M. Heemskerk

Basisuitbreidingen en de Combinatorische Nullstellensatz

Bachelorscriptie

Scriptiebegeleider: prof.dr. H.W. Lenstra

Datum Bachelorexamen: 25 augustus 2014

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

0 Inleiding

We zullen kijken naar toepassingen van de Combinatorische Nullstellensatz, die als volgt luidt.

Stelling 0.1 (De Combinatorische Nullstellensatz, 1999, [1])**.** *Zij k een lichaam en $n \in \mathbb{Z}_{\geq 0}$. Laat f een polynoom over k zijn in n variabelen met een niet-nul term $cX_1^{t_1}X_2^{t_2}\dots X_n^{t_n}$ met $\sum_i t_i = \deg(f)$ voor zekere $c \in k, t_1, t_2, \dots, t_n \in \mathbb{Z}_{\geq 0}$ en laat $S_1, S_2, \dots, S_n \subset k$ een stel verzamelingen zijn met $|S_i| > t_i$ voor alle i. Dan bestaat er een punt $(s_1, s_2, \dots, s_n) \in S_1 \times S_2 \times \dots \times S_n$ zodanig dat $f(s_1, s_2, \dots, s_n) \neq 0$.*

Alon was de eerste die de stelling bewees en belangrijker, hij heeft voor het eerst de grote toepasbaarheid van de Nullstellensatz binnen de combinatoriek en grafentheorie aan het licht gebracht. Wij vinden hier een aantal algebraïsche toepassingen. We gebruiken hierbij de volgende stelling, die de Combinatorische Nullstellensatz in een meer coördinaatvrije vorm helpt gieten.

Stelling 0.2. *Zij k een lichaam, zij $m, n \in \mathbb{Z}_{\geq 0}$ met $n > 0$ en laat $R = k[X_1, X_2, \dots, X_n]$. Schrijf p voor de karakteristiek van k. Voer voor $q > 0$ de notatie $\mathcal{S}_q$ in voor de verzameling van polynomen f met een niet-nul term waarin voor iedere i de macht van X_i hoogstens $q-1$ is en waarvan de graad gelijk is aan de graad van f. De verzameling $\mathcal{S}_0$ nemen we gelijk aan $R \setminus \{0\}$. Schrijf $q = p^m$ als $p > 0$ en $q = 0$ als $p = 0$. Dan geldt voor ieder automorfisme σ van de ring R dat de totale graad bewaart*

$$\sigma(\mathcal{S}_q) = \mathcal{S}_q.$$

Deze stelling bewijzen we in stelling 1.2. De toepassingen die we vinden handelen over basisuitbreidingen van modulen over een algebra over een lichaam. Door een basisuitbreiding toe te passen kunnen we meer informatie krijgen over de modulen in kwestie en de vraag is of deze informatie gereflecteerd wordt. Isomorfie is onder zekere eindigheidsvoorwaarden een van de eigenschappen die gereflecteerd wordt door basisuitbreiding. We verwijzen voor de notatie naar paragraaf 3.

Stelling 0.3. *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra zijn. Als M en N twee A-modulen van eindige dimensie over k zijn met $M_K \cong N_K$ als A_K-modulen, dan geldt $M \cong N$ als A-modulen.*

Verrassend is dat we bij het bewijs van deze stelling, dat te vinden is in stelling 5.1, het grootste deel van het werk kunnen laten doen door de Combinatorische Nullstellensatz.

Voordat we beginnen, stellen we nog wat definities vast. Ringen bevatten een eenheid. Voor een commutatieve ring R is een R-algebra A een ring met een ringhomomorfisme $R \to Z(A)$, waar $Z(A)$ het centrum van A is. Met de graad van een polynoom wordt tenzij anders vermeld de totale graad bedoeld.

1 De Combinatorische Nullstellensatz

De versie van de Nullstellensatz die we geven is de volgende.

Stelling 1.1 (De Combinatorische Nullstellensatz, 1999, [1])**.** *Zij k een lichaam en $n \in \mathbb{Z}_{\geq 0}$. Laat f een polynoom over k zijn in n variabelen met een niet-nul term $cX_1^{t_1}X_2^{t_2}\dots X_n^{t_n}$ met $\sum_i t_i = \deg(f)$ voor zekere $c \in k, t_1, t_2, \dots, t_n \in \mathbb{Z}_{\geq 0}$ en laat voor iedere i, $1 \leq i \leq n$ een verzameling $S_i \subset k$ gegeven zijn met $|S_i| > t_i$. Dan bestaat er een punt $(s_1, s_2, \dots, s_n) \in S_1 \times S_2 \times \dots \times S_n$ zodanig dat $f(s_1, s_2, \dots, s_n) \neq 0$.*

Waar Alon deze stelling meer als gevolg van een andere stelling bewees, kiezen wij ervoor om het bewijs direct te voeren.

Bewijs. We bewijzen de stelling door middel van inductie naar de graad van het polynoom f. Voor $m = 0$ en $\deg(f) = m$ is f constant ongelijk nul, want f heeft een niet nul term. Merk op dat de verzamelingen S_i in de hypothese minstens 1 punt bevatten. Ieder punt is een niet-nulpunt van f en in dit geval klopt de uitspraak dus.

Zij $m \geq 1$ nu willekeurig gegeven, neem aan dat $\deg(f) = m$ en neem aan dat de uitspraak waar is voor alle lagere graden. Neem verder aan, om een tegenspraak af te leiden, dat f nul is op de hele verzameling $S_1 \times S_2 \times \dots \times S_n$. De gegeven term van f is niet constant en we mogen dus zonder verlies van algemeenheid aannemen dat $t_1 > 0$. Beschouw f als polynoom in X_1 over $R = k[X_2, X_3, \dots, X_n]$ en kies $s_1' \in S_1$. Schrijf f als

$$f = (X_1 - s_1')q + r$$

met $q, r \in k[X_1, X_2, \dots, X_n]$ en $\deg_{X_1}(r) < \deg_{X_1}(X_1 - s_1') = 1$, dat wil zeggen, $\deg_{X_1}(r) \leq 0$. Het polynoom q heeft een niet nul term $cX_1^{t_1-1}X_2^{t_2}\dots X_n^{t_n}$. Immers, omdat de onbekende X_1 niet voorkomt in r moet de in de hypothese gegeven term van f komen van het product $(X_1 - s_1')q = X_1q - s_1'q$. De hoogstegraads termen van X_1q hebben hogere graad dan die van $s_1'q$, dus de term moet van X_1q komen. Merk op dat de genoemde term van q graad $m-1$ heeft. Het polynoom q kan verder ook geen termen hebben van graad groter dan $m-1$ want deze zouden vermenigvuldigd met X_1 niet meer weg kunnen vallen tegen de termen van r en dit zou betekenen dat de graad van f groter is dan m.

Vullen we een punt $s \in \{s_1'\} \times S_2 \times S_3 \times \dots \times S_n$ in, dan krijgen we

$$0 = f(s) = (s_1' - s_1')q(s) + r(s) = r(s)$$

en omdat r niet van X_1 afhangt, krijgen we voor iedere $s \in S_1 \setminus \{s_1'\} \times S_2 \times S_3 \times \dots \times S_n$ ook

$$0 = f(s) = (s_1 - s_1')q(s) + r(s) = (s_1 - s_1')q(s).$$

Omdat k een domein is betekent dit dat $q(s) = 0$.

We kunnen echter ook de inductiehypothese toepassen op q met de term $cX_1^{t_1-1}X_2^{t_2}\dots X_n^{t_n}$ en de verzamelingen $S_1 \setminus \{s_1'\}, S_2, \dots S_n$. Merk hierbij op dat $S_1 \setminus \{s_1'\}$ niet leeg is omdat t_1 groter gelijk 1 aangenomen is. Dit geeft dat q niet op de hele verzameling $S_1 \times S_2 \times \dots \times S_n$ nul is en dit is in tegenspraak met wat we hiervoor afleidden. We concluderen dat f niet nul kan zijn op de hele verzameling en dus dat er een punt $s \in S_1 \times S_2 \times \dots \times S_n$ is zodanig dat $f(s) \neq 0$. □

Een familie verzamelingen van polynomen die we later vaak tegenkomen is die waar de S_i uit de stelling allemaal evengroot genomen kunnen worden. Dit zijn de verzamelingen $\mathcal{S}_q$ van polynomen met een niet-nul term van hoogste graad waarvan de graad in iedere onbekende kleiner is dan $q \in \mathbb{Z}_{>0}$. Merk op dat we deze definitie niet laten afhangen van het aantal onbekenden. We zullen altijd werken met een constant aantal onbekenden en uit de context zal dus altijd duidelijk zijn wat dit aantal is. We zullen met name kijken naar de verzamelingen $\mathcal{S}_{p^m}$ met p een priemgetal en $m \in \mathbb{Z}_{\geq 0}$. De verzamelingen $\mathcal{S}_0$ definiëren we als de gehele verzameling van niet-nul polynomen $R \setminus \{0\} = k[X_1, X_2, \dots, X_n] \setminus \{0\}$.

Wanneer dit getal q een macht is van de karakteristiek van het lichaam k zegt de volgende stelling dat deze verzameling invariant is onder ieder automorfisme van de polynoomring dat de totale graad bewaart. De verzameling van deze automorfismen

$$\mathrm{Aut}_{\deg}(R) := \{\sigma \in \mathrm{Aut}(R) \mid \forall f \in R\colon \deg(\sigma(f)) = \deg(f)\}$$

vormt een ondergroep van de groep $\mathrm{Aut}(R)$ van ringautomorfismen van R.

Stelling 1.2. *Zij k een lichaam, zij $m, n \in \mathbb{Z}_{\geq 0}$ en laat $R = k[X_1, X_2, \dots, X_n]$. Schrijf p voor de karakteristiek van k en schrijf $q = p^m$ als $p > 0$ en $q = 0$ als $p = 0$. Dan geldt voor iedere $\sigma \in \mathrm{Aut}_{\deg}(R)$*

$$\sigma(\mathcal{S}_q) = \mathcal{S}_q.$$

Ten eerste moeten we wat meer weten over de groep $\mathrm{Aut}_{\deg}(R)$. De ring R wordt als k-algebra voortgebracht door de onbekenden $X_1, \dots, X_n$. Dit betekent dat ieder automorfisme van de ring R vaststaat door waar k en de onbekenden afbeelden. Iedere $\sigma \in \mathrm{Aut}_{\deg}(R)$ beeldt k (het graad kleiner gelijk 0 stuk) af in k en werkt dus op k als een element van $\mathrm{Aut}(k)$. Verder hebben we voor iedere i

$$\sigma(X_i) = a_{1i}X_1 + a_{2i}X_2 + \dots + a_{ni}X_n + c_i$$

voor zekere $a_{1i}, \dots, a_{ni}, c_i \in k$ met minstens één a_{ji} niet gelijk aan nul, want het element X_i van graad 1 wordt afgebeeld op een element van graad 1.

Voor $p = 0$ is de uitspraak van stelling 1.2 triviaal, dus neem aan dat $p > 0$. We zullen laten zien dat de gelijkheid van het lemma geldt voor het complement $\mathcal{C} = (\mathcal{S}_q)^c = R \setminus \mathcal{S}_q$. Omdat iedere $\sigma \in \mathrm{Aut}_{\deg}(R)$ een bijectie is, is dit equivalent met het lemma. Verder is het zelfs genoeg te laten zien dat $\sigma(\mathcal{C}) \subset \mathcal{C}$, omdat σ^{-1} ook een graadbewarend automorfisme is.

Bewijs. De verzameling $\mathcal{C}$ is die van de polynomen waarvan er voor iedere leidende term, waarmee we een term van hoogste graad in het polynoom bedoelen, een i met $1 \leq i \leq n$ is zodanig dat deze term deelbaar is door X_i^q. Dit betekent dat dit precies de polynomen zijn waarvan de leidende termen bevat zijn in het ideaal $I = (X_1^q, X_2^q, \ldots, X_n^q)$. Schrijven we $f \in \mathcal{C}$ als som $f = g + h$ met g homogeen, $\deg(g) = \deg(f)$ en $\deg(h) < \deg(f)$, dan zien we dat $\sigma(f) = \sigma(g) + \sigma(h)$ en omdat σ de totale graad bewaart, betekent dit dat de leidende termen van $\sigma(f)$ precies de leidende termen van $\sigma(g)$ zijn. We mogen dus zonder verlies van algemeenheid aannemen dat f homogeen is.

Voor $f_1 \in \mathcal{C}$ en $r \in R$ zijn de leidende termen van $\sigma(rf_1) = \sigma(r)\sigma(f_1)$ producten van de leidende termen van $\sigma(f_1)$ met de leidende termen van $\sigma(r)$ en deze zijn dus ook in I bevat. Dit betekent dat $\sigma(r)\sigma(f_1)$ bevat is in $\mathcal{C}$. Als f_1 nu homogeen is en $f_2 \in \mathcal{C}$ is een homogeen polynoom van graad $\deg(f_1)$, zodanig dat $f_1 + f_2 \neq 0$. Dan heeft $f_1 + f_2$ dezelfde graad als f_1 en omdat σ de graad bewaart, krijgen we de leidende termen van $\sigma(f_1 + f_2) = \sigma(f_1) + \sigma(f_2)$ door alle leidende termen van van $\sigma(f_1)$ en $\sigma(f_2)$ bij elkaar te nemen en te versimpelen. We hebben in dit geval dus ook $\sigma(f_1) + \sigma(f_2) \in \mathcal{C}$.

Ieder homogeen polynoom is de som van monomen van gelijke graad, dus we hoeven alleen de voortbrengers van het ideaal I te bekijken. Door de symmetrie van het probleem kunnen we ons beperken tot X_1^q. In dit geval geldt

$$\sigma(X_1^q) = (a_{11}X_1 + a_{21}X_2 + \ldots + a_{n1}X_n + c_1)^q = a_{11}^q X_1^q + a_{21}^q X_2^q + \ldots + a_{n1}^q X_n^q + c_1^q$$

en de leidende termen van deze laatste uitdrukking zijn bevat in I omdat niet iedere a_{j1} nul is, dus $\sigma(X_1^q)$ is bevat in $\mathcal{C}$. □

De Combinatorische Nullstellensatz heeft het nadeel dat de vorm van de verzameling waar we punten vandaan halen erg beperkend is. De volgende stelling geeft ons iets meer vrijheid.

Stelling 1.3. *Zij k een lichaam van karakteristiek p en $m, n \in \mathbb{Z}_{\geq 0}$ met $n > 0$. Schrijf $q = p^m$ voor $p > 0$ en $q = 0$ voor $p = 0$. Voor iedere $f \in \mathcal{S}_q \subset k[X_1, X_2, \ldots, X_n] = R$, iedere basis $b_1, \ldots, b_n$ van k^n en ieder stel verzamelingen $S_i \subset k$ met $|S_i| \geq q$ als $p > 0$ en $|S_i|$ oneindig als $p = 0$ voor $1 \leq i \leq n$, bestaat er een*

$$x \in \sum_{i=1}^{n} S_i b_i$$

zodanig dat $f(x) \neq 0$.

Bewijs. De getransponeerde van de inverteerbare matrix horende bij het automorfisme σ van de k-vectorruimte k^n gegeven door

$$e_i \mapsto b_i, 1 \leq i \leq n$$

met $e_1, e_2, \ldots, e_n$ de standaardbasis van k^n geeft aanleiding tot een automorfisme $\sigma' \in \mathrm{Aut}_{\mathrm{deg}}(R)$ van de ring R door iedere X_i overeen te laten komen met e_i. Deze werking wordt samengevat door $(\sigma' f)(x_1, x_2, \ldots, x_n) = f(\sigma(x_1, x_2, \ldots, x_n))$ voor iedere $(x_1, x_2, \ldots, x_n) \in k^n$. Schrijven we voor iedere i namelijk $b_i = \sum_{j=1}^n b_{ij} e_j$, dan krijgen we

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \mapsto \begin{pmatrix} \sum_{i=1}^n b_{i1} X_i \\ \vdots \\ \sum_{i=1}^n b_{in} X_i \end{pmatrix} = \sum_{i=1}^n \begin{pmatrix} b_{i1} \\ \vdots \\ b_{in} \end{pmatrix} X_i = \sum_{i=1}^n b_i X_i.$$

Met behulp van lemma 2.2 hebben we $\sigma' f \in \mathcal{S}_q$ en dus bestaan er $x_i \in S_i$ voor alle i zodanig dat $(\sigma' f)(x_1, x_2, \ldots, x_n) \neq 0$, of

$$f(\sigma(x_1, x_2, \ldots, x_n)) = (\sigma' f)(x_1, x_2, \ldots, x_n) \neq 0.$$

Het punt $\sigma(x_1, x_2, \ldots, x_n)$ is het punt van k^n met coördinaten $x_1, x_2, \ldots, x_n$ ten opzichte van de basis $b_1, b_2, \ldots, b_n$ en is dus een punt van $\bigoplus_{i=1}^n S_i b_i$. □

Als korte toepassing van deze stelling hebben we het volgende. Neem $p > 0$, $f = X_1 X_2 \ldots X_n$ en laat iedere S_i het priemlichaam van k zijn. De verzameling $\bigoplus_{i=1}^n S_i b_i$ is nu een ondergroep van k^n en de stelling zegt dat iedere ondergroep van k^n voortgebracht door n lineair onafhankelijke elementen een punt bevat waarvan alle coördinaten niet nul zijn.

2 Semisimpliciteit en het Jacobson-radicaal

We beginnen met een aantal definities.

Definitie 2.1. Zij R een ring. Een R-moduul M heet *simpel* als M niet-nul is en 0 en M de enige deelmodulen van M zijn.

Een voorbeeld hiervan is het $\mathbb{Z}$-moduul $\mathbb{Z}/p\mathbb{Z}$ voor iedere priem p. Deze groep heeft alleen triviale ondergroepen. Het $\mathbb{Z}$-moduul $\mathbb{Z}$ is niet semisimpel, deze heeft namelijk voor iedere n de ondergroep $n\mathbb{Z}$.

De kern en het beeld van ieder homomorfisme $\varphi\colon M \to N$ van simpele R-modulen zijn deelmodulen van M respectievelijk N. Dit betekent dat er slechts twee mogelijkheden zijn. Als φ niet de nul-afbeelding is, dan is de kern van φ triviaal omdat M simpel is en het beeld van φ is geheel N omdat N simpel is. Als gevolg hiervan krijgen we het volgende lemma.

Lemma 2.2 (Schur's Lemma)**.** *Zij R een ring. Als M een simpel R-moduul is, dan is* $\mathrm{End}_R(M)$ *een delingsring.*

Definitie 2.3. Een R-moduul M heet *semisimpel* als hij een directe som van simpele modulen is.

Definitie 2.4. Een ring R heet *semisimpel* als hij semisimpel is als moduul over zichzelf.

We hebben informatie nodig over hoe een algebra over een algebraïsch afgesloten lichaam eruit ziet en we zullen zien dat de stellingen over simpele modulen hierbij zullen helpen.

Zoals bij veel eigenschappen van ringen die afgeleid zijn uit die van modulen hebben we de volgende eigenschap.

Propositie 2.5. *Zij R een semisimpele ring. Dan is ieder R-moduul semisimpel.*

Het bewijs hiervan is te vinden in [2], XVII.4.1.

De volgende stelling, te danken aan Wedderburn en Artin, stelt ons in staat de structuur van de ring af te lezen uit bepaalde modulen over deze ring. We noemen een moduul *trouw* als het enige element van R dat als 0 werkt de 0 zelf is.

Stelling 2.6 (Stelling van Artin-Wedderburn)**.** *Laat R een semisimpele ring zijn. Dan geldt*

$$R = \prod_{i=1}^{m} M_{n_i}(D_i)$$

voor zekere delingsringen D_i en zekere gehele getallen $m \in \mathbb{Z}_{\geq 0}$ en $n_i \in \mathbb{Z}_{>0}$.

Het volgende lemma verzorgt een kort bewijs van deze stelling.

Lemma 2.7. *Zij R een ring. Laat M, M_1, M_2, N, N_1, N_2 een zestal R-modulen zijn. Dan hebben we de volgende isomorfismen.*

- $\mathrm{Hom}_R(M, N_1 \oplus N_2) \cong \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2)$,
- $\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$.

Bewijs. Definiëer bij ieder R-moduul-homomorfisme $\varphi\colon M \to N_1 \oplus N_2$ de homomorfismen φ_1, φ_2 door $\varphi_1 = \pi_1 \circ \varphi$ en $\varphi_2 = \pi_2 \circ \varphi$, waar $\pi_1\colon N_1 \oplus N_2 \to N_1$ en $\pi_2\colon N_1 \oplus N_2 \to N_2$ de projecties zijn. Het verkregen R-homomorfisme $\phi \mapsto (\phi_1, \phi_2)$ is duidelijk injectief en surjectiviteit volgt uit $\phi' := (m \mapsto (\phi_1(m), \phi_2(m)) \in \mathrm{Hom}_R(M, N_1 \oplus N_2))$.

Definiëer bij ieder R-moduul-homomorfisme $\varphi\colon M_1 \oplus M_2 \to N$ de afbeeldingen $\phi_1\colon M_1 \to N$ en $\phi_2\colon M_2 \to N$ door $\phi_1(m_1) = \phi(m_1, 0)$ en $\phi_2(m_2) = \phi(0, m_2)$ voor alle $m_1 \in M_1, m_2 \in M_2$. Het verkregen R-homomorfisme $\phi \mapsto (\phi_1, \phi_2)$ is injectief omdat $\phi(m_1, m_2) = \phi_1(m_1) + \phi_2(m_2)$ en surjectief omdat voor iedere (ϕ_1, ϕ_2) de afbeelding $\phi' := ((m_1, m_2) \mapsto \phi_1(m_1) + \phi_2(m_2))$ bevat is in $\mathrm{Hom}_R(M_1 \oplus M_2, N)$. □

Bewijs van stelling 2.6. De ring R is per aanname te schrijven als $R = \bigoplus_{i \in I} S_i$ voor zekere simpele R-modulen S_i, $i \in I$. Omdat R eindig voortgebracht is als R-moduul, moet de directe som-decompositie eindig zijn. Als we isomorfe S_i ook bij elkaar nemen, mogen we $R = \bigoplus_{i=1}^{m} S_i^{n_i}$ schrijven voor zekere $m, n_i \in \mathbb{Z}_{>0}$ en R-modulen S_i voor $1 \leq i \leq m$.

Voor $i \neq j$ hebben we eerder gezien dat geldt $\mathrm{Hom}_R(S_i, S_j) = 0$ en dus hebben we

$$\begin{aligned} R^o &\cong \mathrm{End}_R(R) \\ &= \mathrm{Hom}_R(\bigoplus_{i=1}^{m} S_i^{n_i}, \bigoplus_{i=1}^{m} S_i^{n_i}) \\ &\cong \bigoplus_{i=1}^{m} \mathrm{Hom}_R(S_i^{n_i}, S_i^{n_i}) \\ &= \bigoplus_{i=1}^{m} \mathrm{End}_R(S_i^{n_i}) \\ &\cong \prod_{i=1}^{m} M_{n_i}(\mathrm{End}(S_i)), \end{aligned}$$

waar R^o de tegengestelde ring is van R. Nemen we tegengestelden, dan krijgen we

$$R = (R^o)^o \cong \prod_{i=1}^{m} M_{n_i}(\mathrm{End}(S_i))^o \cong \prod_{i=1}^{m} M_{n_i}(\mathrm{End}(S_i)^o).$$

Iedere $\mathrm{End}(S_i)$ is een delingsring door Schur's Lemma en de tegengestelde van een delingsring is een delingsring, dus dit bewijst het gevraagde. □

Gevolg 2.8. *Zij A een eindig-dimensionale semisimpele algebra over een algebraïsch afgesloten lichaam k. Dan geldt*

$$A = \prod_{i=1}^{m} M_{n_i}(k)$$

voor zekere gehele getallen $m \in \mathbb{Z}_{\geq 0}$ en $n_i \in \mathbb{Z}_{>0}$.

Bewijs. Via de decompositie van A wordt iedere D_i een k-algebra van eindige dimensie over k. Laat i nu een geheel getal $1 \leq i \leq m$ zijn en laat α een element van D_i zijn. De verzameling $k(\alpha)$ is dan een commutatieve deelring van de delingsring D_i. Omdat D_i eindig-dimensionaal is over k, is $k(\alpha)$ dat ook. Het element α is dus algebraïsch over k en dit betekent $\alpha \in k$ omdat k algebraïsch afgesloten is. We concluderen dat $D_i = k$ en dus geldt

$$A = \prod_{i=1}^{m} M_{n_i}(k).$$

□

Het volgende ideaal geeft ons meer grip op semisimpliciteit.

Definitie 2.9. Zij R een ring. Het *Jacobson-radicaal* J van R is het ideaal gedefiniëerd door de volgende eigenschap:

- $a \in R$ is bevat in J dan en slechts dan als ieder simpel linksmoduul geannihileerd wordt door a.

Nu is lang niet iedere ring semisimpel, maar over een lichaam k hebben we het volgende.

Lemma 2.10. *Zij A een eindig-dimensionale algebra over een lichaam k. Laat J het Jacobson-radicaal van A zijn. Dan is de k-algebra A/J semisimpel.*

Bewijs. De algebra A is Artins (en Noethers). Idealen zijn namelijk deelruimtes van A als k-vectorruimte en in elkaar bevatte deelruimtes zijn gelijk als hun dimensies gelijk zijn. Verschillende idealen in een keten hebben dus verschillende dimensies. Er zijn dan slechts eindig veel keuzes over omdat A eindig-dimensionaal is, dus iedere keten stabiliseert in eindig veel stappen.

Het Jacobson-radicaal J is een doorsnede van maximale linksidealen $J = \bigcap_{L\in\mathcal{L}} L$. Omdat A Artins is, mogen we aannemen dat J een eindige doorsnede $J = \bigcap_{i=1}^{m} L_i$ van maximale linksidealen is. We maken namelijk als volgt een keten van idealen. Neem $N_0 \in \mathcal{L}$ willekeurig. Stel dat we een keten $N_0 \supset N_1 \supset \ldots \supset N_n$ hebben voor zekere $n \in \mathbb{Z}_{\geq 0}$ waar $N_n \neq J$, dan is er een $L \in \mathcal{L}$ zodanig dat $N_n \cap L \subsetneq N_n$ en we nemen dan $N_{n+1} = N_n \cap L$. Dit proces moet stoppen in eindig veel stappen omdat A Artins is. Dan hebben we $N_l = J$ voor zekere l en dit is een eindige doorsnede van maximale linksidealen.

Verder mogen we aannemen dat geen echte deelverzameling van $\{L_i\}$ dezelfde doorsnede heeft, omdat er eindig veel L_i zijn. De rij

$$0 \longrightarrow J \longrightarrow A \longrightarrow \bigoplus_{i=1}^{m} A/L_i$$

is exact en we krijgen dus een injectie $A/J \to \bigoplus_{i=1}^{m} A/L_i$. Schrijf voor iedere i, $1 \leq i \leq m$ het ideaal $\bigcap_{j\neq i} L_j \neq J$ als J_i. De restricties van de quotiëntafbeelding tot de J_i geeft een stel homomorfismen $J_i \to A/L_i$. De kernen van deze afbeeldingen zijn de doorsnedes $J_i \cap L_i = J$. We krijgen dus injecties $J_i/J \to A/L_i$. Omdat iedere J_i/J niet-nul is en omdat iedere A/L_i simpel is zijn deze injecties zelfs bijecties en dus krijgen we $J_i/J \cong A/L_i$. Dit laat zien dat het homomorfisme $A/J \to \bigoplus_{i=1}^{m} A/L_i$ ook surjectief is. Er geldt dus $A/J \cong \bigoplus_{i=1}^{m} A/L_i$ en dus is A/J semisimpel. □

Merk op dat A/J als quotiënt van een eindig-dimensionale ruimte zelf ook eindig-dimensionaal is. Dit betekent dat we gevolg 2.8 kunnen toepassen.

Een handige eigenschap van het Jacobson-radicaal wordt verwoord door het volgende lemma.

Lemma 2.11. *Zij R een ring. Dan geldt*

$$r \in R^* \iff r + J \in (R/J)^*.$$

Voor we beginnen aan het bewijs hebben we nog een lemma nodig, dat handelt over een eis waaronder een verzameling S met een bewerking $S \times S \to S$ een groep is.

Lemma 2.12. *Zij S een verzameling met een associatieve bewerking $\cdot\colon S \times S \to S$ die we op de gebruikelijke manier aangeven. Neem aan dat S een linkseenheid e heeft waarvoor tevens geldt dat ieder element $a \in S$ links-inverteerbaar is, in de zin dat er een $b \in S$ bestaat zo dat $ba = e$. Dan is S met de bewerking $\cdot$ een groep.*

Bewijs. We moeten laten zien dat ieder element van S een inverse heeft en dat S een eenheid heeft. Laat e een linkseenheid van S zijn met de genoemde eigenschap. Zij $a \in S$ willekeurig en laat b een linksinverse zijn van a. Laat c een linksinverse zijn van b. We krijgen

$$ab = e(ab) = (cb)(ab) = c(ba)b = ceb = cb = e$$

en dus is b ook een rechtsinverse van a, dus a is inverteerbaar. Hierdoor krijgen we tevens

$$ae = a(ba) = (ab)a = ea = a$$

en e is dus ook een rechtseenheid. Hiermee is S een groep. □

Dit gebruiken we voor lemma 2.11 om te laten zien dat voor $q\colon R \to R/J$ de quotiëntafbeelding $q^{-1}((R/J)^*)$ een groep is onder vermenigvuldiging, wat betekent dat deze bevat is in R^*.

Bewijs van lemma 2.11. Eenheden worden afgebeeld op eenheden, dus als $r \in R$ een eenheid is, dan is $r + J \in R/J$ dat ook.

Stel nu dat $r + J$ een eenheid van R/J is. Laat $r' + J$ de inverse van $r + J$ zijn. We laten zien dat r een linksinverse heeft in R.

Hiertoe laten we eerst zien dat $Rr + J = R$. Dat $Rr + J$ in R bevat is, is triviaal. Laat andersom $a \in R$ gegeven zijn. Modulo J geldt $a \bmod J = ar'r \bmod J$ en dus bestaat er een $b \in J$ zodanig dat $a = ar'r + b \in Rr + J$.

Stel nu dat $Rr \subsetneq R$. Dan bestaat er een maximaal linksideaal L zodanig dat $Rr \subset L \subsetneq R$. Per definitie is J bevat in L en dus geldt $R = Rr + J \subset L$ en dit is onmogelijk. We concluderen dat $Rr = R$ en r heeft dus een linksinverse.

Ieder element van $q^{-1}((R/J)^*)$ heeft dus een linksinverse en ook $1 \in R$ is bevat in $q^{-1}((R/J)^*)$, dus we kunnen met behulp van Lemma 2.12 concluderen dat $q^{-1}((R/J)^*)$ een groep is. We krijgen dus ook $q^{-1}((R/J)^*) \subset R^*$. □

3 Basisuitbreidingen

Als we kijken naar het diagonaliseren van matrices over $\mathbb{R}$ dan zien we dat dit niet altijd kan, bijvoorbeeld omdat het karakteristiek polynoom van de matrix niet volledig splitst over $\mathbb{R}$. Om toch een volledige karakterisatie te kunnen krijgen van zo een matrix, wordt vaak gekeken naar de complexificatie van de matrixalgebra; we doen 'alsof' de matrices ook complexe componenten mogen hebben. Dit komt er op neer dat we het tensorproduct van deze algebra met $\mathbb{C}$ bekijken, om zo een algebra over $\mathbb{C}$ te krijgen. Het karakteristiek polynoom van de oorspronkelijke matrix splitst volledig over het algebraïsch afgesloten lichaam $\mathbb{C}$ en zo kunnen we de Jordan-normaalvorm van de matrix vinden.

Het blijkt dat dit veel algemener een lonende aanpak is.

Definitie 3.1. Zij $k \subset K$ een lichaamsuitbreiding, M een k-vectorruimte. We noemen de K-vectorruimte $K \otimes_k M$ de basisuitbreiding van M met K en schrijven hiervoor M_K.

Wanneer uit de context duidelijk is waarover het tensorproduct genomen wordt, wordt het subscript in het tensorproduct weggelaten. Waar we gebruik van zullen maken is dat het optensoren met een vast moduul N functorieel is.

Laat voor de rest van deze paragraaf R een commutatieve ring zijn. Ieder tensorproduct in deze paragraaf gebeurt over R.

Lemma 3.2. *Zij N een R-moduul. Bij ieder homomorfisme $\varphi\colon M \to M'$ van R-modulen krijgen we een homomorfisme $1 \otimes \varphi\colon N \otimes M \to N \otimes M'$ vastgelegd door*

$$(1 \otimes \varphi)(n \otimes m) \mapsto n \otimes \varphi(m).$$

Iedere R-algebra A is met name een R-moduul via het homomorfisme van R naar A. Dit betekent dat we ook het tensorproduct van en met algebras kunnen bekijken. Hierover kunnen we het volgende zeggen.

Laat A en B twee R-algebras zijn, M een R-moduul en N, N' twee B-modulen. Het moduul $A \otimes B$ is een R-algebra met componentsgewijze vermenigvuldiging. Het moduul $A \otimes M$ is een A-moduul met vermenigvuldiging in de eerste component. Het moduul $A \otimes N$ is een $A \otimes B$-moduul met componentsgewijze vermenigvuldiging. Verder hebben we het volgende lemma.

Lemma 3.3. *Laat A en B twee R-algebras zijn. Als $\varphi\colon N \to N'$ een B-moduul-homomorfisme is, dan is $1 \otimes \varphi\colon A \otimes N \to A \otimes N'$ een $A \otimes B$-moduul-homomorfisme.*

Bewijs. Voor iedere $a \otimes b \in A \otimes B$ en iedere $a' \otimes n \in A \otimes N$ hebben we

$$\begin{aligned}(1 \otimes \varphi)((a \otimes b)(a' \otimes n)) &= (1 \otimes \varphi)(aa' \otimes bn) \\ &= aa' \otimes \varphi(bn) \\ &= (a \otimes b) \cdot (a' \otimes \varphi(n)) \\ &= (a \otimes b) \cdot (1 \otimes \varphi)(a' \otimes n)\end{aligned}$$

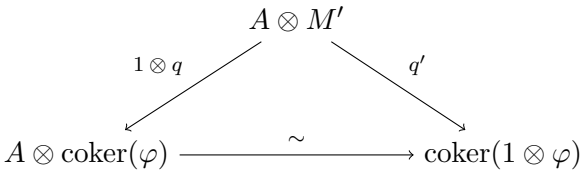
en met lineaire voortzetting over $A \otimes B$ krijgen we het genoemde.

□

Deze laatste eigenschap laat ons het optensoren met een R-algebra A voor iedere R-algebra B beschouwen als een functor $\mathrm{Mod}_B \to \mathrm{Mod}_{A \otimes B}$.

Merk op dat deze functor verkregen wordt als beperking van de originele functor $\mathrm{Mod}_R \to \mathrm{Mod}_R$ horende bij optensoren met een vast moduul. Dit betekent dat veel eigenschappen, zoals rechtsexactheid, direct overdragen.

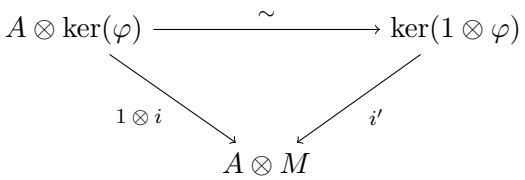
Lemma 3.4. *Laat A en B twee R-algebras zijn. Dan hebben we voor ieder homomorfisme $\varphi\colon M \to M'$ van B-modulen een commutatief diagram*



van $A \otimes B$-modulen, waar $q\colon M' \to \mathrm{coker}(\varphi)$ en $q'\colon A \otimes M' \to \mathrm{coker}(1 \otimes \varphi)$ de quotiëntafbeeldingen zijn. De functor $A \otimes -\colon \mathrm{Mod}_B \to \mathrm{Mod}_{A \otimes B}$ is rechtsexact.

Wanneer optensoren met een R-moduul M linksexact is, heet M *plat*. Zo kunnen we een R-algebra ook plat noemen als hij plat is als R-moduul. Een voldoende eis voor het plat zijn van M is dat hij vrij is.

Lemma 3.5. *Laat A en B twee R-algebras zijn. Neem aan dat A plat is over R. Dan hebben we voor ieder homomorfisme $\varphi\colon M \to M'$ van B-modulen een commutatief diagram*



van $A \otimes B$-modulen, waar $i\colon \ker(\varphi) \to M'$ en $i'\colon \ker(1 \otimes \varphi) \to A \otimes M'$ de inclusies zijn. De functor $A \otimes -\colon \mathrm{Mod}_B \to \mathrm{Mod}_{A \otimes B}$ is linksexact.

Een R-moduul M noemen we *trouwplat* als voor iedere rij

$$N_1 \longrightarrow N_2 \longrightarrow \ldots \longrightarrow N_m$$

van R-modulen geldt dat hij exact is dan en slechts dan als

$$M \otimes N_1 \longrightarrow M \otimes N_2 \longrightarrow \ldots \longrightarrow M \otimes N_m$$

dat is.

Een voldoende eis voor het trouwplat zijn van een moduul M blijkt weer te zijn dat M niet-nul en vrij is als R-moduul.

Lemma 3.6. *Laat A en B twee R-algebras zijn. Neem aan dat A vrij is als moduul over R en neem aan dat A niet-nul is. Dan geldt voor iedere rij*

$$N_1 \longrightarrow N_2 \longrightarrow \ldots \longrightarrow N_m$$

dat hij exact is dan en slechts dan als

$$A \otimes N_1 \longrightarrow A \otimes N_2 \longrightarrow \ldots \longrightarrow A \otimes N_m$$

dat is.

Bewijs. Het moduul A is van de vorm $A = \bigoplus_{i \in I} R$ voor een zekere indexverzameling I. Is M een R-moduul, dan geldt $A \otimes M = \left(\bigoplus_{i \in I} R\right) \otimes M \cong \bigoplus_{i \in I} M$. De rij

$$N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{m-1}} N_m$$

geeft na het nemen van het tensorproduct met A de rij

$$\bigoplus_{i \in I} N_1 \xrightarrow{\bigoplus_{i \in I} f_1} \bigoplus_{i \in I} N_2 \xrightarrow{\bigoplus_{i \in I} f_2} \ldots \xrightarrow{\bigoplus_{i \in I} f_{m-1}} N_m$$

en deze rij is exact dan en slechts dan als de vorige dat is. □

Trouwplatte modulen respecteren de structuur van andere modulen in de volgende zin.

Lemma 3.7. *Zij M een trouwplat R-moduul. Voor ieder R-moduul N geldt*

$$M \otimes N = 0 \iff N = 0.$$

Bewijs. De rijen

$$0 \longrightarrow N \longrightarrow 0$$

en

$$0 \longrightarrow M \otimes N \longrightarrow 0$$

zijn exact dan en slechts dan als N respectievelijk $M \otimes N$ nul zijn. Omdat M trouwplat is, is de ene rij exact dan en slechts dan als de ander dat is en dit impliceert het genoemde. □

Hieruit is gemakkelijk het volgende af te leiden.

Lemma 3.8. *Zij M een trouwplat R-moduul en laat $\varphi\colon N \to N'$ een homomorfisme van R-modulen zijn. Het homomorfisme φ is surjectief dan en slechts dan als $1\otimes\varphi\colon M\otimes N \to M\otimes N'$ dat is. Hetzelfde geldt voor injectiviteit.*

Bewijs. Bekijk de rijen

$$N \longrightarrow N' \longrightarrow 0$$

en

$$0 \longrightarrow N \longrightarrow N'.$$

Deze zijn exact dan en slechts dan als φ surjectief respectievelijk injectief is. Nemen we het tensorproduct met M, dan krijgen we de rijen

$$M \otimes N \longrightarrow M \otimes N' \longrightarrow 0$$

en

$$0 \longrightarrow M \otimes N \longrightarrow M \otimes N'$$

en deze zijn per definitie exact dan en slechts dan als de bijhorende van de vorige dat is. Verder zijn ze exact dan en slechts dan als $1 \otimes \varphi$ surjectief respectievelijk injectief is en dit concludeert het bewijs. □

Merk op dat de twee uitspraken samen zeggen dat $\varphi\colon N \to N'$ een isomorfisme is dan en slechts dan als $1 \otimes \varphi$ dat is.

4 Eenheden van eindig-dimensionale algebras over algebraïsch afgesloten lichamen

In dit deel leggen we de verbinding tussen de eindig-dimensionale algebras en de Combinatorische Nullstellensatz.

Lemma 4.1. *Zij k een algebraïsch afgesloten lichaam en laat A een eindig-dimensionale k-algebra zijn. Schrijf n voor de dimensie van A. Dan bestaan er een basis $b_1, b_2, \ldots, b_n$ van A over k en een polynoom $f \in k[X_1, X_2, \ldots, X_n]$ zodanig dat voor iedere $(x_1, x_2, \ldots, x_n) \in k^n$ geldt*

$$\sum_{i=1}^{n} x_i b_i \in A^* \iff f(x_1, x_2, \ldots, x_n) \neq 0$$

en met $\deg_{X_i}(f) \leq 1$ voor iedere i.

Bewijs. Met behulp van gevolg 2.8 en lemma 2.10 kunnen we voor J het Jacobson-radicaal van A en voor zekere positieve gehele getallen $n_1, \ldots, n_m$ schrijven

$$A/J = \prod_{i=1}^{m} M_{n_i}(k).$$

We laten eerst zien dat de uitspraak van de stelling geldt voor matrixalgebras $M_l(k)$ met $l \in \mathbb{Z}_{>0}$, vervolgens laten we zien dat we producten van algebras mogen nemen en als laatste laten we zien dat we mogen uitdelen naar het Jacobson-radicaal J.

De matrixalgebra $M_l(k)$ heeft een basis bestaande uit de matrices met precies één coëfficiënt gelijk aan 1 en de rest gelijk aan 0. Schrijf A_{ij} voor de matrix in deze basis met op de i,j-de plek een 1. De matrix (a_{ij}) laat zich schrijven als

$$(a_{ij}) = \sum_{i,j=1}^{l} a_{ij} A_{ij}.$$

De matrix (a_{ij}) is een eenheid dan en slechts dan als hij een niet nul determinant heeft. Deze determinant is gegeven door de formule van Leibniz

$$\det((a_{ij})) = \sum_{\sigma \in S_l} \operatorname{sgn}(\sigma) \prod_{i=1}^{l} a_{\sigma(i)i}$$

en we kunnen dus het polynoom

$$f = \sum_{\sigma \in S_l} \operatorname{sgn}(\sigma) \prod_{i=1}^{l} X_{\sigma(i)i}$$

gebruiken. De graad van f in iedere variabele is kleiner gelijk 1 omdat iedere $\sigma \in S_l$ een bijectie op $\{1, 2, \ldots, l\}$ induceert.

Stel nu dat A en B twee eindig-dimensionale k-algebras zijn waarvoor de uitspraak geldt. Schrijf $b_1, b_2, \ldots, b_l$ en $c_1, c_2, \ldots, c_n$ voor de respectievelijke bases. Laat f het polynoom horende bij A zijn uitgeschreven over $X_1, X_2, \ldots, X_l$ en laat g het polynoom horende bij B zijn uitgeschreven over $Y_1, Y_2, \ldots, Y_n$. De k-algebra $A \times B$ heeft een basis $(b_i, 0), (0, c_j)$ met $1 \leq i \leq l$ en $1 \leq j \leq n$. Een element $(a, b) \in A \times B$ is een eenheid dan en slechts dan als $a \in A$ en $b \in B$ beide eenheden zijn. Schrijven we (a, b) als

$$(a, b) = (\sum_{i=1}^{l} x_i b_i, \sum_{j=1}^{n} y_j c_j),$$

dan kunnen we het polynoom $fg \in k[X_1, \ldots, X_l, Y_1, \ldots, Y_n]$ nemen. Het product

$$(fg)(x_1, x_2, \ldots, x_l, y_1, y_2, \ldots, y_n)$$

is niet nul dan en slechts dan als $f(x_1, x_2, \ldots, x_l)$ en $g(y_1, y_2, \ldots, y_n)$ beide niet nul zijn, dus dan en slechts dan als a en b beide eenheden zijn. De variabelen van f en g zijn verschillend, dus hun product heeft nog steeds graad kleiner gelijk 1 in iedere variabele. Samen met het vorige geval impliceert dit dat de uitspraak geldt voor ieder product van eindig veel matrixalgebras.

Laat A nu een eindig-dimensionale k-algebra zijn. Het lemma geldt voor A/J. Laat $b_1, b_2, \ldots, b_n$ de basis zijn voor A/J die we krijgen en laat $f \in k[X_1, X_2, \ldots, X_n]$ het bijhorende polynoom zijn. Kies voor iedere b_i een representant b_i' in A. Dan zijn de b_i' lineair onafhankelijk en we kunnen deze verzameling aanvullen met een basis $c_1, c_2, \ldots, c_l$ voor J om een basis $b_1', b_2', \ldots, b_n'$, $c_1, c_2, \ldots, c_l$ van A te krijgen. Dankzij 2.11 kunnen we voor het polynoom het polynoom f opgevat als element van $k[X_1, X_2, \ldots, X_{l+n}]$ nemen.

Dit laat zien dat de uitspraak geldt voor iedere eindig-dimensionale k-algebra. □

Stelling 1.2 samen met Lemma 4.1 geeft ons het volgende gevolg, dat ons de basis in het vorige lemma willekeurig kiezen, mits we bereid zijn de eis op het polynoom te verzwakken.

Gevolg 4.2. *Zij k een algebraïsch afgesloten lichaam en laat A een eindig-dimensionale k-algebra zijn. Schrijf n voor de dimensie van A over k en laat $b_1, b_2, \ldots, b_n$ een k-basis zijn voor A. Laat p de karakteristiek van k zijn. Dan is er een polynoom $f \in \mathcal{S}_p \subset k[X_1, X_2, \ldots, X_n]$ zodanig dat voor iedere $x_1, x_2, \ldots, x_n \in k$ geldt*

$$\sum_{i=1}^{n} x_i b_i \in A^* \iff f(x_1, x_2, \ldots, x_n) \neq 0.$$

Bewijs. Laat $c_1, c_2, \ldots, c_n$ de basis zijn die we krijgen uit de stelling en laat f het speciale polynoom zijn. Omdat A minstens één eenheid heeft, de 1 zelf, is f niet het nulpolynoom. Merk op dat f bevat is in $\mathcal{S}_p$; ieder van de termen van f heeft graad kleiner gelijk 1 in iedere variabele, wat voor $p > 0$ kleiner is dan p. De basisverandering van $b_1, b_2, \ldots, b_n$ naar $c_1, c_2, \ldots, c_n$ geeft als in het bewijs van 1.3 aanleiding tot een graadbewarend automorfisme σ van de polynoomring. Hiervoor geldt voor iedere $x_1, x_2, \ldots, x_n \in k$

$$(\sigma f)(x_1, x_2, \ldots, x_n) = f(x_1', x_2', \ldots, x_n')$$

voor $x_1', x_2', \ldots, x_n'$ zodanig dat

$$\sum_{i=1}^{n} x_i b_i = \sum_{i=1}^{n} x_i' c_i.$$

Stelling 1.2 vertelt ons dat σf ook bevat is in $\mathcal{S}_p$ en σf voldoet dus aan alle eisen. □

Een interessante vraag die we hierbij krijgen is of de eis op k verzwakt kan worden. Het blijkt dat het in ieder geval goed gaat voor k perfect. Een polynoom van deze vorm hoeft niet te bestaan wanneer k niet perfect is. Zo gaat het bijvoorbeeld mis wanneer k separabel afgesloten maar niet algebraïsch afgesloten is. Voor de algebra waar het mis gaat is dan een eindige lichaamsuitbreiding ongelijk k te nemen. We zullen het bewijs hiervan niet behandelen.

Om het geval met k perfect te kunnen bewijzen hebben we het volgende lemma nodig.

Lemma 4.3. *Zij k een algebraïsch afgesloten lichaam en n een positief geheel getal. Laat $f, g \in k[X_1, X_2, \ldots, X_n]$ kwadraatvrije polynomen zijn. Dan hebben f en g dezelfde nulpunten in k^n dan en slechts dan als er een $u \in k^*$ bestaat zodanig dat $g = uf$.*

Bewijs. Een polynoomring over een lichaam is een ontbindingsring en we mogen f en g dus factoriseren als $f = v_1 \prod_{i=1}^{n} f_i$ en $g = v_2 \prod_{j=1}^{m} g_j$ in irreducibele polynomen op de eenheden v_1 en v_2 na. De Nullstellensatz van Hilbert [2] IX.1.5 vertelt ons

$$\sqrt{(f)} = I(Z(f)) = I(Z(g)) = \sqrt{(g)}$$

waar $I(S)$ het ideaal horende bij een algebraïsche verzameling S is en waar $Z(J)$ de nulpuntsverzameling is van het ideaal J. Ten eerste betekent dit dat g bevat is in $\sqrt{(f)}$: er bestaat een n_1 zodanig dat $g^{n_1} = h_1 f$ voor een zeker polynoom h_1. We hebben dus

$$\prod_{j=1}^{m} g_j^{n_1} = h_1 \prod_{i=1}^{n} f_i$$

en omdat irreducibele elementen priem zijn in een ontbindingsring, bestaat er voor iedere i een j zodanig dat $f_i | g_j$, ofwel $f_i = u_i g_j$ voor een zekere eenheid u_i. Verschillende f_i geven verschillende g_j, want f is kwadraatvrij. Dit betekent tevens dat $m \geq n$. Hetzelfde argument voor $f \in \sqrt{(g)}$ geeft $m \leq n$ en daarmee $m = n$ en dus $g = uf$. □

We weten nu genoeg om het volgende te bewijzen.

Stelling 4.4. *Zij k een perfect lichaam en laat A een eindig-dimensionale k-algebra zijn. Schrijf n voor de dimensie van A en laat $b_1, b_2, \ldots, b_n$ een basis zijn voor A. Laat p de karakteristiek van k zijn. Dan is er een polynoom $f \in \mathcal{S}_p \subset k[X_1, X_2, \ldots, X_n]$ zodanig dat voor iedere $x_1, x_2, \ldots, x_n \in k$ geldt*

$$\sum_{i=1}^{n} x_i b_i \in A^* \iff f(x_1, x_2, \ldots, x_n) \neq 0.$$

Bewijs. Laat K een algebraïsche afsluiting van k zijn. Laat $b_1, b_2, \ldots, b_n$ een basis zijn voor A over k. Definiëren we voor iedere i het product $b_i' = 1 \otimes b_i \in A_K$, dan worden de $b_1', b_2', \ldots, b_n'$ een basis voor A_K over K. Nu is A_K een eindig-dimensionale algebra over een algebraïsch afgesloten lichaam, dus kunnen we gevolg 4.2 toepassen om een polynoom $f \in \mathcal{S}_p$ te krijgen. Iedere macht van een polynoom heeft dezelfde nulpunten, dus we mogen aannemen dat f kwadraatvrij is.

De uitbreiding $k \subset K$ is Galois omdat k perfect is. Laat G de bijhorende Galoisgroep zijn. De groep G werkt op $K[X_1, X_2, \ldots, X_n]$ via de coëfficiënten. Voor iedere $\sigma \in G$ en iedere $x_1, x_2, \ldots, x_n \in K$ hebben we

$$(\sigma f)(\sigma(x_1, x_2, \ldots, x_n)) = \sigma(f(x_1, x_2, \ldots, x_n)) = 0 \iff f(x_1, x_2, \ldots, x_n) = 0$$

en dus heeft σf precies de nulpunten $\sigma(Z(f))$.

Het automorfisme σ werkt op $A_K = K \otimes A$ via K en omdat voor iedere $\lambda_1 \otimes a_1, \lambda_2 \otimes a_2 \in A_K$ geldt

$$\sigma(\lambda_1 \otimes a_1 \cdot \lambda_2 \otimes a_2) = \sigma(\lambda_1\lambda_2 \otimes a_1a_2) = \sigma(\lambda_1\lambda_2) \otimes a_1a_2 = \sigma(\lambda_1 \otimes a_1) \cdot \sigma(\lambda_2 \otimes a_2)$$

werkt σ op A_K als ringautomorfisme. Dit betekent dat σ met name een automorfisme induceert op de eenhedengroep van A_K.

Voor iedere $x_1, x_2, \ldots, x_n \in K$ hebben we

$$\sum_{i=1}^{n} \sigma(x_i) \cdot b_i' = \sum_{i=1}^{n} \sigma(x_i)\sigma(b_i') = \sigma\left(\sum_{i=1}^{n} x_i \cdot b_i'\right)$$

en dit is dus bevat in A_K^* dan en slechts dan als $\sum_{i=1}^{n} x_i \cdot b_i'$ dat is. Dit laat zien dat $\sigma(Z(f)) = Z(f)$ en dus hebben σf en f dezelfde nulpunten. Het vorige lemma laat zien dat $\sigma f = u_\sigma f$ voor zekere $u_\sigma \in K$.

Omdat σ werkt op f via de coëfficiënten, betekent dit dat ieder van de coëfficiënten van f door σ met u_σ wordt vermenigvuldigd. Is c een van de niet-nul coëfficiënten van f, dan geldt

$$\sigma(f/c) = \sigma(f)/\sigma(c) = (u_\sigma f)/(u_\sigma c) = f/c$$

en f/c wordt dus op zijn plek gelaten door σ. De definitie f/c is onafhankelijk van de gekozen σ, dus f/c wordt op zijn plek gelaten door de hele groep G. Dit betekent dat f/c coëfficiënten in $k = K^G$ heeft. Omdat f/c dezelfde nulpunten heeft als f zullen we f door f/c vervangen.

Het enige wat we nog hoeven te laten zien is dat onder de inbedding $A \to A_K : a \mapsto 1 \otimes a$ de eenhedengroep van A gegeven is door $A^* = A_K^* \cap A$. Als $a \in A$ een eenheid is en b zijn inverse, dan is $1 \otimes b$ de inverse van $1 \otimes a \in A_K$ en geldt dus $1 \otimes a \in A_K^* \cap A$. Als andersom $1 \otimes a \in A_K^* \cap A$, dan is de afbeelding $\varphi : A_K \to A_K : b \mapsto b \cdot (1 \otimes a)$ een A_K-moduul-isomorfisme. Definiëren we de afbeelding $\varphi' : A \to A$ als $b \mapsto ba$, dan geldt $1 \otimes \varphi' = \varphi$. Lemma 3.8 zegt nu dat φ' een A-moduul-isomorfisme is. Dit betekent dat a een rechtsinverse heeft in A. Deze rechtsinverse is net zo goed een rechtsinverse van a in A_K en daar is deze uniek, dus we kunnen concluderen dat de gevonden rechtsinverse van a ook een linksinverse is en dus is a een eenheid in A.

Dit alles impliceert dat f een polynoom is met de gezochte eigenschap voor de k-algebra A met basis $b_1, b_2, \ldots, b_n$. □

5 Varianten van de stelling van Noether-Deuring

In een aantal bewijzen van de normale basis-stelling wordt gebruik gemaakt van het idee dat we uit een opgetensord moduul informatie kunnen halen over het originele moduul. Meer specifiek, er wordt gebruik gemaakt van de volgende stelling. Voor een commutatieve ring R, een R-algebra A en een R-moduul M, zullen we M_A schrijven voor het A-moduul $A \otimes M$.

Stelling 5.1. *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra zijn. Als M een A-moduul van eindige dimensie over k is met $A_K \cong M_K$ als A_K-modulen, dan geldt $A \cong M$ als A-modulen.*

Deze stelling zullen we na de volgende discussie bewijzen. Geïnspireerd door deze stelling, kunnen we ons ook afvragen of hetzelfde opgaat voor injecties of surjecties $A \to M$. Verder zouden we ook A kunnen vervangen door A^m voor m willekeurig of door een willekeurig A-moduul N. Een gelijkaardige stelling is er een van Noether en Deuring.

Stelling 5.2 (Noether-Deuring)**.** *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra zijn. Laat M en N twee A-modulen zijn van eindige dimensie over k en neem aan dat geldt $M_K \cong V \oplus N_K$ voor een zeker A_K-moduul V. Dan bestaat er een A-moduul W zodanig dat $M \cong W \oplus N$.*

Het bewijs van deze stelling is terug te vinden in [3]. Deze stelling impliceert de vorige en de versie met willekeurige modulen links van de isomorfie. We hebben echter nog geen nieuw bewijs kunnen vinden voor deze stelling.

In de bewijzen van stelling 5.1 die je meestal ziet worden veel gevallen onderscheiden. De Combinatorische Nullstellensatz en stelling 4.2 stellen ons in staat het bewijs als het ware samen te vatten.

Bewijs van stelling 5.1. Merk ten eerste op dat als M isomorf is met A als A-moduul, we het isomorfisme van K-modulen $A_K \cong M_K$ hebben. Dit betekent dat we naar de toren $k \subset K \subset \overline{K}$ met $\overline{K}$ een algebraïsche afsluiting van K kunnen kijken. Verder geldt

$$\overline{K} \otimes_K A_K = \overline{K} \otimes_K (K \otimes_k A) \cong (\overline{K} \otimes_K K) \otimes_k A \cong \overline{K} \otimes_k A = A_{\overline{K}}$$

als $\overline{K}$-modulen. Hierom mogen we zonder verlies van algemeenheid aannemen dat K algebraïsch afgesloten is.

Schrijf p voor de karakteristiek van k. Laat n de dimensie zijn van A over k. Het isomorfisme $A_K \cong M_K$ impliceert direct dat M ook dimensie $n < \infty$ over k heeft. Laat $c'_1, c'_2, \ldots, c'_n$ een k-basis zijn van M. Optensoren met K geeft een basis $c_1, c_2, \ldots, c_n$ van M_K. Laat ψ het isomorfisme $A_K \to M_K$ zijn en laat $b_1, b_2, \ldots, b_n$ de basis van A_K zijn die we krijgen door inverse beelden te nemen onder ψ. Met behulp van stelling 4.2 krijgen we een polynoom $f \in \mathcal{S}_p \subset K[X_1, X_2, \ldots, X_n]$ dat de eenheden van A_K over deze basis beschrijft. Het lichaam k heeft minstens p elementen als $p > 0$ en oneindig veel als

$p = 0$. Dit betekent dat we stelling 1.3 kunnen toepassen op $f \in \mathcal{S}_p$ met de verzamelingen $S_1 = S_2 = \ldots = S_n = k$. We krijgen een eenheid

$$u = \sum_{i=1}^{n} x_i b_i \in A_K$$

waar alle x_i bevat zijn in k.

Laat v het beeld van u zijn onder ψ. Dit betekent dat v er uitziet als

$$v = \psi(u) = \sum_{i=1}^{n} x_i c_i.$$

Definiëer de afbeelding $\varphi\colon A_K \to M_K$ door $\varphi(a) = av$. Deze afbeelding is een isomorfisme van A_K-modulen. Voor iedere $m \in M_K$ hebben we namelijk voor zekere a:

$$m = \psi(a) = \psi(au^{-1}u) = au^{-1}\psi(u) = au^{-1}v = \varphi(au^{-1}).$$

Dus φ is surjectief en omdat A_K en M_K dezelfde dimensie hebben is φ daarmee automatisch bijectief.

Laat v' het element $\sum_{i=1}^{n} x_i c_i'$ zijn en definiëer het A-moduul-homomorfisme $\varphi'\colon A \to M$ door $a \mapsto av'$. Er geldt $1 \otimes v' = v$ en dus hebben we net als in het bewijs van 4.4 de gelijkheid $\varphi = 1 \otimes \varphi'$. Omdat φ een isomorfisme is, vertelt lemma 3.8 ons dat φ' ook een isomorfisme is en dus hebben we $A \cong M$ als A-modulen. □

Met behulp van dit resultaat kunnen we ook het eerder genoemde geval waar we A vervangen door een willekeurig A-moduul bewijzen. Hierbij is het volgende lemma zeer handig.

Lemma 5.3. *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra zijn. Laat M en N twee A-modulen zijn met $\dim_k(M) < \infty$. Schrijf $V = \mathrm{Hom}_A(M, N)$ en $B = \mathrm{End}_A(N)$. Dan is V op natuurlijke wijze een B-moduul en de natuurlijke afbeelding*

$$V_K \to \mathrm{Hom}_{A_K}(M_K, N_K)$$

is een B_K-isomorfisme.

Bewijs. Laat ψ de natuurlijke afbeelding $V_K \to \mathrm{Hom}_{A_K}(M_K, N_K)$ zijn. We laten eerst zien dat ψ een B_K-homomorfisme is. De afbeelding ψ wordt gegeven door $\lambda \otimes \varphi \mapsto l_\lambda \otimes \varphi$, waar l_λ de linksvermenigvuldiging $K \to K$ met λ is. Omdat tensorproducten van afbeeldingen componentsgewijs afbeelden, krijgen we voor iedere $\mu \otimes \varphi \in V_K$ en iedere $\lambda \otimes \tilde{\varphi} \in B_K$ de gelijkheid

$$\begin{aligned}
\psi((\lambda \otimes \tilde{\varphi})(\mu \otimes \varphi)) &= \psi(\lambda\mu \otimes \tilde{\varphi}\varphi) \\
&= l_{\lambda\mu} \otimes \tilde{\varphi}\varphi \\
&= (\lambda \otimes \tilde{\varphi})(l_\mu \otimes \varphi) \\
&= (\lambda \otimes \tilde{\varphi})\psi(\mu \otimes \varphi)
\end{aligned}$$

en door lineaire voortzetting is ψ dus een B_K-homomorfisme.

Zij $\varphi \in \mathrm{Hom}_{A_K}(M_K, N_K)$. Laat $(b_i)_{i\in I}$ een k-basis zijn van K. Dan heeft M_K een decompositie $M_K = \bigoplus_{i\in I} b_i \otimes M$ en N_K soortgelijk. Omdat φ een K-lineaire afbeelding is, bestaan er $g_i \colon M \to N$ zodanig dat voor iedere $m \in M$ geldt

$$\varphi(1 \otimes m) = \sum_{i\in I} b_i \otimes g_i(m).$$

Voor iedere $r \in A$ en iedere $m \in M$ geldt aan de ene kant

$$\varphi(1 \otimes rm) = \sum_{i\in I} b_i \otimes g_i(rm)$$

en aan de andere kant

$$\varphi(1 \otimes rm) = (1 \otimes r)\varphi(1 \otimes m) = (1 \otimes r)\sum_{i\in I} b_i \otimes g_i(m) = \sum_{i\in I} b_i \otimes rg_i(m)$$

en dus hebben we voor iedere $i \in I$ de gelijkheid $g_i(rm) = rg_i(m)$. De g_i zijn dus allen A-homomorfismen. Omdat M eindig-dimensionaal is over k, is het beeld van $1 \otimes M$ onder φ eindig-dimensionaal over k en dus zijn er slechts eindig veel g_i niet-nul. Dit betekent dat het element $\sum_{i\in I} b_i \otimes g_i \in V_K$ welgedefiniëerd is. Dit element wordt afgebeeld op de afbeelding die op de monomen van A_K werkt als

$$\lambda \otimes m \mapsto \sum_{i\in I} b_i\lambda \otimes g_i(m)$$

en dit is precies φ. De afbeelding ψ is dus surjectief.

Stel nu dat een element $\varphi = \sum_{i\in I} b_i \otimes \phi_i \in V_K$ afbeeldt op 0. Het beeld $\psi(\varphi)$ beeldt ieder monoom $1 \otimes m \in M_K$ af op

$$\sum_{i\in I} b_i 1 \otimes \phi_i(m) = \sum_{i\in I} b_i \otimes \phi_i(m)$$

en dit is nul dan en slechts dan als iedere $\phi_i(m)$ dat is, want de b_i vormen een basis voor K over k en vectorruimtes zijn plat. Dit betekent dat iedere ϕ_i nul is en dus geldt $\varphi = 0$. De afbeelding ψ is dus ook injectief en is dus een B_K-isomorfisme. □

Stelling 5.4. *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra zijn. Als M en N twee A-modulen van eindige dimensie over k zijn met $M_K \cong N_K$ als A_K-modulen, dan geldt $M \cong N$ als A-modulen.*

Bewijs. Definiëer V en B weer als in het vorige lemma. Merk op dat V en B beide eindig-dimensionaal zijn over k. Laat $h \colon M_K \to N_K$ een isomorfisme zijn. Er geldt $V_K \cong \mathrm{Hom}_{A_K}(M_K, N_K)$ en $B_K \cong \mathrm{End}_{A_K}(N_K)$ als A_K-modulen en we krijgen dus een B_K-homomorfisme $\varphi \colon B_K \to V_K$ gegeven door $b \mapsto bh$.

Omdat h een isomorfisme is, is φ dat ook en dus geldt $B_K \cong V_K$ als B_K-modulen. Stelling 5.1 zegt nu dat B en V isomorf zijn als B-modulen. Er bestaat dus een $v \in V$ zodanig dat $V = Bv$.

Omdat v het B-moduul V voortbrengt, brengt $1 \otimes v$ het B_K-moduul V_K voort en dus is er een $b \in B_K$ zodanig dat $b \cdot (1 \otimes v) = h \in V_K$. De samenstelling $b \cdot (1 \otimes v)$ is injectief en dus is $1 \otimes v$ injectief. Isomorfie van M_K en N_K zegt onder andere dat de dimensies van M en N over k gelijk zijn. Dit betekent dat $1 \otimes v$ ook surjectief is en lemma 3.8 zegt dus dat v een isomorfisme $M \to N$ is. □

Het bewijs van stelling 5.1 laat zich gemakkelijk aanpassen om de versie voor surjecties $A \to M$ te bewijzen.

Stelling 5.5. *Zij $k \subset K$ een uitbreiding van lichamen en laat A een k-algebra van eindige dimensie over k zijn. Als M een A-moduul van eindige dimensie over k is waarvoor er een surjectief A_K-homomorfisme $A_K \to M_K$ bestaat, dan bestaat er een surjectief A-homomorfisme $A \to M$.*

Bewijs. Omdat het tensorproduct exact is, geeft een surjectie $A_K \to M_K$ een surjectie $A_{\overline{K}} \to M_{\overline{K}}$ en we mogen dus weer aannemen dat K algebraïsch afgesloten is. De surjectie $A_K \to M_K$ laat zien dat de dimensie van A minstens zo hoog is als die van M. Laat m de dimensie van M zijn en n de dimensie van A. Maak als in het bewijs van stelling 5.1 een basis $c_1, c_2, \ldots, c_m$ van M_K via M. Laat ψ de surjectie $A_K \to M_K$ zijn. Nemen we voor iedere c_i één inverse beeld, dan krijgen we een lineair onafhankelijke verzameling en als we deze aanvullen met een basis van de kern van ψ, dan krijgen we een basis $b_1, b_2, \ldots, b_n$ van A_K.

We krijgen weer een eenheid

$$u = \sum_{i=1}^{n} x_i b_i$$

waar alle x_i bevat zijn in k. Laat v weer het beeld van u onder ψ zijn. De toegevoegde elementen in de basis $b_1, b_2, \ldots, b_n$ beelden op 0 af, dus er geldt

$$v = \psi(u) = \sum_{i=1}^{m} x_i c_i.$$

Definiëer de afbeelding φ weer als hiervoor. Dan volgt ook weer dat φ een surjectief A_K-homomorfisme is. Definiëer ook weer het A-homomorfisme $\varphi' \colon A \to M$ waarvoor geldt $1 \otimes \varphi' = \varphi$. De cokern van φ' wordt nul na optensoren en moet dus al nul geweest zijn. De afbeelding φ' is dus surjectief. □

Het geval van injecties $A \to M$ gaat mis. Neem aan dat k een eindig lichaam is van karakteristiek p. Schrijf $q = p^m$ voor het aantal elementen van k. Schrijf

V voor de k-vectorruimte k^{q+1}. Voor A nemen we de vectorruimte $k \oplus V$ met vermenigvuldiging gegeven door de scalaire vermenigvuldiging met k en $V \cdot V = 0$. Laat $\lambda_1, \lambda_2, \ldots, \lambda_q$ een aftelling zijn van de elementen van k. Definiëer homomorfismen $\alpha, \beta \colon V \to V$ door

$$\alpha = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_1 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_q \end{pmatrix}.$$

Merk op dat iedere k-lineaire combinatie van deze twee afbeeldingen een niet-nul kern heeft. Wanneer we de scalairen in een strikte uitbreiding $K \supsetneq k$ nemen, dan kunnen we wel een combinatie vinden die injectief is. Laat X de k-vectorruimte in $\mathrm{End}_k(V)$ zijn voortgebracht door α en β. De k-vectorruimte $M = X \oplus V$ wordt een A-moduul door k als verwacht te laten werken en door V te laten werken door $(0, v_1)(x, v_2) = (0, x(v_1))$. Er bestaan geen A-lineaire injecties $A \to M$. Wordt 1 namelijk op (x_0, v_0) afgebeeld, dan bestaat er een $0 \neq v \in V$ zodanig dat $x_0(v) = 0$ en dus wordt $(0, v) \neq 0$ afgebeeld op $(0, v)(x_0, v_0) = (0, x_0(v)) = (0, 0)$.

Definiëren we een homomorfisme $A_K \to M_K$ door $1 \mapsto (x_0, v_0)$ waar x_0 injectief is en v_0 niet-nul, dan is deze injectief. Namelijk: het element $(\lambda, v) \in A_K$ beeldt af op $(\lambda, v)(x_0, v_0) = (\lambda x_0, x_0(v) + \lambda v_0)$. Als de eerste coördinaat nul is, dan is λ nul en dan houden we $(0, x_0(v))$ over. Dit is nul dan en slechts dan als $v = 0$, dus dan en slechts dan als $(\lambda, v) = (0, 0)$. Zo zien we direct dat het beeld nul is dan en slechts dan als $(\lambda, v) = (0, 0)$. Er bestaat dus wel een A_K-lineaire injectie $A_K \to M_K$ en niet een A-lineaire injectie $A \to M$.

Referenties

[1] Alon, Noga. Combinatorial Nullstellensatz. Recent trends in combinatorics (M'atrah'aza, 1995). Combin. Probab. Comput. 8 (1999), no. 1-2, 7–29. .

[2] Lang, Serge. Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. ISBN: 0-387-95385-X

[3] Lam, T. Y. A first course in noncommutative rings. Second edition. Graduate Texts in Mathematics, 131. Springer-Verlag, New York, 2001. ISBN: 0-387-95183-0