STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
AFDELING ZUIVERE WISKUNDE

ZW 1968-015

Voordracht in de serie
"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof.dr. F. Oort

"De volledige doorsnede van twee vlakke algebraïsche krommen"

Inleiding: Laat gegeven zijn twee polynomen in twee veranderlijken

$$\phi = \phi(X,Y) \quad \text{en} \quad \psi = \psi(X,Y);$$

onderstel dat ϕ en ψ geen factor gemeen hebben. Dan bestaan er eindig veel punten

$$P_1 = (a_1,b_1), \ldots, P_m = (a_m,b_m)$$

die gelegen zijn op de beide vlakke algebraïsche krommen

$$\phi = 0 = \psi,$$

dat wil zeggen $\phi(a_i,b_i) = 0 = \psi(a_i,b_i)$ voor $1 \leq i \leq m$.

We zeggen in dit geval dat $\{P_1, \ldots, P_m\}$ de volledige doorsnede is van deze twee krommen.

We kunnen ons afvragen of elk eindig stelsel punten in een vlak de volledige doorsnede is van twee algebraïsche krommen, en we komen zo tot het probleem (provisorische vorm):

Laat gegeven zijn $P_1 = (a_1,b_1)$, ..., $P_m = (a_m,b_m)$; is er te vinden een tweetal polynomen ϕ en ψ, zo dat de snijpunten van $\phi = 0$ en $\psi = 0$ precies deze punten zijn?

In een nadere precizering (zie §1) zullen we aangeven hoe we de "snijpuntsmultipliciteit" in de verschillende punten P_i kunnen voorschrijven. Als die multipliciteit in elk punt één is, dan is er een elementaire oplossing van het probleem (over een algebraïsch afgesloten lichaam) van P. van EMDE BOAS (zie §2). In het algemene geval is het probleem opgelost door J.-P. SERRE (zie §4). Het zou zeker interessant zijn om ook voor het algemene geval een elementaire oplossing te vinden.

§1. Formulering van de stelling met behulp van idealen

We beschouwen commutatieve ringen met een eenheidselement. Een ring heet noethers als elk ideaal eindig voortgebracht kan worden (equivalent: als aan de "stijgende rijen conditie" is voldaan). Als R een noetherse ring is, dan is $R[X]$ dat ook (basisstelling van Hilbert; zie bij voorbeeld [13], II, Kap. 12).

Een ideaal $\mathfrak{p} \subset R$ heet een priem ideaal, als uit $xy \in \mathfrak{p}$ en $x \notin \mathfrak{p}$ volgt $y \in \mathfrak{p}$ (generalisatie van het begrip priemgetal). Een ideaal $\mathfrak{q} \subset R$ heet een primair ideaal als uit $xy \in \mathfrak{q}$ en $x \notin \mathfrak{q}$ volgt dat er een geheel getal n bestaat, zo dat $y^n \in \mathfrak{q}$ (generalisatie van het begrip macht van een priemgetal). Factorontbinding kan als volgt gegeneraliseerd worden:

Primaire ontbinding van idealen: Zij R een noetherse ring, en $\mathfrak{a} \subset R$ een ideaal in R. Dan zijn er primaire idealen $\mathfrak{q}_1$, ..., $\mathfrak{q}_m$ in R, zo dat

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$$

(vgl. [13], II, Kap. 12; [6], 1.8, theorem 5).

Zij $\mathfrak{a}$ een ideaal in een ring R. We definiëren:

$$\sqrt{\mathfrak{a}} := \{x | x \in R, \exists n : x^n \in \mathfrak{a}\},$$

en we zeggen het radicaal van $\mathfrak{a}$. Het is duidelijk dat het radicaal van een primair ideaal een priemideaal is:

$$\mathfrak{q} \text{ is primair } \Longrightarrow \mathfrak{p} := \sqrt{\mathfrak{q}} \text{ is priem}$$

(en vandaar de notatie die het wortelteken gebruikt).

Onderstel dat $\mathfrak{q} \subset R$ een primair ideaal is, zodanig dat $\mathfrak{p} := \sqrt{\mathfrak{q}}$ een maximaal ideaal is in R. We zeggen dat $\mathfrak{q}$ locaal voortgebracht kan worden door 2 elementen uit R, als er bestaan $\phi, \psi \in R$, zodat het ideaal

$$\phi R + \psi R = \mathfrak{q} \cap \mathfrak{b}, \text{ met } \mathfrak{p} \neq \mathfrak{b}.$$

Voorbeelden: Zij k een lichaam, $R = k[X,Y]$, en $\mathfrak{q} = (X^2, XY, Y^2) \cdot R$; het is duidelijk dat dit ideaal locaal niet voortgebracht kan worden door 2 elementen uit R.

Zij K een algebraïsch afgesloten lichaam, en $\mathfrak{q} = \mathfrak{p} \subset R = K[X,Y]$ een maximaal ideaal. Dan is $R/\mathfrak{p}$ een lichaam en het kan bewezen worden dat dit lichaam eindig is over K; dus $R/\mathfrak{p} = K$ omdat K algebraïsch afgesloten is. Dan zijn er $a,b \in K$, zo dat

$$X \equiv a \bmod \mathfrak{p} \qquad \text{en} \qquad Y \equiv b \bmod \mathfrak{p},$$

en het is duidelijk dat $\mathfrak{p} = (X-a, Y-b) \cdot R$. Dus in dit geval kan $\mathfrak{q} = \mathfrak{p}$ door twee elementen worden voortgebracht.

Stelling. (SERRE, zie [10], pag. 2-11, remarque, en de daaraan voorafgaande stellingen): Zij k een lichaam, $R = k[X,Y]$, de polynoomring in twee veranderlijken over k, en $\mathfrak{a} \subset R$ een ideaal in R met primaire ontbinding

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m.$$

Onderstel dat de idealen $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ maximaal zijn en onderling verschillend. Het ideaal $\mathfrak{a}$ kan voortgebracht worden door twee elementen uit R (d.w.z. er bestaan $\phi, \psi \in R$ zo dat

$$\mathfrak{a} = (\phi,\psi) \cdot R \quad)$$

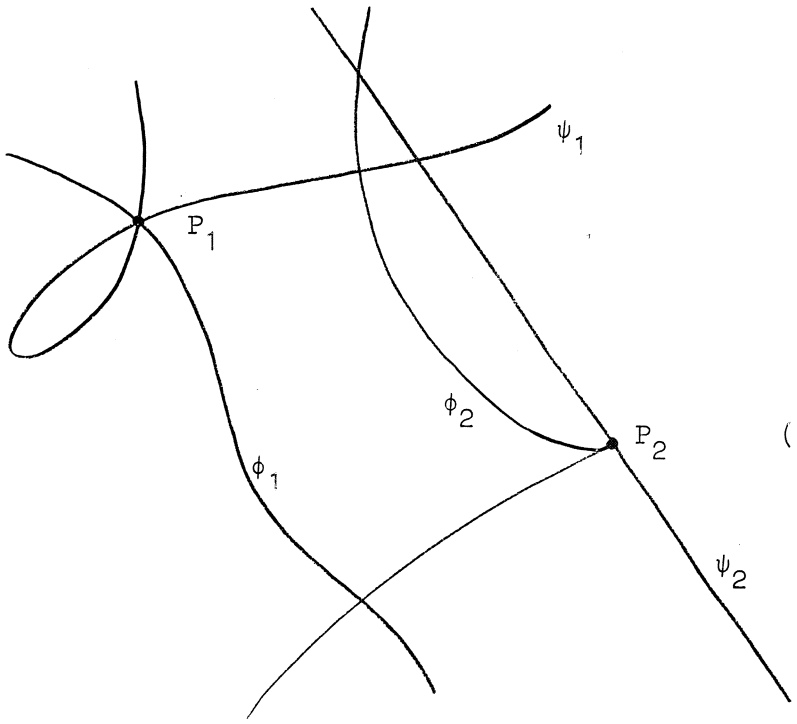
dan en slechts dan als $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ elk afzonderlijk locaal kunnen worden voortgebracht door twee elementen uit R (d.w.z. er bestaan $\phi_i, \psi_i \in R$ zo dat

$$\mathfrak{q}_i \cap \mathfrak{b}_i = (\phi_i, \psi_i) \cdot R$$

met $\sqrt{\mathfrak{q}_i} \supsetneq \mathfrak{b}_i$, $1 \leq i \leq m$).

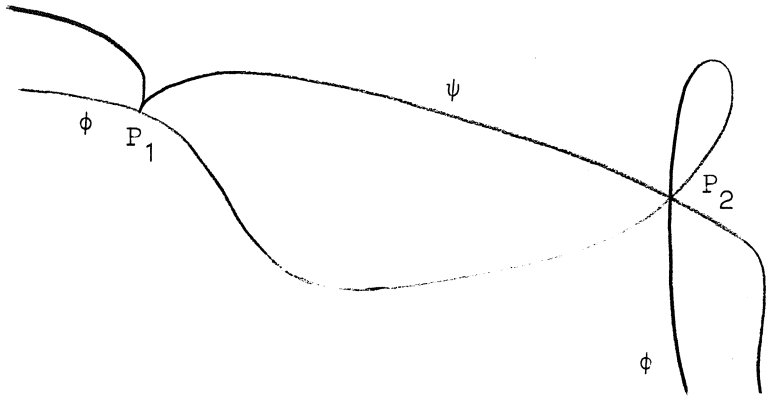
Natuurlijk volgt uit $\mathfrak{a} = (\phi,\psi) \cdot R$, dat elke $\mathfrak{q}_i$ locaal door twee elementen kan worden voortgebracht; de omkering is het moeilijke deel van de stelling.

Als:



(etc. ..., P_m),

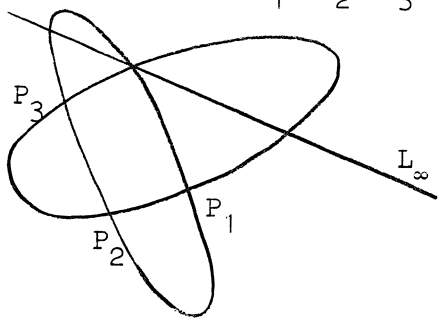
dan bestaan er $\phi,\psi \in R = k[X,Y]$, zo dat:



(etc. ..., tot P_m, en $\phi = 0$, $\psi = 0$ geen punten gemeen behalve de P_i).

Opmerking: Zij graad(ϕ) = c en graad(ψ) = d; dan is het aantal snijpunten (geteld met de goede multipliciteit) van $\phi = 0$ en $\psi = 0$, precies cd, als we de krommen in het projectieve vlak beschouwen (stelling van Bezout; zie bv. [ ] , §17 en §41, zie ook [15]); dus eigenlijk zijn de gemeenschappelijke nulpunten van ϕ en ψ gelegen in P_1, ..., P_m, plus (misschien) nog een aantal punten in het "oneindige".

Voorbeeld: Neem P_1, P_2 en P_3 niet op een rechte lijn, en neem $\mathcal{q}_i = \mathcal{p}_i$, i = 1, 2, 3. We krijgen deze 3 punten (met multipliciteit één) als volledige doorsnede van $\phi = 0$ en $\psi = 0$, door een P_4 op L_∞ te kiezen, en voor ϕ en ψ twee verschillende tweedegraads vormen te kiezen uit de schaar bepaald door P_1, P_2, P_3 en P_4:



$P_1 = (0,0)$, d.w.z. $\mathcal{q}_1 = (X,Y) \cdot R$
$P_2 = (1,0)$, $\mathcal{q}_2 = (X-1, Y) \cdot R$
$P_3 = (0,1)$, $\mathcal{q}_3 = (X, Y-1) \cdot R$;

kies $P_4 = (1,1,0)$ (in homogene coördinaten); de schaar is dan:

$$F_{\lambda,\mu} \equiv \lambda(X^2 - XZ) + \mu(Y^2 - YZ) - (\lambda + \mu)XY.$$

en er geldt:

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 = (F_{\lambda,\mu}, F_{\alpha,\beta}) \circ R \quad \text{als} \quad \frac{\lambda}{\mu} \neq \frac{\alpha}{\beta}.$$

Maar zo eenvoudig kan het algemene geval niet opgelost worden (?)!

Opmerking: Zij $\mathfrak{q}$ een primair ideaal, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ het bijbehorende priemideaal, en

$$\mathfrak{q} = \mathfrak{b}_1 \underset{\neq}{\subset} \mathfrak{b}_2 \underset{\neq}{\subset} \dots \underset{\neq}{\subset} \mathfrak{b}_d = \mathfrak{p}$$

een keten van primaire idealen, die niet meer langer gemaakt kan worden; in dit geval schrijven we $l(\mathfrak{q}) = d$, de "multipliciteit" van $\mathfrak{q}$ (en bewezen kan worden dat andere maximale ketens dezelfde lengte hebben). Als $\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{b}}$, en $l(\mathfrak{q}) = l(\mathfrak{b})$, dan hoeft daar nog niet uit te volgen dat $\mathfrak{q} = \mathfrak{b}$; b.v. $R = k[X,Y]$,

$$l((X^2,XY,Y^2) \circ R = 3 = l((X^3,Y) \circ R).$$

We zien dus dat het geven van $\mathfrak{q}_1$ een veel gedetailleerder informatie is, dan alleen maar het getal $l(\mathfrak{q}_1)$, de "snijpunts multipliciteit"; vandaar de ogenschijnlijk wat gecompliceerde formulering van de stelling.

Terzijde: In ons geval is inderdaad de snijpuntsmultipliciteit van $\phi = 0$ en $\psi = 0$ ter plaatse P_1 gegeven door $l(\mathfrak{q}_1)$, waar $(\phi,\psi)R = \mathfrak{q}_1 \cap \dots$, maar in het algemeen is $l(\mathfrak{q})$ niet hetzelfde als de meetkundige multipliciteit. Dat het fout kan gaan, zien we in [5], 144.11; wat dan wel de goede opzet is, vinden we in [9], in het bijzonder chap. V, C.1, théorème 1. Zie ook [3].

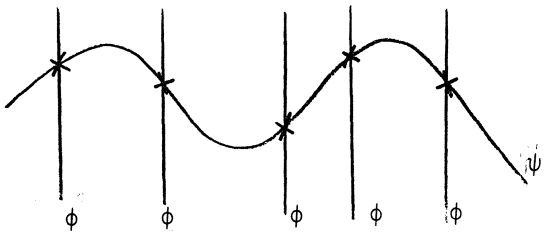
Opmerking: Veronderstel gegeven $\mathfrak{q}_1, \dots, \mathfrak{q}_m$, $\phi_1, \dots, \phi_m$ en $\psi_1, \dots, \psi_m$, zoals in de stelling. We kunnen construeren een ϕ, die ter plaatse $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ "voldoende lijkt" op ϕ_i, voor $i = 1, \dots, m$ (b.v. $\phi \equiv \phi_i$ modulo een voorgeschreven hoge macht van $\mathfrak{p}_i$). Maar er is geen garantie, dat daarbij een ψ gevonden kan worden met de gewenste eigenschap, zoals blijkt uit het volgende:

Voorbeeld: $m = 1, \mathcal{O}_1 = \mathfrak{p}_1 = (X,Y) \cdot R$; we kiezen (ongelukkigerwijze) $\phi = X - X^3 - Y^2$. Bewering: als kar(k) $\neq 2$ (dus bv. k het lichaam van de complexe getallen), dan bestaat er niet een $\psi \in R = k[X,Y]$ met $(\phi,\psi) = \mathcal{O}_1$ (want, als graad(ψ) = m, dan hebben ϕ en ψ projectief gezien 3m snijpunten; als daarvan 3m-1 gelegen zijn in (0,1,0), dan is het laatste daar ook gelegen, zoals volgt uit de theorie van de elliptische krommen).

§2. Bewijs van de stelling (in het enkelvoudige geval)

Gegeven is een lichaam k met oneindig veel elementen, verder $a_1, \ldots, a_m, b_1, \ldots, b_m$, en $\mathcal{O}_i = \mathfrak{p}_i = (X - a_i, Y - b_i)R$, $1 \leq i \leq m$, waar $R = k[X,Y]$ (b.v. het geval dat k algebraïsch is afgesloten, en alle $\mathfrak{p}_i \subset R$ maximaal).

Constructie van P. van EMDE BOAS: In dit geval bestaan er $\phi,\psi \in R$ met $(\phi,\psi)R = \bigcap \mathcal{O}_i$. Kies namelijk (zo nodig) een lineaire transformatie λ van het X-Y-vlak, zodat alle a_i onderling verschillend worden (dat kan omdat k oneindig veel elementen heeft). Neem dan



$\phi = \prod_{i=1}^{m} (X - a_i)$, en neem $\psi = Y - F(X)$, waar $F(X)$ een "functie" is die in het punt a_i de waarde b_i heeft, bijvoorbeeld:

(m=3)

$$\psi = Y - b_1 \frac{(X-a_2)(X-a_3)}{(a_1-a_2)(a_1-a_3)} - b_2 \frac{(X-a_1)(X-a_3)}{(a_2-a_1)(a_2-a_3)} - b_3 \frac{(X-a_1)(X-a_2)}{(a_3-a_1)(a_3-a_2)};$$

in het algemeen:

$$\psi = \Big\{ \prod_{1\leq k<l\leq m} (a_k - a_l) \Big\} \cdot Y + \sum_{i=1}^{m} \Big\{ (-1)^i \, b_i \, \frac{\prod_{j=1}^{m} (X-a_j)}{X - a_i} \cdot \prod_{\substack{1\leq k<l\leq m \\ k\neq i \\ l\neq i}} (a_k - a_l) \Big\}.$$

Het is duidelijk dat $X - a_i = 0$ en $\psi = 0$ elkaar slechts snijden in (a_i,b_i); de raaklijnen vallen niet samen, dus het snijpunt is enkelvoudig.

Bestaat er een dergelijke elementaire en elegante oplossing voor de stelling in het algemene geval?

Om althans tot een oplossing te komen enige voorbereiding:

§3. Ext

Een abelse groep M heet een A-moduul, waar A een ring is, als voor elke $a \in A$, $x \in M$ gegeven is $ax \in M$, zodat aan de gebruikelijke voorwaarden is voldaan: voor alle $a,b \in A$, $x,y \in M$ geldt:

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$(ab)x = a(bx),$$

$$1x = x;$$

(als A niet commutatief is, spreken we van een links-A-moduul, etc.). Een voorbeeld: een ideaal van A is een A-moduul. Als A = lichaam, dan spreken we van een lineaire ruimte, of een vectorruimte. Een groepshomomorfisme $f: M \to N$ tussen A-modulen heet A-lineair als voor alle $a \in A$, $x \in M$ geldt $af(x) = f(ax)$.

Een A-moduul M heet eindig voortgebracht en vrij als M isomorf met A^m (cartesisch product) voor zekere m.

Een A-moduul P heet projectief en eindig voortgebracht als een surjectief A-lineair homomorfisme $f: A^n \to P$ bestaat, en een

$$s: P \to A^n, \quad \text{zodat} \quad fs = 1_P.$$

Elk eindig voortgebracht eindig vrij moduul is projectief, maar de omkering is niet juist voor alle A! De essentiële stap in het bewijs zal zijn dat we werken over een ring waar de omkering wél juist is, en het aantal voortbrengers van een bepaald projectief moduul te tellen, door te werken over het lichaam van quotiënten van A (en dan is het gewone lineaire algebra).

We zeggen dat een rij

$$0 \to M \xrightarrow{i} T \xrightarrow{p} N \to 0$$

van A-modulen met A-lineaire homomorfismen exact is, als i injectief is (d.w.z. een-een-duidig), als p surjectief is (d.w.z. p(T) = N), en als N = T/iM). Twee exacte rijen van dit type heten equivalent als er een isomorfisme $T \cong T'$ bestaat zodat het diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & T & \xrightarrow{p} & N & \longrightarrow & 0 \\ & & \| & & \downarrow f & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow{i'} & T' & \xrightarrow{p'} & N & \longrightarrow & 0 \end{array}$$

commutatief is (d.w.z. $i' = f \circ i$ en $p = p' \circ f$). De verzameling van equivalentieklassen schrijven we als $\mathrm{Ext}_A(N,M)$. Een constructie, die door R. BAER gevonden werd, maakt het mogelijk op een natuurlijke manier een groepsstructuur te leggen op de verzameling $\mathrm{Ext}_A(N,M)$ (zie [1], zie ook [4], p. 290). Bij een exacte rij

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

behoort een exacte rij

$$0 \to \mathrm{Hom}_A(N_3,M) \to \mathrm{Hom}_A(N_2,M) \to \mathrm{Hom}_A(N_1,M) \to$$

$$\to \mathrm{Ext}_A(N_3,M) \to \mathrm{Ext}_A(N_2,M) \to \mathrm{Ext}_A(N_1,M)$$

(d.w.z. elke pijl heeft als beeld de kern van de volgende pijl). Ook kan bewezen worden dat P een projectief A-moduul is dan en slechts dan als $\mathrm{Ext}_A(P,M) = 0$ voor alle A-modulen M. De bovenstaande exacte rij kan nog verder voortgezet worden; we schrijven dan $\mathrm{Ext}_A = \mathrm{Ext}_A^1$, en definiëren ook Ext_A^2, Ext_A^3 etc. Dit kan op vele manieren gebeuren (zie b.v. [4], chap. VI; [7] chap. 7, etc.). Deze begrippen en verschillende andere zullen vrijelijk gebruikt worden in de volgende paragraaf.

§4. Bewijs van de stelling

We gebruiken de notatie van de stelling, en we voeren verder nog in:

A_i is de localisatie van R naar $\mathfrak{p}_i$, d.w.z.

$$A_i = \{\frac{f}{g} \mid f,g \in R,\ g \notin \mathfrak{p}_i\};$$

elk der ringen A_i is een locale ring, d.w.z. er is in A_i precies één maximaal idelaal:

$$\mathfrak{m}_i = \{\frac{f}{g} \mid f,g \in R,\ f \in \mathfrak{p}_i,\ g \notin \mathfrak{p}_i\} = \mathfrak{p}_i \cdot A_i \subset A_i.$$

Het gegeven "$\mathfrak{q}_i$ wordt locaal voortgebracht door twee elementen" is equivalent met: "het ideaal $\mathfrak{q}_i \cdot A_i$ wordt over A_i door twee elementen voortgebracht".

De bewijsgang zal zijn:

(het ideaal $\mathfrak{q}_i \cdot A_i \subset A_i$ kan over A_i worden voortgebracht door twee elementen, voor $1 \leq i \leq m$)

$\Downarrow$ 1

(het A_i-moduul $\mathrm{Ext}_{A_i}(\mathfrak{q}_i \cdot A_i, A_i)$ kan worden voortgebracht door één element, voor $1 \leq i \leq m$)

$\Downarrow$ 2

(het R-moduul $\mathrm{Ext}_R(\mathfrak{a},R)$ kan worden voortgebracht door één element)

$\Downarrow$ 3

(het R-ideaal $\mathfrak{a} \subset R$ kan worden voortgebracht door twee elementen).

Dat is de truc: "voortgebracgr door twee elementen" is kennelijk niet zo gemakkelijk te "globaliseren" (zie de laatste opmerking van §1); door (1) en (3) vertalen we het gegeven (en de conclusie) in een stap die wél te globaliseren is:

Bewijs van (2): Eerst merken we op dat $Q_i = \mathrm{Ext}_{A_i}(\mathfrak{q}_i A_i, A_i)$ geannuleerd wordt door een macht van $\mathfrak{m}_i = \mathfrak{p}_i A_i$; dus Q_i is een moduul over

$$A_i/\mathfrak{m}_i^N = R/\mathfrak{p}_i^N \quad \text{voor zekere } N.$$

Dus het is voldoende om te bewijzen dat

$$\mathrm{Ext}_R(\mathfrak{a},R) \cong \bigoplus_{i=1}^{m} Q_i$$

(isomorfisme van R-modulen). En het bewijs daarvan kan gegeven worden omdat de $\mathfrak{p}_i$ maximaal zijn en onderling verschillend; b.v.:

$$\mathrm{Ext}_R(\mathfrak{a},R) \cong \mathrm{Ext}_{\underline{\mathcal{O}}_V}(\underline{\mathfrak{a}},\underline{\mathcal{O}}_V) \cong$$

$$\cong \Gamma(V, \underline{\mathrm{Ext}}_{\underline{\mathcal{O}}_V}(\underline{\mathfrak{a}},\underline{\mathcal{O}}_V)) \cong$$

$$\cong \oplus\, (\underline{\mathrm{Ext}}_{\underline{\mathcal{O}}_V}(\underline{\mathfrak{a}},\underline{\mathcal{O}}_V))_{P_i} \quad ,$$

waar $V = \mathrm{Spec}(k[X,Y])$, de strepen onder symbolen duiden op verschoving, en het laatste isomorfisme geldt omdat de schoof $\underline{\mathrm{Ext}}_{\underline{\mathcal{O}}_V}(\underline{\mathfrak{a}},\underline{\mathcal{O}}_V)$ nul is buiten de punten $P_i \in V$.

(2) q.e.d.

Propositie (zie [10], prop. 4, prop. 2, prop. 1, en lemma 9): Zij B een integriteitsgebied, en I een ideaal in B. Veronderstel dat elk eindig voortgebracht projectief B-moduul vrij is (!). Onderstel dat de homologische dimensie van I kleiner dan twee is. Dan:

$$\left(\begin{array}{l}\text{I kan worden voortgebracht}\\ \text{door twee elementen}\end{array}\right) \Longleftrightarrow \left(\begin{array}{l}\mathrm{Ext}_B(I,B) \text{ kan worden voortgebracht}\\ \text{door één element}\end{array}\right).$$

Bewijs, ==>: Omdat I door twee elementen kan worden voortgebracht, bestaat er een exacte rij van B-modulen:

$$0 \to M \to B^2 \to I \to 0 \quad (*).$$

Omdat $\mathrm{hd}(I) < 2$ volgt dat M projectief is, dus vrij, $M = B^N$. Zij L het lichaam van quotiënten van B. Stel $I \neq 0$ (anders is de uitspraak allang duidelijk); dan is $\dim_L(I \otimes_B L) = 1$, dus $\dim_L(B^N \otimes_B L) = N = 2 - 1 = 1$. Dus $M = B$. Schrijf met behulp van (*) en van $\mathrm{Ext}_B(-,B)$ de exacte Hom - Ext rij uit, er komt:

$$\begin{array}{ccccccccc} \ldots & \to & \mathrm{Hom}_B(B,B) & \to & \mathrm{Ext}_B(I,B) & \to & \mathrm{Ext}_B(B^2,B) & \to & \ldots \\ & & \downarrow\wr & & \| & & \| & & \\ \ldots & \to & B & \to & \mathrm{Ext}_B(I,B) & \to & 0 & & \end{array},$$

en het eerste deel is bewezen.

Bewijs, <==: Laat de klasse van

$$0 \to B \to T \to I \to 0 \quad (**)$$

een voortbrenger zijn van $\mathrm{Ext}_B(I,B)$. De exacte Hom • Ext behorende bij (**) geeft:

$$\ldots \to \mathrm{Hom}_B(B,B) \xrightarrow{\delta} \mathrm{Ext}_B(I,B) \to \mathrm{Ext}_B(T,B) \to \mathrm{Ext}_B(B,B);$$

omdat $\mathrm{Hom}_B(B,B) = B$, en omdat $\mathrm{Ext}_B(I,B)$ voortgebracht wordt door (**), volgt dat δ surjectief is. Bovendien is $\mathrm{Ext}_B(B,-) = 0$, dus we concluderen: $\mathrm{Ext}_B(T,B) = 0$. Uit $\mathrm{hd}(I) < 2$, en uit $I = T/B$ volgt $\mathrm{hd}(T) < 2$. Bovendien is T eindig voortgebracht (B is noethers, etc.). Kies een exacte rij

$$0 \to M \to B^n \xrightarrow{f} T \to 0;$$

uit $\mathrm{hd}(T) < 2$ volgt dat M projectief is. Dus is M vrij, $M = B^m$; wegens $\mathrm{Ext}(T,B) = 0$ geldt dat deze exacte rij splitst, d.w.z. er bestaat een $s \in \mathrm{Hom}_B(T,B^n)$ met $fs = 1_T$. Dus is T projectief, dus vrij over B. Analoog zoals boven leiden we af, dat ($I \neq 0$) de rang van T gelijk is aan 2 ($I \otimes_B L = L$, $B \otimes_B L = L$, en gebruik lineaire algebra). Dus $T = B^2$, en we hebben bewezen dat I door twee elementen kan worden voortgebracht.

q.e.d.

Verificatie van (1): kies een index i, $1 \leq i \leq m$; $B = A_i$, $I = \mathfrak{q}_i A_i$. Bekend is dat

$$\mathrm{gl\ dim}(k[X_1, \ldots, X_n]) = n$$

(zie [4], IX, th. 7.11, N.B. k is een lichaam); omdat A_i een localisatie is van $R = k[X,Y]$, geldt:

$$\mathrm{gl\ dim}(A_i) \leq \mathrm{gl\ dim}(R) = 2$$

(zie [4], 9.2, th. 8). Bekend is dat elk eindig voortgebracht moduul dat projectief is over een locale ring, vrij is (b.v. zie [7], 9.3, th. 12, of enig ander boek dat het "lemma van Nakayama" beschrijft). Dus aan de eisen van de propositie is voldaan, en (1) is bewezen.

Verificatie van (3): kies B = R, I = $\mathfrak{a}$; bekend is gl dim(R) = 2 (zie boven), en dus $hd_R(\mathfrak{a}) < 2$. C. SESHADRI bewees dat in het geval R = k[X,Y], elk eindig voortgebracht projectief moduul vrij is! (en dit is, technisch gesproken, het lastigste deel van het bewijs), zie [11], en [12]. Dus aan de voorwaarden van de propositie is voldaan, (3) is bewezen, en het bewijs van de stelling van §1 is voltooid.

Achtergrond van deze stelling van SESHADRI: is elk e.v. projectief moduul over $k[X_1, \ldots, X_n]$ vrij?, zie [8], pag. 243, regels 5-8 van boven. Voor n = 1 is het antwoord bevestigend, en het bewijs eenvoudig. Voor n = 2 komen we in het geval, dat bevestigend werd beantwoord door SESHADRI. Voor $n \geq 3$ schijnt er nog geen definitief eindresultaat te zijn behaald (voor partiële resultaten, en verwijzingen, zie bij voorbeeld [2]).

Literatuur

[1] R. BAER - Erweiterungen von Gruppen und ihren Isomorphismen.
Math. Z. 38 (1934), 375-416.

[2] H. BASS und P. MURTHY -Grothendieck groups and Picard groups of abelian group rings.
Ann. Math. 86 (1967), 16-73.

[3] J.H. de BOER - The intersection multiplicity of a connected component.
Math. Ann. 172 (1967), 238-246.

[4] H. CARTAN & S. EILENBERG - Homological algebra.
Princeton University Press, 1956.

[5] W. GRÖBNER - Moderne algebraische Geometrie.
Springer Verlag, 1949.

[6] D.G. NORTHCOTT - Ideal theory.
Cambridge University Press, 1960.

[7] D.G. NORTHCOTT - An introduction to homological algebra.
Cambridge University Press, 1960.

[8] J.-P. SERRE - Faisceaux algébriques cohérents.
Ann. Math. 61 (1955), 197-278.

[9] J.-P. SERRE - Algèbre locale, multiplicités.
Collège de France 1957-1958, gestencild dictaat.

[10] J.-P. SERRE - Sur les modules projectifs.
Sém. Dubeil-Pisot, 14 (1960/61), exp. 2
(21 november 1960).

[11] C.S. SESHADRI - Triviality of vector bundles over the affine space K^2.
Proc. Nat. Acad. Sc. USA, 44 (1958), 456-458.

[12] C.S. SESHADRI - Algebraic vector bundles over the product of an affine curve and the affine line.
Proc. Amer. Math. Soc., 10 (1959), 670-673.

[13] B.L. van der WAERDEN - Moderne Algebra, II.

[14] B.L. van der WAERDEN - Einführung in die algebraische Geometrie.
Berlijn, 1939.

[15] R.J. WALKER - Algebraic curves.
Princeton University Press, 1950.