De combinatorische Nullstellensatz

De *combinatorial Nullstellensatz* van Noga Alon (Combin. Probab. Comput. **8** (1999), 7–29) is een stelling uit de algebra die een groot aantal toepassingen heeft in de grafentheorie, de combinatoriek en de combinatorische getaltheorie. Niet lang geleden is ontdekt dat de stelling ook in de algebra zelf interessante gevolgen heeft.

Voor een commutatieve ring R en $n \in \mathbf{Z}_{>0}$ kan men elke $f \in R[X_1, \ldots, X_n]$ opvatten als afbeelding van R^n naar R; men moet echter f niet met die afbeelding *identificeren*, want er zijn vele situaties waarin twee verschillende elementen van $R[X_1, \ldots, X_n]$ aanleiding geven tot dezelfde afbeelding $R^n \to R$.

Voor een *oneindig domein* R 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, waarin R niet oneindig hoeft te zijn, 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 relatie van de getallen $d_1, \ldots, d_n$ tot f. 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 en elegant 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 kan, na bestudering van de voornaamste varianten van de combinatorische Nullstellensatz en hun bewijs, verschillende kanten uitgaan. Enerzijds kan een overzicht van de bestaande combinatorisch getinte toepassingen van de stelling gegeven worden. Anderzijds kan de student de eerder genoemde algebraïsche toepassingen, die nog niet gepubliceerd zijn, uitdiepen. Hiertoe behoort een nieuw bewijs van de *stelling van de normale basis* uit de Galoistheorie; zoals het er nu naar uitziet, komt hier ook enige niet-commutatieve ringentheorie bij kijken.

Begeleider: H. W. Lenstra