De combinatorische Nullstellensatz

Laat R een commutatieve ring zijn, zij n een positief geheel getal, en $f \in R[X_1, \ldots, X_n]$. Als we in f voor elke i een element $x_i \in R$ voor X_i substitueren, dan krijgen we een element $f(x_1, \ldots, x_n)$ van R. Op deze manier kunnen we f opvatten als een afbeelding $R^n \to R$. Men moet er echter voor oppassen om f met die afbeelding te *identificeren*, want er zijn situaties dat twee *verschillende* elementen van $R[X_1, \ldots, X_n]$ aanleiding geven tot *dezelfde* afbeelding $R^n \to R$. Dit zal in het bijzonder moeten gebeuren als R *eindig* is, maar niet de nulring; dan is $R[X_1, \ldots, X_n]$ immers *oneindig*, terwijl er maar *eindig* veel afbeeldingen $R^n \to R$ zijn. Voorbeelden met *oneindige* R kan men met een beetje moeite ook maken.

Als men voor R een oneindig *domein* neemt, ziet de situatie er veel beter uit: twee verschillende polynomen in $R[X_1, \ldots, X_n]$ geven dan nooit dezelfde afbeelding $R^n \to R$; equivalent: als $f \neq 0$, dan bestaat er $(x_1, \ldots, x_n) \in R^n$ met $f(x_1, \ldots, x_n) \neq 0$. In feite is het niet lastig de volgende kwantitatieve verscherping hiervan te bewijzen.

Stelling. *Zij R een domein, n een positief geheel getal, en $f \in R[X_1, \ldots, X_n]$, $f \neq 0$. Zij d_i de graad van f in X_i, en stel, voor elke i, dat $A_i \subset R$ een deelverzameling is met $\#A_i > d_i$. Dan bestaat er een element $(x_1, \ldots, x_n) \in \prod_{i=1}^n A_i$ met de eigenschap $f(x_1, \ldots, x_n) \neq 0$.*

De *combinatorische Nullstellensatz* geeft scherpere versies van deze stelling. Men werkt steeds met dezelfde aannamen op R, n en A_i, en ook de conclusie van de stelling is dezelfde, maar het verschil zit in de manier waarop de getallen $d_1, \ldots, d_n$ gedefinieerd zijn. Een populaire versie van de combinatorische Nullstellensatz is bijvoorbeeld de volgende.

Stelling. *Zij R een domein, n een positief geheel getal, en $f \in R[X_1, \ldots, X_n]$, $f \neq 0$. Zij d de totale graad van f, en stel dat $aX_1^{d_1} \cdots X_n^{d_n}$ een term van f is met $a \in R$, $a \neq 0$, en $d_1 + \ldots + d_n = d$. Stel verder dat $A_i \subset R$ een deelverzameling is met $\#A_i > d_i$. Dan bestaat er een element $(x_1, \ldots, x_n) \in \prod_{i=1}^n A_i$ met de eigenschap $f(x_1, \ldots, x_n) \neq 0$.*

Toepassingen van deze stelling zijn vaak combinatorisch van aard. Men kan er bijvoorbeeld een kort bewijs mee geven van de volgende stelling, waar eerder alleen maar veel prutseriger bewijzen van bestonden.

Stelling. *Zij p een priemgetal, en stel dat A en B twee niet-lege deelverzamelingen van $\mathbf{Z}/p\mathbf{Z}$ zijn. Schrijf $A + B = \{x + y : x \in A, y \in B\} \subset \mathbf{Z}/p\mathbf{Z}$. Dan geldt*

$$\#(A + B) \geq \min\{p, \#A + \#B - 1\}.$$

Het project bestaat uit de bestudering van de combinatorische Nullstellensatz en zijn wiskundige context. Hoe worden alle bovengenoemde stellingen bewezen? Wat voor verscherpingen en verdere toepassingen zijn er? Is er een relatie met de zogenaamde *Hilbert Nullstellensatz*? Ook historische vragen zijn interessant. Hoe oud is de stelling? Van wie is hij afkomstig, en voor welk doel werd de stelling oorspronkelijk bedacht?

De begeleider kent zelf niet alle antwoorden, en verheugt zich erop meer over het onderwerp te weten te komen.

Begeleider: H. W. Lenstra