x_n]$. Lauseen 5.9 nojalla

$$Af + Bg = \mathrm{Res}(f, g, x_1),$$

missä A ja B ovat polynomeja muuttujan x_1 suhteen ja joiden kertoimet ovat kokonaislukupolynomeja a_i, b_i. Niinpä $A, B \in k(x_2, \ldots, x_n)[x_1] = k[x_1, \ldots, x_n]$ ja $\mathrm{Res}(f, g, x_1) \in \langle f, g\rangle$, mikä todistaa väitteen kohdan (i). Toisen osan todistamiseksi huomataan, että lause 5.9 pätee myös polynomirenkaassa, kun f ja g ovat polynomeja renkaassa $k[x_1]$, joiden kertoimet ovat renkaasta $k[x_2, \ldots, x_n]$ ja siis kunnasta $k(x_2, \ldots, x_n)$. On osoitettu, että $\mathrm{Res}(f, g, x) = 0$ jos ja vain jos polynomeilla f ja g on yhteinen tekijä renkaassa $k(x_2, \ldots, x_n)[x_1]$, missä $\deg(x_1) \geq 0$. Lause 5.6 osoittaa, että tämä on yhtäpitävää sen kanssa, että polynomeilla on yhteinen tekijä renkaassa $k[x_1, \ldots, x_n]$, kun $\deg(x_1) \geq 0$, mikä todistaa väitteen. □

Laajennuslauseen todistuksessa tarkastellaan resultanttien ja osittaisten ratkaisujen vuorovaikutusta. Polynomeille $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ saadaan resultantti

$$h = \mathrm{Res}(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$$

kuten edeltävässä lauseessa. Jos sijoitetaan $\mathbf{c} = (c_2, \ldots, c_n)$ polynomiin h saadaan resultantin erikoistapaus. Seuraava lause kertoo, milloin h varmasti vastaa polynomeja $f(x_1, \mathbf{c})$ ja $g(x_1, \mathbf{c})$.

Lause 5.11. *(Ks. [1, s. 164].) Olkoon $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ polynomeja, joiden asteet ovat l, m ja olkoon $\boldsymbol{c} = (c_2, \ldots, c_n) \in \mathbb{C}^{n-1}$ piste, joka täyttävät seuraavat ehdot:*

(i) polynomin $f(x_1, \boldsymbol{c}) \in \mathbb{C}[x_1]$ aste on l.

(ii) polynomin $g(x_1, \boldsymbol{c}) \in \mathbb{C}[x_1]$ aste on $p \leq m$.

Tällöin polynomille $h = Res(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$ pätee

$$h(\boldsymbol{c}) = a_0(c)^{m-p} Res(f(x_1, \boldsymbol{c}), g(x_1, \boldsymbol{c}), x_1), \tag{5.3}$$

missä $a_0 \neq 0$ ja se on polynomin f muuttujan x_1 korkeimman potenssin kerroin kuten Sylvesterin matriisin määritelmässä.

Todistus. Jos korvataan muuttujat $x_2, \ldots, x_n$ polynomilla $\mathbf{c} = (c_2, \ldots, c_n)$ resultanttiin $h = \mathrm{Res}(f, g, x_1)$ saadaan

$$h(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & b_0(\mathbf{c}) & & \\ \vdots & \ddots & & & \vdots & \ddots \\ \vdots & & a_0(\mathbf{c}) & \vdots & & b_0(\mathbf{c}) \\ a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix}.$$

Oletetaan ensin, että polynomin $g(x_1, \mathbf{c})$ aste on $p = m$. Tällöin oletusten nojalla

$$f(x_1, \mathbf{c}) = a_0(\mathbf{c})x_1^l + \cdots + a_l(\mathbf{c}),\ a_0(\mathbf{c}) \neq 0,$$
$$g(x_1, \mathbf{c}) = b_0(\mathbf{c})x_1^m + \cdots + b_m(\mathbf{c}),\ a_0(\mathbf{c}) \neq 0.$$

Siispä ylläoleva determinantti on polynomien $f(x_1, \mathbf{c})$ ja $g(x_1, \mathbf{c})$ resultantti, joten

$$h(\mathbf{c}) = \mathrm{Res}(f(x_1, \mathbf{c}), (g(x_1, \mathbf{c}), x_1).$$

Tämä todistaa väitteen, kun $p = m$.
Tapauksen $p < m$ todistus ohitetaan. □

Jos toinen yhtälöistä, joista resultantti otetaan on vakio, pätee seuraava lause.

Lause 5.12. *(Ks. [1, s. 161].) Olkoon $f \in k[x]$ ja olkoon b_0 vakio. Tällöin Res $(f, b_0, x) = b_0^N$.*

Todistus. (Vrt. [1, s.161]) Nyt Res $(f, b_0, x) = \det(\mathrm{Syl}(f, b_0, x))$. Tässä Sylvesterin matriisi on matriisi, jonka lävistäjällä on vakioita b_0 ja muut kohdat ovat nollia, sillä polynomin b_0 aste on nolla, joten matriisiin ei tule termejä polynomista f. Olkoon polynomin f aste N, jolloin Sylvesterin matriisiin tulee N kappaletta vakioita b_0, joten Sylvesterin matriisin determinantti on b_0^N, mikä todistaa väitteen. □

Lause 5.13 (Laajennuslause)**.** *(Ks. [1, s. 118].)*

Olkoon $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ *ja olkoon* I_1 *ensimmäinen eliminaatioideaali* I*:ssä. Kirjoitetaan* f_i *muotoon*
$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i}$ *+termit, joiden* x_i*:n aste* $< N_i$*, missä* $N_i \geq 0$ *ja* $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ *poikkeaa nollasta. Oletetaan, että on osittainen ratkaisu:* $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$*. Jos* $(a_2, \ldots, a_n) \notin \mathbb{V}(g_1, \ldots, g_s)$*, niin on sellainen* $a_1 \in \mathbb{C}$*, jolla*
$(a_1, a_2, \ldots, a_n) \in \mathbb{V}(I)$.

Todistus. (Ks. [1, s. 165].) Valitaan $\mathbf{c} = (c_2, \ldots, c_n)$. Tarkastellaan rengashomomorfismia

$$\mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}[x_1]$$

jonka määrittää polynomit $f(x_1, \ldots, x_n) \mapsto f(x_1, \mathbf{c})$. Nyt ideaali I kuvautuu joukoksi $I' \subset \mathbb{C}[x_1]$. Osoitetaan, että ideaalin I kuva $f(I) = I' \subset \mathbb{C}[x_1]$ on ideaali.

(1) Nyt siis x_1 kuvautuu x_1:si. Kun $x_1 = 0$, niin myös $0 \in I'$.

(2) Summa kuvautuu rengashomomorfismissa summaksi, joten polynomien $g_1, g_2 \in I$ summa $g_1(x_1, \ldots, x_s) + g_2(x_1, \ldots, x_t) \mapsto g_1(x_1, \mathbf{c}) + g_2(x_1, \mathbf{c})$. Koska polynomien summa $g_1(x_1, \ldots, x_s) + g_2(x_1, \ldots, x_t) \in I$, niin myös $g_1(x_1, \mathbf{c}) + g_2(x_1, \mathbf{c}) \in I' \subset \mathbb{C}[x_1]$, sillä $\mathbf{c} \in \mathbb{C}$.

(3) Nyt polynomi $h \in k[x_1, \ldots, x_n]$ kuvautuu polynomiksi, joka riippuu muuttujasta x_1. Merkitään $h' = h(x_1, \mathbf{c})$. Nyt tulo hf, missä $f \in I$ kuvautuu homomorfismissa tuloksi $h' \cdot f(x_1, \mathbf{c}) = f'(x_1, \mathbf{c})$. Näin ollen $f'(x_1, \mathbf{c}) \in I'$, joten I' on ideaali.

Koska $\mathbb{C}[x]$ on pääideaalialue, niin I:n kuva on yhden polynomin $u(x_1)$ virittämä. Toisin sanoen

$$\{f(x_1, \mathbf{c}) \colon f \in I\} = \langle u(x_1) \rangle. \tag{5.4}$$

Jos $u(x_1)$ ei ole vakio, on kompleksiluvuilla suljettuna kuntana sellainen ominaisuus, että löytyy sellainen $c_1 \in \mathbb{C}$, jolla $u(c_1) = 0$. Siitä seuraa, että $f(c_1, \mathbf{c}) = 0$ kaikilla polynomeilla $f \in I$, joten $(c_1, \mathbf{c}) = (c_1, c_2, \ldots, c_n) \in \mathbb{V}(I)$. Tämä pätee myös, jos $u(x_1)$ on nollapolynomi. Jos $u(x_1) \neq 0$ on vakio, niin tällöin yhtälön 5.4 mukaan on olemassa polynomi, jolla $f(x_1, \mathbf{c}) = u_0$, eikä väite päde. Osoitetaan vastaoletuksella, ettei näin voi olla. Oletusten nojalla $\mathbf{c} \notin \mathbb{V}(g_1, \ldots, g_s)$. Siispä jollain indeksillä $i \colon g_i(\mathbf{c}) \neq 0$. Otetaan tarkasteluun yhtälö

$$h = \mathrm{Res}(f_i, f, x_1) \in \mathbb{C}[x_2, \ldots, x_n].$$

Käytetään lauseen 5.11 tulosta polynomeihin f_i ja f, jolloin kaavasta 5.3 saadaan

$$h(\mathbf{c}) = g_i(\mathbf{c})^{deg(f)}\mathrm{Res}(f_i(x_1, \mathbf{c}), u_0, x_1),$$

sillä ollaan oletettu, että $f(x_1, \mathbf{c}) = u_0$. Nyt lauseen 5.12 nojalla
$\mathrm{Res}(f_i(x_1, \mathbf{c}), u_0, x_1) = u_0^{N_i}$. Niinpä

$$h(\mathbf{c}) = g_i(\mathbf{c})^{deg(f)}u_0^{N_i} \neq 0.$$

Toisaalta tiedetään, että $f_i, f \in I$ jolloin lauseesta 5.11 tiedetään, että $h \in I_1$, joten $h(\mathbf{c}) = 0$, sillä $\mathbf{c} \in \mathbb{V}(I_1)$. Tämä on ristiriita, eli $u(x_1)$ ei ole nollasta poikkeava vakio, mikä todistaa väitteen.

□

Kun ensimmäiset eli johtavat termit katoavat yhtä aikaa, osittainen ratkaisu ei "laajene"ratkaisuksi. Muutoin osittainen ratkaisu laajenee kokonaiseksi ratkaisuksi.

5.3 Geometrinen laajennuslause

Olkoon $V = \mathbb{V}(f_1, \ldots, f_n) \in \mathbb{C}^n$ annettu. Jos halutaan eliminoida ensimmäiset l -kappaletta muuttujia, käytetään *projektiokuvausta*

$$\pi_i : \mathbb{C}^n \to \mathbb{C}^{n-l},$$

joka kuvaa $(a_1, \ldots, a_n)$:n pisteeksi $(a_{l+1}, \ldots, a_n)$, eli $\pi(a_1, \ldots, a_n) = (a_{l+1}, \ldots, a_n)$. (Ks. [1, s. 123].) Jos käytetään kuvausta π_l varistoon $V \subset \mathbb{C}^n$ saadaan $\pi_l(V) \subset \mathbb{C}^{n-1}$. Tämä voidaan liittää l:nteen eliminaatioideaaliin seuraavasti.

Seurauslause 5.14. *(Ks. [1, s. 123].) Olkoon merkinnät kuten edellä ja olkoon $I_l = \langle f_1, \ldots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ l:s eliminaatioideaali. Tällöin $\mathbb{C}^{n-1}$:ssä pätee*

$$\pi_l(V) \subset \mathbb{V}(I_l).$$

Todistus. Olkoon $f \in I_l$ polynomi. Jos $(a_1, \ldots . a_n) \in V$, niin f katoaa $(a_1, \ldots, a_n)$:ssä, koska $f \in \langle f_1, \ldots, f_s \rangle$. Ja koska f koskee vain muuttujia $x_{l+1}, \ldots, x_n$, voidaan kirjoittaa

$$f(a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)) = 0.$$

Mikä osoittaa, että f katoaa $\pi_l(V)$:n jokaisessa pisteessä. □

Lause 5.15. *(Ks. [1, s. 124].) Olkoon g_i samoin määritelty, kuin lauseessa 5.13 annetulle varistolle $V = \mathbb{V}(f_1, \ldots, f_s) \subset \mathbb{C}$. Jos I_1 on ensimmäinen eliminaatioideaali $\langle f_1, \ldots, f_s \rangle$:ssä, niin seuraava pätee $\mathbb{C}^{n-1}$:ssä.*

$$\mathbb{V}(I_l) = \pi_1(V) \cup (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(I_1)),$$

missä $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$ on projektio viimeisille $n-1$:lle komponentille.

Todistus. Lauseen 5.14 nojalla $\mathbb{V}(I_l) \subset \pi_1(V)$, joten $\mathbb{V}(I_l) \subset \pi_1(V) \cup (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(I_1))$.
Olkoon sitten $(a_2, \ldots, a_n) \in \pi_1(V) \cup (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(I_1))$. Nyt $(a_2, \ldots, a_n) \in \pi_1(V)$ tai $(a_2, \ldots, a_n) \in (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(I_1))$. Jos $(a_2, \ldots, a_n) \in \pi_1(V)$, niin $(a_2, \ldots, a_n) \in \mathbb{V}(I_l)$, sillä $f(a_t, \ldots, a_n) = 0$. Jos taas $(a_2, \ldots, a_n) \in (\mathbb{V}(g_1, \ldots, g_s) \cap \mathbb{V}(I_1))$, niin $(a_2, \ldots, a_n) \in \mathbb{V}(g_1, \ldots, g_s)$, missä g_i:t ovat polynomien f_i johtavia termejä, sekä $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$, kun $1 \leq i \leq s$. Nyt koska $\mathbb{V}(I_l) \subset \mathbb{V}(I_1)$, kun $l \geq 1$, niin $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$. □

Seurauslause 5.16. *(Ks.[1, s. 127].) Olkoon* $V = \mathbb{V}(f_1, \ldots, f_s) \in \mathbb{C}^n$ *ja olkoon* f_i *jollain* i *muotoa*

$f_i = cx_1^N +$ *termit, joissa* x_1*:n aste* $< N$,

missä $c \in \mathbb{C}, c \neq 0$ *ja* $N > 0$. *Jos* $I_1 = \langle f_1, \ldots, f_s \rangle \cap \mathbb{C}[x_2, \ldots, x_n]$ *on ensimmäinen eliminaatioideaali, niin* $\mathbb{C}^{n-1}$*:ssä pätee*

$$\pi_1(V) = \mathbb{V}(I_1),$$

missä π_1 *on viimeisille* $n - 1$ *muuttujille.*

Todistus. Olkoon $f \in I_l$ kiinnitetty polynomi. Jos $(a_1, \ldots, a_n) \in V$, niin f katoaa pisteessä $(a_1, \ldots, a_n)$, sillä $f \in \langle f_1, \ldots, f_s \rangle$. Nyt f riippuu vain muuttujista $x_2, \ldots, x_n$, joten voidaan kirjoittaa

$$f(a_2, \ldots, a_n) = f(\pi_1(a_1, \ldots, a_n)) = 0,$$

joten f katoaa kaikissa $\pi_1(V)$:n pisteissä. □

Lause 5.17. *(Vrt. [1, s. 165, 167].) Lause 5.15 ja sen seurauslauseet pätevät kaikkien suljettujen kuntien yli.*

Todistus. Kunta k on myös suljettu. Nyt siis samoin kuin lauseen 5.15 todistuksessa on polynomilla $u(x_1)$, joka virittää ideaalin I', joka on homomorfismin

$$k[x_1, \ldots, x_n] \mapsto k[x_1]$$

kuva, sellainen juuri $c_1 \in k$, jolla $u(c_1) = 0$. Muilta osin todistetaan samoin kuin kompleksilukujenkin kunnassa. □

6 Hilbertin nollakohtalauseen todistus

Todistetaan heikko nollakohtalause hyödyntäen laajennuslausetta ja sen seurauslausetta. Todistusta varten tarvitaan vielä muutama lause.

Määritelmä 6.1. (Ks. [1, s. 174].) Polynomi on *homogeeninen* jos sen jokaisen termin kokonaisaste on i, jollain $i \in \mathbb{Z}$.

Esimerkki 6.2. Esimerkiksi polynomi $x^4y + 3x^5 + 2x^2y^3$ on homogeeninen ja sen aste on 5.
Polynomi $x^5 + xy^2 + y^5$ ei ole homogeeninen, sillä termin xy^2 aste on 3, kun muiden termien aste on 5.

Lause 6.3. *(Vrt. [2, s. 9].) Olkoon $f \in I \subset k[x_1, \ldots, x_n]$ ja $\deg(f) = d$. Voidaan löytää sellaiset $a_1, \ldots, a_{n-1} \in k$ joilla*

$$f(x_1 + a_1x_n, \ldots, x_{n-1} + a_{n-1}, x_n) = c \cdot x_n^d + \textit{alemmat } x_n\textit{:n termit},$$

jollain vakiolla $c \neq 0$.

Todistus. (Vrt. [2, s. 10]) Kirjoitetaan f summana homogeenisia monomeja, niin että ensimmäinen termi $f_{(d)}$on muuttujan x_n astetta d. Nyt riittää, että tarkastellaan ensimmäistä termiä, joka on muotoa

$$f_{(d)}(x_1 + a_1x_n, \ldots, x_{n-1} + a_{n-1}x_n, x_n)$$

sillä muiden termistä x_n riippuvien termien aste on pienempi kuin d. Nyt $f_{(d)}(x_1 + a_1x_n, \ldots, x_{n-1} + a_{n-1}x_n, x_n) = x_n^d f(a_1, \ldots, a_{n-1}, 1) + $ termit, joissa x_n:n aste $< d$.

Lauseen 2.6 nojalla suljetut kunnat ovat äärettömiä, jolloin lauseen 2.16 nojalla polynomilla f on nollasta poikkeava juuri, eli

$$f(a_1, \ldots, a_n) \neq 0.$$

□

Lause 6.4 (Heikko nollakohtalause)**.** *(Vrt. [1, s. 170]). Olkoon k algebrallisesti suljettu kunta ja $k[x_1, \ldots, x_n]$ polynomirengas yli k:n. Ja olkoon $I \subset k[x_1, \ldots, x_n]$ ideaali, jolle $\mathbb{V}(I) \neq \emptyset$. Tällöin $I = k[x_1, \ldots, x_n]$.*

Todistus. Todistetaan, että $1 \in I$, koska tällöin määritelmän 2.7 nojalla $f \cdot 1 \in I$ pätee kaikille $f \in k[x_1, \cdots, x_n]$, jolloin $I = k[x_1, \ldots, x_n]$. Todistetaan tämä induktiolla, missä n on muuttujien määrä. Olkoon ensin $n = 1$. Koska $k[x]$ on lauseen 3.3 nojalla pääideaalirengas, voidaan merkitä $I = \langle f \rangle$, jolloin $f \in k[x]$. Jokaisella vakiosta poikkeavalla polynomilla on juuri k:ssa, joten jos $\mathbb{V}(I) = \emptyset$ täytyy f:n olla nollasta poikkeava vakio ja tällöin $\frac{1}{f} \in k$. Tällöin $\frac{1}{f} \cdot f \in I$, mistä seuraa, että $g = g \cdot 1 \in I$ pätee jokaisella $g \in k[x]$, jolloin $I = k[x]$ on k:n ainoa ideaali ja $\mathbb{V}(I) = \emptyset$.

Oletetaan, että väite pätee $n - 1$:llä muuttujalla. Tarkastellaan mielivaltaista ideaalia, joka on muotoa $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \cdots, x_s]$, ja jolle $\mathbb{V}(I) = \emptyset$. Jos f_1

on vakiofunktio väite pätee. Oletetaan sitten, että $\deg(f_1) = N \geq 1$. Vaihdetaan koordinaatit seuraavasti, jotta saadaan f_1 muotoon, josta lause voidaan todistaa.

$$\begin{aligned} x_1 &= \hat{x}_1 \\ x_2 &= \hat{x}_2 + a_2\hat{x}_1 \\ &\vdots \\ x_n &= \hat{x}_n + a_n\hat{x}_1, \end{aligned} \tag{6.1}$$

missä $a_i \in k$:t ovat toistaiseksi määrittelemättömiä vakioita.

Huomataan, että koska $\mathbb{V}(I) = \emptyset$ ei $f_i(x)$ ole nolla millään x, joten myöskään $x_1 = \hat{x_1} \neq 0$. Koska $\hat{x_1} \in \hat{f_i}$ kaikilla indekseillä i, jokaisessa termissä, joten $\mathbb{V}(\hat{I}) = \emptyset$. Nyt siis merkitään joukko $\hat{I} = \{\hat{f} : f \in I\}$. Edellisestä seuraa, että jos muokatuilla yhtälöillä olisi ratkaisuja, niin täytyisi myös alkuperäisillä yhtälöillä olla. Huomataan myös, että jos $1 \in \hat{I}$, niin myös $1 \in I$, sillä muunnos ei vaikuta vakioihin.

Lauseessa 6.3 osoitettiin, että f_1 voidaan kirjoittaa

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\hat{x_1}, \hat{x}_2 + a_2\hat{x}_1, \cdots, \hat{x}_n + a_n\hat{x}_1) \\ &= c(a_1, \ldots, a_n)\hat{x}_1^N + \text{ termit, joissa } \hat{x}_1\text{:n aste } < N, \end{aligned}$$

missä $c(a_1, \ldots, a_n)$ ei ole nolla.
Kun kertoimet $a_2, \ldots, a_n$ on valittu näin, niin kaikki polynomit $f \in k[x_1, \ldots, x_n]$ kuvautuvat muunnoksessa 6.1 polynomeiksi $\hat{f} \in k[\hat{x}_1, \ldots, \hat{x}_n]$.

Osoitetaan, että joukko $\hat{I} = \{\hat{f} : f \in I\}$ on ideaali $k[\hat{x}_1, \ldots, \hat{x}_n]$:ssa.

1. Jos $x_1 = 0$, niin $\hat{x_1} = x_1 = 0$, joten $0 \in \hat{I}$.

2. Olkoon $g = g_1 + g_2$ ja $g, g_1, g_2 \in I$. Nyt polynomit g, g_1, g_2 kuvautuvat lineaarimuunnoksessa polynomeiksi $\hat{g}, \hat{g_1}, \hat{g_2}$, joille pätee edelleen, että $\hat{g_1} + \hat{g_2} = \hat{g}$ ja polynomit kuuluvat ideaaliin $\hat{I}$.

3. Olkoon $\hat{h} \in k[\hat{x_1}, \ldots, \hat{x_n}]$ ja $\hat{f} \in \hat{I}$. Nyt tulo

   $$\begin{aligned} \hat{h}\hat{f} &= \hat{h}(\hat{x_1}, \hat{x_2}, \ldots, \hat{x_n})\hat{f}(\hat{x_1}, \ldots, \hat{x_n}) \\ &= \hat{h}(x_1, x_2 - a_n x_1, \ldots, x_n - a_n x_1)\hat{f}(x_1, x_2 - a_n x_1 \ldots, x_n - a_n x_1) \in I \end{aligned}$$

   joten $\hat{h}\hat{f} \in \hat{I}$.

Nyt voidaan käyttää lausetta 5.15, sillä laajennuslause ja sen korollaarit pätevät minkä tahansa suljetun kunnan yli. Olkoon $\pi : k^n \to k^{n-1}$ projektiokuvaus viimeisille $n-1$ muuttujille. Merkitään nyt $\hat{I}_1 = \hat{I} \cap k[\hat{x}_2, \ldots, \hat{x}_n]$, jolloin laajennuslauseen nojalla $\mathbb{V}(\hat{I}_1) = \pi_1(\mathbb{V}(\hat{I}))$, mistä seuraa, että

$$\mathbb{V}(\hat{I}_1) = \pi_1(\mathbb{V}(\hat{I})) = \pi_1(\emptyset) = \emptyset.$$

Induktioletuksen nojalla $1 \in \hat{I}$, mikä todistaa väitteen.

□

Jos suljettu kunta $k = \mathbb{C}$, niin heikko nollakohtalause vastaa algebran peruslausetta useammalle muuttujalle.

Polynomeilla f_i ei ole yhteistä ratkaisua, jos $V(f_1, \ldots, f_s) = \emptyset$. Heikon nollakohtalauseen mukaan edellinen on totta jos ja vain jos $1 \in \langle f_1, \ldots, f_s \rangle$. Kun halutaan selvittää, onko variston ideaaleilla ratkaisua, täytyy selvittää kuuluuko 1 ideaaliin. Tämä voidaan selvittää redusoitujen Gröbnerin kantojen avulla.

Huomautus 6.5. (Ks. [1, s. 172].) Ideaalin $\langle I \rangle$ ainoa redusoitu Gröbnerin kanta on $\{1\}$.

Todistus. Olkoon $\{g_1, \ldots, g_t\}$ ideaalin $I = \langle 1 \rangle$ Gröbnerin kanta. Nyt siis $1 \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ määritelmän perusteella. Tällöin seurauslauseen 3.11 nojalla 1 on jaollinen jollain $LT(g_i)$:llä. Oletetaan esimerkiksi, että $LT(g_i) = LT(g_1)$. Tällöin pakosti $LT(g_1)$ on vakio. Siitä seuraa, että joka toinen $LT(g_i)$ on jaollinen sillä vakiolla, jolloin termit $g_2, \ldots, g_t$ voidaan poistaa Gröbnerin kannasta seurauslauseen 3.20 nojalla. Ja koska $LT(g_1)$ on vakio, niin myös polynomi g_1 on vakio sillä jokaisen monomin g_i aste on suurempi tai yhtä suuri kuin g_1:n aste (Ks.[1, s.72]Cor 6). Koska $LT(g_i)$ on vakio, niin myös g_i on vakio, jolloin se voidaan kertoa sopivalla vakiolla, jotta saadaan $g_1 = 1$. Redusoitu Gröbnerin kanta on siis $\{1\}$. □

Näin on siis saatu keino sen määrittämiseksi, onko varisto tyhjä joukko, eli $V(f_1, \ldots, f_s) = \emptyset$, eli onko yhtälöllä $f_1 = \cdots = f_s = 0$ ratkaisua.

Lause 6.6 (Hilbertin nollakohtalause)**.** *(Ks.[1, s. 173].) Olkoon k algebrallisesti suljettu kunta. Jos $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ toteuttavat $f \in \mathbb{I}(\mathbb{V}(f_1, \ldots, f_s))$, niin on olemassa sellainen kokonaisluku $m \geq 1$, jolla*

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

ja päinvastoin.

Todistus. Täytyy siis osoittaa, että annetulle polynomille f, joka katoaa polynomien $f_1, \ldots, f_s$ yhteisissä nollakohdissa, löytyy kokonaisluku $m \geq 1$ ja polynomit $A_1, \ldots, A_s$ joilla

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Merkitään ideaalia $\hat{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$, ja väitetään, että $\mathbb{V}(\hat{I}) = \emptyset$. Tätä kutsutaan myös Rabinowitchin keinoksi (Vrt. [5, s. 25]). Tämän todistamiseksi olkoon $(a_1, \ldots, a_n, a_{n+1})$ piste k^{n+1}:ssä. Nyt joko $(a_1, \ldots, a_n, a_{n+1})$ on polynomien $f_1, \ldots, f_s$ yhteinen nollakohta, tai $(a_1, \ldots, a_n, a_{n+1})$ ei ole polynomien $f_1, \ldots, f_s$ nollakohta. Oletetaan ensin ensimmäinen vaihtoehto, jolloin $f(a_1, \ldots, a_n) = 0$, sillä f katoaa polynomien yhteisissä nollakohdissa. Tällöin polynomi $1 - yf$ saa arvon $1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0$ pisteessä $(a_1, \ldots, a_n, a_{n+1})$. Erityisesti tällöin $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbb{V}(\hat{I})$. Oletetaan sitten ettei $(a_1, \ldots, a_n, a_{n+1})$ ole polynomien yhteinen nollakohta, jolloin jollain i pätee $f_i(a_1, \ldots, a_n) \neq 0$, kun $1 \leq i \leq s$. Mielletään f_i funktioksi, jossa on $n + 1$ muuttujaa, jotka eivät riipu viimeisestä muuttujasta $f_i(a_1, \ldots, a_n) \neq 0$. Tästä saadaan $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbb{V}(\hat{I})$. Koska

$(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$ valittiin mielivaltaiseksi pisteeksi pätee $\mathbb{V}(\hat{I}) = \emptyset$ kaikille pisteille.

Osoitetaan vielä, että $1 \in \hat{I}$, eli joillain polynomeilla $p_i, q \in k[x_1, \ldots, x_n, y]$ pätee

$$1 = \sum_{i=1}^{s} p_i(x_i, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf). \tag{6.2}$$

Valitaan $y = 1/f(x_1, \ldots, x_n)$. Edellinen yhtälö saadaan muotoon

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i + q(x_1, \ldots, x_n, 1/f)(1 - y/f(x_1, \ldots, x_n), \tag{6.3}$$

josta saadaan asettamalla $y = \dfrac{1}{f}$

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i. \tag{6.4}$$

Kerrotaan tämä puolittain f^m:llä, missä m on valittu niin suureksi, että kaikki nimittäjissä olevat polynomit f katoavat. Nyt yhtälö saadaan muotoon

$$f^m = \sum_{i=1}^{s} A_i f_i, \tag{6.5}$$

joillain $A_i \in k[x_1, \ldots, x_n]$, mikä todistaa väitteen. □

Tästä saadaan yksi todistus algebran peruslauseelle.

Lause 6.7. *Jokaisella vakiosta poikkeavalla polynomilla $f \in \mathbb{C}[x]$ on juuri joukossa $\mathbb{C}$.*

Todistus. Olkoon $I \subset k[x] = \mathbb{C}[x]$. Lauseen 3.3 nojalla voidaan kirjoittaa $I = \langle f \rangle$, sillä $k[x] = \mathbb{C}[x]$ on pääideaalialue. Jos $\mathbb{V}(I) = \emptyset$ suljetussa kunnassa, niin heikon nollakohtalauseen nojalla $I = k[x] = \mathbb{C}[x]$, jolloin f on vakiopolynomi. Muissa tapauksissa funktiolla f on juuri joukossa $\mathbb{C}[x]$. □

Esimerkki 6.8. Olkoon $J = \langle x^2 + y^2 - 1, y - 1 \rangle \subset \mathbb{R}[x, y]$. Etsitään sellainen funktio $f \in \mathbb{I}(\mathbb{V}(J))$, jolla $f \notin J$. Kaikki polynomit $g \in J$ ovat muotoa $g = h_1(x^2 + y^2 - 1) + h_2(y - 1)$, missä $h_1, h_2, g \in k[x, y]$. Kun ratkaistaan yhtälö $x^2 + y^2 - 1 = y - 1 = 0$ saadaan $\mathbb{V}(J) = \{(0, 1)\}$, jolloin $\mathbb{I}(\mathbb{V}(J)) = \langle h \rangle$. Nyt $x \in \langle h \rangle$, mutta polynomia $f = x$ ei voida kirjoittaa muotoon $h_1(x^2 + y^2 - 1) + h_2(y - 1)$, joten kun $f = x$, niin $f \notin J$.

7 Radikaalit ideaalit ja vahva nollakohtalause

Joissain tapauksissa joukon ideaali voi olla suurempi kuin joukon variston ideaali. Määritellään nyt radikaalit ideaalit, jotka nollakohtalauseen mukaan vastaavat aina variston ideaalia.

Seurauslause 7.1. *(Ks. [1, s. 175].) Olkoon V varisto. Jos $f^m \in \mathbb{I}(V)$, niin tällöin myös $f \in \mathbb{I}(V)$.*

Todistus. Olkoon $x \in V$. Jos $f^m \in \mathbb{I}(V)$, niin $(f(x))^m = 0$. Tämä pätee ainoastaan, kun $f(x) = 0$. Koska $x \in V$ valittiin mielivaltaiseksi, niin $f \in \mathbb{I}(V)$. □

Määritelmä 7.2. (Vrt. [1, s. 175].) Ideaali I on *radikaali*, jos ehdosta $f^m \in I$ jollain positiivisella kokonaisluvulla m, seuraa, että $f \in I$.

Seurauslause 7.3. *(Ks. [1, s. 176].) $\mathbb{I}(V)$ on radikaali-ideaali.*

Todistus. Seuraa seurauslauseesta 7.1. □

Määritelmä 7.4. (Vrt. [1, s. 176], [5, s. 19].) Olkooon $I \in k[x_1, \ldots, x_n]$ ideaali. Sen radikaali, merkitään $\sqrt{I}$, on joukko

$$\sqrt{I} = \{f : f^m \in I \text{ jollain kokonaisluvulla } m \geq 1\}.$$

Seurauslause 7.5. *(Ks. [1, s. 176].) Kun $I \in k[x_1, \ldots, x_n]$ on ideaali, niin myös $\sqrt{I}$ on ideaali renkaassa $k[x_1, \ldots, x_n]$ ja se sisältää ideaalin I.*

Todistus. Määritelmästä seuraa suoraan, että $I \subset \sqrt{I}$, sillä $f \in I$ tarkoittaa, että $f^1 \in I$, joten $f \in \sqrt{I}$. Osoitetaan, että $\sqrt{I}$ on ideaali.

(1) Koska $0^m \in I$, niin $0 \in \sqrt{I}$

(2) Jos $f^m, g^l \in I$, niin on osoitettava, että $(f+g)^{m+l} \in I$. Binomilauseen nojalla voidaan kirjoittaa $(f+g)^{m+l} = \sum_{k=0}^{m+l} \binom{m+l}{k} f^{m+l-k} g^k$. Nyt jos $m + l - k \geq m$, niin $\binom{m+l}{k} f^{m+l-k} g^k \in I$, sillä tällöin $f^{m+l-k} = f^{m+p} = f^m f^p \in I$, sillä $f^p \in k[x_1, \ldots, x_n]$. Tällöin myös $\binom{m+l}{k} f^{m+l-k} g^k \in I$. Jos taas $m + l - k \leq m$, niin $l - k < 0$, jolloin $k > l$ eli $g^k = g^{l+n} = g^l g^n \in I, n > 0$, sillä $g^l \in I$ ja $g^n \in k[x_1, \ldots, x_n]$. Näin ollen summan $\sum_{k=0}^{m+l} \binom{m+l}{k} f^{m+l-k} g^k$ jokainen termi kuuluu ideaaliin I.

(3) Oletetaan vielä, että $f \in \sqrt{I}$ ja $h \in k[x_1, \ldots, x_n]$. Tällöin $f^m \in I$, jollain $m \in \mathbb{N}, m \geq 1$. Ideaalin määritelmän nojalla $(h \cdot f)^m = h^m f^m \in I$. Siispä $hf \in \sqrt{I}$.

□

Seurauslause 7.6. *(Vrt. [5, s. 19], [1, s. 182], harjoitustehtävä 4.) Ideaali $\sqrt{I} \in R$ on radikaali-ideaali ja I on radikaali, vain jos $I = \sqrt{I}$.*

Todistus. Täytyy todistaa vain, että $\sqrt{I} \subset I$, sillä aiemmin todettiin, että aina $I \subset \sqrt{I}$. Olkoon $f \in I$ ja jos I on radikaali ideaali, niin $f^m \in I$ jollain kokonaisluvulla $m \geq 1$, jolloin $f \in \sqrt{I}$. Eli $\sqrt{I} \subset I$. □

Esimerkki 7.7. Osoitetaan, että $\sqrt{\sqrt{I}} = \sqrt{I}$. Merkitään $C = \sqrt{I}$. Jos $f \in C$, niin $f \in \sqrt{C}$, eli $f \in \sqrt{\sqrt{I}}$ kaikilla f, joten $\sqrt{\sqrt{I}} \subset \sqrt{I}$. Osoitetaan sitten, että $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Olkoon nyt $f \in \sqrt{C}$, jolloin $f^m \in C$. Nyt $(f^m)^n \in I$, eli $f^{mn} \in I$, missä mn on positiivinen kokonaisluku, joten $f \in \sqrt{I}$.

Seuraavaan lauseeseen viitataan usein myös Hilbertin nollakohtalauseena.

Lause 7.8 (Vahva nollakohtalause)**.** *Olkoon k algebrallisesti suljettu kunta. Jos $I \in k[x_1, \ldots, x_n]$ on ideaali, niin*

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}.$$

Todistus. (Vrt. [1, s. 176]). Todetaan ensin, että $\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I))$, sillä $f \in \sqrt{I}$ tarkoittaa, että $f^m \in I$, pätee jollain m. Siispä f^m katoaa joukossa $\mathbb{V}(I)$, mistä seuraa että f katoaa joukossa $\mathbb{V}(I)$, eli $f \in \mathbb{I}(\mathbb{V}(I))$. Oletetaan sitten, että $f \in \mathbb{I}(\mathbb{V}(I))$. Tällöin, määritelmän 4.1 nojalla, f katoaa joukossa $\mathbb{V}(I)$. Lauseen 6.6 nojalla on olemassa sellainen kokonaisluku $m \geq 1$, jolla $f^m \in I$. Tämä tarkoittaa seurauslauseen 7.6 mukaan samaa kuin $f \in \sqrt{I}$. Koska f oli mielivaltainen, niin $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$. □

7.1 Hilbertin vastaavuus

Nollakohtalauseiden merkittävin seuraus on ns. Hilbertin vastaavuus, eli toisilleen käänteiset kuvaukset varistojen alijoukosta ideaalien joukolle ja päin vastoin. Näin ollaan saatu yhteys algebrallisen käsitteen ja geometrisen käsitteen välille.

Lause 7.9. *(Vrt. [1, s. 177] : [5, s. 23].) Olkoon k mielivaltainen kunta.*

(i) Kuvaukset

$$\mathbb{I}\colon varistot \longrightarrow ideaalit$$

ja

$$\mathbb{V}\colon ideaalit \longrightarrow varistot$$

kääntävät joukkojen inkluusion järjestyksen, eli, jos $I_1 \subset I_2$, niin $\mathbb{V}(I_2) \subset \mathbb{V}(I_1)$ ja vastaavasti jos $V_1 \subset V_2$ ovat varistoja, niin $\mathbb{I}(V_2) \subset \mathbb{I}(V_1)$. Edelleen, mille tahansa varistolle V pätee:

$$\mathbb{V}(\mathbb{I}(V)) = V.$$

(ii) Jos k on algebrallisesti suljettu kunta ja ideaalit ovat radikaaleja ideaaleja, niin kuvaukset

$$\mathbb{I}\colon varistot \longrightarrow ideaalit$$

ja

$$\mathbb{V}\colon ideaalit \longrightarrow varistot$$

ovat bijektiokuvauksia.

Todistus. (Vrt. [1, s. 177, 182].) Osoitetaan ensimmäinen kohta (i). Oletetaan ensin, että $V_1 \subset V_2$. Lauseen 4.8 nojalla $\mathbb{I}(V_2) \subset \mathbb{I}(V_1)$. Samoin, jos $I_1 \subset I_2$, lauseen 4.8 nojalla $\mathbb{V}(I_2) \subset \mathbb{V}(I_1)$.

Esimerkissä 4.13 osoitettiin, että $\mathbb{V}(\mathbb{I}(V) = V$.

Kohdan (ii) todistamiseksi oletetaan, että I_1 ja I_2 ovat radikaaleja ja k on algebrallisesti suljettu kunta. Koska $\mathbb{I}(V)$ on radikaali lauseen 7.3 nojalla, voidaan $\mathbb{I}$ mieltää kuvauksena varistoilta ideaaleille. Halutaan siis todistaa vielä, että $\mathbb{I}(\mathbb{V}(I)) = I$. Koska I on nyt radikaali, nollakohtalauseen nojalla $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$ pätee. □

Hilbertin vastaavuudesta seuraa, että varistoihin liittyviä kysymyksä voidaan tarkastella algebrallisena kysymyksenä, joka koskee radikaali-ideaaleja ja myös päin vastoin. Tämä pätee tosin vain suljetuissa kunnissa.

Lause 7.10. *(Ks. [1, s. 178].)*
Olkoon k mikä tahansa kunta ja olkoon $I = \langle f_1, \ldots, f_s\rangle \subset k[x_1, \ldots, x_n]$ ideaali. Tällöin $f \in \sqrt{I}$ jos ja vain jos vakiopolynomi 1 sisältyy ideaaliin $\hat{I} = \langle f_1, \ldots, f_s, 1 - yf\rangle \subset k[x_1, \ldots, x_n, y]$. Tällöin siis $\hat{I} = k[x_1, \ldots, x_n, y]$.

Todistus. Lauseen 6.6 todistuksessa nähtiin, että jos $1 \in \hat{I}$, niin $f^m \in I$ jollain m, jolloin $f \in \sqrt{I}$.

Toisaalta, jos $f \in \sqrt{I}$, niin tälllöin $f^m \in I \subset \hat{I}$ jollain m. Toisaalta myös $1 - yf \in \hat{I}$, joten

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

□

Tästä saadaan siis keino sen määrittämiselle kuuluuko jokin funktio radikaaliin $\sqrt{\langle f_1, \ldots, f_s\rangle} \subset k[x_1, \ldots, x_n]$.
Lasketaan ideaalille $\langle f_1, \ldots, f_s, 1-yf\rangle \subset k[x_1, \ldots, x_n, y]$ jonkin monomijärjestyksen mukaan redusoitu Gröbnerin kanta. Jos tulos on $\{1\}$, niin $f \in \sqrt{I}$. Muutoin $f \notin \sqrt{I}$.

Esimerkki 7.11. (a.) Määritetään, kuuluuko polynomi $x + y$ radikaaliin $\sqrt{\langle x^3, y^3, xy(x + y)\rangle}$. Tarkastellaan ideaalia $\hat{I} = \langle x^3, y^3, xy(x + y), 1 - z(x + y)\rangle$. Muodostetaan sen varisto $V(\hat{I})$. Koska $x^3 = 0, y^3 = 0$ ja $xy(x + y) = 0$, niin $x = y = 0$, mutta yhtälöstä $1 - z(x + y) = 0$ saadaan $1 = 0$, joten $V(\hat{I}) = \emptyset$. Tällöin heikon nollakohtalauseen, eli lauseen 6.4, nojalla $\hat{I} = R$ joten $1 \in \hat{I}$. Polynomi $x + y$ siis sisältyy ideaaliin.

Selvitetään, mikä on pienin potenssi, jolla polynomi $(x + y)$ sisältyy radikaaliin. Koska $xy(x + y) = x^2y + xy^2 = h_1y + h_2x$, missä $h_1 = y^2$ ja $h_2 = x^2$, niin $x + y$

kuuluu radikaaliin, kun potenssi on 1.

(b.) Määritetään kuuluuko polynomi $x^2 - 3xz$ radikaaliin $\sqrt{\langle x + z, x^2y, x - z^2\rangle}$. Tarkastellaan nyt ideaalia $\hat{I} = \langle x + z, x^2y, x - z^2, 1 - h(x^2 + 3xz)\rangle$ ja määritetään sen varisto $\mathbb{V}(\hat{I})$. Yhtälöistä

$$\begin{aligned} x + z &= 0 \\ x^2y &= 0 \\ x - z^2 &= 0 \\ 1 - h(x^2 + 3xz) &= 0 \end{aligned}$$

nähdään, että kun $y = 0, x = 1, z = -1$ ja $h = -\frac{1}{2}$ varisto ei ole tyhjä joukko, joten heikon nollakohtalauseen nojalla $1 \notin \hat{I}$.

Esimerkki 7.12. Olkoon $J = \langle xy, x(x - y)\rangle$, $J \in k[x, y]$. Määritetään $\mathbb{V}(J)$ ja osoitetaan, että $\sqrt{J} = \langle x\rangle$.

Ideaalin varisto $\mathbb{V}(J)$ on joukko pisteitä, joilla $xy = x(x - y) = 0$, eli $\mathbb{V}(J) = \{(0, t)\}$, missä $t \in k$. Voidaan siis merkitä, että $t = x$, jolloin $\mathbb{I}(\mathbb{V}(J)) = \langle x\rangle$. Lauseen 7 nojalla $\sqrt{J} = \langle x\rangle$.

Lause 7.13 (Jaottomuus)**.** *(Vrt. [1, s. 153, 179].) Jokainen polynomi $f \in k[x_1, \ldots, x_n]$, joka ei ole vakio, voidaan kirjoittaa jaottomien polynomien tulona: $f = f_1 \cdot f_1 \cdots f_r$. Lisäksi, jos $f = g_1 \cdot g_2 \cdots g_s$ on polynomin toinen ositus, niin $r = s$ ja kaikki g_i:t voidaan permutoida sellaiseen muotoon, että ne ovat f_i:n moninkertoja, eli f_i kerrottuna vakiolla.*

Polynomin sanotaan olevan *jaoton*, jos sillä on seuraava ominaisuus: jos $f = g \cdot h$, niin jompikumpi, g tai h, on vakio. Edellisen lauseen nojalla pääideaalin, eli yhden polynomin generoiman ideaalin ositus on yksikäsitteinen, lukuunottamatta vakiokertoimia.

Lause 7.14. *(Ks. [1, s. 180] Olkoon $f \in k[x_1, \ldots, x_n]$ ja $I = \langle f\rangle$ funktion f generoima pääideaali. Jos $f = cf_1^{a_1} \cdots f_r^{a_r}$ on f:n ositus jaottomiin polynomitekijöihin, niin*

$$\sqrt{I} = \sqrt{\langle f\rangle} = \langle f_1 f_2 \cdots f_r\rangle.$$

Todistus. Osoitetaan ensin, että $f_1 f_2 \ldots f_r$ kuuluu radikaaliin $\sqrt{I}$. Olkoon N suurempi kuin potenssien $a_1, \ldots, a_r$ maksimi. Tällöin

$$(f_1 f_2 \cdots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} f$$

on polynomi, joka on f:n monikerta. Tämä osoittaa, että $(f_1 f_2 \cdots f_r)^N \in I$, mistä seuraa että $f_1 f_2 \cdots f_r \in \sqrt{I}$. Siispä $\langle f_1 f_2 \cdots f_r\rangle \in \sqrt{I}$.

Oletetaan sitten, että $g \in \sqrt{I}$. Nyt on olemassa positiivinen kokonaisluku M jolla $g^M \in I$. Tällöin on myös $g^M = h \cdot f$, jollain polynomilla h. Olkoon $g =$

$g_1^{b_1} g_2^{b_2} \cdots g_s^{b_s}$ polynomin g:n ositus jaottomien polynomien tuloksi. Tällöin $g^M = g_1^{b_1 M} g_2^{b_2 M} \cdots g_s^{b_s M}$ on polynomin g^M ositus jaottomien polynomien tuloksi ja niinpä

$$g_1^{b_1 M} g_2^{b_2 M} \cdots g_s^{b_s M} = h \cdot f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r}.$$

Koska lauseen 7.13 nojalla ositus on yksikäsitteinen, lukuunottamatta vakiokertoimia, on jokaisen polynomin f_i oltava jonkin g_i:n moninkerta, kerrottuna vakiolla. Niinpä g on joukon $f_1 f_2 \cdots f_r$ moninkerta ja sisältyy siten ideaaliin $\langle f_1 f_2 \cdots f_r \rangle$, mikä todistaa väitteen. □

Määritelmä 7.15. (Ks. [1, s. 180].) Jos $f \in k[x_1, \ldots, x_n]$ on polynomi, niin määritellään f:n *reduktio*, merkitään f_{red}, mikä on polynomi, jolla $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. Polynomin sanotaan olevan *neliövapaa*, jos $f = f_{red}$.

8 Ideaalien laskuoperaatiot

Tässä osiossa käsitellään ideaalien summaa, tuloa ja leikkausta, jotka kukin tuottavat uuden ideaalin. Tarkastellaan myös radikaalien laskutoimituksia ja ideaalien osamäärää, johon tarvitaan Zariskin sulkeumaa.

8.1 Ideaalien summa

Määritelmä 8.1. Ideaalien summa (Ks. [1, s. 183].) Olkoon $I, J \subset k[x_1, \ldots, x_n]$ ideaaleja. Tällöin niiden *summa* on joukko

$$I + J = \{f + g \colon f \in I \text{ ja } g \in J\}.$$

Lause 8.2. *(Ks. [1, s. 183].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin myös niiden summa $I + J$ on ideaali renkaassa $k[x_1, \ldots, x_n]$. Summa $I + J$ on pienin ideaali, joka sisältää ideaalit I ja J. Edelleen, jos $I = \langle f_1, \ldots, f_r \rangle$ ja $J = \langle g_1, \ldots, g_s \rangle$, niin $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Todistus. Huomataan ensin, että $0 = 0+0 \in I+J$. Olkoon $h_1, h_2 \in I+J$. Määritelmän 8.1 mukaan on olemassa polynomit $f_1, f_2 \in I$ ja $g_1, g_2 \in J$, joilla $h_1 = f_1 + g_1, h_2 = f_2 + g_2$. Tällöin myös $h_1 + h_2 = f_1 + f_2 + g_1 + g_2$ josta ideaalin määritelmän nojalla nähdään, että $f_1 + f_2 \in I$ ja $g_1 + g_2 \in J$, eli $h_1 + h_2 \in I + J$.

Olkoon sitten $h \in I + J$ ja olkoon $l \in k[x_1, \ldots, x_n]$ mielivaltainen polynomi. Tällöin on määritelmän mukaan olemassa polynomit $f \in I$ ja $g \in J$, joilla $h = f + g$. Tästä seuraa, että $l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g$, jolloin $l \cdot f \in I$ ja $l \cdot g \in J$, koska I ja J ovat ideaaleja. Näin ollen $l \cdot h \in I + J$, joten $I + J$ on ideaali.

Jos $I \subset J$ ja $J \subset H$, niin H:n täytyy sisältää kaikki alkiot $f \in I$ ja $g \in J$. Koska H on ideaali, niin H sisältää myös kaikki summat $f + g$, missä $f \in I$ ja $g \in J$. Erityisesti $I + J \subset H$. Näin ollen ideaali, joka sisältää ideaalit I ja J sisältää summan $I + J$ ja niinpä $I + J$ on pienin tällainen ideaali. Lisäksi jos $I = \langle f_1, \ldots, f_r \rangle$ ja $J = \langle g_1, \ldots, g_s \rangle$, niin $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ on ideaali, joka sisältää ideaalit I ja J ja $I + J \subset \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$, mikä todistaa myös niiden yhtäsuuruuden, eli $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

Lause 8.3. *(Ks. [1, s. 184].) Jos $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, niin tällöin*

$$\langle f_1, \ldots, f_r \rangle = \langle f_1 \rangle + \cdots + \langle f_r \rangle.$$

Todistus. Ideaalien summan määritelmän nojalla summa $\langle f_1 \rangle + \cdots + \langle f_r \rangle$ on ideaali ja se on muotoa $\langle f_1, \ldots, f_r \rangle$, mikä todistaa väitteen. □

Lause 8.4. *(Ks. [1, s. 184].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$.*

Todistus. Jos $x \in \mathbb{V}(I+J)$, niin $x \in \mathbb{V}(I)$, sillä $I \subset I+J$. Sama pätee, kun $x \in \mathbb{V}(J)$. Siispä myös $x \in \mathbb{V}(I) \cap \mathbb{V}(J)$, josta seuraa, että $\mathbb{V}(I+J) \subset \mathbb{V}(I) \cap \mathbb{V}(J)$.

Oletetaan sitten, että $x \in \mathbb{V}(I) \cap \mathbb{V}(J)$. Olkoon $h \in I+J$, mikä tahansa polynomi. Tällöin on olemassa polynomi $f \in I$ ja $g \in J$, joilla $h = f+g$. Tällöin $f(x) = 0$, koska $x \in \mathbb{V}(I)$ ja $g(x) = 0$, koska $g \in V(J)$. Niinpä siis $h(x) = f(x)+g(x) = 0$. Polynomin h mielivaltaisuuden nojalla $x \in \mathbb{V}(I+J)$. Siispä myös $\mathbb{V}(I) \cap \mathbb{V}(J) \subset \mathbb{V}(I+J)$. □

Esimerkki 8.5. Yleisesti polynomirenkaassa $k[x_1, \ldots, x_n]$ ei päde väite

$$\sqrt{I+J} = \sqrt{I} + \sqrt{J}.$$

Jos esimerkiksi $I = \langle x \rangle$ ja $J = \langle x - y^2 \rangle$ renkaassa $\mathbb{R}[x, y]$, niin $\sqrt{\langle x \rangle + \langle x - y^2 \rangle} = \sqrt{\langle x, y^2 \rangle} = \langle x, y \rangle \neq \sqrt{\langle x \rangle} + \sqrt{\langle x - y^2 \rangle} = \langle x \rangle + \langle x - y^2 \rangle = \langle x, y^2 \rangle$.

8.2 Ideaalien tulo

Lauseessa 2.24 todettiin, että

$$V(f_1, \ldots, f_r) \cup V(g_1, \ldots, g_s) = V(f_i g_j, 1 \leq i \leq r, 1 \leq j \leq s)$$

ja tarkasteltiin (x, y)-tason ja z-akselin yhdistettä.

Määritelmä 8.6. (Ks. [1, s. 185].) Jos I ja J ovat ideaaleja polynomirenkaassa, niin niiden *tulo*, jota merkitään $I \cdot J$ tai vain IJ, määritellään polynomien $f \cdot g$ generoimaksi ideaaliksi, missä $f \in I$ ja $g \in J$. Ideaalien I ja J tulo $I \cdot J$ on joukko

$$IJ = \{f_1 g_1 + \cdots + f_r g_r \colon f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, \text{missä } r \in \mathbb{Z}_{\geq 0}\}.$$

Tarkistetaan, että IJ on ideaali.

(i) Koska $0 \in I$ ja $0 \in J$, niin huomataan, että $0 = 0 \cdot 0 \in I \cdot J$.

(ii) Olkoon $h_1, h_2 \in I \cdot J$. Tällöin $h_1 = \sum_{i=1}^{s} f_i g_i$ ja $h_2 = \sum_{i=1}^{t} \hat{f}_i \hat{g}_i$ ja $f_i, \hat{f}_i \in I, g_i, \hat{g}_i \in J$. Nyt $h_1 + h_2 = f_1 g_1 + \hat{f}_1 \hat{g}_1 + \cdots + f_s g_s + \hat{f}_t \hat{g}_t = \sum_{i=1}^{s} f_i g_i + \sum_{i=1}^{t} \hat{f}_i \hat{g}_i$, mikä on haluttua muotoa, joten $h_1 + h_2 \in IJ$.

(iii) Jos $h = f_1 g_1 + \ldots + f_r g_r \in I \cdot J$ ja p on mielivaltainen polynomi, niin

$$ph = (pf_1)g_1 + \cdots + (pf_r)g_r \in I \cdot J$$

sillä $pf_i \in I$ kaikilla $i, 1 \leq i \leq r$.

Ideaalien tulo vastaa geometrisesti varistojen yhdisteen ottamista, kuten seuraavassa lauseessa todetaan.

Lause 8.7. *(Ks. [1, s. 185].)*
Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin $\mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

Todistus. Olkoon $x \in \mathbb{V}(I \cdot J)$. Tällöin $g(x)h(x) = 0$ kaikilla $g \in I$ ja kaikilla $h \in J$. Jos $g(x) = 0$ kaikilla $g \in I$, niin $x \in \mathbb{V}(I)$. Jos $g(x) \neq 0$ jollain $g \in I$, niin tällöin täytyy olla $h(x) = 0$ kaikilla $h \in J$. Kummassakin tapauksessa $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$.

Oletetaan sitten, että $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$. Nyt joko $g(x) = 0$ kaikilla $g \in I$ tai $h(x) = 0$ kaikilla $h \in J$. Siispä $g(x)h(x) = 0$ kaikilla $g \in I$ ja $h \in J$. Näin ollen $f(x) = 0$ kaikilla $f \in I \cdot J$ ja niinpä $x \in \mathbb{V}(I \cdot J)$. □

Esimerkki 8.8. Radikaaleille ei välttämättä päde $\sqrt{I} \cdot \sqrt{J} = \sqrt{IJ}$. Esimerkkinä tästä olkoon $I = J = 2Z$ ideaali, $I, J \subset \mathbb{Z}$. Nyt $\sqrt{2\mathbb{Z} \cdot 2\mathbb{Z}} = \sqrt{4Z} = 2Z \neq \sqrt{2Z} \cdot \sqrt{2Z} = 2Z \cdot 2Z = 4Z$.

8.3 Ideaalien leikkauksista

Määritelmä 8.9. (Ks. [1, s. 186].) Renkaan $k[x_1, \ldots, x_n]$ ideaalien I ja J *leikkaus* $I \cap J$ on sellaisten polynomien joukko, jotka kuuluvat molempiin ideaaleihin I ja J.

Lause 8.10. *(Ks. [1, s. 186].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin leikkaus $I \cap J$ on myös ideaali.*

Todistus. Huomataan ensin, että $0 \in I \cap J$, sillä $0 \in I$ ja $0 \in J$.
Jos polynomit $f, g \in I \cap J$, niin tällöin $f + g \in I$, sillä $f, g \in I$. Samaten myös $f + g \in J$ sekä $f + g \in I \cap J$.
Olkoon $f \in I \cap J$ ja $h \in k[x_1, \ldots, x_n]$ mikä tahansa polynomi renkaasta. Koska $f \in I$ ja I on ideaali, niin $h \cdot f \in I$. Samaten myös $h \cdot f \in J$ joten $h \cdot f \in I \cap J$. □

Huomautus 8.11. (Ks. [1, s. 186].) Huomataan, että aina pätee $IJ \subset I \cap J$, sillä kaikki IJ:n alkiot ovat muotoa fg, missä $f \in I$ ja $g \in J$. Leikkauksessa taas molemmat kuuluvat sekä I:hin, että J:hin.

Ideaalien leikkauksen generaattorien määrittäminen ei ole yhtä suoraviivaista, kuin ideaalien summan ja -tulon tapauksissa. Kun polynomit f ja g ovat jaottomia, on generaattoreihin jako yksinkertaisempaa. Yleisessä tapauksessa generaattoreiden määrittämiseksi voidaan käyttää menetelmää, jota on sivuttu eliminaatiolauseen yhteydessä. Olkoon I ideaali renkaassa $k[x_1, \ldots, x_n]$ ja $f(t) \in k[t]$ yhden muuttujan t polynomi. Tällöin fI merkitsee ideaalia renkaassa $k[x_1, \ldots, x_n, t]$, joka on polynomien $f \cdot h \colon h \in I$ generoima. Nyt siis $f(t)$ ja $k[t]$ kuuluvat eri renkaisiin, eikä ideaali $I \subset k[x_1, \ldots, x_n]$ ole ideaali renkaassa $k[x_1, \ldots, x_n, t]$, sillä se ei ole suljettu, kun kerrotaan t:llä. Polynomi $f \in k[t]$kirjoitetaan $f = f(t)$, kun halutaan korostaa, että se on vain yhden muuttujan polynomi. Samoin polynomi $h \in k[x_1, \ldots, x_n]$ kirjoitetaan $h = h(x)$, kun halutaan korostaa, että se sisältää vain muuttujia $x_1, \ldots, x_n$. Samoin voidaan korostaa polynomin $g \in k[x_1, \ldots, x_n, t]$ muuttujia molemmista renkaista kirjoittamalla $g = g(x, t)$. Tällöin käytetään merkintätapaa $fI = f(t)I = \langle f(t)h(x) \colon h(x) \in I \rangle$.

Lause 8.12. *(Ks. [1, s. 187].) Olkoon I polynomien $p_1(x), \ldots, p_r(x)$ generoima ideaali renkaassa $k[x_1, \ldots, x_n, t]$. Tällöin*

(i) $f(t)I$ *on polynomien* $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$ *generoima.*

(ii) Jos $g(x,t) \in f(t)I$ *ja* $a \in k$*, niin* $g(x,a) \in I$*.*

Todistus. Ensimmäisen kohdan todistamiseksi huomataan, että mikä tahansa polynomi muotoa $g(x,t) \in f(t)I$ voidaan ilmaista muodossa, jossa se on termien $h(x,t) \cdot f(t) \cdot p(x)$ summa, sillä $h \in k[x_1, \ldots, x_n, t]$ ja $p \in I$. Mutta koska I on polynomien $p_1, \ldots, p_r$ generoima voidaan polynomi $p(x)$ ilmaista termien $q_i(x)p_i(x)$, $1 \leq i \leq r$ summana. Eli

$$p(x) = \sum_{i=1}^{r} q_i(x)p_i(x).$$

Joten

$$h(x,t) \cdot f(t) \cdot p(x) = \sum_{i=1}^{r} h(x,t)q_i(x)f(t)p_i(x).$$

Nyt jokaisella $i, 1 \leq i \leq r$ pätee $h(x,t) \cdot q_i(x) \in k[x_1, \ldots, x_n, t]$. Siispä $h(x,t) \cdot f(t) \cdot p(x)$ kuluu ideaaliin renkaassa $k[x_1, \ldots, x_n, t]$, joka on polynomien $f(t) \cdot p_1(x), \ldots, f(t)p_r(x)$ generoima. Ja koska $g(x,t)$ on sellaisten termien summa, niin

$$g(x,t) \in \langle f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x) \rangle,$$

mikä todistaa kohdan (i). Kohta (ii) seuraa suoraan kohdasta (i), kun sijoitetaan $a \in k$ muuttujan t paikalle. □

Lause 8.13. *(Ks. [1, s. 191].) Jos I ja J ovat ideaaleja missä tahansa renkaassa, niin*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Todistus. Oletetaan ensin, että $f \in \sqrt{I \cap J}$, jolloin $f^m \in I \cap J$, jollain kokonaisuvulla $m > 0$. Koska nyt $f^m \in I$, niin $f \in \sqrt{I}$. Samoin $f \in \sqrt{J}$. Ja niinpä $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

Oletetaan sitten, että $f \in \sqrt{I} \cap \sqrt{J}$. Nyt on olemassa sellaiset kokonaisluvut $m, p > 0$, joilla $f^m \in I$ ja $f^p \in J$. Siispä $f^{m+p} \in I \cap J$, joten $f \in \sqrt{I \cap J}$. □

Lause 8.14. *(Ks. [1, s. 187].) Olkoon I, J ideaaleja renkaassa* $k[x_1, \ldots, x_n]$*. Tällöin*

$$I \cap J = (tI + (1-t)J) \cap k[x_1, \ldots, x_n].$$

Todistus. Huomataan ensin, että $tI + (1-t)J$ on ideaali renkaassa $k[x_1, \ldots, x_n, t]$. Oletetaan ensin, että $f \in I \cap J$. Koska $f \in I$ pätee $t \cdot f \in tI$. Vastaavasti, koska $f \in J$, siitä seuraa että $(1-t) \cdot f \in (1-t)J$. Siispä $f = t \cdot f + (1-t) \cdot f \in tI + (1-t)J$. Koska $I, J \in k[x_1, \ldots, x_n]$ pätee, että $f \in (tI + (1-t)J) \cap k[x_1, \ldots, x_n]$. Tämä osoittaa, että $I \cap J \subset (tI + (1-t)J) \cap k[x_1, \ldots, x_n]$.

Oletetaan sitten, että $f \in (tI + (1-t)J) \cap k[x_1, \ldots, x_n]$. Tällöin $f(x) = g(x,t) + h(x,t)$, missä $g(x,t) \in tI$ ja $h(x,t) \in (1-t)J$. Olkoon ensin $t = 0$. Koska jokainen tI on t:n moninkerta ja niinpä $g(x,0) = 0$. Siispä $f(x) = h(x,0)$ ja niinpä $f(x) \in J$ seurauslauseen 8.12 nojalla. Toisaalta jos asetetaan $t = 1$, niin relaatio $f(x) =$

$g(x,t) + h(x,t)$. Ja koska jokainen $(1-t)J$:n tekijä on $1-t$:n moninkerta, saadaan $h(x,1) = 0$. Siispä $f(x) = g(x,1)$, jolloin $f(x) \in I$ seurauslauseen 8.12 nojalla. Ja nyt f kuuluu ideaaleihin I ja J, jolloin $(tI + (1-t)J) \cap k[x_1, \ldots, x_n] \subset I \cap J$, mikä todistaa väitteen. □

Lauseesta 8.14 ja eliminaatiolauseesta, eli lause 5.2 saadaan algoritmi ideaalien leikkausten laskemiseksi. Jos $I = \langle f_1, \ldots, f_r \rangle$ ja $J = \langle g_1, \ldots, g_s \rangle$ ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin tarkastellaan ideaalia

$$\langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle \in k[x_1, \ldots, x_n, t]$$

ja lasketaan sille Gröbnerin kanta aakkosellisen monomijärjestyksen mukaan, missä $t > x_i$. Ne tekijät, jotka eivät sisällä muuttujaa t muodostavat kannan, joka on itseasiassa Gröbnerin kanta, ideaalille $I \cap J$.

Esimerkki 8.15. (Ks. [1, s. 188].) Esimerkkinä tästä ideaalien $I = \langle x^2 y \rangle$ ja $J = \langle xy^2 \rangle$, $IJ \in \mathbb{Q}[x,y]$ leikkaus. Nyt siis tarkastellaan ideaalia

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

renkaassa $k[t,x,y]$. Kun lasketaan generaattoreiden S-polynomi, niin saadaan $tx^2y^2 - (tx^2y^2 - x^2y^2) = x^2y^2$. Nyt $\{tx^2, txy^2 - xy^2, x^2y2\}$ on ideaalin $(tI+(1-t)J$ Gröbnerin kanta monomijärjestyksen mukaan, missä $t > x > y > z$, sillä $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle tx^2y, txy^2, x^2 \rangle = \langle tx^2y, txy^2 \rangle = \langle LT(I) \rangle$. Eliminaatioteorian nojalla $\{x^2y^2\}$ on Gröbnerin kanta ideaalille $(tI + (1-t)J) \cap \mathbb{Q}[x,y]$. Siispä

$$I \cap J = \langle x^2 y^2 \rangle.$$

Määritelmä 8.16. (Ks. [1, s. 189].) Polynomia $h \in k[x_1, \ldots, x_n]$ sanotaan polynomien $f, g \in k[x_1, \ldots, x_n]$ pienimmäksi yhteiseksi jakajaksi ja merkitään $h = LCM(f,g)$ jos

(i) f ja g jakavat h:n.

(ii) h jakaa kaikki sellaiset polynomit, jotka sekä g että f jakavat.

Lause 8.17. *(Ks. [1, s. 189].)*

(i) Kahden pääideaalin, $I, J \subset k[x_1, \ldots, x_n]$ leikkaus $I \cap J$ on pääideaali.

(ii) Jos $I = \langle f \rangle$, ja $J = \langle g \rangle$ ja $I \cap J = \langle h \rangle$, niin

$$h = LCM(f,g).$$

Todistus. (Vrt. [1, s. 191])

(i) Olkoon $I, J \subset k[x_1, \ldots, x_n]$ pääideaaleja, eli ne ovat muotoa $I = \langle f \rangle$ ja $J = \langle g \rangle$. Tällöin jos $h \in I \cap J$, niin $h \in \langle f \rangle$ ja $h \in \langle g \rangle$. Niinpä ideaalin $I \cap J$ täytyy olla muotoa $\langle h \rangle$, eli pääideaali.

(ii) Oletetaan ensin, että $p = LCM(f, g)$, jolloin se on muotoa $p = u_1 f$ ja $p = u_2 g$, joillain polynomeilla $u_1, u_2 \in k[x_1, \ldots, x_n]$, sillä f ja g jakavat p:n. Tästä seuraa, että $p \in \langle f \rangle = I$ ja $p \in \langle g \rangle = J$, joten $p \in I \cap J$.
Oletetaan sitten, että $p \in I \cap J$. Tällöin $p \in I = \langle f \rangle$ ja $p \in J = \langle g \rangle$, jolloin p on muotoa $p = h_1 f$ ja $p = h_2 g$, joillain $h_1, h_2 \in k[x_1, \ldots, x_n]$. Nyt f ja g jakavat p:n ja koska p jakaa kaikki polynomit, jotka f ja g jakavat, joten $p = h = LCM(f, g)$.

□

Näin ideaalien leikkausten algoritmista saadaan myös algoritmi kahden polynomin pienimmän yhteisen tekijän määrittämiseksi laskemalla $\langle f \rangle \cap \langle g \rangle$ ideaalien leikkausten algoritmilla.

Määritelmä 8.18. (Ks. [1, s. 41].) Polynomien $f, g \in k[x]$ suurin yhteinen tekijä on polynomi h, jolle pätee seuraavat ominaisuudet

1. h jakaa polynomit f ja g.

2. Jos p on sellainen polynomi, joka jakaa polynomit f ja g, niin polynomi p jakaa myös polynomin h.

Tällöin merkitään $h = GCD(f, g)$.

Lause 8.19. *(Ks. [1, s. 190].) Olkoon $f, g \in k[x_1, \ldots, x_n]$. Tällöin*

$$LCM(f, g) \cdot GCD(f, g) = fg.$$

Edellistä lausetta voidaan hyödyntää myös suurimman yhteisen tekijän (GCD) laskemiseen

$$GCD(f, g) = \frac{f \cdot g}{LCM(f, g)}$$

kun on ensin laskettu LCM ideaalien avulla.

Lause 8.20. *(Ks.[1, s. 190].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.*

Todistus. Olkoon $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$. Tällöin $x \in \mathbb{V}(I)$ tai $x \in \mathbb{V}(J)$. Tämä tarkoittaa, että joko $f(x) = 0$ kaikilla $f \in I$ tai $f(x) = 0$ kaikilla $f \in J$, eli $f \in I \cap J$. Tällöin $x \in V(I \cap J)$. Niinpä $\mathbb{V}(I) \cup \mathbb{V}(J) \subset \mathbb{V}(I \cap J)$.

Toisaalta huomatuksessa 8.11 todettiin, että $IJ \subset I \cap J$, joten $\mathbb{V}(I \cap J) \subset \mathbb{V}(IJ)$ lauseen 4.8 nojalla. Lauseessa 8.7 on todistettu, että $\mathbb{V}(IJ) = \mathbb{V}(I) \cup \mathbb{V}(J)$, eli $\mathbb{V}(I \cap J) \subset \mathbb{V}(I) \cup \mathbb{V}(J)$. □

Esimerkki 8.21. Osoitetaan, että $\sqrt{IJ} = \sqrt{I \cap J}$.

Jos $f \in \sqrt{IJ}$, niin $f^m \in IJ$, Huomautuksen 8.11 nojalla aina pätee $IJ \subset I \cap J$ ja ollaan todettu, että aina $I \subset \sqrt{I}$, joten $\sqrt{IJ} = \sqrt{I \cap J}$.
Nyt väite pätee molempiin suuntiin, sillä vahvan nollakohtalauseen nojalla $\sqrt{I \cap J} = \mathbb{I}(\mathbb{V}(I \cap J))$. Tämä on taas edellisen lauseen nojalla $\mathbb{I}(\mathbb{V}(I \cap J)) = \mathbb{I}(\mathbb{V}(I) \cup \mathbb{V}(J))$. Lauseen 8.7 nojalla ideaalien varistojen yhdiste on sama, kuin ideaalien tulon varisto, joten $\mathbb{I}(\mathbb{V}(I) \cup \mathbb{V}(J)) = \mathbb{I}(\mathbb{V}(IJ)) = \sqrt{IJ}$.

Esimerkki 8.22. Olkoon I ja J ideaaleja renkaassa $k[x_1, \ldots, x_n]$. Osoitetaan, että tällöin

$$(I_1 + I_2)J = I_1J + I_2J.$$

Olkoon ensin $f \in (I_1 + I_2)J$, jolloin $f = (g_1 + g_2)j$, joillain polynomeilla $g_1 \in I_1, g_2 \in I_2, j \in J$. Nyt $(g_1 + g_2)j = g_1h + g_2j \in I_1J + I_2J$, joten $(I_1 + I_2)J \subset I_1J + I_2J$.

Toisaalta jos $f \in I_1J + I_2J$, niin $f = g_1j_1 + g_2j_2, g_1 \in I_1, g_2 \in I_2, j_1 \in J, j_2 \in J$. Tällöin $j_1 = a_1h_1 + \cdots + a_nh_n$ ja $j_2 = b_1h_1 + \cdots + b_kh_k$. Oletetaan esimerkiksi, että $k \geq n$. Nyt $f = g_1(a_1h_1 + \cdots + a_nh_n) + g_2(b_1h_1 + \cdots + b_kh_k) = (g_1a_1 + g_2b_1)h_1 + \cdots + (g_1a_n + g_2b_n)h_n + g_2b_{n+1}h_{n+1} + \cdots + g_2b_kh_k$, jolloin summan jokainen termi kuuluu ideaaliin $(I_1 + I_2)J$, joten $f \in (I_1 + I_2)J$ ja siis $I_1J + I_2J \subset (I_1 + I_1)J$.

Esimerkki 8.23. Olkoon $I_1, \ldots, I_r$ ideaaleja renkaassa $k[x_1, \ldots, x_n]$. Osoitetaan, että $(I_1 \cdots I_r)^m = I_1^m \cdots I_r^m$.
Osoitetaan ensin induktiolla aputulos: $(I_1 \cdot I_2)^m = I_1^m \cdot I_2^m$. Olkoon ensin $m = 1$, jolloin $(I_1 \cdot I_2)^1 = I_1 \cdot I_2$. Tehdään sitten induktio-oletus, että väite pätee, kun $(I_1 \cdot I_2)^m = I_1^m \cdot I_2^m$, jolloin $(I_1 \cdot I_2)^{m+1} = I_1^m \cdot I_2^m \cdot I_1 \cdot I_2$. Nyt induktio-oletuksen nojalla $(I_1 \cdot I_2)^m = I_1^m \cdot I_2^m \cdot I_1 \cdot I_2$. Koska ideaalien tulolle pätee määritelmän nojalla $I \cdot J = J \cdot I$, niin $(I_1 \cdot I_2)^m = I_1^m \cdot I_1 \cdot I_2^m \cdot I_2 = I_1^{m+1} \cdot I_2^{m+1}$, mikä osoittaa, että $(I_1 \cdot I_2)^{m+1} = I_1^m \cdot I_2^m$.
Todistetaan sitten varsinainen tulos induktiolla r:n suhteen. Olkoon ensin $r = 1$, jolloin $I_1^1 = I_1$. Oletetaan sitten, että $(I_1 \cdots I_r)^m = I_1^m \cdots I_r^m$. Nyt $(I_1 \cdot \ldots \cdot I_{r+1})^m = ((I_1 \cdots I_r) \cdot I_{r+1})^m = (\hat{I} \cdot I_{r+1})^m = \hat{I}^m \cdot I_{r+1}^m$, missä $\hat{I} = (I_1 \cdot \ldots \cdot I_r)$ ja viimeisin yhtäsuuruus pätee alussa todistetun aputuloksen nojalla.
Nyt siis $\hat{I}^m \cdot I_{r+1}^m = (I_1 \cdot \ldots \cdot I_r)^m \cdot I_{r+1}^m$, joka voidaan induktio-oletuksen nojalla kirjoittaa $(I_1 \cdot \ldots \cdot I_r)^m \cdot I_{r+1}^m = I_1^m \cdot \ldots \cdot I_r^m \cdot I_{r+1}^m$. Induktioperiaatteen nojalla väite on tosi, eli $(I_1 \cdots I_r)^m = I_1^m \cdots I_r^m$.

Esimerkki 8.24. Olkoon I ja J ideaaleja renkaassa $k[x_1, \ldots, x_n]$. Osoitetaan, että jos $I^l \subset J$, jollain kokonaisluvulla $l > 0$, niin $\sqrt{I} \subset \sqrt{J}$.

Koska $I \subset \sqrt{I}$ ja $I^l \subset I$, niin saadaan inkluusiot

$$I^l \subset I \subset \sqrt{I} \subset J \subset \sqrt{J}.$$

8.4 Zariskin sulkeuma ja ideaalien osamäärä

Kaikki joukot eivät ole varistoja ja kuten on jo todettu ei varistojen erotus välttämättä ole varisto. Olipa joukko $S \subset k^n$ varisto tai ei, niin sille voidaan määritellä Zariskin sulkeuma.

Lause 8.25. *Joukko*

$$\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] \colon f(a) = 0,\ \forall a \in S\}$$

on ideaali renkaassa $k[x_1, \ldots, x_n]$.

Todistus. (1) Selvästi $0 \in S$.

(2) Jos $f, g \in \mathbb{I}(S)$, niin $f(a) + g(a) = 0$, kaikilla a, joten $f(a) + g(a) \in \mathbb{I}(S)$.

(3) Jos $f(a) \in \mathbb{I}(S)$ ja $h \in k[x_1, \ldots, x_n]$, niin $hf(a) = 0$, joten $hf \in \mathbb{I}(S)$, eli $\mathbb{I}(S)$ on ideaali.

□

Lisäksi $\mathbb{I}(S)$ on radikaali, sillä jos $f(a) = 0$, niin $(f(a))^m = 0$ kaikilla $m \in \mathbb{Z}_{\geq 0}$. Hilbertin vastaavuuden nojalla $\mathbb{V}(\mathbb{I}(S))$ on varisto ja seuraavan lauseen nojalla pienin mahdollinen varisto, joka sisältää joukon S.

Lause 8.26. *(Ks. [1, s. 193].) Jos* $S \subset k^n$*, niin varisto* $\mathbb{V}(\mathbb{I}(S))$ *on pienin varisto, joka sisältää joukon S, eli jos* $W \subset k^n$ *on mikä tahansa varisto, joka sisältää joukon S, niin* $\mathbb{I}(\mathbb{V}(S)) \subset W$.

Todistus. Jos $S \subset W$, niin $\mathbb{I}(W) \subset \mathbb{I}(S)$, mutta tällöin $\mathbb{V}(\mathbb{I}(S)) \subset \mathbb{V}(\mathbb{I}(W))$ lauseen 7.9 nojalla. Koska W on varisto, niin $\mathbb{V}(\mathbb{I}(W)) = W$ myös lauseen 7.9 nojalla, mistä väite seuraa. □

Määritelmä 8.27. (Ks. [1, s. 193].) Affiinin avaruuden joukon *Zariskin sulkeuma* on pienin affiini varisto, joka sisältää joukon $S \subset k^n$. Jos $S \subset k^n$, niin joukon S Zariskin sulkeumaa merkitään $\overline{S}$:llä ja se on yhtenevä joukon $\mathbb{V}(\mathbb{I}(S))$ kanssa.

Huomataan myös, että $\mathbb{I}(\overline{S}) = \mathbb{I}(S)$, sillä $\mathbb{I}(\overline{S}) \subset \mathbb{I}(S)$, koska $S \subset \overline{S}$. Toisaalta, jos $f \in \mathbb{I}(S)$, niin $S \subset V(f)$. Tällöin $S \subset \overline{S} \subset V(f)$ Zariskin sulkeuman määritelmän nojalla, joten $f \in \mathbb{I}(\overline{S})$. Yksi esimerkki Zariskin sulkeumasta on eliminaatioideaalit.

Lause 8.28. *(Ks. [1, s. 193].) Olkoon* k *algebrallisesti suljettu kunta. Oletetaan, että* $V = \mathbb{V}(f_1, \ldots, f_s) \subset k^n$ *ja olkoon* $\pi_l \colon k^n \to k^{n-l}$ *projektiokuvaus viimeisille* $n - l$*:lle muuttujalle. Jos* I_l *on* l*:s eliminaatioideaali* $I_l = \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n]$*, niin tällöin* $\mathbb{V}(I_l)$ *on joukon* $\pi_l(V)$ *Zariskin sulkeuma, jolloin* $\pi_l(V) = \mathbb{V}(I_l)$.

Todistus. Kuten lauseesta 8.26 nähdään, täytyy todistaa, että $\mathbb{V}(I_l) = \mathbb{V}(\mathbb{I}(\pi_l(V)))$. Seurauslauseen 5.14 nojalla $\pi_l(V) \subset \mathbb{V}(I_l)$. Koska $\mathbb{V}(\mathbb{I}(\pi_l(V)))$ on pienin varisto, joka sisältää joukon $\pi_l(V)$, niin $f \in \mathbb{I}(\pi_l(V))$ eli $f(a_{l+1}, \ldots, a_n) = 0$ kaikilla $(a_{l+1}, \ldots, a_n) \in \pi_l(V)$. Tällöin, kun sen huomataan olevan renkaan $k[x_1, x_2, \ldots, x_n]$ osa, pätee $f(a_1, a_2, \ldots, a_n) = 0$ kaikilla $(a_1, \ldots, a_n) \in V$. □

On jo todettu, ettei varistojen erotus ole välttämättä varisto. Olkoon nyt $V = \mathbb{V}(I)$, missä $I = z$ ja $W = \mathbb{V}(K)$, missä $K = \langle xz, yz \rangle \subset k[x, y, z]$. Eli V on xy- taso ja K on yhdiste xy- tasosta ja z-akselista. Nyt erotus $W - V$ on z-akseli, josta on otettu pois origo, sillä origo kuuluu xy-tasoon. Nyt z-akseli, eli varisto $\mathbb{V}(x, y)$ on pienin varisto, joka sisältää joukon $W - V$.

Lause 8.29. *(Ks. [1, s. 194].) Jos V ja W ovat varistoja, joilla $V \subset W$, niin $W = V \cup (\overline{W - V})$.*

Todistus. Koska W sisältää joukon $W - V$ ja W on varisto, niinpä myös pienin mahdollinen varisto, joka sisältää joukon $W - V$ sisältyy W:en. Siispä $(\overline{W - V}) \subset W$. Oletusten mukaan $V \subset W$, joten $V \cup (\overline{W - V}) \subset W$. Toisaalta huomataan, että oletuksesta $V \subset W$ seuraa, että $W = V \cup (\overline{W - V})$. Huomataan, että $W - V \subset (\overline{W - V})$, josta seuraa, että $W \subset V \cup (\overline{W - V})$. □

Muiden laskutoimitusten tapaan tutkitaan myös variston $\overline{W - V}$ yhteyttä ideaaleihin. Siihen tarvitaan myös seuraavaa käsitettä.

Määritelmä 8.30. (Ks. [1, s. 194].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$ niin $I : J$ on joukko

$$I : J = \{f \in k[x_1, \ldots, x_n] : fg \in I \ \forall g \in J\}$$

ja sitä kutsutaan ideaalien I ja J osamääräksi.

Esimerkki 8.31. (Vrt. [1, s. 194].) Otetaan esimerkki renkaasta $k[x, y, z, t]$, missä

$$\begin{aligned}
&\langle xy, zy, ty, y^2 \rangle : \langle y \rangle \\
&\quad = \{f \in k[x, y, z, t] : f \cdot y \in \langle xy, zy, ty, y^2 \rangle\} \\
&\quad = \{f \in k[x, y, z, t] : f \cdot y = Axy + Bzy + Cty + Dy^2\} \\
&\quad = \{f \in k[x, y, z, t] : f \cdot y = Ax + Bz + Ct + Dy\} \\
&= \langle x, z, t, y \rangle.
\end{aligned}$$

Lause 8.32. *(Ks. [1, s. 194].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin $I : J$ on ideaali renkaassa $k[x_1, \ldots, x_n]$ ja $I \subset I : J$.*

Todistus. Huomataan, että jos $f \in I$, niin $fg \in I$ kaikilla $g \in k[x_1, \ldots, x_n]$ ja niinpä $fg \in J$ myös kaikilla $g \in J$, joten $I \subset I : J$.

Todistetaan sitten, että $I : J$ on ideaali. Koska $I \subset I : J$ ja $0 \in I$, niin $0 \in I : J$. Oletetaan sitten, että $f_1, f_2 \in I : J$. Tällöin $f_1 g$ ja $f_2 g$ sisältyvät ideaaliin I kaikilla $g \in J$. Ja edelleen, koska I on ideaali, niin $(f_1 + f_2)g = f_1 g + f_2 g \in I \subset I : J$ kaikilla $g \in J$. Jolloin myös $f_1 + f_2 \in I : J$. Jos $f \in I : J$ ja $h \in k[x_1, \ldots, x_n]$, niin $fg \in I$ ja koska I on ideaali, niin $hfg \in I$ kaikilla $g \in J$, joten $hf \in I : J$. □

Osoitetaan ideaalien osamäärän ja ideaalien erotuksen Zariskin sulkeuman yhtäpitävyys.

Lause 8.33. *(Ks. [1, s. 195].) Jos I ja J ovat ideaaleja renkaassa $k[x_1, \ldots, x_n]$, niin*

$$\overline{\mathbb{V}(I) - \mathbb{V}(J)} \subset \mathbb{V}(I : J).$$

Jos lisäksi k on algebrallisesti suljettu ja jos I on radikaali, niin

$$\overline{\mathbb{V}(I) - \mathbb{V}(J)} = \mathbb{V}(I : J).$$

Todistus. Nyt täytyy siis todistaa, että $I : J \subset \mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))$ Hilbertin vastaavuuden mukaan. Oletetaan, että $f \in I : J$ ja $x \in \mathbb{V}(I) - \mathbb{V}(J)$. Tällöin $fg \in I$ kaikilla $g \in J$. Koska $x \in \mathbb{V}(I)$ kaikille $g \in J$ pätee $f(x)g(x) = 0$. Nyt kuitenkin $x \notin \mathbb{V}(J)$, joten on olemassa sellainen $g \in J$, jolla $g(x) \neq 0$. Siispä $f(x) = 0$ millä tahansa $x \in \mathbb{V}(I) - \mathbb{V}(J)$). Niinpä $f \in \mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))$, mikä todistaa väitteen. Kuten lausessa 7.9 osoitettiin, $\mathbb{V}$ kääntää inkluusion järjestyksen, joten $\mathbb{V}(\mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))) \subset \mathbb{V}(I : J)$, mikä todistaa väitteen ensimmäisen osan.

Toisen osan todistamiseksi oletetaan, että k on suljettu ja $I = \sqrt{I}$. Olkoon $x \in \mathbb{V}(I : J)$, jolloin ideaalien osamäärän määritelmän perusteella

$$\text{jos } hg \in I \text{ kaikilla } g \in J, \text{ niin } h(x) = 0.$$

Olkoon nyt $h \in \mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))$. Jos $g \in J$, niin hg katoaa joukossa $\mathbb{V}(I)$, koska h katoaa joukossa $\mathbb{V}(I) - \mathbb{V}(J)$ ja $g = 0$ joukossa $\mathbb{V}(J)$. Niinpä lauseen 6.6 nojalla $hg \in \sqrt{I} = I$. Näin ollen $x \in \mathbb{V}(\mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J)))$, mistä seuraa, että

$$\mathbb{V}(I : J) \subset \mathbb{V}(\mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))),$$

mikä todistaa väitteen. □

Edellisen lauseen todistus johtaa lauseeseen, joka pätee minkä tahansa kunnan yli.

Lause 8.34. *(Ks. [1, s. 195].) Olkoon V ja W varistoja avaruudessa k^n. Tällöin*

$$\mathbb{I}(V) : \mathbb{I}(W) = \mathbb{I}(V - W).$$

Todistus. Edellisessä lauseessa osoitettiin, että $I : J \subset \mathbb{I}(\mathbb{V}(I) - \mathbb{V}(J))$. Yhdistetään tämä tulos siihen, kun $I = \mathbb{I}(V)$ ja $J = \mathbb{I}(W)$, jolloin $\mathbb{I}(V) : \mathbb{I}(W) \subset \mathbb{I}(V - W)$. Nyt koska $V - W \subset V$, niin $\mathbb{I}(V) \subset \mathbb{I}(V - W)$ ja koska $\mathbb{I}(V) \subset \mathbb{I}(V) : \mathbb{I}(W)$, niin $\mathbb{I}(V - W) \subset \mathbb{I}(V) : \mathbb{I}(W)$. □

Seuraavat ideaalien osamäärän ominaisuudet herättävät pohtimaan, mikä on niiden vastaavuus varistoilla.

Lause 8.35. *(Ks. [1, s. 196].) Olkoon I, J ja K ideaaleja renkaassa $k[x_1, \ldots, x_n]$. Tällöin*

(i) $I : k[x_1, \ldots, x_n] = I$.

(ii) $IJ \subset K$ *jos ja vain jos* $I \subset K\colon J$.

(iii) $J \subset I$ *jos ja vain jos* $I\colon J = k[x_1, \ldots, x_n]$.

Todistus. (i) Ideaalin osamäärän määritelmän mukaan

$$\begin{aligned} &I\colon k[x_1, \ldots, x_n] \\ &\quad = \{f \in k[x_1, \ldots, x_n]\colon fg \in I \ \forall g \in k[x_1, \ldots, x_n]\} \\ &\quad = \{fg \in I, \ \forall f, g \in k[x_1, \ldots, x_n]\} = I. \end{aligned}$$

(ii) Olkoon $IJ \subset K$. Jos $f \in IJ$, niin $f = hg \in K$. Nyt koska $I\colon J = \{h \in k[x_1, \ldots, x_n]\colon hg \in K \ \forall g \in J\}$, niin $f \in K\colon J$.
Olkoon sitten $I \subset K\colon J$, eli kun $f \in I$, niin $fg \in K \ \forall g \in J$, jolloin $IJ \subset K$.

(iii) Jos $I\colon J = k[x_1, \ldots, x_n]$, niin kun $g \in J$, niin $fg \in I$ kaikilla polynomeilla $f \in k[x_1, \ldots, x_n]$, jolloin $g \in I$, eli $J \subset I$.
Jos taas $J \subset I$, niin $I\colon J = \{f \in k[x_1, \ldots, x_n]\colon fg \in I \ \forall g \in I\} = k[x_1, \ldots, x_n]$ eli kaikilla polynomeilla $f \in k[x_1, \ldots, x_n]$ pätee $fg \in I$.

□

Esimerkki 8.36. Kirjoitetaan, mitä edellinen lause tarkoittaa varistojen tapauksessa muistaen että ideaalien tulo kuvautuu varistojen yhdisteeksi ja ideaalien osamäärä varistojen erotukseksi, sekä että inkluusioiden suunnat vaihtuvat.

(i) Ensimmäinen kohta on triviaali. $\mathbb{V}(I\colon k[x_1, \ldots, x_n]) = \mathbb{V}(I) - \mathbb{V}(k^n) = \mathbb{V}(I\colon \emptyset) = \mathbb{V}(I)$.

(ii) Varistojen tapauksessa siis $\mathbb{V}(K) \subset (\mathbb{V}(I) \cup \mathbb{V}(J))$ jos ja vain jos $\overline{\mathbb{V}(K) - \mathbb{V}(J)} \subset \mathbb{V}(I)$. Osoitetaan tämä.
Oletetaan ensin, että $\mathbb{V}(K) \subset (\mathbb{V}(I) \cup \mathbb{V}(J))$. Eli jos $a \in \mathbb{V}(K)$, niin $a \in \mathbb{V}(I)$ tai $a \in \mathbb{V}(J)$. Zariskin sulkeumalle pätee $\overline{\mathbb{V}(K) - \mathbb{V}(J)} \subset \mathbb{V}(K) - \mathbb{V}(J)$. Nyt jos edelleen $a \in \mathbb{V}(K)$, niin $a \in \mathbb{V}(K) - \mathbb{V}(J)$. Nyt $a \notin \mathbb{V}(J)$, joten $a \in \mathbb{V}(I)$, eli $\overline{\mathbb{V}(K) - \mathbb{V}(J)} \subset \mathbb{V}(I)$.
Oletetaan sitten, että $\overline{\mathbb{V}(K) - \mathbb{V}(J)} \subset \mathbb{V}(I)$. Eli jos $a \in \overline{\mathbb{V}(K) - \mathbb{V}(J)}$, niin $a \in \mathbb{V}(K)$, mutta $a \notin \mathbb{V}(J)$. Nyt kuitenkin $a \in \mathbb{V}(I)$, joten $a \in (\mathbb{V}(I) \cup \mathbb{V}(J))$.

(iii) $\mathbb{V}(I) \subset \mathbb{V}(J)$ jos ja vain jos $\mathbb{V}(I) - \mathbb{V}(J) = \mathbb{V}(k[x_1, \ldots, x_n]) = \emptyset$. Tämäkin kohta selvästi pätee.

8.5 Jaottomat varistot ja alkuideaalit

Kahden variston yhdiste on varisto. Kaikkia varistoja ei voida ilmaista erillisten varistojen yhdisteenä. Määritellään tällainen varisto seuraavasti.

Määritelmä 8.37. (Ks. [1, s. 198].) Varisto $V \subset k^n$ on *jaoton* jos ehdosta $V = V_1 \cup V_2$ seuraa, että $V = V_1$ tai $V = V_2$, ja $V_1 \neq \emptyset$ ja $V_2 \neq \emptyset$ ovat varistoja.

Varistoja voi olla vaikea osoittaa jaottomiksi tämän määritelmän avulla.

Määritelmä 8.38. (Ks. [1, s. 198].) Ideaali $I \subsetneq k[x_1, \ldots, x_n]$ on *alkuideaali* jos ehdosta $f, g \in k[x_1, \ldots, x_n]$ ja $fg \in I$ seuraa, että joko $f \in I$ tai $g \in I$.

Jaottomuuden todistamisessa voidaan hyödyntää sitä, että jaoton varisto ja alkuideaali vastaavat toisiaan, kuten seuraava lause sanoo.

Lause 8.39. *(Ks. [1, s. 198].) Olkoon $V \subset k^n$ varisto. Jos $V = V_1 \cup V_2, V_1 \neq \emptyset \neq V_2$, niin V on jaoton jos ja vain jos $\mathbb{I}(V)$ on alkuideaali.*

Todistus. Oletetaan ensin, että V on jaoton ja olkoon $fg \in \mathbb{I}(V)$. Nyt joukko $V_1 = V \cap V(f)$ ja $V_2 = V \cap V(g)$. Nämä ovat siis nyt varistoja, kuten on todistettu. Koska $fg \in \mathbb{I}(V)$, niin voidaan kirjoittaa, että $V = V_1 \cup V_2$. Mutta koska V on jaoton on nyt $V = V_1$ tai $V = V_2$. Oletetaan, että ensimmäinen näistä pätee, jolloin $V = V_1 = V \cap V(f)$, mistä seuraa, että f katoaa V:ssä, eli $f \in \mathbb{I}(V)$, mikä osoittaa, että $\mathbb{I}(V)$ on alkuideaali.

Oletetaan sitten, että $\mathbb{I}(V)$ on alkuideaali ja olkoon $V = V_1 \cup V_2$. Oletetaan, että $V \neq V_1$. Väite on nyt siis muotoa $\mathbb{I}(V) = \mathbb{I}(V_2)$. Huomataan, että $\mathbb{I}(V) \subset \mathbb{I}(V_2)$ sillä $V_2 \subset V$. Huomataan myös, että $\mathbb{I}(V) \subsetneq \mathbb{I}(V_1)$ sillä $V_1 \subsetneq V$. Näin ollen voidaan valita $f \in \mathbb{I}(V_1) - \mathbb{I}(V)$. Olkoon $g \in \mathbb{I}(V_2)$ mikä tahansa polynomi siitä ideaalista. Koska $V = V_1 \cup V_2$, niin fg katoaa varistossa V ja niinpä $fg \in \mathbb{I}(V)$. Mutta koska $\mathbb{I}(V)$ on alkuideaali, niin f tai g kuuluu ideaaliin $\mathbb{I}(V)$. Tiedetään, että $f \notin \mathbb{I}(V)$, joten $g \in \mathbb{I}(V)$, mikä todistaa että $\mathbb{I}(V) = \mathbb{I}(V_2)$, eli $V = V_2$, joten V on jaoton. □

Esimerkki 8.40. Osoitetaan, että jokainen alkuideaali on radikaali-ideaali. Olkoon $I \subset k[x_1, \ldots, x_n]$ alkuideaali ja olkoon $f \in \sqrt{I}$, jolloin $f^m \in I$. Koska nyt $f \cdot f^{m-1} \in I$ ja koska I on alkuideaali, niin joko $f \in I$ tai $f^{m-1} \in I$. Nyt jos $f^{m-1} \in I$, niin $f \cdot f^{m-2} \in I$. Nyt taas jos $f^{m-2} \in I$, niin joko $f \in I$ tai $f^{m-3} \in I$. Tätä voidaan toistaa, kunnes jollain kokonaisluvulla i pätee, että potenssi $m - i = 1$, jolloin $f \in I$, mikä todistaa, että $f \in I$ kaikilla $f \in \sqrt{I}$, eli I on radikaali.

Seurauslause 8.41. *(Ks. [1, s. 199].) Kun k on suljettu kunta, niin kuvaus $\mathbb{I}$ kuvaa avaruuden k^n jaottomat varistot yksikäsitteisesti polynomirenkaan $k[x_1, \ldots, x_n]$ alkuideaaleiksi.*

Todistus. Koska $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ ja koska $\mathbb{V}(I)$ on jaoton, on $\sqrt{I}$ alkuideaali. Näin ollen $\mathbb{I}$ kuvaa jaottomat varistot alkuideaaleiksi. □

Esimerkki 8.42. (Vrt. [1, s. 34, 199].) Varisto $V = \mathbb{V}(y - x^2, z - x^3)$ voidaan parametrisoida muotoon $c(t) = (t, t^2, t^3)$. Osoitetaan, että käyrän $c(t) = (t, t^2, t^3)$ ideaali $\mathbb{I}(V)$ on alkuideaali. Oletetaan, että $fg \in \mathbb{I}(V)$. Nyt siis kaikilla t pätee

$$f(t, t^2, t^3)g(t, t^2, t^3) = 0.$$

Nyt joko $f(t, t^2, t^3) = 0$ tai $g(t, t^2, t^3) = 0$, joten f tai g katoaa V:ssä, eli jompikumpi kuuluu ideaaliin $\mathbb{I}(V)$, joten $\mathbb{I}(V)$ on alkuideaali. Näin ollen vino kuutio $c(t) = (t, t^2, t^3)$ on jaoton varisto.

Seuraava lause yleistää tämän.

Lause 8.43. *(Ks. [1, s. 199].) Jos k on ääretön kunta ja $V \subset k^n$ on varisto, joka määritellään parametrisesti*

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

missä $f_1, \ldots, f_m$ ovat polynomeja renkaassa $k[t_1, \ldots, t_m]$, niin V on jaoton.

Todistus. Ohitetaan. Ks. [1, s. 199]. □

Yksinkertaisin varisto, joka saadaan parametrisoimalla, on k^n yksittäinen piste $\{(a_1, \ldots, a_n)\}$. Käyttäen edellisen lauseen notaatioita, missä jokainen f_i on vakiopolynomi $f_i(x_1, \ldots, x_n) = a_i$, $1 \leq i \leq n$. Saatu varisto on jaoton ja koska

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m) = a_1, \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m) = a_m, \end{aligned}$$

niin $\mathbb{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Ideaalilla $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ on sellainen merkittävä ominaisuus, että se on maksimaalinen. Osoitetaan tämä.

Määritelmä 8.44. (Ks. [1, s. 201].) Ideaalia $I \subset k[x_1, \ldots, x_n]$ sanotaan *maksimaaliseksi*, jos $I \neq k[x_1, \ldots, x_n]$ ja kaikille ideaaleille J, jotka sisältävät ideaalin I pätee $J = I$ tai $J = k[x_1, \ldots, x_n]$.

Lause 8.45. *(Ks. [1, s. 201].) Jos k on mikä tahansa kunta, niin ideaali $I \subset k[x_1, \ldots, x_n]$, joka on muotoa*

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

missä $a_1, \ldots, a_n \in k$, on maksimaalinen ideaali.

Todistus. Oletetaan, että J on ideaali, joka sisältää I:n, mutta $I \neq J$. Tällöin on oltava sellainen $f \in J$, jolla $f \notin I$. Jakoalgoritmin, eli lauseen 3.13, nojalla voidaan kirjoittaa f muodossa $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) + b$, jollain $b \in k$. Nyt koska $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) + b \notin I$ ja $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) \in I$, niin täytyy olla $b \neq 0$. Kuitenkin, koska $f \in J$ ja koska $I \subset J$ täytyy myös päteä, että

$$b = f - (A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n)) \in J.$$

Ja koska b ei ole nolla $1 = \frac{1}{b} \cdot b \in J$, niin $J = k[x_1, \ldots, x_n]$, eli I on maksimaalinen. □

Nyt koska

$$\mathbb{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n), \}$$

niin jokainen piste avaruudessa k^n vastaa maksimaalista ideaalia renkaassa $k[x_1, \ldots, x_n]$ ja tämä ideaali on $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Vastakkaiseen suuntaan korrelaatio pätee vain, kun k on suljettu.

Lause 8.46. *(Ks. [1, s. 202].) Jos k on mikä tahansa kunta, maksimaalinen ideaali renkaassa $k[x_1, \ldots, x_n]$ on alkuideaali.*

Todistus. Olkoon I aito ideaali, joka ei ole alkuideaali ja olkoon $fg \in I$, missä $f \notin I$ ja $g \notin I$. Tarkastellaan ideaalia $\langle f \rangle + I$. Tähän ideaaliin siis sisältyy I, mutta ne eivät ole yhtäsuuria, koska $f \notin I$. Jos nyt pätisi, että $\langle f \rangle + I = k[x_1, \ldots, x_n]$, niin $1 = cf + h$ jollain polynomilla c ja jollain $h \in I$. Jos molemmat puolet kerrottaisiin polynomilla g saataisiin $g = cfg + hg \in I$, mikä on ristiriidassa oletusten kanssa. Näin ollen $\langle f \rangle + I$ on aito ideaali, joka sisältää ideaalin I, joten I ei ole maksimaalinen. □

Seuraava lause on siitä mielenkiintoinen, että sitä olisi voitu käyttää heikon nollakohtalauseen todistamiseen. Siitä seuraa suoraan heikko nollakohtalause, sillä ne ovat saman sisältöiset.

Lause 8.47. *(Ks. [1, s. 202].) Jos k on suljettu kunta, niin jokainen maksimaalinen ideaali renkaassa $k[x_1, \ldots, x_n]$ on muotoa $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ jollain $a_1, \ldots, a_n \in k$.*

Todistus. Olkoon $I \subset k[x_1, \ldots, x_n]$ maksimaalinen ideaali. Koska määritelmän mukaan $I \neq k[x_1, \ldots, x_n]$ lauseen 6.4 nojalla $\mathbb{I}(V) \neq \emptyset$. Näin ollen on olemassa jokin piste $a_1, \ldots, a_n \in \mathbb{I}(V)$. Se tarkoittaa, että jokainen $f \in I$ katoaa pisteessä $(a_1, \ldots, a_n)$, eli $f \in \{(a_1, \ldots, a_n)\}$. Näin ollen voidaan kirjoittaa

$$I \subset \mathbb{I}(\{(a_1, \ldots, a_n)\}).$$

Nyt koska $\mathbb{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, kun piste parametrisoidaan, niin ylläoleva inkluusio saadaan muotoon

$$I \subset \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subsetneq k[x_1, \ldots, x_n].$$

Nyt koska I on maksimaalinen, niin $I \subset \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ tarkoittaa, että $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Seurauslause 8.48. *(Ks. [1, s. 203].) Jos k on algebrallisesti suljettu kunta, niin maksimaaliset ideaalit renkaassa $k[x_1, \ldots, x_n]$ vastaavat affiinin avaruuden yksittäisiä pisteitä.*

Todistus. Lause seuraa pisteen parametrisoinnista ja edellisestä lauseesta. □

8.6 Taulukko

Tässä kappaleen asiat tiivistettynä yhteen taulukkoon. Ks. [1, s. 214].

ALGEBRA		GEOMETRIA
radikaalit		varistot
I	$\longrightarrow$	$\mathbb{V}(I)$
$\mathbb{I}(V)$	$\longleftarrow$	V
ideaalien summa		varistojen leikkaus
$I + J$	$\longrightarrow$	$\mathbb{V}(I) \cap \mathbb{V}(J)$
$\sqrt{\mathbb{I}(V) + \mathbb{I}(W)}$	$\longleftarrow$	$V \cap W$
ideaalien tulo		varistojen yhdiste
IJ	$\longrightarrow$	$\mathbb{V}(I) \cup \mathbb{V}(J)$
$\sqrt{\mathbb{I}(V)\mathbb{I}(W)}$	$\longleftarrow$	$V \cup W$
ideaalien leikkaus		varistojen yhdiste
$I \cap J$	$\longrightarrow$	$\mathbb{V}(I)\mathbb{V}(J)$
$\mathbb{I}(V) \cap \mathbb{I}(W)$	$\longleftarrow$	$V \cup W$
ideaalien osamäärä		varistojen erotus
$I : J$	$\longrightarrow$	$\overline{\mathbb{V}(I) - \mathbb{V}(J)}$
$\mathbb{I}(V) : \mathbb{I}(W)$	$\longleftarrow$	$\overline{V - W}$
muuttujien eliminointi		varistojen projektio
$\sqrt{I \cap k[x_{l+1}, \ldots, x_n]}$	$\longleftrightarrow$	$\overline{\pi_l(\mathbb{V}(I))}$
alkuideaalit		jaottomat varistot
maksimaaliset ideaalit		affiinin avaruuden pisteet

Lähteet

[1] Cox, D., Little J., O'Shea D. *Ideals, Varieties, and Algorithms* 3rd ed. Springer Science+Business Media, LLC, 2007.

[2] http://math.ucsd.edu/ doprea/resultants.pdf, 19.6.2017.

[3] Finkbeinrer, D.T. II *INTRODUCTION TO MATRICES AND LINEAR TRANSFORMATIONS* 3rd. ed. Kenyon College, 1978.

[4] Hassett, B. *Algebraic Geometry*. Cambridge University Press 2007.

[5] Hulek, K. *Elementary Algebraic Geometry*. American Mathematical Society, 2003.

[6] Häsä, J., Rämö J. *Algebra I, luentomateriaali, Matematiikan- ja tilastotieteen laitos, Helsingin yliopisto, kevät 2011*. http://aq.nerds.fi/algebraI.pdf

[7] Häsä, J. *Algebra II, luentomateriaali, Matematiikan- ja tilastotieteen laitos, Helsingin yliopisto, kevät 2010*.

[8] Kahanpää L., Smith K., Kekäläinen P. *Johdattelua algebralliseen geometriaan* Otatieto. Oy Yliopistokustannus University Press Finland Ltd. HYY-yhtymä 2000.

[9] Garcia-Puente, L. D. Oppimateriaali Sam Houston State University http://www.shsu.edu/ldg005/data/689/L1.pdf