Gröbner bases toegepast op Euclidische meetkunde

Sisan, N.

N. Sisan

Gröbner bases toegepast op Euclidische meetkunde

Bachelorscriptie

Scriptiebegeleider: Prof.dr. R.M. van Luijk

Datum: 31 juli 2020

Universiteit Leiden

Inhoudsopgave

1 Introductie

Op school heb je kennis met de stellingen uit Euclidische meetkunde gemaakt met bewijzen. In dit project ga je zien dat je veel stellingen uit Euclidische meetkunde kan bewijzen met de computer met behulp van zogeheten Gröbner bases. In eerste instantie ga je het begrip van Gröbner bases en de berekeningen die je daarmee kunt doen leren. Daarna ga je in hoofdstuk 6 een voorbeeld lezen over het bewijs van een stelling met het gebruik van een Gröbner basis. Het bepalen van Gröbner bases is theoretisch altijd beschikbaar maar in de praktijk hebben we een voorbeeld gevonden waarvan je ziet dat het niet lukt om een Gröbner basis te bepalen omdat het lang duurt en heel veel geheugen nodig heeft. Je gaat kennismaken met dit voorbeeld in hoofdstuk 6. Vervolgens gaan we ons afvragen of alle stellingen uit Euclidische meetkunde over reële getallen direct met Gröbner bases bewijsbaar zijn. Je gaat in sectie 6.3 lezen wat ik hiermee bedoel. En je gaat zien dat het antwoord nee is door een voorbeeld uit hoofdstuk 7.

Een Gröbner basis is een verzameling voortbrengers die aan bepaalde eigenschappen voldoet voor een ideaal I in een ring van veeltermen. De theorie van Gröbner-bases werd in 1965 ontwikkeld door Bruno Buchberger. Buchberger vernoemde de Gröbner-bases naar zijn promotiebegeleider Wolfgang Gröbner. Buchberger heeft een algoritme gevonden om Gröbner bases te berekenen. We gaan dat zien in het hoofdstuk 5.

Wiskundigen maken gebruik van Gröbner bases om veel problemen op te lossen. Het is bijvoorbeeld heel moeilijk om te checken of een polynoom in een gegeven ideaal zit maar met Gröbner bases wordt dat heel makkelijk. Je gaat dat zien in de stelling 4.2.

2 Inleiding

Zij K een lichaam. De verzameling van alle polynomen in de variabelen $x_1, ..., x_n$ over het lichaam K met de optelling en de vermenigvuldigingen van polynomen vormt een commutatieve *ring* die we de *ring van polynomen in* $x_1, ..., x_n$ *over* K noemen, en aangeven met $R = K[x_1, ..., x_n]$.

Definitie 2.1. *Een monoom in R is een eindig product van positieve machten van de variabelen $x_1, x_2, ..., x_n$.*

Opmerking 2.2. *1. Zij $f : \mathbb{Z}^n_{\geq 0} \longrightarrow R$ de injectieve afbeelding gegeven door*

$$\alpha = (a_1, ..., a_n) \longmapsto x^\alpha = x_1^{a_1} x_2^{a_2} ....x_n^{a_n}.$$

Het beeld van f is de verzameling $\mathcal{M}$ van alle monomen in R, dus induceert f een bijectie tussen $\mathcal{M}$ en $\mathbb{Z}^n_{\geq 0}$.

2. Omdat we de polynomen kunnen optellen en vermenigvuldiging met een element van K is de polynoomring R een vectorruimte over het lichaam K.

Elk polynoom kan je op een unieke manier als eindige som van monomen met coëfficiënten schrijven. Met andere woorden, $\mathcal{M}$ is een basis voor R over K want monomen zijn onafhankelijk en ze brengen de hele vectorruimte R voort.

Voorbeeld 2.3.

- *Voor $\alpha = (3,5,1)$ en $R = K[x_1, x_2, x_3]$ geldt dat: $x^\alpha = x_1^3 x_2^5 x_3 \in R = K[x_1, x_2, x_3]$.*
- *Voor $\alpha = (1,3,2)$ en $R = K[x,y,z]$ geldt dat: $x^\alpha = xy^3z^2 \in R = K[x,y,z]$.*

Definitie 2.4 (Monomiale ordening)**.** *Een monomiale ordening $>$ op $\mathcal{M}$ is een relatie op $\mathcal{M}$ zodat voor de corresponderende relatie op $\mathbb{Z}^n_{\geq 0}$ geldt:*

1. *De relatie $>$ is een totale ordening op $\mathbb{Z}^n_{\geq 0}$. Dus het is een ordening waar bovendien geldt dat voor alle $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$*

$$\alpha \geq \beta \text{ of } \alpha \leq \beta;$$

2. *laat $\alpha, \beta, \lambda \in \mathbb{Z}^n_{\geq 0}$ zijn met $\alpha > \beta$. Dan geldt*

$$\alpha + \lambda > \beta + \lambda;$$

3. *De relatie $>$ is wel ordening op $\mathbb{Z}^n_{\geq 0}$. Dus het is een ordening waar bovendien geldt dat iedere niet lege deelverzameling van $\mathbb{Z}^n_{\geq 0}$ een kleinste element heeft.*

Definitie 2.5 (Lexicografische ordening)**.** *Laat $\alpha = (\alpha_1, ..., \alpha_n)$ en $\beta = (\beta_1, ..., \beta_n)$ elementen in $\mathbb{Z}^n_{\geq 0}$ zijn. We zeggen dat $\alpha >_{lex} \beta$ als de meest linkse niet-nul-coëfficiënt van de verschilvector $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ positief is. Als $\alpha > \beta$ dan zullen we $x^\alpha > x^\beta$ schrijven.*

Lemma 2.6. *De lexicografische ordening is een monomiale ordening.*

Bewijs. je kunt het bewijs lezen in het hoofdstuk (2), propositie (2.4) van het boek [1]. □

Voorbeeld 2.7. *Laat $\alpha = (\alpha_1, ..., \alpha_n)$ en $\beta = (\beta_1, ..., \beta_n)$ elementen in $\mathbb{Z}^n_{\geq 0}$ zijn.*

1. *Voor $\alpha = (1,2,0)$ en $\beta = (0,3,4)$ gedt dat $\alpha >_{lex} \beta$ want $\alpha - \beta = (1,-1,-4)$.*
2. *De variabelen $x_1, x_2, ..., x_n$:*
   Omdat $(1,0,....,0) >_{lex} (0,1,....,0) >_{lex} .... >_{lex} (0,0,....,1)$; geldt dat $x_1 >_{lex} x_2 >_{lex} .... >_{lex} x_n$.

Definitie 2.8 (Gegradeerde lexicografische Ordening)**.** *Laat* $\alpha = (\alpha_1, ..., \alpha_n)$ *en* $\beta = (\beta_1, ..., \beta_n)$ *elementen in* $\mathbb{Z}^n_{\geq 0}$ *zijn.*

We zeggen dat $\alpha >_{grlex} \beta$ *als:*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

of als

$$|\alpha| = |\beta| \text{ en } \alpha >_{lex} \beta.$$

Voorbeeld 2.9. *Laat* $\alpha = (\alpha_1, ..., \alpha_n)$ *en* $\beta = (\beta_1, ..., \beta_n)$ *elementen in* $\mathbb{Z}^n_{\geq 0}$ *zijn.*

1. *Voor* $\alpha = (1, 2, 3)$ en $\beta = (3, 2, 0)$ *geldt dat* $\alpha >_{grlex} \beta$ *want* $|\alpha| = 6 > |\beta| = 5$.
2. *Voor* $\alpha = (1, 2, 4)$ en $\beta = (1, 1, 5)$ *geldt dat* $\alpha >_{grlex} \beta$ *want* $|\alpha| = |\beta| = 7$ *en* $\alpha >_{lex} \beta$.
3. *De variabelen* $x_1, x_2, ..., x_n$*:*
   omdat $(1, 0, ..., 0) >_{grlex} (0, 1, ..., 0) >_{grlex} .... >_{grlex} (0, 0, ..., 1)$*; geldt dat* $x_1 >_{grlex} x_2 >_{grlex} .... >_{grlex} x_n$.

Definitie 2.10 (Gegradeerde omgekeerd lexicografische Ordening)**.** *Laat* $\alpha = (\alpha_1, ..., \alpha_n)$ *en* $\beta = (\beta_1, ..., \beta_n)$ *elementen in* $\mathbb{Z}^n_{\geq 0}$ *zijn.*

We zeggen dat $\alpha >_{grevlex} \beta$ *als:*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

of als

$$|\alpha| = |\beta| \text{ en}$$

de meest rechtse niet-nul-coëfficiënt van de verschilvector $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ negatief is.

Voorbeeld 2.11. *Laat* $\alpha = (\alpha_1, ..., \alpha_n)$ *en* $\beta = (\beta_1, ..., \beta_n)$ *elementen in* $\mathbb{Z}^n_{\geq 0}$ *zijn.*

1. *Voor* $\alpha = (4, 7, 1)$ en $\beta = (4, 2, 3)$ *geldt dat* $\alpha >_{grevlex} \beta$ *want* $|\alpha| = 12 > |\beta| = 9$.
2. *Voor* $\alpha = (1, 5, 2)$ en $\beta = (4, 1, 3)$ *geldt dat* $\alpha >_{grevlex} \beta$ *want* $|\alpha| = 8 = |\beta|$ en $\alpha - \beta = (-3, 4, -1)$.
3. *De variabelen* $x_1, x_2, ..., x_n$*:*
   omdat $(1, 0, ..., 0) >_{grevlex} (0, 1, ..., 0) >_{grevlex} .... >_{grevlex} (0, 0, ..., 1)$*; geldt dat* $x_1 >_{grevlex} x_2 >_{grevlex} .... >_{grevlex} x_n$.

Definitie 2.12. *Schrijf* $f = \sum_\alpha a_\alpha x^\alpha$ *een polynoom in* $K[x_1, ..., x_n]$ *dat niet gelijk aan nul is. En laat* $>$ *een monomiale ordening zijn.*

- *De* ***Multigraad*** *van f is :*

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0).$$

- *De* ***Leidende coëfficiënt*** *van f is :*

$$LC(f) = a_{\text{multideg}(f)} \in K.$$

- *Het* ***Leidende monoom*** *is :*

$$LM(f) = x^{\text{multideg}(f)}.$$

- *De* ***Leidende term*** *van f is :*

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

Voorbeeld 2.13. *Neem $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in R = K[x, y, z]$. En laat $>$ naar de lexicografische ordening verwijzen met $x > y > z$. Dan geldt*
multideg$(f) = (3, 0, 0)$.
$LC(f) = -5$.
$LM(f) = x^3$.
$LT(f) = -5x^3$.

Definitie 2.14 (Noetherse Ring)**.** *Een Noetherse ring is een ring die aan één van de volgende equivalente eigenschappen voldoet:*

1. *Ieder ideaal van deze ring wordt voorgebracht door een eindig aantal elementen.*
2. *Iedere stijgende keten $I_1 \subset I_2 \subset ..... \subset I_n \subset ....$ van idealen van deze ring wordt constant.*
3. *Iedere niet lege collectie idealen van deze ring heeft een maximaal element.*

Stelling 2.15. *De ring $R = K[x_1, ..., x_n]$ is een noethers ring.*

Ik neem deze stelling in deze scriptie voor het gemak aan. Maar we kunnen deze stelling wel bewijzen met onze technieken.

Bewijs. Je kunt ook het bewijs lezen in het hoofdstuk (4), Theorem(4.1) van het boek [2]

□

Definitie 2.16 (Monomiaal ideaal)**.** *Een ideaal $I \in R$ is een monomiaal ideaal als het door monomen voortgebracht kan worden. Dat wil zeggen er is een deelverzameling $A \subseteq \mathbb{Z}^n_{\geq 0}$ zodanig dat*

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

Lemma 2.17. *Voor elk monomiaal ideaal $I \subset R$ is er een eindige verzameling $A \subseteq \mathbb{Z}^n_{\geq 0}$ met $I = \langle x^\alpha : \alpha \in A \rangle$.*

Bewijs. Laat I een monomiaal ideaal van R zijn dat voortgebracht is door een oneindige verzameling B van monomen.

$$I = \langle x^\alpha : \alpha \in B \rangle.$$

Stel dat er geen eindige deelverzameling $A \subset B$ is met

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

Laat I_1 het ideaal dat voortgebracht is door een monoom $\alpha_1 \in B$.

$$I_1 = \langle x^{\alpha_1} \rangle.$$

Omdat $I_1 \subsetneq I$, is er een $\alpha_2 \in B$ met $x^{\alpha_2} \notin I_1$. Definieer

$$I_2 = \langle x^{\alpha_1}, x^{\alpha_2} \rangle.$$

Dan definiëren we $I_3, I_4, ..., I_j, I_{j+1}, ...$ op het zelfde manier. Het ideaal I_j wordt voortgebracht door j elementen voor alle $j \in \{1, 2, ...\}$. In dit geval krijgen we een strikt stijgende keten van idealen van deze ring

$$I_1 \subsetneq I_2 \subsetneq ..... \subsetneq I_j \subsetneq I_{j+1} \subsetneq ....$$

Dat is een tegenspraak met het feit dat de ring R noethers is, dus we concluderen dat er wel een eindige deelverzameling $A \subset B$ is met

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

□

Lemma 2.18. *Laat $I = \langle m_1, m_2, ..., m_r \rangle \subset R$ een ideaal zijn met $m_1, m_2, ..., m_r$ monomen. En laat $M \in \mathcal{M}$ zijn. Dan geldt:*

$$M \in I \iff \text{ er bestaat een } i \in \{1, 2, ...r\} \text{ zodanig dat } m_i \mid M.$$

Bewijs. ($\Rightarrow$) Stel dat $M \in I$. Dus M wordt geschreven als lineair combinatie van $m_1, ..., m_r$.

$$M = \sum_{i=1}^{r} h_i \cdot m_i \text{ waarbij } h_i \in R.$$

we kunnen h_i schrijven als $h_i = \sum_{m \in \mathcal{M}} c_{i,m} \cdot m$. Dan geldt

$$1 \cdot M = \sum_{i=1}^{r} \sum_{m \in \mathcal{M}} c_{i,m} \cdot m \cdot m_i \tag{1}$$

Stel dat voor alle i het monoom m_i niet een deler is van M. Dan geldt voor alle $m \in \mathcal{M}$ dat $m \cdot m_i \neq M$. Omdat $\mathcal{M}$ een basis is volgt dat de coëfficiënt van M in het rechterlid van (1) nul is. Maar de coëfficiënt van M in het linkerlid van (1) is 1. We krijgen een tegenspraak dus bestaat er een i met $m_i \mid m$.

($\Leftarrow$) Volgens de definitie van een ideaal volgt dat $M \in I$. □

Definitie 2.19. *Laat $0 \neq I \subseteq R$ een ideaal zijn. Laat $>$ een monomiale ordening op $\mathbb{Z}_{\geq 0}^n$ zijn.*

- *De verzameling van leidende termen van het ideaal I is*

$$LT(I) = \{LT(f) : f \in I\}.$$

- *Het ideaal $\langle LT(I)\rangle$ is het ideaal dat voortgebracht wordt door alle elementen van de verzameling $LT(I)$.*

3 Reductiealgoritme

Stelling 3.1. *Laat $>$ een monomiale ordening zijn. En laat $F = (f_1, f_2, ..., f_s)$ een rijtje van elementen van R zijn. Dan kan elk polynoom $f \in R$ geschreven worden als:*

$$f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r$$

waarbij $u_1, u_2, ..., u_s, r \in R$ en r is som van monomen met coëfficiënten zodanig dat geen enkele term van r deelbaar is door een van de $LT(f_1), ..., LT(f_s)$.

Noem r de rest en merk op dat als r gelijk aan 0 is, dan zit f in het ideaal $I = \langle f_1, f_2, ..., f_s\rangle$. En merk op dat $u_1, ..., u_s$ en r niet uniek zijn. Zie opmerking 3.5.

Om zulke $u_1, ..., u_s, r$ te bepalen, gebruiken we het volgende algoritme.

Reductiealgoritme.

Definitie 3.2. *Invoer: $(f_1, f_2, ..., f_s, f)$ rijtje van elementen van R.*
Uitvoer: $(u_1, u_2, ..., u_s, r)$ rijtje van elementen van R zodanig dat

$$f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r,$$

waarbij r voldoet aan de waarden van de stelling 3.1.

1 *Begin met $u_1 := 0, u_2 := 0, ..., u_s := 0, r := 0, h := f$.*

2 *Zolang $h \neq 0$ doe:*

- *Als er een $i \in \{1, 2, ..., s\}$ bestaat met $LM(f_i) \mid LM(h)$, neem dan de kleinste i met $LM(f_i) \mid LM(h)$ en vervang h en u_i door*

$$h' = h - \frac{LT(h)}{LT(f_i)} \cdot f_i \text{ en } u_i' = u_i + \frac{LT(h)}{LT(f_i)}.$$

- *Anders vervangen we h en r door*

$$h' = h - LT(h) \text{ en } r' = r + LT(h).$$

3 *Voer uit: $(u_1, u_2, ..., u_s, r)$.*

Merk op dat het algoritme deterministisch is, ook al zijn $u_1, u_2, ..., u_s, r$ niet uniek, doordat we de kleinste i kiezen.

We schrijven $\overline{f}^F$ voor de rest van f na reduceren met $F = (f_1, f_2, ..., f_s)$.

Propositie 3.3. *Het reductiealgoritme termineert. En de uitvoer is* $(u_1, u_2, ..., u_s, r)$ *zodanig dat* $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r$ *correct is.*

Bewijs. Stel dat het algoritme niet zou termineren. Als we het algoritme toepassen, kunnen we opmerken dat elke stap de multideg van h kleiner wordt want de $LM(h)$ wordt steeds kleiner. Dan krijgen we een oneindige dalende rij van multigraden van h. Maar dat kan niet omdat $>$ een wel ordening is. Dus op een gegeven moment zal h gelijk aan nul zijn. Dus het algoritme termineert.

Om te bewijzen dat het algoritme correcte uitvoer geeft, zullen we laten zien dat tijdens het algoritme altijd geldt dat $f - h = u_1 f_1 + ... + u_s f_s + r$. En we gaan dat bewijzen met inductie.

We schrijven h_j voor het polynoom waar h aan gelijk is aan het eind van stap j en r_j voor het polynoom waar r aan gelijk is aan het eind van stap j en $u_{j,i}$ voor elke $i \in \{1, 2, ..., s\}$ voor het polynoom waar u_i aan gelijk is aan het eind van stap j en $h_o = f, u_{0,i} = 0$ en $r_0 = 0$.

Aan het begin van de eerste stap met $f = h_0$ geldt dat

$$f - h_0 = 0 = 0 \cdot f_1 + 0 \cdot f_2 + ... + 0 \cdot f_s + 0$$

met $u_{0,i} = 0$ voor elke $i \in \{1, 2, ..., s\}$ en $r_0 = 0$.

Zij $n \geq 0$ en neem aan dat het goed is aan het begin van stap $n + 1$. Dus

$$f - h_n = u_{n,1} \cdot f_1 + ... + u_{n,s} \cdot f_s + r_n.$$

We gaan laten zien dat het goed is aan het eind van stap $n + 1$. We hebben twee gevallen.

- Als er een $k \in \{1, 2, ..., s\}$ bestaat met $LM(f_k) \mid LM(h_n)$, neem dan de kleinste k met $LM(f_k) \mid LM(h_n)$. Dan is

$$h_{n+1} = h_n - \frac{LT(h_n)}{LT(f_k)} \cdot f_k.$$

$$u_{n+1,k} = u_{n,k} + \frac{LT(h_n)}{LT(f_k)}.$$

$$u_{n+1,i} = u_{n,i} \text{ met } i \in \{1, 2, ..., s\} \text{ en } i \neq k.$$

En

$$r_{n+1} = r_n.$$

Dan geldt
$f - h_{n+1} = f - (h_n - \frac{LT(h_n)}{LT(f_k)} \cdot f_k) = f - h_n + \frac{LT(h_n)}{LT(f_k)} \cdot f_k$
$= u_{n,1} \cdot f_1 + ... + (u_{n,k} + \frac{LT(h_n)}{LT(f_k)}) \cdot f_k + ... + u_{n,s} \cdot f_s + r_n$
$= u_{n+1,1} \cdot f_1 + ... + u_{n+1,s} \cdot f_s + r_{n+1}$.

- Als er geen $k \in \{1, 2, ..., s\}$ bestaat met $LM(f_k) \mid LM(h_n)$, dan is

$$h_{n+1} = h_n - LT(h_n)$$

$$u_{n+1,i} = u_{n,i} \text{ voor elke } i \in \{1, 2, ..., s\}$$

en

$$r_{n+1} = r_n + LT(h_n).$$

Dan geldt
$f - h_{n+1} = f - (h_n - LT(h_n)) = f - h_n + LT(h_n)$
$= u_{n,1} \cdot f_1 + ... + u_{n,s} \cdot f_s + (r_n + LT(h_n)) = u_{n+1,1} \cdot f_1 + ... + u_{n+1,s} \cdot f_s + r_{n+1}$.

□

Voorbeeld 3.4. *Laat $R = \mathbb{Q}[x, y]$ zijn. En laat $>$ naar de lexicografische ordening verwijzen met $x > y$ zijn. En laat $F = (f_1, f_2)$ een rijtje van elementen van R zijn met: $f_1 = y^2 - 1$, $f_2 = xy - 1$.*
Reduceer $f = x^2y - y^3$ met F.
Invoer: f_1, f_2, f.
Uitvoer: (u_1, u_2, r) rijtje van elementen van R zodat $f = u_1 f_1 + u_2 f_2 + r$.
Begin met $u_1 := 0, u_2 := 0, r := 0, h := f$.
We hebben $LM(f_1) = y^2$ en $LM(f_2) = xy$ en $LM(h) = x^2y$. We zien dat $LM(f_1) \nmid LM(h)$ en $LM(f_2) \mid LM(h)$. Dus

$$h_1 = x^2y - y^3 - x \cdot (xy - 1) = x - y^3 \text{ en } u_{1,2} = x.$$

We hebben nu $LM(h_1) = x$. En we zien dat

$$LM(f_1) \nmid LM(h_1) \text{ en } LM(f_2) \nmid LM(h_1).$$

Dus

$$h_2 = -y^3 \text{ en } r_2 = x.$$

We zien dat $LM(f_1) \mid LM(h_2)$ en $LM(f_2) \nmid LM(h_2)$. Dan krijgen we

$$h_3 = -y^3 - -y \cdot (y^2 - 1) = -y \text{ en } u_{3,1} = -y \text{ en } r_3 = r_2 = x.$$

We hebben nu $LM(h_3) = -y$. En we zien dat

$$LM(f_1) \nmid LM(h_3) \text{ en } LM(f_2) \nmid LM(h_3).$$

Dus

$$h_4 = 0 \text{ en } r_4 = x - y.$$

Nadat we het algoritme toepassen, kunnen we f schrijven als

$$f = -y \cdot f_1 + x \cdot f_2 + x - y.$$

Merk op dat geen enkele term van $r = r_4 = x - y$ deelbaar is door $LT(f_1)$ en $LT(f_2)$.

Opmerking 3.5. *In voorbeeld* 3.4 *hebben we één manier gezien om* f *te schrijven als* $f = u_1 \cdot f_1 + u_2 \cdot f_2 + r$ *met* $u_1 = -y, u_2 = x$ *en* $r = x - y$.

Er zijn ook andere manieren. We kunnen bijvoorbeeld f *schrijven als* $f = u_1' \cdot f_1 + u_2' \cdot f_2 + r'$ *met* $u_1' = -x - y, u_2' = x + y$ *en* $r' = 0$. *Dus* f *zit in* I *omdat* r' *gelijk aan* 0 *is.*

Dus je ziet dat u_1 *en* u_2 *niet uniek zijn en dat je uit het feit dat* $r \neq 0$ *niet kan concluderen dat* f *niet in het ideaal* I *zit.*

Merk op dat we in voorbeeld 3.4 voortbrengers hadden voor het ideaal I namelijk $y^2 - 1$ en $xy - 1$ maar we konden niet makkelijk testen of f in I zit.

In het algemeen willen we voor een ideaal een verzameling voortbrengers vinden waarvoor voor alle $f \in R$ geldt

$$f \in I \Leftrightarrow \text{ De reductie van } f \text{ met } G \text{ is gelijk aan nul.}$$

We noemen zo een verzameling Gröbner basis en dat is equivalent met de volgende definitie.

4 Gröbner Bases

Definitie 4.1. *Laat* $>$ *een monomiale ordening op* $\mathbb{Z}_{\geq 0}^n$ *zijn. Laat* I *een ideaal van* R *zijn. Een eindig rijtje* $G = (g_1, ..., g_t)$ *van elementen uit het ideaal* I *is een Gröbner basis voor het ideaal* I *is als*

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

Stelling 4.2. *Laat* $G = (g_1, g_2, ..., g_t)$ *een Gröbner basis voor het ideaal* $I \subseteq R$ *zijn. En laat* $f \in R$ *zijn. Dan geldt*

$$f \in I \Leftrightarrow \overline{f}^G = 0.$$

Bewijs. ($\Rightarrow$) Stel dat $f \in I$. We zullen laten zien dat $\overline{f}^G = 0$. Als je het reductie algoritme toepast, Dan kan f geschreven worden als:

$$f = u_1 g_1 + u_2 g_2 + ... + u_t g_t + r$$

waarbij $u_1, u_2, ..., u_t, r \in R$ en r is een som van monomen met coëfficiënten zodanig dat geen enkele term van r deelbaar is door een van de $LT(g_1), ..., LT(g_t)$. We hebben twee mogelijkheden

- Als $r = 0$, dan is $\overline{f}^G = 0$.
- Als $r \neq 0$. dan $r = f - (u_1 g_1 + u_2 g_2 + ... + u_t g_t)$. Dat impliceert dat $r \in I$. Omdat G Gröbner basis is voor I geldt wegens Definitie 4.1 dat

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

  Volgens Lemma 2.18 geldt

  $LT(r) \in \langle LT(I) \rangle \iff$ er bestaat een $i \in \{1, 2, ...t\}$ zodanig dat $LT(g_i) \mid LT(r)$.

  Dat is een tegenspraak.

Dus $r = 0$. Dat geeft $\overline{f}^G = 0$. ($\Leftarrow$) Stel dat $\overline{f}^G = 0$. Dan geldt dat

$$f = u_1 g_1 + u_2 g_2 + ... + u_t g_t$$

Waarbij $u_1, u_2, ..., u_t, \in R$. Dus f kan geschreven worden als combinatie van $(g_1, ..., g_t)$. Dat impliceert dat $f \in I$.

□

Lemma 4.3. *Laat $>$ een monomiale ordening op $\mathbb{Z}^n_{\geq 0}$ zijn. Laat $G = (g_1, g_2, ..., g_t)$ een Gröbner basis voor het ideaal $I \subseteq R$ zijn. Dan geldt dat G het ideaal I voortbrengt.*

Bewijs. We gaan laten zien dat $G = (g_1, g_2, ..., g_t)$ het ideaal I voortbrengt. Met andere woorden

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

Uit het feit dat $g_1, ..., g_t$ elementen van I zijn, volgt dat

$$\langle g_1, ..., g_t \rangle \subseteq I.$$

Omdat G een Gröbner basis voor het ideaal I is, geldt volgens Definitie 4.1 dat

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

Laat f een willekeurig polynoom in I zijn. Dan volgt uit de stelling 4.2 dat $\overline{f}^G = 0$. Dus

$$f = u_1 \cdot g_1 + ... + u_t \cdot g_t + 0,$$

waarbij $(u_1, ...u_t)$ een rijtje van elementen in R is.
Dat impliceert $f \in \langle g_1, ..., g_t \rangle$. Dus $I \subseteq \langle g_1, ..., g_t \rangle$. Dus

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

□

5 Buchberger's algoritme

Definitie 5.1. *laat M_1 en M_2 twee monomen van $\mathcal{M}$ zijn.*

- *Schrijf* $\text{multideg}(M_1) = \alpha = (\alpha_1, ..., \alpha_n)$ *en* $\text{multideg}(M_2) = \beta = (\beta_1, ..., \beta_n)$. *En schrijf* $\lambda = (\lambda_1, ..., \lambda_n)$ *met* $\lambda_i = min(\alpha_i, \beta_i)$.
  Het monoom x^λ *is* ***de grootste gemene deler*** *van M_1 en M_2.*

- *Laat f en g twee polynomen van R met $0 \neq f$ en $0 \neq g$ zijn.En laat x^λ de grootste gemene deler van $LM(f)$ en $LM(g)$ zijn. Het* ***S-polynoom*** *van f en g is:*

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

Stelling 5.2 (Buchberger's criterium)**.** *Laat $G = (g_1, ..., g_t)$ een eindig rijtje van elementen in R zijn. Definieer $I = \langle g_1, ..., g_t \rangle$. En laat $>$ een monomiale ordening zijn. Dan geldt*

$$G \text{ is een gröbner basis voor het ideaal } I \iff \forall g_i, g_j \in G \text{ geldt } \overline{S(g_i, g_j)}^G = 0.$$

Bewijs. je kunt het bewijs lezen in hoofdstuk 2, stelling 6.6 van het boek [1]. □

We kunnen een Gröbner basis voor een ideaal I bepalen als we dit algoritme toepassen:

Buchberger's algoritme:
Invoer: $F = (g_1, g_2, ..., g_t)$ zodanig dat het ideaal $I = \langle g_1, ..., g_t \rangle \neq 0$ is.
Uitvoer: $G = (g_1, g_2, ..., g_s)$ zodat G een Gröbner basis voor het ideaal I is.

1 Neem $G = (g_1, ...g_t)$ en $B = \{(g_i, g_j) : g_i, g_j \in G; g_i \neq g_j\}$.

2 Zolang B niet leeg is,herhaal:

- **a)** Kies $b = (g_i, g_j) \in B$ en vervang B door $B \setminus \{b\}$.
- **b)** Bepaal $\overline{S(g_i, g_j)}^G$.
- **c)** Als $\overline{S(g_i, g_j)}^G \neq 0$, voeg dan $\overline{S(g_i, g_j)}^G$ achteraan G toe en voor alle $g \in G$ voeg $(g, \overline{S(g_i, g_j)}^G)$ aan B toe.

3 Voer uit $G = (g_1, g_2, ..., g_s)$.

Voordat ik laat zien dat het Buchberger's algoritme termineert en als output een Gröbner basis voor I geeft, ga ik eerst een lemma formuleren.

Lemma 5.3. *Laat $G_1 = (f_1, ..., f_t)$ een rijtje van polynomen in R zijn. En laat $G_2 = (f_1, ..., f_t, f_{t+1}, ..., f_n)$ een rijtje van polynomen dat begint met het rijtje G_1 zijn.*

1. *Voor alle $g \in R$ geldt als $\overline{g}^{G_1} = 0$, dan ook $\overline{g}^{G_2} = 0$.*
2. *Voor alle $g \in R$ en $s = \overline{g}^{G_1}$ en $G^* = (f_1, ..., f_t, s)$ geldt dat $\overline{g}^{G^*} = 0$.*

Bewijs. 1. Omdat $\overline{g}^{G_1} = 0$ is, volgt dat je g kan schrijven als

$$g = u_1 f_1 + ... + u_t f_t$$

En omdat G_2 begint met het rijtje G_1 met de zelfde volgorde en omdat het reductie algoritme die we gebruiken de kleinste index pakt, volgt dat $\overline{g}^{G_2} = 0$.

2. Laat $g \in R$ een polynoom zijn en laat $s = \overline{g}^{G_1}$ de rest van g zijn na de reductie met G_1. We definiëren $h_0 = g$ en we schrijven h_j voor het polynoom waar h van het reductie algoritme aan gelijk is aan het einde van stap j. Ook $u_{j,i}$ voor elke $i \in \{1, 2, ...t\}$ voor het polynoom waar u_i

van het reductie algoritme aan gelijk is aan het einde van stap j. En r_j voor het polynoom waar r van het reductie algoritme aan gelijk is aan het einde van stap j. Als het algoritme termineert na J stappen, dan geldt $s = r_J$.

Als je bij stap j het polynoom u_i verandert, dan is dat omdat het leidende monoom van h aan het begin van stap j wel deelbaar is door het leidende monoom van een element van G_1 maar als je een leidende term van h hebt die niet deelbaar is door het leidende monoom van een element van G_1 dan stop je die in de rest en die wordt term van r.

Noem $j_1, j_2, ...$ de stappen waarin r wordt aangepast in de reductie van g met G_1. Dan geldt

$$LT(s) = LT(h_{j_1-1}) \text{ als } s \neq 0.$$

Nu gaan we zien wat gebeurt als je g reduceert met $G^* = (f_1, ..., f_t, s)$. We definiëren

$$\mathbf{h}_j = \begin{Bmatrix} h_j & \text{als } j < j_1 \\ h_j - (s - r_j) & \text{als } j \geq j_1 \end{Bmatrix}$$

In het begin loopt de reductie van g met G^* het zelfde als de reductie met G_1 tot het stapje j_1. aan het begin van die stap is het leidende term $LT(h_{j_1-1})$ van h is wel deelbaar door het leidende monoom van s. Dus je gaat hier s aftrekken en dat betekent dat alles vanaf dat stapje anders wordt.

Met de definitie van $\mathbf{h}$ krijg je niet precies de stappen die het algoritme met G^* doet maar je krijgt iets te veel. Er zijn polynomen in de nieuwe rijtje die hetzelfde zijn als de vorige want dan geldt

$$\mathbf{h}_{J_i} = \mathbf{h}_{J_{i-1}}.$$

Als je de dubbele polynomen weglaat, dan krijg je een nieuw rijtje waarvan je kunt laten zien dat precies is wat gebeurt met h tijdens het reductie algoritme van g met G^*. Bovendien kun je laten zien dat de rest r uit de reductie algoritme van g met G^* nooit wordt aangepast. Dus als $(u_1, u_2, ..., u_t, s)$ de output bij G_1 is, dat de output bij G^* als dan $(u_1, u_2, ..., u_t, -1, 0)$ is, dus met coëfficiënt -1 voor s en met rest 0. Dus $\overline{g}^{G^*} = 0$.

□

In de volgende propositie gaan we bewijzen dat het Buchberger's algoritme termineert en een Gröbner basis voor I geeft.

Propositie 5.4. *Het algoritme termineert en geeft een Gröbner basis voor I.*

Bewijs. Als je het algoritme toepast en als je alleen de stappen nummert dat je een polynoom toevoegt en als je G_ℓ schrijft voor de verzameling waar G aan gelijk is in stap ℓ, dan heb je

$$G_0 \subset G_1 \subset ..... \subset G_t \subset ....$$

Dus we krijgen steeds grotere verzamelingen van polynomen omdat we in de stap $\ell + 1$ het polynoom $\overline{S(g_i, g_j)}^{G_\ell}$ aan $G_{\ell+1}$ toevoegen. En dus krijgen we meer leidende termen. Merk op dat de rest $\overline{S(g_i, g_j)}^{G_\ell}$ bevat is in het ideaal voortgebracht door G_ℓ, dus we krijgen

$$\langle G_{\ell+1} \rangle = \langle G_\ell \rangle = ... = \langle G_1 \rangle = \langle G_0 \rangle = I.$$

We defineren $J_m = \langle LM(g) : g \in G_m \rangle$. Dan heb je

$$J_0 \subset J_1 \subset .... \subset J_t \subset ....$$

Het is duidelijk per definitie dat $G_{\ell-1} \neq G_\ell$ en dat impliceert volgens lemma 2.18 en het feit dat het leidende monoom van een niet-nul rest bij reductie met $(g_1, g_2, ..., g_j)$ niet deelbaar is door $LM(g_1), LM(g_2), ..., LM(g_j)$ dat $J_{\ell-1} \subsetneq J_\ell$.

Omdat R een noetherse ring is, volgt dat elke stijgende keten van idealen constant wordt. Dus kan deze rij van idealen niet oneindig lang worden. En dat betekent dat het algoritme termineert, zeg na N stappen. Dan geldt

$$G_0 \subset G_1 \subset ..... \subset G_N.$$

En laat $B = \{(g_i, g_j) : g_i, g_j \in G_N; g_i \neq g_j\}$ zijn. Voor elke $p, q \in G_N$ heeft (p, q) in B gezeten. Op een gegeven moment is dus $\overline{S(p, q)}^{G_\ell}$ bepaald voor zekere $\ell \leq N$.
We hebben twee mogelijkheden:

1. $\overline{S(p, q)}^{G_\ell} = 0$.
2. $\overline{S(p, q)}^{G_\ell} \neq 0$. In dit geval geldt dat $\overline{S(p, q)}^{G_\ell} \in G_{\ell+1}$ en dus volgens Lemma 5.3 is $\overline{S(p, q)}^{G_{\ell+1}} = 0$.

Dus volgens Lemma 5.3 geldt voor elke $p, q \in G_N$ dat $\overline{S(p, q)}^{G_N} = 0$. En dus volgens Stelling 5.2 is G_N een Gröbner basis voor $\langle G_N \rangle = I$. □

Voorbeeld 5.5. *Laat $R = \mathbb{Q}[x, y]$ zijn. En laat $>$ naar de gegradeerde lexicografische ordening verwijzen met $x > y$. En laat $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x$ twee polynomen in R zijn. Definieer $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle \subset R$. We gaan een Gröbner basis voor het ideaal I bepalen.*

Laat $G_0 = (f_1, f_2)$ zijn.
Er geldt $LT(f_1) = x^3$ en $LT(f_2) = x^2y$ dus

$$S(f_1, f_2) = \frac{LT(f_2) \cdot f_1 - LT(f_1) \cdot f_2}{ggd(LM(f_1), LM(f_2))} = -x^2.$$

$LM(f_1), LM(f_2)$ zijn geen deler van $LM(S(f_1, f_2))$,dus $\overline{S(f_1, f_2)}^{G_0} = -x^2$.
We voegen $f_3 = -x^2$ aan G_0 toe.
We hebben nu $G_1 = (f_1, f_2, f_3)$ met $\overline{S(f_1, f_2)}^{G_1} = 0$ volgens lemma 5.3.
Er geldt $LT(f_1) = x^3$ en $LT(f_3) = -x^2$ dus

$$S(f_1, f_3) = \frac{LT(f_3) \cdot f_1 - LT(f_1) \cdot f_3}{ggd(LM(f_1), LM(f_3))} = 2xy.$$

$LM(f_1), LM(f_2), LM(f_3)$ zijn geen deler van $LM(S(f_1, f_3))$,dus $\overline{S(f_1, f_3)}^{G_1} = 2xy$.
We voegen $f_4 = 2xy$ aan G_1 toe.
We hebben nu $G_2 = (f_1, f_2, f_3, f_4)$ met $\overline{S(f_1, f_3)}^{G_2} = 0$ volgens lemma 5.3.
Er geldt $LT(f_1) = x^3$ en $LT(f_4) = 2xy$ dus

$$S(f_1, f_4) = \frac{LT(f_4) \cdot f_1 - LT(f_1) \cdot f_4}{ggd(LM(f_1), LM(f_4))} = -4xy^2 = -2y \cdot f_4.$$

Het is nu makkelijk om te controleren dat $\overline{S(f_1, f_4)}^{G_2} = 0$.
Er geldt $LT(f_2) = x^2y$ en $LT(f_3) = -x^2$ dus

$$S(f_2, f_3) = \frac{LT(f_3) \cdot f_2 - LT(f_2) \cdot f_3}{ggd(LM(f_2), LM(f_3))} = 2y^2 - x.$$

$LM(f_1), LM(f_2), LM(f_3), LM(f_4)$ zijn geen deler van $LM(S(f_2, f_3)) = y^2$, en ook niet van x. Dus $\overline{S(f_2, f_3)}^{G_2} = 2y^2 - x$.
We voegen $f_5 = 2y^2 - x$ aan G_2 toe.
We hebben nu $G_3 = (f_1, f_2, f_3, f_4, f_5)$ met $\overline{S(f_2, f_3)}^{G_3} = 0$ volgens lemma 5.3.
Als we het algoritme op het zelfde manier toepassen, krijgen we:

$$\overline{S(f_i, f_j)}^{G_3} = 0 \qquad \text{voor alle } 1 \leq i < j \leq 5.$$

Volgens Buchberger's criterium volgt dat $G_3 = (f_1, f_2, f_3, f_4, f_5)$ een grlex Gröbner basis voor het ideaal I is.

Voorbeeld 5.6. *We gaan een Gröbner basis voor het ideaal I in het voorbeeld 3.4 bepalen. Laat $G_0 = (f_1, f_2)$ zijn met $f_1 = y^2 - 1, f_2 = xy - 1$.*
Er geldt $LT(f_1) = y^2$ en $LT(f_2) = xy$ dus

$$S(f_1, f_2) = \frac{LT(f_2) \cdot f_1 - LT(f_1) \cdot f_2}{ggd(LM(f_1), LM(f_2))} = -x + y.$$

$LM(f_1), LM(f_2)$ zijn geen deler van $LM(S(f_1, f_2)) = x$ en ook niet van y, dus $\overline{S(f_1, f_2)}^{G_0} = -x + y$.
We voegen $f_3 = -x + y$ aan G_0 toe.
We hebben nu $G_1 = (f_1, f_2, f_3)$ met $\overline{S(f_1, f_2)}^{G_1} = 0$ volgens lemma 5.3.

Er geldt $LT(f_1) = y^2$ *en* $LT(f_3) = -x$ *dus*

$$S(f_1, f_3) = \frac{LT(f_3) \cdot f_1 - LT(f_1) \cdot f_3}{ggd(LM(f_1), LM(f_3))} = x - y^3 = -f_3 - yf_1$$

Het is makkelijk om na te gaan dat $\overline{S(f_1, f_3)}^{G_1} = 0$.

Er geldt $LT(f_2) = xy$ *en* $LT(f_3) = -x$ *dus*

$$S(f_2, f_3) = \frac{LT(f_3) \cdot f_2 - LT(f_2) \cdot f_3}{ggd(LM(f_2), LM(f_3))} = -y^2 + 1 = -f_1$$

Het is makkelijk om te controleren dat $\overline{S(f_2, f_3)}^{G_1} = 0$.

Volgens Buchberger's criterium volgt dat $G_1 = (f_1, f_2, f_3)$ *een lex Gröbner basis voor het ideaal* I *is.*

In het voorbeeld 3.4 kunnen we niet op een makkelijke manier zien of $f = x^2y - y^3$ *in* I *zit. Omdat je nu een Gröbner basis voor het ideaal* I *hebt, kan je stelling 4.2 gebruiken. Er geldt* $\overline{f}^{G_1} = 0$. *Dat impliceert dat* $f \in I$.

6 Toepassingen

In deze paragraaf ga je zien hoe je een stelling uit meetkunde kan bewijzen met behulp van Gröbner bases. Ook ga je zien de manier die ik gebruik om de stelling te bewijzen. Tot slot zie je een voorbeeld waar ik de Gröbner basis niet kan bepalen met behulp van de computer omdat het te lang duurt.

6.1 Stellingen worden bewezen door Gröbner bases

In deze sectie zie je drie verschillende stellingen die worden bewezen met Gröbner bases.

Stelling 6.1. *Stel* $a, b, c \in \mathbb{R}^2$ *zijn punten die een driehoek vormen. En zij* $s \in \mathbb{R}^2$. *Als* s *het snijpunt is van twee van de drie hoogtelijnen, dan ligt* s *ook op de derde hoogtelijn.*

Bewijs. Schrijf $a = (X_a, Y_a), b = (X_b, Y_b), c = (X_c, Y_c)$ en $s = (X_s, Y_s)$.

Laat $R = \mathbb{Q}[X_a, X_b, X_c, X_s, Y_a, Y_b, Y_c, Y_s]$ zijn. Stel dat s op de hoogtelijnen uit a en b ligt. Dan is $\langle s - a, b - c\rangle = 0$ en $\langle s - b, c - a\rangle = 0$

Definieer

$$f_1 = \langle s - a, b - c\rangle = \langle s, b\rangle - \langle s, c\rangle - \langle a, b\rangle + \langle a, c\rangle =$$
$$X_sX_b + Y_sY_b - X_sX_c - Y_sY_c - X_aX_b - Y_aY_b + X_aX_c + Y_aY_c.$$

En

$$f_2 = \langle s - b, c - a\rangle = \langle s, c\rangle - \langle s, a\rangle - \langle b, c\rangle + \langle b, a\rangle$$
$$X_sX_c + Y_sY_c - X_sX_a - Y_sY_a - X_bX_c - Y_bY_c + X_bX_a + Y_bY_a.$$

We moeten bewijzen dat s op de hoogtelijn uit c ligt. Definieer

$$\begin{aligned} g &= \langle s-c, a-b\rangle = \langle s,a\rangle - \langle s,b\rangle - \langle c,a\rangle + \langle c,b\rangle \\ &= X_sX_a + Y_sY_a - X_sX_b - Y_sY_b - X_cX_a - Y_cY_a + X_cX_b + Y_cY_b. \end{aligned}$$

Definieer $I = \langle f_1, f_2\rangle$. We willen bewijzen dat g in het ideaal I zit want de volgende eigenschap waar is.

Als $f_1(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = f_2(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0$, dan geldt voor elke polynoom $k \in I = \langle f_1, f_2\rangle$ dat

$$k(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0.$$

En dus

$$g(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0.$$

We kunnen meteen zien dat g in I zit want $g = -f_1 - f_2$. Dus s ligt op de hoogtelijn uit c en de hoogtelijnen van een driehoek gaan door één punt.

□

Lemma 6.2. *Laat V een willekeurige verzameling zijn. Laat $R = \mathbb{Q}[X_v, Y_v : v \in V]$ de ring zijn. Voor drie verschillende elementen $u, v, w \in V$ definiëren we*

$$f_{uvw} = (X_v - X_u)(Y_w - Y_u) - (Y_v - Y_u)(X_w - X_u) \in \mathbb{Q}[X_u, X_v, X_w, Y_u, Y_v, Y_w] \subset R.$$

Voor drie punten $P_u(x_u, y_u), P_v(x_v, y_v)$ en $P_w(x_w, y_w)$ geldt dat

$$P_u, P_v \text{ en } P_w \text{ zijn collineair} \iff f_{uvw}(x_u, x_v, x_w, y_u, y_v, y_w) = 0.$$

Bewijs. Ik heb P_u, P_v en P_w drie punten die op één lijn liggen, dan liggen ze nog steeds op één lijn als ik ze allemaal transleer. Dus

$$\begin{aligned} P_u, P_v \text{ en } P_w \text{ zijn collineair } &\iff a = P_u - P_w, b = P_v - P_w \\ &\quad \text{en } 0 = P_w - P_w \text{ zijn collineair }. \end{aligned}$$

We gaan nu zien dat

$$a, b \text{ en } 0 \text{ zijn collineair } \iff a \text{ en } b \text{ lineair zijn afhankelijk.}$$

Als a of b gelijk aan 0 zijn, dan zijn a en b inderdaad lineair afhankelijk en dus $0, a, b$ zijn collineair.

En als a en b allebei niet gelijk aan 0 zijn, dan is de lijn door a en 0 het zelfde als de lijn door b en 0. En dus a ligt op de lijn door b en 0 en b ligt op de lijn door a en 0. Dat betekent dat a en b veelvouden van elkaar zijn en dus dat a en b lineair afhankelijk zijn. Andersom als a en b lineair afhankelijk zijn, dan zijn a en b veelvouden van elkaar. En dus liggen a en b en 0 op één lijn.

$$a \text{ en } b \text{ lineair afhankelijk zijn} \iff det\begin{vmatrix} x_u - x_w & x_v - x_w \\ y_u - y_w & y_v - y_w \end{vmatrix} = 0$$

$$\Leftrightarrow (x_u - x_w)(y_v - y_w) - (y_u - y_w)(x_v - x_w) = 0 \Leftrightarrow f_{uvw}(x_u, x_v, x_w, y_u, y_v, y_w) = 0.$$

□

Stelling 6.3. *Stel $a, b, c \in \mathbb{R}^2$ zijn punten die niet op een lijn liggen, en zij $z \in \mathbb{R}^2$. Schrijf $k = (b+c)/2$, $l = (a+c)/2$. Als a, z, k collineair zijn en b, z, l collineair zijn dan geldt*

$$3 \cdot z = a + b + c.$$

Bewijs. Schrijf $a = (X_a, Y_a), b = (X_b, Y_b), c = (X_c, Y_c)$ en $z = (X_z, Y_z)$.

Laat $R = \mathbb{Q}[X_a, X_b, X_c, X_z, Y_a, Y_b, Y_c, Y_z]$ zijn. En laat $>$ naar de lexicografische ordening verwijzen met $X_a > X_b > X_c > X_z > Y_a > Y_b > Y_c > Y_z$.

We hebben $k = (b+c)/2$ en $l = (a+c)/2$. Definieer

$$f_1 = f_{azk} = (X_z - X_a)((Y_b + Y_c)/2 - Y_a) - (Y_z - Y_a)((X_b + X_c)/2 - X_a);$$

$$f_2 = f_{bzl} = (X_z - X_b)((Y_a + Y_c)/2 - Y_b) - (Y_z - Y_b)((X_a + X_c)/2 - X_b);$$

$$h = f_{abc} = (X_b - X_a)(Y_c - Y_a) - (Y_b - Y_a)(X_c - X_a);$$

We willen $3 \cdot z = a + b + c$ bewijzen.

Definieer

$$g_1 = X_a + X_b + X_c - 3X_z \text{ en } g_2 = Y_a + Y_b + Y_c - 3Y_z.$$

Definieer $I = \langle f_1, f_2 \rangle$. Een Gröbner basis voor het ideaal I is $G = (h_1, h_2, h_3)$ met

$$h_1 = X_aY_b - X_aY_z - X_bY_a - X_bY_c + 2X_bY_z + X_cY_b - X_cY_z + X_zY_a - 2X_zY_b + X_zY_c,$$
$$h_2 = X_aY_c - X_aY_z + X_bY_c - X_bY_z - X_cY_a - X_cY_b + 2X_cY_z + X_zY_a + X_zY_b - 2X_zY_c,$$
$$h_3 = X_bY_aY_c - X_bY_aY_z + X_bY_bY_c - X_bY_bY_z + X_bY_c^2 - 4X_bY_cY_z + 3X_bY_z^2 - X_cY_aY_b +$$
$$X_cY_aY_z - X_cY_b^2 - X_cY_bY_c + 4X_cY_bY_z + X_cY_cY_z - 3X_cY_z^2 + X_zY_aY_b - X_zY_aY_c +$$
$$X_zY_b^2 - 3X_zY_bY_z - X_zY_c^2 + 3X_zY_cY_z$$

Om te bewijzen $3 \cdot z = a + b + c$, is het genoeg om te bewijzen dat

$$h \cdot g_1 \in \sqrt{I} \text{ en } h \cdot g_2 \in \sqrt{I}$$

want voor alle $k \in R$ geldt als $h \cdot k \in \sqrt{I}$ dan zit een macht van $h \cdot k$ in I.

En omdat $f_1(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = f_2(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0$, is dan de macht van $(h \cdot k)(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0$.

En dus

$$(h \cdot k)(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0.$$

Dat geeft

$$h(x_a, x_b, x_c, y_a, y_b, y_c) \cdot g_1(x_a, x_b, x_c, x_z) = 0 \quad en$$
$$h(x_a, x_b, x_c, y_a, y_b, y_c) \cdot g_2(y_a, y_b, y_c, y_z) = 0$$

Omdat a, b en c niet op een lijn liggen, geldt $h(x_a, x_b, x_c, y_a, y_b, y_c) \neq 0$ wegens Lemma 6.2.

Dus als

$h(x_a, x_b, x_c, y_a, y_b, y_c) \cdot g_1(x_a, x_b, x_c, x_z) = 0$. Dan is $g_1(x_a, x_b, x_c, x_z) = 0$.

En als

$h(x_a, x_b, x_c, y_a, y_b, y_c) \cdot g_2(y_a, y_b, y_c, y_z) = 0$. Dan is $g_2(y_a, y_b, y_c, y_z) = 0$.

Met het gebruik van het programma Sage, gaan we zien dat $h \cdot g_1$ en $h \cdot g_2$ wel allebei in $\sqrt{I}$ zitten. kijk hieronder.

In Sage geeft

```
R.<x_a,x_b,x_c,x_z,y_a,y_b,y_c,y_z>= PolynomialRing(Rationals(),8,order="lex")
f1 = (x_z - x_a)*(1/2 *(y_c+y_b) - y_a) - (y_z - y_a)*(1/2 *(x_b + x_c) - x_a)
f2 = (x_z - x_b)*(1/2 *(y_c+y_a) - y_b) - (y_z - y_b)*(1/2 *(x_a + x_c) - x_b))
I = Ideal([f1,f2])
g1 = x_a + x_b + x_c -3*x_z
g2 = y_a + y_b +y_c -3*y_z
h = (x_b - x_a)*(y_c - y_a) - (y_b - y_a)*(x_c - x_a)
h * g1 in I.radical()
```

het antwoord

```
True
```

En ook geeft

```
h * g2 in I.radical()
```

het antwoord

```
True
```

□

Stelling 6.4. $\sin 30^\circ = \frac{1}{2}$.

Bewijs. Neem $f_1 = X^2 + Y^2 - 1$. Dan is de verzameling $\{(x_0, y_0) \in \mathbb{R}^2 : f_1(x_0, y_0) = 0\}$ de eenheidscirkel. Voor $\alpha \in [0, 360]$ is $r_\alpha \colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ de rotatie afbeelding om punt $(0, 0)$ over de hoek α. We weten van lineare algebra dat het gegeven wordt door een matrix.

Voor $M_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ en voor alle $v \in \mathbb{R}^2$ geldt dat $r_\alpha(v) = M_\alpha \cdot v$. De eenheidscirkel C is een groep onder optelling van de hoeken. Inderdaad C is isomorfism met $\mathbb{R}/360\mathbb{Z}$.

Als α correspondeert met het punt (x_0, y_0) op de eenheidscirkel, dan is

$$M_\alpha = \begin{pmatrix} x_0 & -y_0 \\ y_0 & x_0 \end{pmatrix}.$$

Zij (x_0, y_0) het punt dat corespondeert met $30°$.

$$(x_0, y_0) \text{ correspondeert met } 30° \Longrightarrow 3 \cdot (x_0, y_0) = (0, 1).$$

En dat geeft

$$(x_0, y_0) \text{ correspondeert met } 30° \Longrightarrow M_\alpha^3 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

met

$$M_\alpha^3 = \begin{pmatrix} x_0^3 - 3x_0y_0^2 & -3x_0^2y_0 + y_0^3 \\ 3x_0^2y_0 - y_0^3 & x_0^3 - 3x_0y_0^2 \end{pmatrix}.$$

Noem $X^3 - 3XY^2 = f_2$ en $3X^2Y - Y^3 = g$.
En dat geeft

$$(x_0, y_0) \text{ correspondeert met } 30° \Longrightarrow \begin{pmatrix} x_0^3 - 3x_0y_0^2 & -3x_0^2y_0 + y^3 \\ 3x_0^2y_0 - y_0^3 & x_0^3 - 3x_0y_0^2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} x_0^3 - 3x_0y_0^2 \\ 3x_0^2y_0 - y_0^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Leftrightarrow \begin{Bmatrix} x_0^3 - 3x_0y_0^2 = 0 \\ 3x_0^2y_0 - y_0^3 = 1 \end{Bmatrix} \Leftrightarrow \begin{Bmatrix} f_2(x_0, y_0) = 0 \\ g(x_0, y_0) = 1 \end{Bmatrix}$$

Noem $g(x_0, y_0) - 1 = f_3(x_0, y_0)$. Dus

$$(x_0, y_0) \text{ correspondeert met } 30° \Longrightarrow \begin{Bmatrix} f_2(x_0, y_0) = 0 \\ f_3(x_0, y_0) = 0 \end{Bmatrix}.$$

Maar we moeten oppassen want de omkering is niet waar.

Als we $3 \cdot (x_0, y_0) = (0, 1)$ hebben, dan is de hoek die er bij hoort misschien niet $30°$ want voor de hoek $150°$ en $270°$ krijgen we het zelfde. Maar we weten dat

$$(x_0, y_0) \text{ correspondeert met } 270° \Leftrightarrow (x_0, y_0) = (0, -1).$$

Nu hebben we

$$\alpha \in \{30°, 150°\} \Leftrightarrow \begin{Bmatrix} f_1(x_0, y_0) = 0 \\ f_2(x_0, y_0) = 0 \\ f_3(x_0, y_0) = 0 \\ x_0 \neq 0 \text{ of } y_0 \neq -1 \end{Bmatrix}$$

We definiëren het ideaal I dat voortgebracht wordt door f_1, f_2 en f_3. We willen $\sin 30° = \frac{1}{2}$ bewijzen. Met andere woorden wil je bewijzen dat $y_0 = \frac{1}{2}$. Defineer $g = Y - \frac{1}{2}$.

Op de eenheidscirkel is er maar één punt met $y_0 = -1$. Dus als $y_0 = -1$ dan is vanzelf $x_0 = 0$. Daarom is het genoeg om alleen te eisen dat $y_0 \neq -1$. Defineer $h = Y + 1$.

We weten dat voor (x_0, y_0) geldt $f_1(x_0, y_0) = f_2(x_0, y_0) = f_3(x_0, y_0) = 0$. Dus is (x_0, y_0) een nulpunt voor alle polynomen in I.

Nu gaan we een Gröbner basis voor het ideaal $I = \langle f_1, f_2, f_3 \rangle$ bepalen met het gebruik van programma Sage.

```
R.<x,y> = PolynomialRing(Rationals(), 2, order = "lex")
f1 = x^2 + y^2 - 1
f2 =x^3 -3*x*y^2
f3 =+3*x^2*y -y^3 -1
I = Ideal([f1,f2,f3])
I.groebner_basis()
```

Dan geeft Sage het volgende antwoord

$$(X^2 - \frac{1}{2}Y - \frac{1}{2}, \quad XY - \frac{1}{2}X, \quad Y^2 + \frac{1}{2}Y - \frac{1}{2}).$$

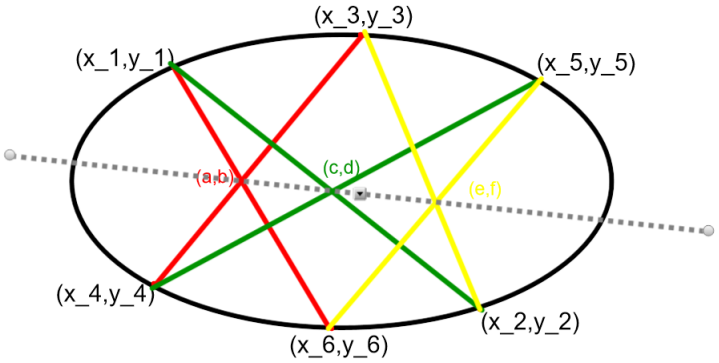
Om te bewijzen dat $y_0 = \frac{1}{2}$ is het genoeg om te bewijzen dat $h \cdot g \in \sqrt{I}$.

We hebben geluk want het polynoom waar we naar zoeken, zit in de verzameling van de Gröbner basis. namelijk het polynoom $Y^2 + \frac{1}{2}Y - \frac{1}{2} = (Y + 1)(Y - \frac{1}{2}) = h \cdot g$. Omdat we al hebben geëist dat $y_0 \neq -1$, geldt $(y_0 - \frac{1}{2}) = 0$ en dus $y_0 = \frac{1}{2}$. We concluderen dat $\sin 30° = \frac{1}{2}$. □

6.2 Voorbeeld waar het bepalen van Gröbner bases heel lang duurt

Je kan niet altijd de stellingen uit meetkunde bewijzen met het gebruik van Gröbner basis want het bepalen van Gröbner basis duurt soms heel lang en het heeft heel veel geheugen nodig. Hieronder maak je kennis met zo'n stelling.

Stelling 6.5 (Stelling van pascal)**.** *Neem de hoekpunten van een zeshoek op een cirkel, ellips, hyperbool of parabool en laat de drie paren van tegenovergestelde zijlijnen elkaar alle drie snijden. Hiermee zijn drie snijpunten van steeds twee lijnen bepaald. Deze drie punten liggen op één lijn.*



We gaan kijken naar een ellips. Een ellips is de verzameling van alle punten waarvoor de som van de afstanden tot brandpunten een vaste waarde heeft. Laat de brandpunten $(0,0)$ en $(0,1)$ zijn. En noem de vaste waarde z . Dan kan je de vergelijking van die ellips uitrekenen. Je krijgt dan

$$F = Z^4 - 2Z^2(2X^2 + Y^2 + (Y-1)^2) + (Y^2 - (Y-1)^2)^2.$$

Laat $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5), (x_6, y_6)$ zes punten op de ellips zijn.

Laat (a, b) het snijpunt zijn van de lijnen door $(x_1, y_1), (x_6, y_6)$ en $(x_3, y_3), (x_4, y_4)$, (c, d) het snijpunt van de lijnen door $(x_1, y_1), (x_2, y_2)$ en $(x_5, y_5), (x_4, y_4)$ en (e, f) het snijpunt van de lijnen door $(x_5, y_5), (x_6, y_6)$ en $(x_3, y_3), (x_2, y_2)$.

Laat $R = \mathbb{Q}[X_1, X_2, X_3, X_4, X_5, X_6, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, A, B, C, D, E, F, Z]$ zijn. En laat $>$ naar de lexicografische ordening verwijzen met $X_1 > X_2 > X_3 > X_4 > X_5 > X_6 > Y_1 > Y_2 > Y_3 > Y_4 > Y_5 > Y_6 > A > B > C > D > E > F > Z$ zijn.

Omdat (x_1, y_1) op de ellips ligt, dan hebben we

$$f_1(x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, y_5, y_6, a, b, c, d, e, f, z) = 0$$

met

$$f_1 = Z^4 - 2Z^2(2X_1^2 + Y_1^2 + (Y_1 - 1)^2) + (Y_1^2 - (Y_1 - 1)^2)^2.$$

Omdat er nog vijf punten op de ellips liggen , krijgen we op de zelfde manier f_2, f_3, f_4, f_5 en f_6.

Omdat $(x_1, y_1), (a, b)$ en (x_6, y_6) op één lijn liggen dan hebben we

$$f_7(x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, y_5, y_6, a, b, c, d, e, f, z) = 0$$

met

$$f_7 = (A - X_6)(Y_1 - Y_6) - (B - Y_6)(X_1 - X_6).$$

Op de zelfde manier krijgen we $f_8, f_9, f_{10}, f_{11}, f_{12}$.

We definiëren het ideaal $I = \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}, f_{12} \rangle$.

We willen graag een Gröbner bases voor het ideaal I bepalen met behulp van het programma Sage.

In sage geeft

```
R.<x_1,x_2,x_3,x_4,x_5,x_6,y_1,y_2,y_3,y_4,y_5,y_6,a,b,c,d,e,f,z> =
PolynomialRing(Rationals(), 19, order = "lex")
f1 = z^4 - 2*z^2*( 2*(x_1)^2 + (y_1)^2 + (y_1 - 1)^2) + (((y_1)^2 - (y_1 - 1)^2)^2)
f2 = z^4 - 2*z^2*( 2*(x_2)^2 + (y_2)^2 + (y_2 - 1)^2) + (((y_2)^2 - (y_2 - 1)^2)^2)
f3 = z^4 - 2*z^2*( 2*(x_3)^2 + (y_3)^2 + (y_3 - 1)^2) + (((y_3)^2 - (y_3 - 1)^2)^2)
f4 = z^4 - 2*z^2*( 2*(x_4)^2 + (y_4)^2 + (y_4 - 1)^2) + (((y_4)^2 - (y_4 - 1)^2)^2)
f5 = z^4 - 2*z^2*( 2*(x_5)^2 + (y_5)^2 + (y_5 - 1)^2) + (((y_5)^2 - (y_5 - 1)^2)^2)
f6 = z^4 - 2*z^2*( 2*(x_6)^2 + (y_6)^2 + (y_6 - 1)^2) + (((y_6)^2 - (y_6 - 1)^2)^2)
f7 = ((a - x_6)*(y_1 - y_6)) - ((b - y_6)*(x_1 - x_6))
f8 = ((a - x_4)*(y_3 - y_4)) - ((b - y_4)*(x_3 - x_4))
```

```
f9 = ((c - x_2)*(y_1 - y_2)) - ((d - y_2)*(x_1 - x_2))
f10 = ((c - x_4)*(y_5 - y_4)) - ((d - y_4)*(x_5 - x_4))
f11 = ((e - x_2)*(y_3 - y_2)) - ((f - y_2)*(x_3 - x_2))
f12 = ((e - x_6)*(y_5 - y_6)) - ((f - y_6)*(x_5 - x_6))
I = Ideal( [ f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,f12])
```

het volgende antwoord:

$$
\begin{aligned}
[&-4x_1^2z^2 - 4y_1^2z^2 + 4y_1^2 + 4y_1z^2 - 4y_1 + z^4 - 2z^2 + 1,\\
&-4x_2^2z^2 - 4y_2^2z^2 + 4y_2^2 + 4y_2z^2 - 4y_2 + z^4 - 2z^2 + 1,\\
&-4x_3^2z^2 - 4y_3^2z^2 + 4y_3^2 + 4y_3z^2 - 4y_3 + z^4 - 2z^2 + 1,\\
&-4x_4^2z^2 - 4y_4^2z^2 + 4y_4^2 + 4y_4z^2 - 4y_4 + z^4 - 2z^2 + 1,\\
&-4x_5^2z^2 - 4y_5^2z^2 + 4y_5^2 + 4y_5z^2 - 4y_5 + z^4 - 2z^2 + 1,\\
&-4x_6^2z^2 - 4y_6^2z^2 + 4y_6^2 + 4y_6z^2 - 4y_6 + z^4 - 2z^2 + 1,\\
&x_1y_6 - x_1b - x_6y_1 + x_6b + y_1a - y_6a,\\
&x_3y_4 - x_3b - x_4y_3 + x_4b + y_3a - y_4a,\\
&x_1y_2 - x_1d - x_2y_1 + x_2d + y_1c - y_2c,\\
&-x_4y_5 + x_4d + x_5y_4 - x_5d - y_4c + y_5c,\\
&-x_2y_3 + x_2f + x_3y_2 - x_3f - y_2e + y_3e,\\
&x_5y_6 - x_5f - x_6y_5 + x_6f + y_5e - y_6e.]
\end{aligned}
$$

Bij de vraag over Gröbner basis van het ideaal I

```
I.groebner_basis()
```

geeft programma sage geen antwoord.

Ik heb twee dagen mijn computer Gröbner bases laten berekenen en helaas lukt het niet. Als je dat gaat proberen, krijg je een groene lijn en dat betekent dat de computer bezig is met het berekenen.

6.3 Uitleg van de manier van het bewijzen

In deze paragraaf gaan we zien wat we eigenlijk in de vorige stellingen gedaan hebben. Alle stellingen die we eerder gezien hebben in hoofdstuk 6.1 zijn uitspraken die we aanduiden met (A, B, C) over rijtjes van punten $(P_1, P_2, ...P_n)$ in $\mathbb{R}^2$ met $P_i = (x_i, y_i)$ waarbij er uitspraken A, B, C zijn waarvoor we kijken naar de volgende uitspraak.

"Voor alle rijtjes $(P_1, P_2, ...P_n)$ in $\mathbb{R}^2$ met $P_i = (x_i, y_i)$ geldt dat als uitspraak $A(P_1, P_2, ...P_n)$ niet waar is en de uitspraak $B(P_1, P_2, ...P_n)$ wel waar is, dat dan de uitspraak $C(P_1, P_2, ...P_n)$ waar is".

En het bewijs van alle stellingen is van de vorm (J, I, g) waarbij J een ideaal is dat hoort bij de uitspraak A, I een ideaal dat hoort bij de uitspraak B en g een polynoom dat hoort bij de uitspraak C, en dat J en I idealen zijn in $R = \mathbb{Q}[X_1, X_2, ...X_n, Y_1, Y_2, ...Y_n]$ en $g \in R$.

Definitie 6.6. *Stel J en I zijn idealen in $R = \mathbb{Q}[X_1, X_2, ...X_n, Y_1, Y_2, ...Y_n]$, en $g \in R$. We zeggen dat het rijtje (J, I, g) de uitspraak (A, B, C) bewijst als*

1) *Voor alle punten $P_1, ..., P_n \in \mathbb{R}^2$ met $P_i = (x_i, y_i)$ geldt dat de uitspraak $A(P_1, ..., P_n)$ waar is als voor $m = (x_1, ..., x_n, y_1, ..., y_n) \in \mathbb{R}^{2n}$ en voor alle $f \in J$ geldt dat $f(m) = 0$.*

2) *Voor alle punten $P_1, ..., P_n \in \mathbb{R}^2$ met $P_i = (x_i, y_i)$ geldt de volgende Als de uitspraak $B(P_1, ..., P_n)$ waar is, dan geldt voor $m = (x_1, ..., x_n, y_1, ..., y_n) \in \mathbb{R}^{2n}$ en voor alle $h \in I$ dat $h(m) = 0$.*

3) *Voor alle punten $P_1, ..., P_n \in \mathbb{R}^2$ met $P_i = (x_i, y_i)$ geldt voor $m = (x_1, ..., x_n, y_1, ..., y_n) \in \mathbb{R}^{2n}$ dat $g(m) = 0 \Rightarrow$ de uitspraak $C(P_1, ..., P_n)$.*

4) *$g \cdot J \subset \sqrt{I}$.*

Opmerking 6.7. *Als het rijtje (J, I, g) de uitspraak (A, B, C) bewijst, dan is de uitspraak (A, B, C) ook inderdaad waar want als je aanneemt dat de uitspraak $A((P_1(x_1, y_1), ..., P_n(x_n, y_n))$ niet waar is en $B((P_1(x_1, y_1), ..., P_n(x_n, y_n))$ wel waar is, dan geldt voor alle $h \in I$ dat $h(x_1, ..., x_n, y_1, ..., y_n) = 0$.*

We weten dat als een polynoom in het radicaal van een ideaal zit, dan zit een macht van dat polynoom in het ideaal zelf. En als je een macht van dat polynoom invult en nul krijgt, dan is het ingevulde polynoom zelf nul.

Dat geeft dus dat voor alle $h \in \sqrt{I}$ geldt $h(x_1, ..., x_n, y_1, ..., y_n) = 0$. En dus ook voor alle $h \in J \cdot g \subset I$. Dus voor alle $f \in J$ geldt $(f \cdot g)(x_1, ..., x_n, y_1, ..., y_n) = 0$.

Omdat de uitspraak $A((P_1(x_1, y_1), ..., P_n(x_n, y_n))$ niet waar is, zijn er een polynomen $f \in J$ met $f(x_1, ..., x_n, y_1, ..., y_n) \neq 0$. Voor zo'n f geldt dus $f(x_1, ..., x_n, y_1, ..., y_n) \neq 0$. En dus geeft $(f \cdot g)(x_1, ..., x_n, y_1, ..., y_n) = 0$ dat $g(x_1, ..., x_n, y_1, ..., y_n) = 0$. Dus de uitspraak $C((P_1(x_1, y_1), ..., P_n(x_n, y_n))$ is waar.

Opmerking 6.8. *In deze opmerkingen gaan we praten over de uitspraken A, B, C en (J, I, g) bij elke stelling van paragraaf 6.1.*

Bij de stelling 6.1 hebben we het rijtjes (a, b, c, s) in $\mathbb{R}^2$ met $a = (x_a, y_a), b = (x_b, y_b), c = (x_c, y_c)$ en $s = (x_s, y_s)$. En $R = \mathbb{Q}[X_a, X_b, X_c, X_s, Y_a, Y_b, Y_c, Y_s]$. De uitspraak $A(a, b, c, s)$ is dat de drie punten a, b en c op één lijn liggen. Dat is equivalent met te zeggen dat

$$f(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0 \text{ met } f = (X_b - X_a)(Y_c - Y_a) - (Y_b - Y_a)(X_c - X_a).$$

De uitspraak $B(a, b, c, s)$ is dat het punt s op de hoogtelijnen uit a en b ligt. Dat is equivalent met te zeggen dat

$$\text{voor alle } k \in I = \langle f_1, f_2 \rangle \text{ geldt dat } k(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0$$

met

$$f_1 = X_s X_b + Y_s Y_b - X_s X_c - Y_s Y_c - X_a X_b - Y_a Y_b + X_a X_c + Y_a Y_c$$

en

$$f_2 = X_sX_c + Y_sY_c - X_sX_a - Y_sY_a - X_bX_c - Y_bY_c + X_bX_a + Y_bY_a.$$

En de uitspraak $C(a,b,c,s)$ is dat het punt s op de hoogtelijnen uit c ligt. Dat is equivalent met te zeggen dat

$$g(x_a, x_b, x_c, x_s, y_a, y_b, y_c, y_s) = 0$$

$$\text{voor } g = X_sX_a + Y_sY_a - X_sX_b - Y_sY_b - X_cX_a - Y_cY_a + X_cX_b + Y_cY_b.$$

We hebben bewezen dat $g \in I$. Dus in deze stelling is de uitspraak $A(a,b,c,s)$ niet nodig maar soms heb je de uitspraak $A(a,b,c,s)$ nodig.

Bij de stelling 6.3 hebben we het rijtjes (a,b,c,z) in $\mathbb{R}^2$ met $a = (x_a, y_a), b = (x_b, y_b), c = (x_c, y_c)$ en $z = (x_z, y_z)$. En $R = \mathbb{Q}[X_a, X_b, X_c, X_z, Y_a, Y_b, Y_c, Y_z]$. De uitspraak $A(a,b,c,z)$ is dat de drie punten a, b en c op één lijn liggen. Dat is equivalent met te zeggen dat

$$f(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0 \text{ met } f = (X_b - X_a)(Y_c - Y_a) - (Y_b - Y_a)(X_c - X_a).$$

De uitspraak $B(a,b,c,z)$ is dat k midden van bc, en l midden van ac. En z op lijn door ak, z op lijn door bl. Dat is equivalent met te zeggen dat

$$\text{voor alle } h \in I = \langle f_1, f_2 \rangle \text{ geldt dat } h(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0$$

met

$$f_1 = (X_z - X_a)((Y_b + Y_c)/2 - Y_a) - (Y_z - Y_a)((X_b + X_c)/2 - X_a)$$

en

$$f_2 = (X_z - X_b)((Y_a + Y_c)/2 - Y_b) - (Y_z - Y_b)((X_a + X_c)/2 - X_b).$$

En de uitspraak $C(a,b,c,z)$ in deze stelling bestaat uit twee delen daarom gaan we deze stelling apart twee keer toepassen. Dus de eerste uitspraak $C(a,b,c,z)$ is dat $3x_z = x_a + x_b + x_c$. Dat is equivalent met te zeggen dat

$$g_1(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0 \text{ voor } g_1 = X_a + X_b + X_c - 3X_z.$$

De tweede uitspraak $C(a,b,c,z)$ is dat $3y_z = y_a + y_b + y_c$. Dat is equivalent met te zeggen dat

$$g_2(x_a, x_b, x_c, x_z, y_a, y_b, y_c, y_z) = 0 \text{ voor } g_2 = Y_a + Y_b + Y_c - 3Y_z.$$

We hebben bewezen dat $f \cdot g_1 \in \sqrt{I}$ en $f \cdot g_2 \in \sqrt{I}$. Dus in deze stelling is de uitspraak $A(a,b,c,s)$ wel gebruikt.

Bij de stelling 6.4 hebben we alleen één punt $a = (x,y)$ in $\mathbb{R}^2$. En $R = \mathbb{Q}[X,Y]$. De uitspraak $A(a)$ is dat het punt $a = (x,y)$ gelijk aan $(0,-1)$ is. Maar als $y = -1$, dan is van zelf $x = 0$ want er is toevallig alleen één punt op

de cirkel met $y = -1$. Dat betekent dat het genoeg om te zeggen dat de uitspraak $A(a)$ is dat $y = -1$. Dat is equivalent met te zeggen dat

$$f(x, y) = 0 \text{ met } f = Y + 1.$$

De uitspraak $B(a)$ is dat het punt (x, y) op de eenheidscirkel ligt en dat $3 \cdot (x, y) = (0, 1)$. Dat is equivalent met te zeggen dat

$$\text{voor alle } k \in I = \langle f_1, f_2, f_3 \rangle \text{ geldt dat } k(x, y) = 0$$

met

$$f_1 = X^2 + Y^2 - 1, f_2 = X^3 - 3XY^2 \text{ en } f_3 = 3X^2Y - Y^3 - 1.$$

De uitspraak $C(a)$ is dat $y = \frac{1}{2}$. Dat is equivalent met te zeggen dat

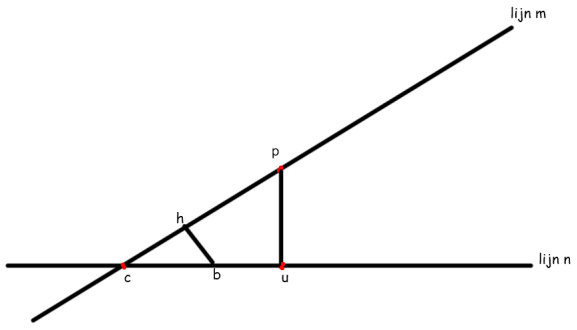
$$g(x, y) = 0 \text{ voor } g = 2Y - 1.$$

We hebben bewezen dat het polynoom $f \cdot g = (Y + 1)(2Y - 1) \in I$. Dus $(f \cdot g)(x, y) = (y + 1)(2y - 1) = 0$. Omdat de uitspraak $A(a)$ niet waar is, volgt dat $y + 1 \neq 0$. Dus $2y - 1 = 0$ en $y = \frac{1}{2}$.

7 Toepassing onmogelijk

In deze paragraaf zien we een voorbeeld waarin de vertaling van meetkunde naar algebra wel helemaal gedaan is en aan de eisen $1, 2$ en 3 van Definitie 6.6 voldaan is maar toch niet aan de eis 4 van Definitie 6.6 .

Stelling 7.1 (Stelling van Sylvester)**.** *Stel $S \subset \mathbb{R}^2$ is een eindige verzameling waarvoor geldt dat op elke lijn door twee punten uit S nog een derde punt uit S ligt. Dan liggen alle punten van S op één lijn.*



Bewijs. Laat S een eindige deelverzameling van $\mathbb{R}^2$ zijn. Laat N de verzameling zijn van alle lijnen die minstens door twee punten uit S gaan. Merk op dat N eindig is want S is eindig.

Laat Z de verzameling van alle afstanden die groter dan nul zijn van een punt uit S tot een lijn uit N . Met andere woorden $Z = \{d(p,n) : n \in N, p \in S \text{ en } p \notin n\}$. Merk op dat Z ook eindig is.

Neem aan dat Z niet leeg is. Dus Z heeft een minimum. Neem e het minimum van de verzameling Z. Kies nu een punt p en een lijn n zodanig dat $d(p,n) = e$.

Noem u de projectie van p op de lijn n. De lijn n is de vereniging van twee halflijnen die bij u beginnen. Dus omdat n minstens drie punten bevat, bevat minstens een van de halflijnen twee punten.

Neem maar twee punten die aan een kant van het punt u liggen. En noem b dat punt dat het dichts bij u ligt. Merk op dat de halflijnen beide u bevatten en dat b dus eventueel gelijk zou kunnen zijn aan u. En noem c het punt dat het verst van u ligt.

Neem de lijn m die door het punt p en c gaat. Noem h de projectie van b op de lijn m. Zie figuur 2.

Kijk nu naar de afstand van b tot m. We hebben $d(b,m) < d(p,n)$ want de driehoeken *puc* en *bhc* zijn gelijkvormig want de overeenkomstige hoeken zijn gelijk aan elkaar.

We krijgen een tegenspraak want we hebben aangenomen dat $d(p,n) = e$. En we hebben gevonden dat $d(b,m) < d(p,n) = e$. Dus Z is wel leeg, dus alle punten liggen op dezelfde lijn. En n zit in N, dus n bevat minstens drie punten. De aanname die tot een tegenspraak leidt is dat Z niet leeg is.

□

Stelling 7.2. *Stel dat we negen verschillende punten $P_v \in \mathbb{R}^2$ voor $v \in V = \mathbb{F}_3^2$ hebben. Stel dat voor elke u, v en $w \in V$ met $u + v + w = 0$ geldt dat P_u, P_v en P_w collineair zijn. Dan geldt ook dat $P_{(0,0)}, P_{(0,1)}$ en $P_{(1,0)}$ collineair zijn.*

Bewijs. Stel $u, v \in V$ zijn verschillend. Dan is ook $w = -u - v$ verschillend van u en v omdat $u + v + w$ gelijk aan 0 is, dus als $w = u$, dan $v = -2u = u = w$. Dan liggen de punten P_u, P_v en P_w op één lijn. Dat betekent dat door elke twee verschillende punten een lijn gaat waar nog één punt op ligt.

Volgens Stelling 7.1 geldt dat alle punten op één lijn liggen. Dan liggen zeker de punten $P_{(0,0)}, P_{(0,1)}$ en $P_{(1,0)}$ op één lijn. □

Opmerking 7.3. *In deze opmerking gaan we de uitspraken A, B en C van de stelling 7.2 definiëren en vertalen naar het rijtje (J, I, g).*

We hebben negen verschillende punten $P_v \in \mathbb{R}^2$ voor $v \in V = \mathbb{F}_3^2$ met $P_v = (X_v, Y_v)$. En R is de ring $\mathbb{Q}[X_v, Y_v : v \in V]$. In deze stelling is de uitspraak $A((P_v \text{ voor } v \in V))$ dat er twee punten tussen die negen punten zijn die hetzelfde zijn. Dat hoort bij het ideaal

$$J = \prod_{\{u,v\} \subset V, u \neq v} J_{uv}; \text{ met } J_{uv} = \langle X_v - X_u, Y_v - Y_u : u, v \in V \text{ en } u \neq v \rangle.$$

De uitspraak $B((P_v \text{ voor } v \in V))$ is dat voor elke u, v en $w \in V$ met $u + v + w = 0$ geldt dat P_u, P_v en P_w collineair zijn. Dat is equivalent met te zeggen dat $f_{uvw}(x_u, x_v, x_w, y_u, y_v, y_w) = 0$ met

$$f_{uvw} = (X_v - X_u)(Y_w - Y_u) - (Y_v - Y_u)(X_w - X_u).$$

Dat is precies wat hoort bij het ideaal I met

$$I = \langle f_{uvw} : u, v, w \in V \text{ met } u + v + w = 0 \rangle.$$

En de uitspraak $C((P_v \text{ voor } v \in V))$ is dat $P_{(0,0)}, P_{(0,1)}$ en $P_{(1,0)}$ collineair zijn. Dat is equivalent met te zeggen dat

$$g(x_{(0,0)}, x_{(0,1)}, x_{(1,0)}, y_{(0,0)}, y_{(0,1)}, y_{(1,0)} = 0$$

met

$$g = (X_{(0,1)} - X_{(0,0)})(Y_{(1,0)} - Y_{(0,0)}) - (Y_{(0,1)} - Y_{(0,0)})(X_{(1,0)} - X_{(0,0)}).$$

Opmerking 7.4. *We hebben nu gezien dat als je die uitspraken A, B en C definieert, voldoet dit rijtje (J, I, g) dan aan de eisen $1, 2$ en 3 van Definitie 6.6. maar we gaan laten zien dat het niet aan 4 van Definitie 6.6 voldoet.*

Stelling 7.5. *Laat V de vectorruimte $\mathbb{F}_3^2$ over het lichaam $\mathbb{F}_3$ zijn. Laat R de ring $\mathbb{Q}[X_v, Y_v : v \in V]$ zijn. Voor drie verschillende elementen u, v en $w \in V$ definiëren we*

$$f_{uvw} = (X_v - X_u)(Y_w - Y_u) - (Y_v - Y_u)(X_w - X_u) \in \mathbb{Q}[X_u, X_v, X_w, Y_u, Y_v, Y_w] \subset R.$$

Neem $I = \langle f_{uvw} : u, v, w \in V \text{ met } u + v + w = 0 \rangle$. Voor $u, v \in V$ met $u \neq v$ nemen we $J_{uv} = \langle X_v - X_u, Y_v - Y_u : u, v \in V \text{ en } u \neq v \rangle$. Schrijf $J = \prod_{\{u,v\} \subset V, u \neq v} J_{uv}$. En Laat $g = f_{(0,0),(0,1),(1,0)}$ zijn. Dan geldt $J \cdot g \not\subset \sqrt{I}$.

Bewijs. We definiëren de kromme $F = 4x^3 + y^3 - 9y$. We bekijken de buigpunten van deze kromme. Dan hebben we negen verschillende punten in $\mathbf{C}^2$. We schrijven α voor $\sqrt{-3}$.

$$P_{(0,0)} = (0,0), P_{(0,1)} = (0,-3), P_{(0,2)} = (0,3), P_{(1,0)} = (\tfrac{1}{2} \cdot (-\alpha - 3), -\alpha),$$
$$P_{(1,2)} = (\frac{1}{2} \cdot (-\alpha + 3), -\alpha), P_{(1,1)} = (\alpha, -\alpha), P_{(2,2)} = (-\alpha, \alpha),$$
$$P_{(2,1)} = (\frac{1}{2} \cdot (\alpha - 3), \alpha), P_{(2,0)} = (\frac{1}{2} \cdot (\alpha + 3), \alpha)\}$$

Kies een totale ordening op V. Definieer $h_{uv} \in J_{uv}$ als

$$h_{uv} = \begin{cases} Y_v - Y_u & \text{als } (u,v) \in \{(0,0),(0,1),(0,2)\} \\ X_v - X_u & \text{anders} \end{cases}$$

Neem $h = \prod_{\{u,v\} \in V, u \neq v} h_{uv} \in \prod_{\{u,v\} \in V, u \neq v} J_{uv} = J$. Er geldt dat $h(x_u, y_u : u \in V) \neq 0$. Er zijn 12 drietallen $u, v, w \subset V$ met $u + v + w = 0$ en $u \neq v$ en waarvoor ook geldt $u \neq v$ en $v \neq w$. Voor elke $u, v, w \subset V$ met $u + v + w = 0$ en $u \neq v$ is het makkelijk om te checken dat $f_{uvw}(x_u, x_v, x_w, y_u, y_v, y_w) = 0$. Volgens Stelling

6.2 kunnen we nu concluderen dat $P_u, P_v,$ en P_w collineair zijn. Dus we hebben 12 lijnen. Hieronder zijn de vergelijkingen van die lijnen.

$$f_1 = \frac{-2}{3}x+\frac{1}{3}y+1, f_2 = \frac{-1}{3}\alpha y+1, f_3 = x+\frac{1}{2}\cdot(\alpha-1)y, f_4 = \frac{1}{3}\cdot(\alpha-1)x-\frac{1}{3}y+1$$

$$f_5 = \frac{2}{3}x-\frac{1}{3}y+1, f_6 = x+\frac{1}{2}\cdot(-\alpha-1)y, f_7 = \frac{1}{3}\cdot(-\alpha-1)x-\frac{1}{3}y+1, f_8 = x+y$$

$$f_9 = \frac{1}{3}\cdot(-\alpha+1)x+\frac{1}{3}y+1, f_{10} = \frac{1}{3}\alpha y+1, f_{11} = x, f_{12} = \frac{1}{3}\cdot(\alpha+1)x+\frac{1}{3}y+1.$$

Laat g het polynoom die hoort bij $P_{(0,0)}, P_{(0,1)}, P_{(1,0)}$. Dan is

$$g(x_{(0,0)}, x_{(0,1)}, x_{(1,0)}, y_{(0,0)}, y_{(0,1)}, y_{(1,0)} = \frac{-5}{2}\alpha - \frac{9}{2} \neq 0.$$

Stel dat $J \cdot g \subset \sqrt{I}$. Er volgt dat $h \cdot g \in \sqrt{I}$. Dus er is een $n > 0$ zodanig dat $(h \cdot g)^n \in I$. We hebben $h \cdot g(x_u, y_u : u \in V) \neq 0$. Dus voor $n > 0$ geldt dat $(h \cdot g)(x_u, y_u : u \in V))^n \neq 0$. Dat is een tegenspraak want voor elke $q \in I$ geldt dat $q(x_u, y_u : u \in V) = 0$ en $(h \cdot g)^n \in I$ maar $(h \cdot g)^n \neq 0$. □

We hebben gezien dat de stelling 7.2 niet te bewijzen is met ons rijtje (J, I, g), maar misschien is er nog wel een andere rijtje of zelfs een andere $\acute{g}$ waarvoor het rijtje $(J, I, \acute{g})$ wel de uitspraken (A, B, C) bewijst.

Referenties

[1] David A . Cox, John Little, Donal O'Shea *Ideals, Varieties, and Algorithms* An Introduction to Computational Algebraic Geometry and Commutative Algebra Fourth Edition, 2015

[2] Serge lang, *Algebra,* Addison-Wesley, Third edition, 1993