

Discrete Wiskunde
2WC15, Lente 2010

Jan Draisma

HOOFDSTUK 3

De Nullstellensatz

1. De zwakke Nullstellensatz

STELLING 1.1. *Zij K een algebraïsch gesloten lichaam en zij I een ideaal in $K[x] = K[x_1, \dots, x_n]$ dat niet heel $K[x]$ is. Dan hebben de polynomen in I een gemeenschappelijk nulpunt in K^n .*

We zullen dit bewijzen voor het geval dat $K = \mathbb{C}$, waar we gebruik maken van het feit dat $\mathbb{C}$ overaftelbaar is. Het algemene bewijs is niet veel moeilijker, maar wel iets.

DEFINITIE 1.1. Zij T een enkele variabele. Met $\mathbb{C}(T)$ bedoelen we het *lichaam van rationale functies in T* , d.w.z. het lichaam bestaande uit uitdrukkingen van de vorm f/h met $f, h \in \mathbb{C}[T]$ en $h \neq 0$, met de gebruikelijke rekenregels.

We zullen $f/h \in \mathbb{C}(t)$ met $\text{ggd}(f, h) = 1$ ook opvatten als functie $\mathbb{C} \rightarrow \mathbb{C}$ die buiten de polen van h gedefinieerd is.

DEFINITIE 1.2. Zij L een lichaam. Met $V(L)$ bedoelen we de L -deelruimte van $L^{\mathbb{N} \times 1}$ bestaande uit alle oneindige kolomvectoren $(c_1, c_2, \dots)^T$ waarvoor slechts eindig veel van de c_i ongelijk aan nul zijn.

Een lineaire afbeelding van $V(L)$ naar zichzelf kan dan worden voorgesteld door middel van een $\mathbb{N} \times \mathbb{N}$ -matrix waarvan elke kolom een element van $V(L)$ is. Een L -lineaire functie van $V(L)$ naar L kan worden voorgesteld door een rijvector met componenten uit L , waarvan er nu *wel* oneindig veel niet nul mogen zijn.

LEMMA 1.3. *Zij $A(T)$ een $\mathbb{C}(T)$ -lineaire afbeelding van $V(\mathbb{C}(T))$ naar $V(\mathbb{C}(T))$, voorgesteld door een $\mathbb{N} \times \mathbb{N}$ -matrix als hierboven, en zij $v(T) \in V(\mathbb{C}(T))$. Neem aan dat er voor elke $t \in \mathbb{C}$ waar zowel alle componenten van $A(T)$ als die van $v(T)$ gedefinieerd zijn een $u \in V(\mathbb{C})$ bestaat met $A(t)u = v(t) \in V(\mathbb{C})$. Dan bestaat er een $u(T) \in V(\mathbb{C}(T))$ met $A(T)u(T) = v(T)$.*

BEWIJS. Laat $R \subseteq V(\mathbb{C}(T))$ de kolomruimte zijn van $A(T)$. We willen laten zien dat R de vector $v(T)$ bevat. Zo niet, dan kun je $v(T)$ van R scheiden met behulp van een $\mathbb{C}(T)$ -lineaire functie $f(T)$; concreet, er is een rijvector $f(T) \in \mathbb{C}(T)^{1 \times \mathbb{N}}$ met de eigenschap dat $f(T)A(T)u(T) = 0$ voor alle $u(T) \in V(\mathbb{C}(T))$ en $f(T)v(T) = 1$. Kies nu echter een $t \in \mathbb{C}$ waar alle componenten van zowel $f(T)$ als $A(T)$ als $v(T)$ gedefinieerd zijn. Dit kan omdat dat in totaal maar aftelbaar veel componenten zijn, die dus in totaal maar aftelbaar veel polen hebben, en anderzijds $\mathbb{C}$ overaftelbaar is. Nu is $f(t)$ een rij-vector in $\mathbb{C}^{1 \times \mathbb{N}}$ die voldoet aan $f(t)A(t)u = 0$ voor alle $u \in V(\mathbb{C})$ en aan $f(t)v(t) = 1$. Dit betekent dat het beeld van $A(t)$ bevat is in de kern van

$f(t)$, terwijl $v(t)$ dat niet is. Het stelsel $A(t)u = v(t)$ heeft dus geen oplossing, in tegenspraak tot de aanname. $\square$

BEWIJS VAN DE ZWAKKE NULLSTELLENSATZ VOOR $K = \mathbb{C}$. We redeneren met inductie naar het aantal variabelen n . We mogen dus aannemen dat als J een ideaal is in $\mathbb{C}[x_1, \dots, x_{n-1}]$ dat 1 niet bevat, J een nulpunt in $\mathbb{C}^{n-1}$ heeft. Zij nu I een ideaal in $\mathbb{C}[x_1, \dots, x_n]$ dat 1 niet bevat, en zij $f_1, \dots, f_k$ een eindig stel voortbrengers van I (die bestaan vanwege Hilberts Basisstelling). Voor elke waarde $t \in \mathbb{C}$ is de verzameling $J_t := \{f(x_1, \dots, x_{n-1}, t) \mid f \in I\}$ een ideaal in $\mathbb{C}[x_1, \dots, x_{n-1}]$ voortgebracht door de k polynomen $f_{i,t} := f_i(x_1, \dots, x_{n-1}, t)$. Als er een $t \in \mathbb{C}$ is waarvoor J_t het polynoom 1 niet bevat, dan zijn we klaar. Dan heeft J_t immers een nulpunt $(t_1, \dots, t_{n-1})$, en is $(t_1, \dots, t_{n-1}, t)$ een nulpunt van I .

Dus we mogen aannemen dat voor alle $t \in \mathbb{C}$ polynomen $u_1, \dots, u_k \in \mathbb{C}[x_1, \dots, x_{n-1}]$ bestaan met

$$u_1 f_{1,t} + \dots + u_k f_{k,t} = 1.$$

Merk op dat dit betekent dat

$$u_1 f_1 + \dots + u_k f_k = 1 + h \cdot (x_n - t)$$

voor zekere $h \in \mathbb{C}[x_1, \dots, x_n]$. Hieruit herleiden we dat

$$-h \cdot (x_n - t) \equiv 1 \pmod{I}.$$

Elk lineaire polynoom $x_n - t$ in $\mathbb{C}[x_n]$ heeft dus een multiplicatieve inverse modulo I . Omdat elk polynoom in $\mathbb{C}[x_n]$ een product is van lineaire polynomen— $\mathbb{C}$ is immers algebraïsch gesloten—volgt dat *elk* polynoom in $\mathbb{C}[x_n] \setminus \{0\}$ een multiplicatieve inverse modulo I heeft. Omdat I het polynoom 1 niet bevat, geldt dus $I \cap \mathbb{C}[x_n] = \{0\}$.

Bekijk aan de andere kant de $\mathbb{C}(T)$ -lineaire afbeelding

$$A(T) : (\mathbb{C}(T)[x_1, \dots, x_{n-1}])^k \rightarrow \mathbb{C}(T)[x_1, \dots, x_{n-1}],$$

$$(u_1, \dots, u_k) \mapsto u_1 f_1(x_1, \dots, x_{n-1}, T) + \dots + u_k f_k(x_1, \dots, x_{n-1}, T).$$

Gegeven is dat voor elke $t \in \mathbb{C}$ het stelsel $A(t)u = 1$ een oplossing $(u_1, \dots, u_k) \in \mathbb{C}[x_1, \dots, x_{n-1}]$ heeft. Zowel $\mathbb{C}(T)[x_1, \dots, x_{n-1}]$ als $(\mathbb{C}(T)[x_1, \dots, x_{n-1}])^k$ hebben aftelbare dimensie over $\mathbb{C}(T)$, dus we kunnen het bovenstaande lemma toepassen, en concluderen dat er een $u(T) = (u_1(T), \dots, u_k(T)) \in (\mathbb{C}(T)[x_1, \dots, x_{n-1}])^k$ bestaat waarvoor $A(T)u(T) = 1$. Uitschrijven geeft

$$u_1(T) f_1(x_1, \dots, x_{n-1}, T) + \dots + u_k(T) f_k(x_1, \dots, x_{n-1}, T) = 1,$$

waarbij de linkerkant rationaal van T afhangt. Kies een polynoom $h \in \mathbb{C}[T] \setminus \{0\}$ zodanig dat $u'_i(T) := h(T)u_i(T) \in \mathbb{C}[T][x_1, \dots, x_{n-1}]$ voor alle i . Dan volgt

$$u'_1(T) f_1(x_1, \dots, x_{n-1}, T) + \dots + u'_k(T) f_k(x_1, \dots, x_{n-1}, T) = h(T)$$

en door de variabele T te vervangen door x_n vinden we

$$u'_1(x_n) f_1 + \dots + u'_k(x_n) f_k = h(x_n).$$

Met andere woorden, $h(x_n)$ zit in I . Maar dit weerspreekt onze eerdere opmerking dat $I \cap \mathbb{C}[x_n] = \{0\}$. $\square$

2. De sterke Nullstellensatz

Bij een ideaal $I \subseteq K[x]$ hoort de nulpuntverzameling $V(I) \subseteq K^n$, een affiene variëteit. Omgekeerd hoort bij elke deelverzameling X van K^n een natuurlijk ideaal, namelijk:

$$\mathcal{I}(X) := \{f \in K[x] \mid f(p) = 0 \text{ voor alle } p \in X\}.$$

LEMMA 2.1. *Er geldt:*

- (1) als $I \subseteq J$ dan $V(I) \supseteq V(J)$;
- (2) als $X \subseteq Y$ dan $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$;
- (3) $\mathcal{I}(V(\mathcal{I}(X))) = \mathcal{I}(X)$;
- (4) $V(\mathcal{I}(V(I))) = V(I)$.

Hieruit volgt dat er een bi-jectie is tussen affiene variëteiten (verzamelingen van de vorm $V(I)$ voor zekere I) en *bepaalde* idealen, namelijk die van de vorm $\mathcal{I}(X)$ voor zekere X . De sterke Nullstellensatz geeft een alternatieve beschrijving van die laatste idealen.

DEFINITION 2.2. Een ideaal I in $K[x]$ heet *radicaal* als elke $f \in K[x]$ waarvan een positieve gehele macht f^n in I zit, zelf al in I zit.

OPGAVE 2.3. Laat zien dat I radicaal is als en alleen als $f \in K[x]$ geldt: als $f^2 \in I$ dan $f \in I$.

LEMMA 2.4. *Zij I een ideaal in $K[x]$. Dan is*

$$\sqrt{I} := \{f \in K[x] \mid \exists n \in \mathbb{Z}_0 : f^n \in I\}$$

een radicaal ideaal in $K[x]$ dat I bevat.

Dit ideaal heet het radicaal ideaal van I ; het is het *kleinste* radicale ideaal dat I bevat.

STELLING 2.1. *Neem aan dat K algebraïsch gesloten is. Dan geldt voor elk ideaal $I \subseteq K[x]$ dat $\mathcal{I}(V(I)) = \sqrt{I}$.*

3. Nullstellensatz-certificaten voor combinatorische problemen

Deze paragraaf is deels gebaseerd op werk van De Loera, Lee, Margulies en Onn. We weten dat $f_1 = 0, \dots, f_k = 0$ een oplossing heeft (over $\mathbb{C}$, of een ander algebraïsch gesloten lichaam) als en alleen als 1 niet in het door $f_1, \dots, f_k$ voortgebrachte ideaal zit. Een uitdrukking

$$1 = a_1 f_1 + \dots + a_k f_k$$

heet een *certificaat* voor het niet oplosbaar zijn van het stelsel. Als dat stelsel equivalent is met het oplosbaar zijn van een combinatorisch probleem, dan heet deze uitdrukking een *Nullstellensatz-certificaat* voor het niet oplosbaar zijn van dat combinatorische probleem. Aan de andere kant weten we dat zo'n uitdrukking altijd gevonden kan worden door een eindige Gröbnerbasisberekening.

OPGAVE 3.1. Een eindige, ongerichte graaf heet *Hamiltoniaans* als er een cykel is die alle knopen precies 1 keer aandoet. Modelleer de vraag of een graaf zo'n Hamiltoniaanse cykel heeft met behulp van een stelsel polynoomvergelijkingen, en

los zo'n stelsel op met behulp van Singular in twee gevallen: een waarbij de graaf Hamiltoniaans is, en een waarbij de graaf niet Hamiltoniaans is.

OPGAVE 3.2. Een *klik* in een graaf is een verzameling knopen die onderling paarsgewijs verbonden zijn. Modelleer de vraag of een graaf een klik ter grootte k heeft als een stelsel polynoomvergelijkingen, en los zo'n stelsel op met Singular, weer voor twee gevallen.