

Discrete Wiskunde
2WC15, Lente 2010

Jan Draisma

Voorwoord

Dit zijn aantekeningen voor het vak Discrete Wiskunde (2WC15), gegeven in het lenteseizoen van 2010. Dit vak bestaat uit twee delen: *algoritmische getaltheorie* van Benne de Weger en *rekenen in polynoomringen* van mijzelf; deze delen worden alternerend gegeven, met een gezamenlijke instructie. Deze aantekeningen betreffen het tweede deel. Ze zijn grotendeels gebaseerd op de tweede editie van het boek *Ideals, Varieties, and Algorithms* van Cox, Little, and O'Shea. Sterker nog, ze vormen slechts een beknopte samenvatting van de hoofdstukken uit dat boek die in het college aan bod komen. Voor motivatie, bewijzen en meer uitleg verwijs ik naar het boek.

Eindhoven, Lente 2010

Jan Draisma

Polynoomringen, variëteiten en idealen

1. Polynoomringen

DEFINITIE 1.1. Een *monoom* in de variabelen $x = (x_1, \dots, x_n)$ is een uitdrukking van de vorm $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ met $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. We schrijven ook wel x^α .

(In dit college begint $\mathbb{N}$ met 0.)

Twee monomen kun je met elkaar vermenigvuldigen volgens $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$. Deze operatie is associatief en heeft een neutraal element x^0 , ook wel met 1 aangeduid. De verzameling $M = M(x)$ van alle monomen in x is zodoende een *monoïde*, die bovendien commutatief is.

Zij K een lichaam. Hierbij mag je voor een groot deel van het college denken aan $\mathbb{C}$ of $\mathbb{R}$, maar ook bijvoorbeeld eindige lichamen zullen weer aan bod komen.

DEFINITIE 1.2. Een *polynoom* in x over K is een uitdrukking

$$\sum_{\alpha \in \mathbb{N}^m} c_\alpha x^\alpha$$

waarbij we eisen dat het aantal $\alpha \in \mathbb{N}^m$ waarvoor c_α ongelijk aan nul is eindig is.

Twee polynomen $f = \sum_\alpha c_\alpha x^\alpha$ en $g = \sum_\alpha d_\alpha x^\alpha$ kun je optellen volgens

$$f + g = \sum_\alpha (c_\alpha + d_\alpha) x^\alpha$$

en vermenigvuldigen volgens

$$f \cdot g = \sum_\gamma \left(\sum_{\alpha, \beta: \alpha+\beta=\gamma} c_\alpha d_\beta \right) x^\gamma.$$

Polynomen in x over K vormen met deze operaties een *ring*, die commutatief is en een neutraal element heeft (namelijk $1 \cdot x^0$, afgekort tot x^0 of 1), net zoals alle ringen in deze aantekeningen. Deze ring heet $K[x]$. Behalve een ring is het ook een *K-algebra*, want je kunt een polynoom met een getal uit K vermenigvuldigen en deze operatie is compatibel met de ringoperaties in R .

DEFINITIE 1.3. Voor $f = \sum_\alpha c_\alpha x^\alpha \in K[x]$ heet c_α de coëfficiënt van x^α in f , en als $c_\alpha \neq 0$ dan heet $c_\alpha x^\alpha$ een term van f . De (*totale*) *graad* $\deg f$ van f is de maximale waarde van

$$|\alpha| := \alpha_1 + \dots + \alpha_n$$

over alle termen $c_\alpha x^\alpha$ van f . Als f geen termen heeft (dus $f = 0$), dan definiëren we $\deg f := -\infty$.

2. Variëteiten

We zien polynomen graag als functies op een ruimte.

DEFINITIE 2.1. Het n -voudig Cartesisch product K^n heet de *n -dimensionale affiene ruimte* over K .

Een polynoom $f \in K[x]$ geeft een functie $K^n \rightarrow K$ als volgt: het punt $p = (c_1, \dots, c_n) \in K^n$ wordt afgebeeld op het element $f(p)$ van K dat je krijgt door in f de variabele x_i te vervangen door c_i en vervolgens alle operaties in f (optellen, vermenigvuldigen, vermenigvuldigen met getallen uit K) uit te voeren in K . Omgekeerd legt de functie $K^n \rightarrow K$ die door f gedefinieerd wordt, het polynoom f vaak eenduidig vast. Maar niet altijd.

VOORBEELD 2.2. Zij $K = \text{GF}(p)$, $n = 1$ en $f = x_1^p - x_1$. Dan is de door f gedefinieerde functie $K \rightarrow K$ overal nul, maar f is niet het nul-polynoom.

OPGAVE 2.3. Laat zien dat als $\deg f$ kleiner is dan het aantal elementen van K , de functie die door f gedefinieerd wordt niet overal 0 is. Hint: gebruik inductie naar n .

In het bijzonder geldt dus: als K oneindig is, dan legt de door een polynoom f gedefinieerde functie f eenduidig vast.

DEFINITIE 2.4. Het lichaam K heet *algebraïsch gesloten* als elk polynoom f over K in één variabele x_1 met $\deg f > 0$ een nulpunt in K heeft.

In dit geval is elk polynoom in $K[x_1]$ te schrijven als een getal maal een product van lineaire polynomen van de vorm $x_1 - c$. Uit een eerder college zul je je herinneren dat $\mathbb{C}$ algebraïsch gesloten is, maar $\mathbb{R}$ niet.

OPGAVE 2.5. Laat zien dat een algebraïsch gesloten lichaam oneindig is.

We komen nu aan de centrale definitie van dit college.

DEFINITIE 2.6. Zij S een deelverzameling van $K[x]$. Dan heet

$$V(S) := \{p \in K^n \mid \forall f \in S : f(p) = 0\} \subseteq K^n$$

de (*affiene*) *variëteit* gedefinieerd door S . Een willekeurige deelverzameling V van K^n heet een affiene variëteit als er een $S \subseteq K[x]$ bestaat waarvoor $V = V(S)$ geldt.

Voorbeelden zijn kegels in $\mathbb{R}^3$, kegelsneden, matrices van rang 2, enzovoorts.

3. Idealen

Merk op dat verschillende verzamelingen S dezelfde variëteit kunnen definiëren. Zo kun je $S = \{f_1, \dots, f_k\}$ vervangen door $S' = \{f_1, \dots, f_{k-1}, f_k + h_1 f_1 + \dots + h_{k-1} f_{k-1}\}$, waarbij $h_1, \dots, h_{k-1}$ willekeurige polynomen zijn—immers, S' heeft precies dezelfde nulpunten in K^n als S . Deze ambiguïteit wordt als volgt gedeeltelijk weggenomen.

DEFINITIE 3.1. Het *ideaal* $\langle S \rangle$ voortgebracht door S is de verzameling van alle polynomen van de vorm $h_1 f_1 + \dots + h_k f_k$ waarbij $f_1, \dots, f_k$ in S en $h_1, \dots, h_k$ in $K[x]$ zitten (en k willekeurig mag zijn).

Ga voor jezelf na dat dit inderdaad een ideaal in $K[x]$ is. Later zullen we effectief leren rekenen in $K[x]/\langle S \rangle$, zoals we dat met behulp van delen met rest al kunnen in het geval dat $n = 1$.

LEMMA 3.2. *De variëteit $V(\langle S \rangle)$ is identiek aan $V(S)$.*

Dit betekent dat we ons zonder verlies van algemeenheid kunnen beperken door affine variëteiten gedefinieerd door een ideaal. Overigens neemt dit de ambiguïteit niet helemaal weg. Zo definiëren $\langle x_1 \rangle$ en $\langle x_1^2 \rangle$ dezelfde variëteit in K^1 , maar zijn het verschillende idealen. Daarover later meer.

OPGAVE 3.3. Laat zien dat

- (1) $\emptyset$ en K^n affine variëteiten zijn;
- (2) de doorsnede van (willekeurig veel) affine variëteiten in K^n er weer een is;
- (3) de vereniging van twee affine variëteiten er weer een is;

Hint voor het laatste onderdeel: bekijk, voor $n = 3$, de variëteit V gedefinieerd door $S = \{x_1, x_2\}$ en de variëteit W gedefinieerd door $T = \{x_3\}$. Door welke polynomen wordt $V \cup W$ gedefinieerd?

4. Impliciet maken

Een belangrijke manier om idealen (en dus variëteiten) te definiëren is *impliciet*, als volgt. Stel we hebben een tweede collectie variabelen $y_1, \dots, y_m$, alsmede m polynomen $f_1, \dots, f_m \in K[x]$. Dan is $I = (f_1 - y_1, \dots, f_m - y_m)$ een ideaal in de ring $K[x_1, \dots, x_n, y_1, \dots, y_m] = K[x, y]$. De doorsnede $I \cap K[y]$ is een ideaal in $K[y]$, en definieert dus een variëteit in K^m .

OPGAVE 4.1. Laat zien dat $I \cap K[y]$ de *kern* is van het ring-homomorfisme $K[y] \rightarrow K[x]$ dat wordt vastgelegd door $y_1 \mapsto f_1$ en $y_2 \mapsto f_2$.

OPGAVE 4.2. Neem $K = \mathbb{R}, n = 1, m = 2, f_1 := 1 - x_1^2, f_2 := x_1(1 - x_1)^2$. Teken de kromme in $\mathbb{R}^2$ geparametriseerd door (f_1, f_2) en laat zien dat het ideaal $\langle f_1 - y_1, f_2 - y_2 \rangle \cap K[y_1, y_2]$ door één enkel polynoom wordt voortgebracht, en vindt dit polynoom.