STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1965-004

Voordracht in de serie

"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof. Dr. A.H.M. Levelt

17 februari 1965

Substitutie van machtreeksen

1. Inleiding

Voor (convergente) machtreeksen met complexe coëfficiënten in één onbepaalde zijn de volgende operaties bekend:

(i) optelling,

(ii) vermenigvuldiging met constanten,

(iii) vermenigvuldiging van twee machtreeksen.

Met deze operaties vormen de machtreeksen een ring $\mathbb{C}\{X\}$ met een aantal mooie eigenschappen:

(a) $\mathbb{C}\{X\}$ is een integriteitsgebied.

(b) $\mathbb{C}\{X\}$ is een lokale ring, d.w.z. er bestaat precies één maximaal ideaal in $\mathbb{C}\{X\}$ (nl. het ideaal door X voortgebracht).

(c) $\mathbb{C}\{X\}$ is een hoofdideaalring (want er is een euclidisch algorithme).

Uit (a) en (c) volgt nog dat $\mathbb{C}\{X\}$ een ontbindingsring is.

Het ligt voor de hand na te gaan of zulke eigenschappen ook gelden voor machtreeksen in meer onbepaalden. De operaties (i), (ii) en (iii) kan men daarvoor ook definiëren, en het is gemakkelijk in te zien dat de machtreeksen in n onbepaalden een commutatieve ring vormen, zelfs een integriteitsgebied en een lokale ring. Het is echter geen hoofdideaalring (net zo min als een veeltermring in meer onbepaalden dat is). Men kan echter bewijzen dat de ring noethers is, d.w.z. ieder ideaal wordt voortgebracht door eindig veel elementen. Ook is het een ontbindingsring.

Deze (al lang bekende) resultaten volgen uit de zgn. Vorbereitungssatz van Weierstrass, die een centrale plaats inneemt in de theorie van de machtreeksen (in meer onbepaalden).

Men kan deze stelling formuleren met behulp van substitutie van machtreeksen. Voor het geval van machtreeksen in één onbepaalde bedoelen we met substitutie de volgende operatie. Laat $U = \sum_{n=1}^{\infty} a_n Y^n$ een machtreeks zijn zonder constante term. Dan kan men voor iedere machtreeks $S = \sum_{m=0}^{\infty} b_m X^m$ de "samengestelde machtreeks"

$$S \circ U = \sum_{m=0}^{\infty} b_m \left(\sum_{n=1}^{\infty} a_n Y^n \right)^m$$

vormen. De toevoeging $S \rightsquigarrow S \circ U$ is een homomorfisme van $\mathbb{C}\{X\}$ in $\mathbb{C}\{Y\}$. Formuleert men de Vorbereitungssatz als een stelling over substitutie van machtreeksen, dan vertoont deze een zekere asymmetrie. J.P. Serre heeft een fraaie veralgemening gevonden, waarin deze asymmetrie is opgeheven. Die stelling is het hoofddoel van deze voordracht (4). In 5 geven we als toepassingen de bewijzen van bovengenoemde resultaten: de ring van machtreeksen in n onbepaalden is noethers en is een ontbindingsring.

In de opbouw van de theorie is het nuttig om de formules en relaties enerzijds en de convergentie anderzijds afzonderlijk te behandelen. Daarom worden in 2 eerst de formele machtreeksen bestudeerd en vervolgens in 3 de convergentie.

2. Formele machtreeksen in meer onbepaalden

Een formele machtreeks in n onbepaalden $X_1,\ldots,X_n$ $(n \geq 1)$ en coëfficiënten in een (commutatief) lichaam K is een uitdrukking

$$S(X_1,\ldots,X_n) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} a_{k_1\ldots k_n} X_1^{k_1}\ldots X_n^{k_n},$$

waarin $a_{k_1\ldots k_n} \in K$ is. De $a_{k_1\ldots k_n}$ heten de coëfficiënten van $S(X_1,\ldots,X_n)$. Wanneer er geen misverstand dreigt, schrijven we S i.p.v. $S(X_1,\ldots,X_n)$.

Is

$$T(X_1,\ldots,X_n) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} b_{k_1\ldots k_n} X_1^{k_1}\ldots X_n^{k_n}$$

een tweede formele machtreeks in $X_1,\ldots,X_n$, dan definiëert men som resp. produkt door

$$S + T = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} (a_{k_1\ldots k_n} + b_{k_1\ldots k_n})X_1^{k_1}\ldots X_n^{k_n},$$

resp.

$$ST = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} c_{k_1\ldots k_n} X_1^{k_1}\ldots X_n^{k_n},$$

waarin

$$c_{k_1\ldots k_n} = \sum_{h_1=0}^{k_1} \cdots \sum_{h_n=0}^{k_n} a_{h_1\ldots h_n} b_{k_1-h_1,\ldots,k_n-h_n}.$$

Is $a \in K$, dan is op voor de hand liggende manier aS gedefiniëerd. De verzameling van de formele machtreeksen in $X_1,\ldots,X_n$ met coëfficiënten in K noteren we $K[[X_1,\ldots,X_n]]$.

Van het volgende eenvoudige lemma wordt - evenals van enkele verdere lemma's - het bewijs aan de lezer overgelaten.

Lemma 1. $K[[X_1,\ldots,X_n]]$ is een integriteitsgebied (en een K-algebra).

Is S een formele machtreeks $\neq 0$, d.w.z. minstens één der coëfficiënten $\neq 0$, dan verstaat men onder de <u>orde $\omega(S)$ van S</u> het kleinste gehele getal $k \geq 0$ met de eigenschap dat er een coëfficiënt $a_{k_1 \ldots k_n} \neq 0$ bestaat met $k_1 + \ldots + k_n = k$.
We stellen nog $\omega(0) = \infty$. Ook stellen we $||S|| = 2^{-\omega(S)}$ als $S \neq 0$ is, en $||0|| = 0$.

<u>Lemma 2</u>. Zijn S en T in $K[[X_1,\ldots,X_n]]$, dan gelden

(a) $0 \leq \omega(S) \leq \infty$, $\omega(S) = \infty \Leftrightarrow S = 0$,
(b) $\omega(S+T) \geq \min(\omega(S),\omega(T))$,
(c) $\omega(ST) = \omega(S) + \omega(T)$,

en eveneens

(a') $1 \geq ||S|| \geq 0$, $||S|| = 0 \Leftrightarrow S = 0$,
(b') $||S+T|| \leq \max(||S||,||T||)$,
(c') $||ST|| = ||S||\,||T||$.

De eigenschap (b') impliceert de driehoeksongelijkheid

$$||S+T|| \leq ||S|| + ||T||,$$

maar is er niet mee equivalent, en heet daarom de verscherpte driehoeksongelijkheid. Een functie $||\ldots||$ met de eigenschappen (a') en (b') heet een <u>niet-archimedische waardering</u>.

<u>Lemma 3</u>. $K[[X_1,\ldots,X_n]]$ is compleet t.o.v. de waardering, d.w.z. iedere Cauchy-rij in deze ring convergeert.

<u>Lemma 4</u>.

(a) $S \in K[[X_1,\ldots,X_n]]$ is dan en slechts dan inverteerbaar als $||S|| = 1$ is.
(b) $K[[X_1,\ldots,X_n]]$ is een lokale ring. Het maximale ideaal wordt voortgebracht door $X_1,\ldots,X_n$.

Voor het bewijs van (a) merken we op dat $1 + T + T^2 + \ldots$ een Cauchy-rij is, als $||T|| < 1$ is, en dat geldt $(1-T)(1+T+T^2+\ldots) = 1$;

voor het bewijs van (b), dat de niet-inverteerbare elementen vanwege de eigenschappen van $\|\ \ \|$ een ideaal vormen.

Wij zullen nu de substitutie van formele machtreeksen beschrijven. Laat $U_1,\ldots,U_n$ elementen zijn van het maximale ideaal voor $K[[Y_1,\ldots,Y_m]]$ (dus $\|U_i\| < 1$, $i=1,\ldots,n$). Is $S \in K[[X_1,\ldots,X_n]]$, dan kunnen we S schrijven in de vorm $\sum_{k=0}^{\infty} S_k$, waarin S_k een (door S éénduidig bepaalde) homogene veelterm is van de graad k. Dus geldt $\omega(S_k(U_1,\ldots,U_n)) \geq k$ in $K[[Y_1,\ldots,Y_m]]$, waaruit volgt dat $\sum_{k=0}^{\infty} S_k(U_1,\ldots,U_n)$ een element van $K[[Y_1,\ldots,Y_m]]$ bepaalt, dat we noteren als $S \circ U$, en het substitutieresultaat van $U = (U_1,\ldots,U_n)$ in S noemen.

Lemma 5.

(a) De afbeelding $S \rightsquigarrow S \circ U$ is een ringhomomorfisme $K[[X_1,\ldots,X_n]] \longrightarrow K[[Y_1,\ldots,Y_m]]$, continu t.o.v. $\|\ldots\|$, en wel een lokaal homomorfisme (d.w.z. het maximale ideaal van de eerste ring wordt in dat van de tweede ring afgebeeld).

(b) Ieder lokaal homomorfisme $\phi : K\|X_1,\ldots,X_n\| \longrightarrow K\|Y_1,\ldots,Y_m\|$ is continu en kan door substitutie verkregen worden.

Het is duidelijk dat men in (b) voor U_i moet nemen $\phi(X_i)$. Er volgt dan direkt $\phi(S) = S \circ U$, als S een veelterm is. Voor willekeurige S volgt het resultaat door limietovergang.

3. Convergentie

Over convergente machtreeksen met coëfficiënten in K kunnen wij slechts spreken, als we in K over een limiet-begrip beschikken. Wij zullen aannemen dat K een gewaardeerd lichaam is, d.w.z. er is een functie $x \rightsquigarrow |x|$ van K naar de reële getallen, die voldoet aan:

(a) $|x| \geq 0$, en $|x| = 0 \leftrightarrows x = 0$,
(b) $|x+y| \leq |x| + |y|$,
(c) $|xy| = |x|\,|y|$.

Als in (b) de scherpere ongelijkheid $|x+y| \leq \max(|x|,|y|)$ geldt, dan heet K niet-archimedisch gewaardeerd. (voorbeeld: p-adische getallen).
Soms is het nodig te veronderstellen, dat de waardering niet-triviaal is (de triviale waardering is: $|x| = 0$ resp. 1 als $x = 0$ resp. $\neq 0$ is).
Is de waardering niet-triviaal dan bevat K ∞ veel elementen.
Wil men over functies spreken, door machtreeksen gedefiniëerd, dan moet men K compleet t.o.v. de waardering veronderstellen. Wij zullen ons daar niet mee bezighouden.

Een formele machtreeks

$$(1) \qquad S(X_1,\ldots,X_n) = \sum_{k_1,\ldots,k_n=0}^{\infty} a_{k_1\ldots k_n} X_1^{k_1}\ldots X_n^{k_n}$$

heet (absoluut) convergent, als er positieve reële getallen $r_1,\ldots,r_n$ bestaan zó, dat

$$\sum_{k_1,\ldots,k_n=0}^{\infty} |a_{k_1\ldots k_n}|\, r_1^{k_1}\ldots r_n^{k_n}$$

convergeert. De verzameling van de convergente machtreeksen in n onbepaalden $X_1,\ldots,X_n$ noteren we als $K\{X_1,\ldots,X_n\}$.
Een formele machtreeks

$$S'(X_1,\ldots,X_n) = \sum_{k_1,\ldots,k_n=0}^{\infty} b_{k_1\ldots k_n} X_1^{k_1}\ldots X_n^{k_n}$$

met niet-negatieve reële coëfficiënten heet een majorant van S (S gedefiniëerd door (1)) als $|a_{k_1\ldots k_n}| \leq b_{k_1\ldots k_n}$ is voor alle $k_1,\ldots,k_n$; notatie $S \ll S'$. Als M , α positieve getallen zijn, verstaan we onder (M,α) de formele machtreeks

$$\sum_{k_1,\ldots,k_n=0}^{\infty} M\,\alpha^{k_1+\ldots+k_n} X_1^{k_1}\ldots X_n^{k_n} .$$

De uitspraak "S convergeert" is equivalent met "er bestaan $M > 0$, $\alpha > 0$ zó, dat $S << (M,\alpha)$ ".

Lemma 6. $K\{X_1,\ldots,X_n\}$ is een deelring van $K[[X_1,\ldots,X_n]]$.

We moeten dus bewijzen dat som en produkt van convergente machtreeksen weer convergente machtreeksen zijn. Daartoe merken we op dat uit $S << S'$, $T << T'$ volgt: $S+T << S'+T'$ en $ST << S'T'$, en dat geldt

$$(M,\alpha) + (N,\beta) << (M+N,\max(\alpha,\beta))$$
$$(M,\alpha)(N,\beta) << (MN,2\max(\alpha,\beta)) .$$

Hieruit volgt het gestelde direkt.
Laat nu $S \in K\{X_1,\ldots,X_n\}$ zijn en $U_1,\ldots,U_n \in K\{Y_1,\ldots,Y_m\}$ met $\omega(U_i) \geq 1$ $(i=1,\ldots,m)$. Dan is $S \circ U \in K[[Y_1,\ldots,Y_m]]$.
Er geldt zelfs $S \circ U \in K\{Y_1,\ldots,Y_m\}$. Voor een bewijs merken we op, dat uit $S << S'$, $U_i << U_i'$ $(i=1,\ldots,n,\ \omega(U_i') \geq 1)$ volgt $S \circ U << S' \circ U'$. We mogen verder aannemen, dat $M,N,\alpha,\beta > 0$ bestaan met $S << (M,\alpha)$, $U_i << (N,\beta)$. We behoeven dan nog slechts aan te tonen dat voor voldoend kleine $r > 0$

$$\sum_{k_1,\ldots,k_n=0}^{\infty} M\,\alpha^{k_1+\ldots+k_n}\left(\sum_{l_1+\ldots+l_p \geq 1} N\,\beta^{l_1+\ldots+l_p}\, r^{l_1+\ldots+l_p}\right)^{k_1+\ldots+k_n}$$

convergeert. Dit is een eenvoudige kwestie uit de reële analyse, welke aan de lezer wordt overgelaten.

Lemma 7. Als lemma 4, maar $K[[X_1,\ldots,X_n]]$ vervangen door $K\{X_1,\ldots,X_n\}$.

Voor het bewijs van (a) merken we op, dat $1 + Y + Y^2 + \ldots$ een convergente machtreeks is, dus ook - vanwege het voorafgaande - $1 + U + U^2 + \ldots$ als $\omega(U) \geq 1$ is. Hieruit volgt dat $1 - U$ inverteerbaar is in $K\{X_1,\ldots,X_n\}$, waaruit (a) direkt volgt. Het bewijs van (b) gaat zoals bij lemma 4.

Lemma 8. Als lemma 5, maar met $K\{X_1,\ldots,X_n\}$ i.p.v. $K[[X_1,\ldots,X_n]]$, en $K\{Y_1,\ldots,Y_m\}$ i.p.v. $K[[Y_1,\ldots,Y_m]]$.

4. Een stelling van J.P. Serre

Stelling 1. Laten $U_1,\ldots,U_n$ elementen van het maximale ideaal van $K\{Y_1,\ldots,Y_m\}$ zijn. Zij verder r een natuurlijk getal en veronderstel dat er elementen $B_{ji} \in K\{Y_1,\ldots,Y_m\}$ bestaan zó, dat

$$Y_i^r = \sum_{j=1}^{n} U_j B_{ji} \qquad (i=1,\ldots,m) .$$

Dan kan men ieder element S van $K\{Y_1,\ldots,Y_m\}$ schrijven in de vorm

$$(2) \qquad S = \sum_{h_1 < r,\ldots,h_m < r} V_{h_1\ldots h_m} \circ U \; Y_1^{h_1}\ldots Y_m^{h_m} ,$$

waarin $V_{h_1\ldots h_m}(X_1,\ldots,X_n) \in K\{X_1,\ldots,X_n\}$ is.

Wij geven een korte schets van een bewijs.
Zij

$$S = \sum_{h_1,\ldots,h_m=0}^{\infty} a_{h_1\ldots h_m} Y_1^{h_1}\ldots Y_m^{h_m}$$

een element van $K\{Y_1,\ldots,Y_m\}$. Dan kan men S schrijven in de vorm

$$(3) \qquad S = \rho(S) + \sum_{j=1}^{n} U_j \, \sigma_j(S) ,$$

waarin $\rho(S) = \sum_{h_1 < r,\ldots,h_m < r} a_{h_1\ldots h_m} Y_1^{h_1}\ldots Y_m^{h_m}$, en $\quad \sigma_j(S) = \sum_{i=1}^{m} B_{ji} \sum_{h_1<r,\ldots,h_{i-1}<r,h_i\geq r} a_{h_1\ldots h_m} Y_1^{h_1}\ldots Y_i^{h_i-r}\ldots Y_m^{h_m}$.

Vervanging van S door $\sigma_j(S)$ in (2) geeft

$$\sigma_j(S) = \rho\sigma_j(S) + \sum_{i=1}^{n} U_i\, \sigma_i\sigma_j(S) \;.$$

Dit resultaat kan men weer in (3) substitueren:

$$S = \rho(S) + \sum_{j=1}^{n} U_j\,\rho\,\sigma_j(S) + \sum_{i,j=1}^{n} U_iU_j\;\sigma_i\sigma_j(S) \;.$$

Door iteratie van dit procédé vindt men

$$S = \rho(S) + \sum_{j=1}^{n} U_j\,\rho\sigma_j(S) + \sum_{j_1,j_2=1}^{n} U_{j_1}U_{j_2}\,\rho\,\sigma_{j_1}\sigma_{j_2}(S) + \ldots$$

$$\ldots \sum_{j_1,\ldots,j_p=1}^{n} U_{j_1}\ldots U_{j_p}\;\rho\;\sigma_{j_1}\ldots\sigma_{j_p}(S) + R_p(S) \;,$$

waarin

$$R_p(S) = \sum_{j_1,\ldots,j_{p+1}=1}^{n} U_{j_1}\ldots U_{j_{p+1}}\;\sigma_{j_1}\ldots\sigma_{j_{p+1}}(S)$$

orde $\geq$ p+1 heeft. In $\rho\sigma_{j_1}\ldots\sigma_{j_q}$ treden slechts monomen $Y_1^{h_1}\ldots Y_m^{h_m}$ op met $h_i < r$. Hieruit volgt dat het rechterlid van (4) in de vorm

$$(5)\quad S = \sum_{h_1<r,\ldots,h_m<r} U^{(p)}_{h_1\ldots h_m}(S)\;Y_1^{h_1}\ldots Y_m^{h_m} \;+\; R_p(S)$$

geschreven kan worden, waarin $U^{(p)}_{h_1\ldots h_m}(S)$ verkregen wordt door in een veelterm $V^{(p)}_{h_1\ldots h_m}(X_1,\ldots,X_n)$ te substitueren $X_1 = U_1,\ldots, X_n = U_n$. Men gaat gemakkelijk na dat $\left(V^{(p)}_{h_1\ldots h_r}\right)_p$ een Cauchy-rij is, zodat men door limietovergang $p \to \infty$ (in de zin van $||\ldots||$) uit (5) de formule (2) afleidt, waarin echter nog aangetoond moet worden dat $V_{h_1\ldots h_m}$ convergent is. Dit geschiedt door een apart convergentie-

onderzoek. Hierover zeggen we slechts het volgende:
Men mag aannemen dat $B_{ji} << (1,1)$ (te bereiken door geschikte automorfismen van $K\{X_1,\ldots,X_n\}$ en $K\{Y_1,\ldots,Y_m\}$). Dan bewijst men: als $S << (M,\alpha)$ dan $\sigma_j(S) << (M\, m\alpha^{r+1},\alpha)$, en hieruit $\sigma_{j_1}\ldots\sigma_{j_p}(S) << (M(m\alpha^{r+1})^p,\alpha)$. Dan heeft $V_{h_1\ldots h_m}\circ U$ als majorant $(M\alpha^h, m\alpha^{r+1})$, waarin $h = h_1+\ldots+h_m$, waaruit de convergentie blijkt.

Opmerking. Eigenlijk heeft men eerst de variant van de stelling bewezen, die ontstaat door overal convergente machtreeksen door formele te vervangen.

Wij geven nu een andere formulering van het in stelling 1 gevonden resultaat. Ter afkorting schrijven we $A = K\{X_1,\ldots,X_n\}$, $B = K\{Y_1,\ldots,Y_m\}$ en M resp. N voor de maximale idealen. $U_1,\ldots,U_n$ in N bepalen een lokaal homomorfisme $\phi: A \to B$ (lemma 8). Hierdoor kunnen wij B opvatten als A-moduul . Wij schrijven kortweg $a.b$ i.p.v. $\phi(a)b$ als $a \in A$, $b \in B$.

Stelling 2. Met de hierboven ingevoerde notaties geldt:
Is r een geheel getal ≥ 1 en is $N^r \subset MB$, dan is B een A-moduul van eindig type, d.w.z. B is een A-moduul met een eindig aantal voortbrengers.

Uit het gegeven $N^r \subset MB$ volgt nl. de hypothese van stelling 1, terwijl de bewering van de stelling juist inhoudt dat $Y_1^{h_1}\ldots Y_m^{h_m}$ $(h_1 < r,\ldots,h_m < r)$ een stel voortbrengers van het A-moduul B is (formule (4)).

Toevoeging bij stelling 2. De monomen $Y_1^{h_1}\ldots Y_m^{h_m}$ met $h_1+\ldots+h_m < r$ brengen reeds B voort.

Zij nl. B' het A-moduul voortgebracht door genoemde monomen, dan is $B = B' + N^r$, dus $B = B' + MB$.
Omdat B een A-moduul van eindig type is volgt nu met het lemma van Nakayama $B = B'$.

We beschouwen nu het speciale geval van stelling 2, waarin $n=m$, $\phi(X_1) = Y_1, \ldots, \phi(X_{n-1}) = Y_{n-1}, \phi(X_n) = U$. De voorwaarde $N^r \subset MB$ ($N^{r-1} \not\subset MB$) komt neer op $Y_n^r \in MB$ ($Y_n^{r-1} \not\in MB$). Er moeten dus elementen $B_j \in K\{Y_1,\ldots,Y_n\}$ bestaan met

$$Y_n^r = Y_1B_1 + \ldots + Y_{n-1}B_{n-1} + UB_n .$$

Een noodzakelijke en voldoende voorwaarde hiervoor is dat U regulier is van orde r in Y_n, d.w.z.

$$U = \sum_{i=0}^{\infty} u_i(Y_1,\ldots,Y_{n-1})Y_n^i ,$$

waarin $u_i(0,\ldots,0) = 0$ voor $i=0,1,\ldots,r-1$, en $u_r(0,\ldots,0) \neq 0$. Uit de toevoeging bij stelling 2 volgt nu, dat $1,Y_n,\ldots,Y_n^{r-1}$ $K\{Y_1,\ldots,Y_n\}$ voortbrengen als $K\{X_1,\ldots,X_n\}$-moduul, d.w.z. dat men iedere $S \in K\{Y_1,\ldots,Y_n\}$ kan schrijven als

$$S = C_0(Y_1,\ldots,Y_{n-1},U) + C_1(Y_1,\ldots,Y_{n-1},U)Y_n + \ldots$$
$$\ldots C_{r-1}(Y_1,\ldots,Y_{n-1},U)Y_n^{r-1} ,$$

waarin $C_i(X_1,\ldots,X_n) \in K\{X_1,\ldots,X_n\}$ is. Hieruit volgt direkt

Stelling 3. (Vorbereitungssatz van Weierstrass). Is $U \in K\{Y_1,\ldots,Y_n\}$ regulier van orde $r \geq 0$ in X_n, dan bestaan voor iedere $S \in K\{Y_1,\ldots,Y_n\}$ een Q en een $R \in K\{Y_1,\ldots,Y_n\}$ met

(a) $S = UQ + R$,

(b) R is een veelterm in Y_n van graad $< r$ (en coëfficiënten in $K\{Y_1,\ldots,Y_{n-1}\}$).

Q en R zijn door (a) en (b) éénduidig bepaald.

Het bewijs van de eenduidigheid is eenvoudig; wij zullen er niet op ingaan.

5. Enkele toepassingen

A. Speciale veeltermen

Een element $P \in K\{Y_1,\ldots,Y_n\}$ heet een speciale veelterm in Y_n van graad r als hij de volgende vorm heeft

$$P = P_0(Y_1,\ldots,Y_{n-1}) + P_1(Y_1,\ldots,Y_{n-1})Y_n + \ldots$$
$$\ldots + P_{r-1}(Y_1,\ldots,Y_{n-1})Y_n^{r-1} + Y_n^r ,$$

met $P_0(0,\ldots,0) = P_1(0,\ldots,0) = \ldots = P_{r-1}(0,\ldots,0) = 0$.
Twee elementen S_1, S_2 van $K\{Y_1,\ldots,Y_n\}$ heten equivalent als er een inverteerbare $T \in K\{Y_1,\ldots,Y_n\}$ bestaat met $S_2 = S_1T$.

Stelling 4. Is $U \in K\{Y_1,\ldots,Y_n\}$ regulier van orde $r \geq 1$ in Y_n, dan is U equivalent met één en slechts één speciale veelterm in Y_n.

Pas nl. stelling 3 toe met $S = Y_n^r$. Dan is $Y_n^r = UQ + R$, waarin R een veelterm van graad $< r$ in Y_n is.
De speciale veelterm in kwestie is dan $Y_n^r - R$.

Speciale veeltermen zijn onder meer van groot nut bij de studie van analytische verzamelingen (en ruimten). Dit zijn deelverzamelingen, die lokaal gedefiniëerd worden door het nul stellen van convergente machtreeksen.

Voor andere toepassingen zie B en C hierna.

B. $K\{Y_1,\ldots,Y_n\}$ is een noetherse ring

Bewijs door induktie naar n. Triviaal voor $n = 0$. Zij nu $n \geq 1$ en laat al bewezen zijn dat $K\{Y_1,\ldots,Y_{n-1}\}$ noethers is. Zij $I \neq 0$ een ideaal van $K\{Y_1,\ldots,Y_n\}$. Wij zullen aantonen dat I eindig veel voortbrengers heeft.

Laat $S \in I$ zijn, $S \neq 0$. Wij mogen aannemen dat S regulier is in Y_n, dus ook - vanwege A - dat S een speciale veelterm is. (De situatie dat S regulier is in Y_n is, in het geval K ∞ veel elementen heeft, steeds te bereiken door een geschikt automorfisme van $K\{Y_1,\ldots,Y_n\}$). De ring $K\{Y_1,\ldots,Y_n\} / (S)$ is een $K\{Y_1,\ldots,Y_{n-1}\}$-moduul van eindig type, dus zelf noethers. Het beeld $\bar{I}$ van I in $K\{Y_1,\ldots,Y_n\} / (S)$ heeft dus eindig veel voortbrengers. Maar dan geldt hetzelfde voor I.

C. $K\{Y_1,\ldots,Y_n\}$ is een ontbindingsring

In het volgende is $A = K\{Y_1,\ldots,Y_n\}$. (Uitspraak en bewijs zijn ook goed voor $K[[Y_1,\ldots,Y_n]]$).
Uit de algebra is bekend, dat een ring een ontbindingsring is dan en slechts dan als gelden:

(a) Iedere stijgende rij hoofdidealen is stationnair.

(b) Ieder priemelement brengt een priemideaal voort.

Voor de ring A is aan (a) voldaan, want A is noethers.
Wij zullen nu (b) door induktie naar n bewijzen. (b) is triviaal voor A als $n = 0$. Zij nu $n \geq 1$, en laat (b) bewezen zijn voor $K\{Y_1,\ldots,Y_{n-1}\}$. Zij P een priemelement van A, dat het produkt van twee elementen Q, Q' van A deelt. We moeten aantonen $P \mid Q$ of $P \mid Q'$
Men mag aannemen dat P regulier is van graad r in Y_n, dus ook dat P een speciale veelterm van graad r is in Y_n. Laat B de ring van de veeltermen in Y_n zijn met coëfficiënten in $K\{Y_1,\ldots,Y_{n-1}\}$. Dan is B een ontbindingsring vanwege de induktieaanname en de stelling van Gauss. P is een priemelement in B. Dit bewijst men als volgt. Laat $P = SS'$ een ontbinding van P in B zijn. Stel hierin $Y_1 = \ldots = Y_{n-1} = 0$. Dan gaat P over in Y_n^p, S in $\bar{S}(Y_n)$, S' in $\bar{S'}(Y_n)$, en er geldt $Y_n^p = \bar{S}(Y_n)\bar{S'}(Y_n)$. Men leidt hieruit af, dat S en S', afgezien van een constante faktor, speciale veeltermen in X_n zijn. Eén ervan moet eenheid zijn in A, dus speciale veelterm van de graad 0 in Y_n, d.w.z. eenheid in B. P is dus priem in B. Laten R en R' de resten van Q resp. Q' zijn bij deling door P (stelling 3). Dan zijn

R en $R' \in B$ en er geldt $P \mid RR'$. Dus $P \mid R$ of $P \mid R'$, waaruit volgt $R = 0$ en dan $P \mid Q$ of $R' = 0$ en dan $P \mid Q'$. Dit voltooit het bewijs.

<u>Literatuur</u>

1. Voor de stelling van J.P. Serre, zie Sém. Cartan 1960/61, exposé 18. In hetzelfde séminaire vindt men een uitvoerige theorie van analytische algebra's (quotientringen van $K\{X_1,\ldots,X_n\}$).

2. Allerlei eenvoudige en minder eenvoudige zaken over machtreeksen-ringen vindt men o.a. in: Abhyankar, Local analytic geometry. Academic Press, 1964.