

Discrete Wiskunde
2WC15, Lente 2010

Jan Draisma

HOOFDSTUK 2

Gröbnerbases

1. Vragen

We hebben gezien dat de studie van stelsels polynoomvergelijkingen in meerdere variabelen op natuurlijke manier leidt tot de begrippen ideaal en affiene variëteit. Daarover is een aantal voor de hand liggende vragen te stellen:

- (1) Is elk ideaal I in $K[x] = K[x_1, \dots, x_n]$ eindig voortgebracht? Dat wil zeggen, is er een eindige deelverzameling S van $K[x]$ zodanig dat $I = \langle S \rangle$? Dit is vanuit praktisch oogpunt wenselijk—hoe moeten we immers rekenen met een oneindig stelsel vergelijkingen?
- (2) Hoe gaan we na of de door I gedefinieerde variëteit niet leeg is, en wat de dimensie daarvan is? Wat is dimensie überhaupt?
- (3) Hoe vinden we het (impliciete) ideaal van relaties tussen m polynomen $f_1, \dots, f_m \in K[x]$?
- (4) Hoe bepalen we of een gegeven polynoom f in een ideaal I zit? Hoe bepalen we de doorsnede van twee idealen? Enzovoorts.

Op veel van deze vragen zullen we in dit college een antwoord geven, al zullen we het onszelf bij vraag (2) makkelijk maken door aan te nemen dat het lichaam K algebraïsch gesloten is. We beginnen met het volgende cruciale lemma.

LEMMA 1.1 (Dixons lemma). *Zij $u_1, u_2, \dots \in M(x)$ een oneindige rij monomen in $x = (x_1, \dots, x_n)$. Dan bestaan er indices i en j met $i < j$ waarvoor u_i een deler is van u_j .*

2. Deling met rest

We weten hoe deling met rest gaat voor polynomen in één variabele: bij deling van $f = ax^d + \text{lagere orde}$ door $g = bx^e + \text{lagere orde}$ met $a, b \neq 0$ wordt d met e vergeleken. Als $d < e$, dan zijn we klaar. Anders wordt $(a/b)x^{d-e}g$ van f afgetrokken, zodat de graad van f omlaag gaat, enz. Maar hoe zou dat moeten in polynomen met meer variabelen? Net zo, maar we hebben meer keuze in wat we de grootste term van f en g noemen.

DEFINITIE 2.1. Een *monomiale ordening* op de verzameling $M = M(x)$ van monomen in $x = (x_1, \dots, x_n)$ is een relatie $\leq$ die voor alle $u, v, w \in M$ voldoet aan:

- (1) $u \leq u$;
- (2) als $u \leq v$ en $v \leq w$ dan $u \leq w$;
- (3) als $u \leq v$ en $v \leq u$ dan $u = v$;
- (4) van de uitspraken $u \leq v$ en $v \leq u$ is er minstens één waar;

- (5) als $u \leq v$ dan $uw \leq uv$; en
 (6) $1 \leq u$.

De eerste twee axioma's zeggen dat $\leq$ een partiële quasi-ordeening is, het derde dat $\leq$ zelfs een partiële ordeening is, het vierde dat $\leq$ zelfs een totale ordeening is en het vijfde dat de ordeening compatibel is met vermenigvuldiging. Als $u \leq v$, dan zeggen we dat u ten hoogste v is, en dat v tenminste u is. We gebruiken ook de symbolen $<, \geq, >$ met de voor de hand liggende betekenis.

VOORBEELD 2.2. De *lexicografische ordeening* op $M(x)$ is de binaire relatie $\leq_{\text{lex}}$ gegeven door $x^\alpha \leq_{\text{lex}} x^\beta$ als en alleen als ofwel $\alpha = \beta$, ofwel de kleinste $i \in \{1, \dots, n\}$ met $\alpha_i \neq \beta_i$ voldoet aan $\alpha_i < \beta_i$. Dit is een monomiale ordeening.

OPGAVE 2.3. Laat zien dat uit de zes axioma's samen volgt dat $\leq$ een welordeening is, dat wil zeggen, dat elke niet-lege deelverzameling een kleinste element heeft. (Hint: gebruik Dixon's lemma.)

OPGAVE 2.4. Laat zien dat de relatie $\leq$ op $M(x)$ gedefinieerd door

$$x^\alpha \leq x^\beta :\Leftrightarrow |\alpha| < |\beta| \text{ of } |\alpha| = |\beta| \text{ en } \alpha \leq_{\text{lex}} \beta$$

een monomiale ordeening is. Deze ordeening heet *deglex*.

OPGAVE 2.5.

- (1) Laat $w_1, \dots, w_n$ positieve reële getallen zijn waartussen geen geheeltallige lineaire relatie bestaat, en zij $w := (w_1, \dots, w_n)$. Bewijs dat de relatie $\leq = \leq_w$ op $M(x)$ gedefinieerd door

$$x^\alpha \leq x^\beta :\Leftrightarrow \sum_i w_i \alpha_i \leq \sum_i w_i \beta_i$$

een monomiale ordeening is.

- (2) Neem aan dat $w' = (w'_1, \dots, w'_n) \neq w$ net zo'n vector is en dat de ordeening $\leq_{w'}$ gelijk is aan de ordeening $\leq_w$. Bewijs dat w' een positief scalair veelvoud is van w .
 (3) Concludeer dat er voor $n \geq 2$ overaftelbaar veel verschillende monomiale ordeeningen zijn. Hoe zit dat voor $n = 1$?
 (4) Is elke monomiale ordeening van de vorm $\leq_w$ voor geschikte w ?

De vector w in de vorige opgave heet een *gewichtsvector*, en $\sum_i w_i \alpha_i$ heet het w -gewicht van het monoom x^α . Als er wel geheeltallige lineaire relaties tussen de componenten van w bestaan, kun je w nog steeds gebruiken om een monomiale ordeening te definiëren, maar dan moet je monomen met hetzelfde w -gewicht nog weer verder ordenen, bijvoorbeeld lexicografisch. De ordeening *deglex* is hier een voorbeeld van, met $w = (1, 1, \dots, 1)$.

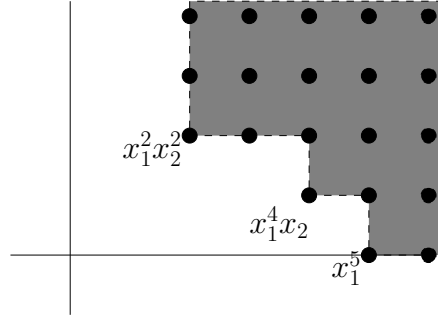
OPGAVE 2.6. Laat A een $n \times m$ -matrix zijn met positieve reële entries en neem aan dat er geen vector $v = (v_1, \dots, v_n) \in \mathbb{Z}^n$ bestaat met $vA = 0 \in \mathbb{R}^m$.

- (1) Bewijs dat de relatie $\leq$ op $M(x)$ gedefinieerd door

$$x^\alpha \leq x^\beta :\Leftrightarrow \alpha A \leq_{\text{lex}} \beta A$$

een monomiale ordeening is.

- (2) (*) Laat zien dat elke monomiale ordeening van deze vorm is.



FIGUUR 1. Het ideaal in $M(x)$ voortgebracht door $x_1^5, x_1^4 x_2, x_1^2 x_2^2$.

DEFINITIE 2.7. Zij $\leq$ een monomiale ordening op $M(x)$. Het *leidende monoom* $\text{lm}(f) = \text{lm}_{\leq}(f)$ van een polynoom $f \in K[x] \setminus \{0\}$ is het grootste monoom waarvan de coëfficiënt in f niet gelijk is aan 0. De *leidende coëfficiënt* $\text{lc}(f)$ van f is de coëfficiënt van $\text{lm}(f)$. De *leidende term* van f is $\text{lc}(f)\text{lm}(f)$.

OPGAVE 2.8. Laat zien dat $\text{lm}(fg) = \text{lm}(f)\text{lm}(g)$ en dat, als $f + g \neq 0$, $\text{lm}(f + g) \leq \max\{\text{lm}(f), \text{lm}(g)\}$.

LEMMA 2.9 (Deling met rest). *Zij S een deelverzameling van $K[x] \setminus \{0\}$ en zij $f \in K[x]$. Laat verder $\leq$ een monomiale ordening zijn. Dan is f te schrijven als $\sum_{s \in S} q_s s + r$ waarbij slechts eindig veel van de $q_s \in K[s]$ ongelijk aan nul zijn, en waarbij geen enkele term van r deelbaar is door een leidend monoom $\text{lm}(s)$ met $s \in S$.*

DEFINITIE 2.10. In dit geval heet r een *rest van f bij deling door S* .

Zo'n rest kan uitgerekend worden door eerst $r := f$ te nemen, en zo lang $r \neq 0$ is en bovendien een term cx^α heeft die door een leidend monoom $\text{lm}(s)$, $s \in S$ deelbaar is, r te vervangen door $r - (cx^\alpha/\text{lt}(s))s$; dit heet een *reductiestap*.

OPGAVE 2.11. Bewijs dat dit niet-deterministische algoritme om een rest van f bij deling door S te vinden altijd eindigt.

De output van dit niet-deterministische algoritme hangt van de monomiale ordening af, maar in het algemeen ook van de gekozen volgorde van de reductiestappen.

3. Hilberts Basisstelling

STELLING 3.1 (Hilberts Basisstelling). *Elk ideaal I in $K[x] = K[x_1, \dots, x_n]$ is eindig voortgebracht, d.w.z. van de vorm $\langle S \rangle$ met S een eindige deelverzameling van $K[x]$.*

In het bewijs gebruiken we een monomiale ordening; bijvoorbeeld $\leq_{\text{lex}}$, en definiëren we $\text{lm}(I) := \{\text{lm}(f) \mid f \in I \setminus \{0\}\}$. Dit is een ideaal in $M(x)$, wat wil zeggen dat het gesloten is onder vermenigvuldiging met elementen uit $M(x)$; zie Figuur 1. De exponenten van monomen in $\text{lm}(I)$ vormen een deelverzameling van $\mathbb{N}^n$ die “naar

boven toe gesloten is”. Uit Dixons lemma volgt dat er $f_1, \dots, f_k \in I$ zijn waarvoor geldt

$$\text{lm}(I) = \{m \in M(x) \mid \exists i \in \{1, \dots, k\} : \text{lm}(f_i) \mid m\};$$

we zeggen dat $\text{lm}(f_1), \dots, \text{lm}(f_k)$ het ideaal $\text{lm}(I)$ in $M(x)$ voortbrengen. Vervolgens volgt eenvoudig dat $\langle f_1, \dots, f_k \rangle = I$.

4. Gröbnerbases

Verzamelingen $\{f_1, \dots, f_k\}$ als in het bewijs van Hilberts basisstelling zijn zo belangrijk dat ze een naam verdienen.

DEFINITIE 4.1. Een *Gröbnerbasis* van een ideaal I in $K[x]$ ten opzichte van een monomiale ordening $\leq$ is een deelverzameling B van $I \setminus \{0\}$ met de eigenschap dat $\text{lm}(B)$ het ideaal $\text{lm}(I)$ in $M(x)$ voortbrengt. Een deelverzameling B van $K[x]$ heet een Gröbnerbasis (zonder meer) als B een Gröbnerbasis van $\langle B \rangle$ is.

(In veel boeken wordt bovendien geëist dat B eindig is; uit het bewijs van Hilberts Basisstelling weten we immers dat elk ideaal I een eindige Gröbnerbasis heeft.) Zo'n basis heeft allerlei belangrijke eigenschappen; we noemen er nu twee.

STELLING 4.1. *Zij B een Gröbnerbasis van een ideaal I en zij $f \in K[x]$. Dan bestaan er unieke $h \in I$ en $r \in K[x]$ zo dat $f = h + r$ en zo dat geen van de termen van r deelbaar is door een leidend monoom van een element uit B .*

Hieruit volgt dat als B een Gröbnerbasis is, de rest bij deling van f door B wel uniek is, en dat $f \in I$ geldt als en alleen als die rest nul is. Dit beantwoordt dus de laatste vraag van ons rijtje vragen aan het begin van dit hoofdstuk—mits we een Gröbnerbasis van een ideaal uit kunnen rekenen.

5. Buchbergers algoritme

Het algoritme van Buchberger heeft als input een eindig stel polynomen in $K[x]$ en als output een Gröbnerbasis van het door die polynomen voortgebrachte ideaal.

DEFINITIE 5.1. Zij $\leq$ een monomiale ordening op $M(x)$ en laat $f, g \in K[x]$ polynomen ongelijk aan nul zijn. Zij $u = \text{lm}(f)$, $v = \text{lm}(g)$ en $w = \text{lcm}(u, v)$. Dan heet

$$S(f, g) = S_{\leq}(f, g) = \text{lc}(g)(w/u)f - \text{lc}(f)(w/v)g$$

het *S-polynoom* van f en g .

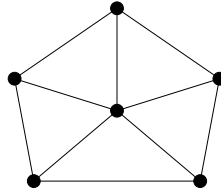
De volgende stelling is van fundamenteel belang in Buchbergers algoritme.

STELLING 5.1. *Zij B een deelverzameling van $K[x] \setminus \{0\}$. Neem aan dat voor elk paar $f, g \in B$ nul een rest is van het S-polynoom $S(f, g)$ bij deling door B . Dan is B een Gröbnerbasis van het ideaal $\langle B \rangle$.*

Dit leidt tot het volgende algoritme.

ALGORITME 5.2.

Input: een eindige deelverzameling T van $K[x] \setminus \{0\}$.



FIGUUR 2. Is deze graaf 3-kleurbaar?

Output: een eindige Gröbnerbasis van het door T voortgebrachte ideaal.

Procedure:

- (1) Stel $B := T$ en $P := \{\{f, g\} \mid f, g \in B\}$.
- (2) Zolang $P \neq \emptyset$ doe het volgende.
 - (a) Kies een paar $\{f, g\} \in P$ en verwijder dit uit P .
 - (b) Bereken een rest r van $S(f, g)$ bij deling door B .
 - (c) Als $r \neq 0$, voeg dan r aan B toe en voeg bovendien, voor alle $f \in B$, het paar $\{r, f\}$ aan P toe.
- (3) Return B .

STELLING 5.2. *Het bovenstaande algoritme geeft na eindig veel stappen als output een Gröbnerbasis van het ideaal dat door T wordt voortgebracht.*

Buchbergers algoritme is in **Singular** aan te roepen met het commando **groebner**. Een Gröbnerbasis van een ideaal I is bepaald niet uniek—als B een Gröbnerbasis van I is, dan is bijvoorbeeld ook $B \cup \{f\}$ een Gröbnerbasis van I , voor alle $f \in I$.

DEFINITIE 5.3. Een Gröbnerbasis B heet gereduceerd als elk element van B leidende coëfficiënt 1 heeft en als voor elk polynoom $f \in B$ geldt dat geen enkele term van f deelbaar is door een $\text{lm}(h)$ met $h \in B \setminus \{f\}$.

STELLING 5.3. *Zij I een ideaal in $K[x]$ en zij $\leq$ een monomiale ordening. Dan heeft I een unieke gereduceerde Gröbnerbasis ten opzichte van $\leq$.*

OPGAVE 5.4. Laat z_{ij} , $i \in \{1, \dots, m\}$, $j \in \{1, \dots, m\}$ variabelen zijn en neem de lexicografische monomiale ordening op $M(z)$ waarbij $z_{k,l} > z_{k',l'}$ als (k, l) lexicografisch groter is dan (k', l') . Leet zien dat de verzameling 2×2 -determinanten $z_{ij}z_{kl} - z_{il}z_{kj}$, $i, k = 1, \dots, m$; $j, l = 1, \dots, n$ een Gröbnerbasis is.

OPGAVE 5.5. Bewijs met een Gröbnerbasisberekening in **Singular** dat de knopen van de graaf in Figuur 2 niet te kleuren zijn met drie kleuren zonder twee naburige knopen dezelfde kleur te geven. Wat gebeurt er met de berekening als je een kant weglaat?