Primaire decomposities van idealen berekenen met Gröbnerbases

Bachelorproject, Leiden
Ronald van Luijk

Zij k een lichaam, n een positief geheel getal en $R = k[x_1, x_2, \ldots, x_n]$ de polynoomring in de n variabelen $x_1, x_2, \ldots, x_n$. Voor elk ideaal $I \subset R$ definiëren we de gezamenlijke nulpuntsverzameling

$$Z(I) = \{\ (a_1, \ldots, a_n) \in k^n\ :\ f(a_1, \ldots a_n) = 0 \text{ voor alle } f \in I\ \}$$

in k^n van alle $f \in I$. Voor $k = \mathbb{R}$ en $n = 2$ en $I = (x_1^2 + x_2^2 - 1)$ is $Z(I)$ bijvoorbeeld de eenheidscirkel in $\mathbb{R}^2$. Het is niet lastig in te zien dat voor twee idealen I_1 en I_2 van R geldt

$$Z(I_1 \cap I_2) = Z(I_1) \cup Z(I_2).$$

Zo kunnen we het ideaal $I = (x, yz) \subset k[x, y, z]$ schrijven als $I = (x, y) \cap (x, z)$, dus de verzameling $Z(I) \subset k^3$ is in dit geval de vereniging van de z-as en de y-as.

Definitie. Een *algebraïsche verzameling* in k^n is een verzameling $T \subset k^n$ waarvoor een ideaal $I \subset R$ bestaat met $Z(I) = T$.

Er is een topologie op k^n waarvan de gesloten verzamelingen precies de algebraïsche verzamelingen zijn. Deze topologie heet de Zariski topologie. Men kan laten zien dat uit het feit dat R noethers is volgt dat elke niet lege algebraïsche verzameling te schrijven is als vereniging van eindig veel algebraïsche verzamelingen die irreducibel zijn in deze topologie.

Dit project gaat over een analogie van deze uitspraak in termen van de idealen zelf. De meetkundige interpretatie hierboven is in die zin slechts een motivatie. Merk op dat voor een ideaal $I \subset R$ en het *radicaal*

$$\sqrt{I} = \{\ f \in R\ :\ \text{er is een } n \in \mathbb{Z}_{>0} \text{ met } f^n \in I\ \}$$

van I geldt $Z(\sqrt{I}) = Z(I)$.

Stelling 1. Zij $I \subset R$ een ideaal. Dan zijn er priemidealen $P_1, P_2, \ldots, P_r \subset R$ met

$$\sqrt{I} = P_1 \cap P_2 \cap \cdots \cap P_r.$$

Als we bovendien eisen $P_i \not\subset P_j$ voor $i \neq j$, dan zijn $P_1, P_2, \ldots, P_r$, op volgorde na, uniek bepaald.

Stelling 1 geldt zelfs als we R vervangen door een willekeurige noetherse commutatieve ring, waarin het radicaal van een ideaal op analoge manier wordt gedefinieerd. Dit project heeft onder andere als doel om bij een gegeven ideaal I in onze polynoomring R ook concreet de bijbehorende priemidealen $P_1, \ldots, P_r$ te bepalen.

Daarnaast willen we nog een stap verder gaan en kijken naar I zelf, in plaats van diens radicaal. Daartoe definiëren we het volgende.

Definitie. Zij S een commutatieve ring. Een ideaal $Q \subset S$ heet *primair* (Engels: primary ideal) als $Q \neq S$ en er voor elke $x, y \in S$ met $xy \in Q$ en $x \notin Q$ een $n \in \mathbb{Z}_{>0}$ is met $y^n \in Q$.

Het is duidelijk dat priemidealen primair zijn, maar niet alle primaire idealen zijn priem. Het radicaal $P = \sqrt{Q}$ van een primair ideaal Q is wel priem; we noemen P het priemideaal geassocieerd aan Q. Andersom is niet elk ideaal waarvan het radicaal priem is, zelf primair. Zo is het radicaal van het ideaal $I = (xy, x^2) \subset k[x, y]$ gelijk aan het priemideaal (x), maar het ideaal I is niet primair, want $xy \in I$ en $x \notin I$ en voor elke $n \in \mathbb{Z}_{>0}$ geldt $y^n \notin I$. Dit ideaal $I = (xy, x^2)$ is wel te schrijven als de doorsnede van primaire idealen, namelijk $I = (x) \cap (x^2, y)$. De volgende stelling zegt dat dit geen verrassing is.

Stelling 2. (Lasker-Noether) Zij S een commutatieve ring en $I \subset S$ een ideaal. Dan zijn er primaire idealen $Q_1, Q_2, \ldots, Q_r \subset S$ met

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r.$$

De primaire idealen $Q_1, Q_2, \ldots, Q_r$ geven een *primaire decompositie* van I. We noemen die decompositie *minimaal* als voor alle $i \neq j$ geldt $\sqrt{Q_i} \neq \sqrt{Q_j}$ en bovendien voor elke j geldt

$\bigcap_{i \neq j} Q_i \not\subset Q_j$. In dit geval geldt er geen uniciteit, zelfs niet voor minimale decomposities. Zo geldt er

$$I = (xy, x^2) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2).$$

We zien dat de geassocieerde priemidealen voor de twee composities wel hetzelfde zijn, namelijk (x) en (x, y). De volgende stelling is een versterking van Stelling 2 die zegt dat ook dit geen verrassing is.

Stelling 3. (Lasker-Noether) Zij S een commutatieve ring en $I \subset S$ een ideaal. Dan is er een minimale primaire decompositie

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r.$$

De radicalen $\sqrt{Q_1}, \ldots, \sqrt{Q_r}$ zijn, op volgorde na, uniek bepaald.

We noemen de idealen $\sqrt{Q_1}, \ldots, \sqrt{Q_r}$ uit de stelling de *priemidealen geassocieerd aan* I. Dit project bestaat eruit te onderzoeken hoe, gegeven een ideaal $I \subset R$, een minimale primaire decompositie van I berekend kan worden, of in elk geval de priemidealen geassocieerd aan I.

We zullen zien dat de zogeheten Gröbnerbases hierbij een belangrijk hulpmiddel zijn. Een Gröbnerbasis voor een ideaal $I \subset R$ is een rij voortbrengers voor I die aan een stel voorwaarden voldoet die het makkelijk maken om te checken of een polynoom $f \in R$ bevat is in I. Deze Gröbnerbases spelen een belangrijke rol bij veel berekeningen over idealen, bijvoorbeeld ook voor het berekenen van de dimensie van $Z(I)$.

Deze Gröbnerbases zijn behandeld in het vak Algorithms in Algebra. Studenten die dat vak niet gedaan hebben kunnen de theorie daarvan leren als onderdeel van het project. We beginnen met het boek [CLOS], in het bijzonder Secties 4.6 en 4.8, en volgen sommige referenties daaruit.

Referenties

[CLOS] D. Cox, J. Little, Donal O'Shea, *Ideals, Varieties, and Algorithms, An introduction to Computational Algebraic Geometry and Commutative Algebra*, fourth edition, Undergraduate Texts in Mathematics, Springer, 2018.