VRIJE UNIVERSITEIT BRUSSEL

Inleiding Algebraische Meetkunde

S. Caenepeel

Syllabus 107 bij 1006927CNR “Inleiding Algebraische Meetkunde”
Derde Bachelor Wiskunde 2017

Inhoudsopgave

1 Voorafgaande begrippen **3**

1.1 Veeltermenringen 3

1.2 Eigenschappen van commutatieve ringen 9

1.3 Lichaamsuitbreidingen 12

1.4 Comaximale idealen 17

1.5 Exacte rijen 18

1.6 Oefeningen 19

2 Affiene algebraische verzamelingen **23**

2.1 Algebraische verzamelingen 23

2.2 Het ideaal behorend bij een stel punten 25

2.3 Irreducibele algebraische verzamelingen 28

2.4 Algebraische delen van het vlak 30

2.5 De Hilbert Nullstellensatz 32

2.6 Oefeningen 35

3 Affiene variëteiten **37**

3.1 Affiene variëteiten en veeltermafbeeldingen 37

3.2 Rationale functies en locale ringen 42

3.3 Idealen met een eindig aantal nulpunten 47

3.4 Affiene coördinatentransformaties 52

3.5 Oefeningen 54

4 Vlakke krommen **57**

4.1 Raaklijnen 57

4.2 Locale ringen 60

4.3 Intersectiegetallen 62

4.4 Oefeningen 72

5 Projectieve variëteiten **76**

5.1 De projectieve ruimte 76

5.2 Projectieve algebraische verzamelingen 77

5.3 Affiene en projectieve variëteiten 81

5.4 Functielichamen en locale ringen 86

5.5 Projectieve coördinatentransformaties 88

5.6 Oefeningen 89

6 Projectieve vlakke krommen **91**

6.1 Projectieve vlakke krommen 91

6.2 Lineaire systemen van krommen 92

6.3 De stelling van Bezout 94

6.4 Grondstelling van Max Noether 98

6.5 Enkele meetkundige toepassingen 102

6.6 Oefeningen 105

Hoofdstuk 1

Voorafgaande begrippen

We herhalen enkele eigenschappen uit de theorie van lichamen en commutatieve ringen. Voor de ontbrekende bewijzen verwijzen we naar de cursus "Algebra II".

1.1 Veeltermenringen

Zij R een commutatieve ring. Een R-algebra is een ring A die ook een R-moduul is, zodanig dat de vermenigvuldiging $m : A \times A \to A$ R-bilineair is. Een morfisme van R-algebras is een ringmorfisme dat tegelijkertijd R-lineair is.
Als $\varphi : R \to S$ een morfisme tussen commutatieve ringen is, dan is S een R-algebra: S is een R-moduul via restrictie van scalairen:

$$r \cdot s = \varphi(r)s.$$

Het is makkelijk na te gaan dat de vermenigvuldiging op S R-bilineair is:

$$(r \cdot s)t = (\varphi(r)s)t = \varphi(r)st = r \cdot (st).$$

Lemma 1.1.1 *Neem twee morfismen $\varphi : R \to S$ en $\psi : R \to T$ tussen commutatieve ringen. Een ringmorfisme $f : S \to T$ is een algebra morfisme als en alleen als*

$$f \circ \varphi = \psi.$$

Bewijs. Onderstel dat f een algebra morfisme is. Dan geldt voor alle $r \in R$ dat $(f \circ \varphi)(r) = f(\varphi(r)) = f(r \cdot 1_S) = r \cdot f(1_S) = \psi(r)1_T = \psi(r)$, en dus is $f \circ \varphi = \psi$.
Omgekeerd, onderstel dat $f \circ \varphi = \psi$. Voor alle $r \in R$ and $s \in S$ hebben we dat

$$f(r \cdot s) = f(\varphi(r)s) = f(\varphi(r))f(s) = \psi(r)f(s) = r \cdot f(s).$$

□

Zij R een commutatieve ring. We noteren $R[X_1, X_2, \cdots, X_n]$ voor de veeltermenring in n veranderlijken. Een algebraische basis van $R[X_1, X_2, \cdots, X_n]$ als R-moduul is

$$\{X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \mid (i_1, i_2, \cdots, i_n) \in \mathbb{N}^n\}$$

De elementen van deze basis worden *monomen* genoemd, en elke veelterm is dus op unieke manier te schrijven als een (eindige) lineaire combinatie van monomen. De vermenigvuldiging wordt gedefinieerd door de formule

$$(X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n})(X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n}) = X_1^{i_1+j_1} X_2^{i_2+j_2} \cdots X_n^{i_n+j_n}$$

en door het feit dat de vermenigvuldiging bilineair is. $R[X_1, X_2, \cdots, X_n]$ is een commutatieve ring, en zelfs een R-algebra. We hebben een ringmonomorfisme

$$i: \ R \to R[X_1, X_2, \cdots, X_n]$$

die $r \in R$ afbeeldt op de constante veelterm r.
Per definitie noemen we $i_1 + i_2 + \cdots + i_n$ de graad van het monoom $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$. Een veelterm F noemen we *homogeen van graad* m als hij een lineaire combinatie is van monomen van graad m. We noemen F ook een *vorm* van graad m.
Elke veelterm F kan op unieke manier geschreven worden onder de vorm

$$F = F_0 + F_1 + \cdots + F_d$$

waarbij F_i een vorm van graad i is. Als $F_d \neq 0$, dan zeggen we dat F van graad d is, genoteerd $\deg(F) = d$. F_0, F_1, F_2 noemen we respectievelijk het constante, lineaire en kwadratische deel van F. Als R een domein is, dan geldt

$$\deg(FG) = \deg(F) + \deg(G).$$

Stelling 1.1.2 *Zij $\varphi: \ R \to S$ een morfisme van commutatieve ringen. De afbeelding*

$$\Delta: \ \mathrm{Alg}_R(R[X_1, \cdots, X_n], S) \to S^n$$

gegeven door de formule

$$\Delta(f) = (f(X_1), \cdots, f(X_n))$$

is een bijectie.

Bewijs. 1) Δ is injectief. Onderstel dat

$$\Delta(f) = \Delta(g) = (s_1, \cdots, s_n).$$

Dan geldt

$$\begin{aligned} f(X_1^{i_1} \cdots X_n^{i_n}) &= f(X_1)^{i_1} \cdots f(X_n)^{i_n} = s_1^{i_1} \cdots s_m^{i_n} \\ &= g(X_1)^{i_1} \cdots g(X_n)^{i_n} = g(X_1^{i_1} \cdots X_n^{i_n}). \end{aligned}$$

f en g vallen dus samen op monomen. Omdat de monomen een basis vormen voor de $R[X_1, \cdots, X_n]$, kunnen we concluderen dat $f = g$.
2) Δ is surjectief. Voor $s = (s_1, \cdots, s_n) \in S^n$ definiëren we $\Gamma(s) = \tilde{s} : \ R[X_1, \cdots, X_n] \to S$ als volgt. Voor een monoom $M = X_1^{i_1} \cdots X_n^{i_n}$ stellen we

$$\tilde{s}(X_1^{i_1} \cdots X_n^{i_n}) = s_1^{i_1} \cdots s_n^{i_n}.$$

We breiden deze formule lineair uit tot de ganse veeltermenring: als $F = \sum_i r_i M_i$, waarbij M_i monomen en $r_i \in R$, dan stellen we

$$\tilde{s}(F) = \sum_i \varphi(r_i)\tilde{s}(M_i).$$

$\tilde{s}$ is dan een morfisme van R-modulen.
Laten we aantonen dat $\tilde{s}$ een ringmorfisme is. Voor monomen M en N geldt duidelijk dat

$$\tilde{s}(MN) = \tilde{s}(M)\tilde{s}(N).$$

Neem een tweede veelterm $G = \sum_j r'_i N_j$, waarbij de N_j monomen zijn. Dan geldt

$$\begin{aligned} \tilde{s}(FG) &= \tilde{s}(\sum_{i,j} r_i r'_j M_i N_j) = \sum_{i,j} \varphi(r_i r'_j)\tilde{s}(M_i N_j) \\ &= (\sum_i \varphi(r_i)\tilde{s}(M_i))(\sum_j \varphi(r'_j)\tilde{s}(N_j)) = \tilde{s}(F)\tilde{s}(G). \end{aligned}$$

Het is duidelijk dat $\Delta\tilde{s} = s$, en dus is Δ surjectief. □

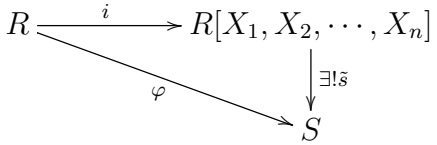
We noteren $\Delta^{-1} = \Gamma$, m.a.w. $\Gamma(s) = \tilde{s}$, voor $s \in S^n$. We noteren ook, voor $F \in R[X_1, \cdots, X_n]$:

$$\tilde{s}(F) = F(s_1, \cdots, s_n),$$

en dit definieert een functie

$$F : \ S^n \to S,$$

genaamd de veeltermfunctie geassocieerd aan F.
Stelling 1.1.2 kan geherformuleerd worden. De veeltermenring voldoet aan volgende universele eigenschap: als $\varphi : \ R \to S$ een morfisme van commutatieve ringen is, dan bestaat er voor elke $s = (s_1, \cdots, s_n) \in S^n$ een uniek ringmorfisme $\tilde{s} : \ R[X_1, \cdots X_n] \to S$ zodat $\tilde{s}(X_i) = s_i$ en $\tilde{s} \circ i = \varphi$: het diagram



is commutatief.

Stelling 1.1.3 *Neem een morfisme van commutatieve ringen $\varphi:\ R \to S$, en*

$$s = (s_1, \cdots, s_n) \in S^n, \quad T = (T_1, \cdots, T_m) \in R[X_1, \cdots, X_n]^m.$$

We hebben dan R-algebra morfismen

$$\tilde{T}:\ R[Y_1, \cdots, Y_m] \to R[X_1, \cdots, X_n] \text{ en } \tilde{s}:\ R[X_1, \cdots, X_n] \to S.$$

Bekijk ook

$$(\tilde{s}(T_1), \cdots, \tilde{s}(T_m)) = (T_1(s_1, \cdots, s_n), \cdots, T_m(s_1, \cdots, s_n)) = T(s) \in S^m,$$

en

$$\widetilde{T(s)}:\ R[Y_1, \cdots, Y_m] \to S.$$

Dan is

$$\widetilde{T(s)} = \tilde{s} \circ \tilde{T}. \tag{1.1}$$

Bewijs. Uit stelling 1.1.2 volgt dat het volstaat om aan te tonen dat $\Delta(\widetilde{T(s)}) = \Delta(\tilde{s} \circ \tilde{T})$, hetgeen erop neerkomt aan te tonen dat beide leden van (1.1) samenvallen in elke Y_i. Voor elke $i \in \{1, \cdots, m\}$ hebben we dat

$$(\tilde{s} \circ \tilde{T})(Y_j) = \tilde{s}(T_j) = T_j(s_1, \cdots, s_n) = \widetilde{T(s)}(Y_j).$$

□

Gevolg 1.1.4 *Neem $T \in R[X_1, \cdots, X_m]$ en $F = (F_1, \cdots, F_m) \in R[Z_1, \cdots, Z_k]^m$. Dan is de veeltermfunctie geassocieerd aan $T(F)$ gelijk aan de samengestelde van de veeltermfuncties geassocieerd aan F en T:*

$$T(F) = T \circ F.$$

Bewijs. Neem $\varphi:\ R \to S$ en $s \in S^k$. Bekijk de algebra afbeeldingen

$$R[Y] \xrightarrow{\tilde{T}} R[X_1, \cdots, X_m] \xrightarrow{\tilde{F}} R[Z_1, \cdots, Z_k] \xrightarrow{\tilde{s}} S.$$

Gebruik makend van stelling 1.1.3 vinden we

$$(T(F))(s) = \tilde{s}(T(F)) = \tilde{s}(\tilde{F}(T)) = \widetilde{F(s)}(T) = T(F(s)) = (T \circ F)(s).$$

□

Merk ook op dat we een kanoniek isomorfisme hebben:

$$R[X_1, X_2, \cdots, X_n] = R[X_1, X_2, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n][X_i]$$

Een veelterm $F \in R[X]$ in één veranderlijke wordt *monisch* genoemd indien de hoogste graadscoëfficiënt 1 is. De *afgeleide* van

$$F(X) = \sum_{i=0}^{d} a_i X^i$$

is per definitie

$$\frac{\mathrm{d}F}{\mathrm{d}X}(X) = \sum_{i=1}^{d} i a_i X^{i-1}$$

De *partiële afgeleide* van een veelterm F in n veranderlijken, is de afgeleide als we de veelterm beschouwen als een veelterm in 1 veranderlijke in $R[X_1, X_2, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n][X_i]$. Zoals gebruikelijk noteren we deze door

$$\frac{\partial F}{\partial X_i}(X_1, \cdots, X_n)$$

We hebben volgende eigenschappen:
1) Partieel afleiden is lineair:

$$\frac{\partial}{\partial X_i}(aF + bG) = a\frac{\partial F}{\partial X_i} + b\frac{\partial G}{\partial X_i}$$

2) Vermenigvuldigingsregel:

$$\frac{\partial FG}{\partial X_i} = \frac{\partial F}{\partial X_i}G + F\frac{\partial G}{\partial X_i}$$

3) Kettingregel: voor veeltermen $G_1, \cdots, G_n \in R[X]$ en $F \in R[X_1, \cdots, X_n]$ hebben we

$$\frac{\mathrm{d}F(G_1(X), \cdots, G_n(X))}{\mathrm{d}X} = \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(G_1(X), \cdots, G_n(X))\frac{\mathrm{d}G_i}{\mathrm{d}X}(X)$$

4) Symmetrie:

$$\frac{\partial^2 F}{\partial X_i \partial X_j} = \frac{\partial^2 F}{\partial X_j \partial X_i}$$

5) Formule van Euler: Als F een vorm is van graad m in $R[X_1, \cdots, X_n]$, dan hebben we

$$mF = \sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i}$$

6) Formule van Taylor: als $F \in R[X_1, \cdots, X_n]$ van graad d is, dan is

$$F(X_1, \cdots, X_n) = \sum_{i=0}^{d} \frac{1}{i!}\left(X_1\frac{\partial}{\partial X_1} + \cdots + X_n\frac{\partial}{\partial X_n}\right)^{(i)} F(0, \cdots, 0)$$

Bij deze laatste formule onderstellen we wel dat R een lichaam van karakteristiek 0 is. Bewijs als oefening zelf al deze formules.

Homogenizatie en dehomogenizatie

Zij R een domein, en $F \in R[X_1, \cdots, X_{n+1}]$ een vorm. We stellen

$$F_*(X_1, \cdots, X_n) = F(X_1, \cdots, X_n, 1)$$

en noemen dit de "gedehomogenizeerde"van F: F_* is een veelterm in een veranderlijke minder, maar is in het algemeen niet langer homogeen.
Omgekeerd, zij $f \in R[X_1, \cdots, X_n]$ een veelterm van graad d. We definiëren dan de gehomogenizeerde vorm $f^* \in R[X_1, \cdots, X_{n+1}]$ op de volgende manier: als

$$f = f_0 + f_1 + \cdots + f_d$$

waarbij f_i een vorm van graad i is, met $f_d \neq 0$, dan stellen we

$$\begin{aligned} f^* &= X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d & (1.2) \\ &= X_{n+1}^d f\Big(\frac{X_1}{X_{n+1}}, \cdots, \frac{X_n}{X_{n+1}}\Big) & (1.3) \end{aligned}$$

Stelling 1.1.5 *Voor vormen $F, G \in R[X_1, \cdots, X_{n+1}]$ en veeltermen $f, g \in R[X_1, \cdots, X_n]$ hebben we volgende eigenschappen.*

$$(FG)_* = F_* G_* \text{ en } (fg)^* = f^* g^* \tag{1.4}$$

$$(f^*)_* = f \tag{1.5}$$

Als $r \in \mathbb{N}$ maximaal is zodat $X_{n+1}^r \mid F$, dan is

$$X_{n+1}^r (F_*)^* = F \tag{1.6}$$

$$(F+G)_* = F_* + G_* \tag{1.7}$$

Als $\deg(f) = r,\ \deg(g) = s$ en $\deg(f+g) = t$, dan is

$$X_{n+1}^{r+s-t}(f+g)^* = X_{n+1}^s f^* + X_{n+1}^r g^* \tag{1.8}$$

Bewijs. (1.4), (1.5) en (1.7) zijn triviaal.
Onderstel dat r is als in (1.6), en schrijf

$$F(X_1, \cdots, X_{n+1}) = \sum_i a_i X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} X_{n+1}^{i_{n+1}} X_{n+1}^r$$

waarbij $i = (i_1, \cdots, i_{n+1})$ loopt over alle $n+1$-tallen natuurlijke getallen met $i_1 + i_2 + \cdots + i_{n+1} = d - r$. We vinden dan

$$F_*(X_1, \cdots, X_n) = \sum_i a_i X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

en F_* is een veelterm in n veranderlijken, van graad $d - r$. Dus

$$\begin{aligned} X_{n+1}^r (F_*)^*(X_1, \cdots, X_{n+1}) &= X_{n+1}^r X_{n+1}^{d-r} F_*\Big(\frac{X_1}{X_{n+1}}, \cdots, \frac{X_n}{X_{n+1}}\Big) \\ &= X_{n+1}^d \sum_i a_i \left(\frac{X_1}{X_{n+1}}\right)^{i_1} \left(\frac{X_2}{X_{n+1}}\right)^{i_2} \cdots \left(\frac{X_n}{X_{n+1}}\right)^{i_n} \\ &= F(X_1, \cdots, X_{n+1}) \end{aligned}$$

Schrijf

$$f = f_0 + f_1 + \cdots + f_r \text{ en } g = g_0 + g_1 + \cdots + g_s$$

Dan is

$$\begin{aligned} f^* &= X_{n+1}^r f_0 + X_{n+1}^{r-1} f_1 + \cdots + f_r \\ g^* &= X_{n+1}^s g_0 + X_{n+1}^{s-1} g_1 + \cdots + g_s \\ (f+g)^* &= X_{n+1}^t (f_0 + g_0) + X_{n+1}^{t-1}(f_1 + g_1) + \cdots + (f_t + g_t) \end{aligned}$$

en (1.8) volgt nadat we de eerste formule vermenigvuldigen met X_{n+1}^s, de tweede met X_{n+1}^r, en de derde met X_{n+1}^{r+s-t}. □

Gevolg 1.1.6 *1) Om een vorm $F \in R[X_1, \cdots, X_{n+1}]$ te ontbinden in factoren, volstaat het om de veelterm $F_* \in R[X_1, \cdots, X_n]$ te ontbinden;*
2) Als k algebraisch gesloten is, dan kan elke vorm $F \in k[X, Y]$ ontbonden worden tot een product van lineaire factoren.

1.2 Eigenschappen van commutatieve ringen

Unieke factorizatie domeinen

Uit de cursus "Algebra II" herhalen we volgende definities en eigenschappen, voor een commutatieve ring R.
Een niet-inverteerbaar element $a \in R$ wordt irreducibel genoemd als en slechts als

$$a = bc \implies b \text{ of } c \text{ is inverteerbaar } in\ R$$

Voor een domein R geldt:

$$(a) \text{ priemideaal} \implies a \text{ irreducibel}$$

De omgekeerde implicatie geldt indien R een UFD is.
Een *hoofdideaaldomein* of *PID* is een domein waarin elk ideaal een hoofdideaal is, dit wil zeggen dat het wordt voortgebracht door één element.
Een domein R noemen we een *uniek factorizatie domein* of *UFD* als elke $x \in R \setminus \{0\}$ onder de volgende vorm kan geschreven worden:

$$x = up_1p_2 \cdots p_n$$

waarbij $u \in R$ inverteerbaar, en $p_1, p_2, \cdots, p_n$ irreducibel. Deze ontbinding moet uniek zijn: als we voor x een andere ontbinding

$$x = vq_1q_2 \cdots q_m$$

kunnen opschrijven, dan is $n = m$, en zijn de p_i gelijk aan de q_i op de volgorde na, en op omkeerbare elementen na:

$$q_i = u_i p_{\sigma(i)}$$

waarbij u_i inverteerbaar, en $\sigma \in S_n$ een permutatie van $\{1, 2, \ldots, n\}$.
Elk Euclidisch domein is een PID, en elke PID is een UFD (zie stellingen 2.11.6 en 2.12.2 in "Algebra II"). Deze twee implicaties zijn geen equivalenties.
Als R een UFD is, dan is ook de veeltermring $R[X]$ een UFD. In het bijzonder is $k[X_1, X_2, \ldots, X_n]$ een UFD, voor elk lichaam k (stelling 2.12.3 in "Algebra II").
Als R een UFD is met breukenlichaam K, en $F \in R[X] \setminus R$ is irreducibel in $R[X]$, dan is F ook irreducibel in $K[X]$ (zie stelling 2.12.9 in "Algebra II"). Als twee veeltermen $F, G \in R[X]$ geen gemene niet-constante deler hebben in $R[X]$, dan ook niet in $K[X]$.

Noetherse ringen en de Hilbert basis stelling

Herhaal dat een commutatieve ring *Noethers* genoemd wordt, als elke stijgende keten idealen in R stationnair is, of, equivalent, als elk ideaal van R eindig voortgebracht is. De *Hilbert basis stelling* vertelt ons dat $R[X]$ Noethers is, als R Noethers is. In het bijzonder is $k[X_1, \cdots, X_n]$ Noethers, voor elk lichaam k (zie stelling 2.8.6 in "Algebra II"). Elk quotiënt van een Noetherse ring is opnieuw Noethers (stelling 2.8.5 in "Algebra II").

Discrete valuatieringen

Een locale, Noetherse ring R, die geen lichaam is, en waarvan het maximale ideaal M een hoofdideaal is, noemen we een *discrete valuatiering* of *DVR* . In stelling 1.2.1 geven we een alternatieve karakterisatie van discrete valuatieringen.

Stelling 1.2.1 *Zij R een domein, maar geen lichaam. Dan zijn volgende eigenschappen equivalent:*
1) R is een DVR;
2) Er bestaat een irreducibel element $t \in R$, zodat elke $z \in R \setminus 0$ op unieke manier geschreven kan worden onder de vorm

$$z = ut^n \tag{1.9}$$

waarbij u inverteerbaar in R, en $n \in \mathbb{N}$.

Bewijs. $1) \Longrightarrow 2)$ Onderstel dat het maximaal ideaal M voortgebracht wordt door $t \in R$.
Neem $z \neq 0 \in R$. Er zijn twee mogelijkheden:
a) z is inverteerbaar. Dan is $z = zt^0$ van de gewenste vorm;
b) z niet inverteerbaar. Dan is $z \in M$, omdat R een locale ring, en dus is $z = z_1 t$. Er zijn weer twee mogelijkheden:
b1) z_1 inverteerbaar. Stel $z_1 = u$, en $z = ut^1$ is van de gewenste vorm;
b2) $z_1 \in M$. Dan is $z_1 = z_2 t$. We herhalen weer onze redenering. We vinden zo een rij $z_1, z_2, \cdots$ in R, met $z_i = z_{i+1} t$. Als z_k inverteerbaar voor een bepaalde index k, dan is $z = z_k t^k$ van de gewenste vorm. Anders vinden we een stijgende keten idealen

$$(z) \subset (z_1) \subset (z_2) \subset \cdots$$

die stationnair is, omdat R noethers. Dus is er een $n \in \mathbb{N}$ zodat

$$z_{n+1} = vz_n$$

Omdat ook $z_n = tz_{n+1}$ vinden we $z_{n+1} = tvz_{n+1}$, en dus $tv = 1$, omdat R een domein. Maar dit vertelt ons dat t inverteerbaar is, en dat is strijdig met onze onderstelling dat t een (echt) ideaal voortbrengt.
De uniciteit tonen we aan als volgt: onderstel

$$ut^n = vt^m$$

met u, v inverteerbaar en $n, m \in \mathbb{N}$. Onderstel bijvoorbeeld dat $n \geq m$. Dan is $ut^{n-m} = v$ inverteerbaar. Dit kan niet als $n > m$ (want dan is $ut^{n-m} \in M$), en dus is $n = m$ en $u = v$.
We tonen tenslotte aan dat t irreducibel is. Schrijf $t = xy$. Omdat $t \neq 0$ zijn ook $x, y \neq 0$, en dus $x = ut^n$, $y = vt^m$, en

$$t = 1t^1 = uvt^{n+m}$$

Uit de uniciteit volgt $n + m = 1$, en er zijn dus twee mogelijkheden.
1) $n = 0,\ m = 1$: dan is $x = u$ inverteerbaar;
2) $n = 1,\ m = 0$: dan is $y = v$ inverteerbaar.
$2) \Longrightarrow 1)$ Stel $M = (t)$. Dan is M een ideaal. Als $z \notin M$, dan is $z = ut^0 = u$ inverteerbaar. Dus alle elementen buiten M zijn inverteerbaar, en dit betekent dat M het maximale ideaal is van een locale ring (zie "Algebra II", stelling 2.10.5).
We moeten nog aantonen dat R Noethers is. Neem een willekeurig ideaal I van R, en stel

$$n = \min\{n \mid ut^n \in I,\ u \text{ inverteerbaar}\}$$

Dan is $t^n \in I$, en $I = (t^n)$ is een hoofdideaal en dus eindig voortgebracht. □

Uit het bewijs van stelling 1.2.1 volgt dat elke DVR een PID is. We hebben zelfs

Stelling 1.2.2 *Elke DVR is een Euclidische ring.*

Bewijs. We verifiëren de voorwaarden uit definitie 2.11.14 uit "Algebra II". We definiëren een afbeelding

$$\text{ord} :\ R \setminus \{0\} \to \mathbb{N}$$

door $\text{ord}(ut^n) = n$, als u inverteerbaar. Het is duidelijk dat

$$\text{ord}(ut^n vt^m) = n + m = \text{ord}(ut^n) + \text{ord}(vt^m) \geq \text{ord}(ut^n) = n$$

Ook het delingsalgoritme is evident: neem $a = ut^n \neq 0 \in R$, en $b = vt^m \in R$. Onderstel eerst $b \neq 0$. Er zijn twee mogelijkheden.
1) $m \geq n$. Dan is

$$b = (vt^{m-n}u^{-1})a + 0 = qa + r$$

en we hebben $r = 0$.
2) $m < n$. Nu is

$$b = 0a + b = qa + r$$

en we hebben $\mathrm{ord}(r) = m < n = \mathrm{ord}(a)$. In beide gevallen is aan de voorwaarden van definitie 1.7.6 voldaan. Als $b = 0$ valt er helemaal niets te bewijzen. □

We noemen t een *uniformiserende parameter* van de DVR R. Andere uniformiserende parameters zijn dan van de vorm ut, waarbij $u \in R$ inverteerbaar. Zij nu K het breukenlichaam van R. Dan is

$$K = \{z = ut^n \mid u \text{ inverteerbaar en } n \in \mathbb{Z}\}$$

We definiëren $\mathrm{ord} : \ K \setminus \{0\} \to \mathbb{Z}$ door

$$\mathrm{ord}(ut^n) = n$$

en per definitie stellen we $\mathrm{ord}(0) = \infty$. Dan hebben we

$$\begin{aligned} R &= \{z \in K \mid \mathrm{ord}(z) \geq 0\} \\ M &= \{z \in K \mid \mathrm{ord}(z) > 0\} \end{aligned}$$

Voorbeeld 1.2.3 Zij p een priemgetal. Omdat (p) een priemideaal is, is de gelocaliseerde ring $R = \mathbb{Z}_{(p)}$ een locale ring (zie "Algebra I", stelling 1.6.6). R is de deelring van $\mathbb{Q}$ die bestaat uit breuken n/m waarbij m geen veelvoud van p is. R is Noethers, en het maximale ideaal $p\mathbb{Z}_{(p)}$ wordt voortgebracht door p. p is dus een uniformiserend element, en $R = \mathbb{Z}_{(p)}$ is een DVR.

1.3 Lichaamsuitbreidingen

Eindige lichaamsuitbreidingen

Beschouw commutatieve ringen R en S, en onderstel dat $R \subset S$. Dan is S een R-moduul, en zelfs een R-algebra: scalaire vermenigvuldiging met $r \in R$ wordt gegeven door de gewone vermenigvuldiging met $r \in R \subset S$.
S is eindig voortgebracht als een R-moduul als er $s_1, \cdots, s_k \in S$ bestaan zodat

$$S = Rs_1 + Rs_2 + \cdots + Rs_k$$

Neem nu $v_1, \cdots, v_n \in S$. Door de universele eigenschap van veeltermringen (zie § 1.1) bestaat er een uniek ringhomomorfisme

$$\tilde{v} : \ R[X_1, \cdots, X_n] \to S$$

waarvoor $\tilde{v}(X_i) = v_i$, en we schrijven

$$\mathrm{Im}\,(\tilde{v}) = R[v_1, v_2, \cdots, v_n]$$

We noemen $R[v_1, v_2, \cdots, v_n]$ de ring voortgebracht door R en $v_1, v_2, \cdots, v_n$. Het is de kleinste R-deelalgebra van S die $v_1, v_2, \cdots, v_n$ bevat. Als R-moduul wordt $R[v_1, v_2, \cdots, v_n]$ voortgebracht door

$$\{v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n} \mid i_1, i_2, \cdots, i_n \in \mathbb{N}\}$$

Als $S = R[v_1, v_2, \cdots, v_n]$, dan zeggen we dat S eindig voortgebracht is als een R-algebra.
We beschouwen nu de speciale situatie waarin $K \subset L$ lichamen zijn. Neem $v_1, \cdots, v_n \in L$. Het breukenlichaam van $K[v_1, \cdots, v_n]$ noteren we door $K(v_1, \cdots, v_n)$. $K(v_1, \cdots, v_n)$ is het kleinste deellichaam van L dat $v_1, \cdots, v_n$ bevat, en we noemen $K(v_1, \cdots, v_n)$ een *eindige lichaamsuitbreiding* van K.

Voorbeeld 1.3.1 Zij R een commutatieve ring. $R[X]$ is eindig voortgebracht als R-algebra, maar niet als R-moduul.

Integrale elementen

Onderstel weer dat $R \subset S$ commutatieve ringen, en neem $v \in S$. We noemen v *integraal* over R als v nulpunt is van een monische veeltermvergelijking met coëffiënten in R:

$$F(v) = v^n + a_1 v^{n-1} + \cdots + a_n = 0$$

met $a_i \in R$.

Stelling 1.3.2 *Onderstel dat $R \subset S$ domeinen, en neem $v \in S$. De volgende uitspraken zijn equivalent.*
1) v is integraal over R;
2) $R[v]$ is eindig voortgebracht als R-moduul;
3) er bestaat een deelring R' van S zodat $R \subset R' \subset S$ met $v \in R'$ en R' eindig voortgebracht als R-moduul.

Bewijs. $1) \Longrightarrow 2)$. Als R-moduul wordt $R[v]$ voortgebracht door $\{1, v, v^2, \cdots, v^{n-1}\}$.
$2) \Longrightarrow 3)$. Stel $R' = R[v]$.
$3) \Longrightarrow 1)$. Onderstel dat R' wordt voortgebracht door $\{w_1, \cdots, w_n\}$, m.a.w.

$$R' = Rw_1 + Rw_2 + \cdots + Rw_n$$

Voor elke $i = 1, \cdots, n$ kunnen we dan schrijven:

$$vw_i = \sum_{j=1}^{n} a_{ji} w_j$$

waarbij $a_{ji} \in R$. Dus

$$\sum_{j=1}^{n} (a_{ji} - \delta_{ji} v) w_j = 0 \tag{1.10}$$

We bekijken (1.10) als een homogeen stelsel lineaire vergelijkingen, met coëfficiënten in (het breukenlichaam van) S. $(w_1, \cdots, w_n)$ is een niet-triviale oplossing van (1.10), en dus is de determinant van het stelsel nul:

$$\det(a_{ji} - \delta_{ji} v) = 0$$

Dit betekent dat v een nulpunt is van de karakteristieke veelterm van de matrix $A = (a_{ij})$. De karakteristieke veelterm is een monische veelterm (eventueel op een minteken na), en v is dus integraal over R. □

Gevolg 1.3.3 *Onderstel dat $R \subset S$ domeinen.*

$$\{v \in S \mid v \text{ integraal over } R\}$$

is een deelring van S. We noemen deze de integrale sluiting van R in S.

Bewijs. Onderstel a en b integraal over R. Dan is b ook integraal over $R[a]$ (want nulpunt van een monische veeltermen met coëfficiënten in R die automatisch ook in $R[a]$ liggen). Omdat $R[a]$ eindig voortgebracht als R-moduul, en $R[a,b] = R[a][b]$ eindig voortgebracht als $R[a]$-moduul, is $R[a,b]$ eindig voortgebracht als R-moduul (zie lemma 1.3.4).
Omdat $a+b, a-b, ab \in R[a,b]$ volgt nu uit deel 3) van stelling 1.3.2 dat $a+b, a-b$ en ab integraal zijn over R, en dit bewijst dat de integrale elementen een deelring vormen. □

We maakten gebruik van volgend Lemma:

Lemma 1.3.4 *Zij $R \subset S$ commutatieve ringen, en M een eindig voortgebracht S-moduul. Als S eindig voortgebracht is als R-moduul, dan is ook M eindig voortgebracht als R-moduul.*

Bewijs. Zij $S = Rs_1 + \cdots + Rs_k$, en $M = Sm_1 + \cdots + Sm_l$, waarbij $s_i \in S$, en $m_j \in M$. Dan is duidelijk

$$M = \sum_{i=1}^{k} \sum_{j=1}^{l} Rs_i m_j$$

waaruit het gestelde volgt. □

Stelling 1.3.5 *Zij k een lichaam. Als een rationale vorm $f \in k(X)$ integraal is over $k[X]$, dan is $f \in k[X]$ een veelterm.*

Bewijs. Schrijf $f = F/G$, waarbij F en G veeltermen zijn zonder gemeenschappelijke factoren. Onderstel f integraal over $k[X]$. Dan bestaan er veeltermen $A_1, \cdots, A_n \in k[X]$ zodat

$$f^n + A_1 f^{n-1} + A_2 f^{n-2} + \cdots + A_n = 0$$

en hieruit volgt dat

$$F^n + A_1 F^{n-1} G + A_2 F^{n-2} G^2 + \cdots + A_n G^n = 0$$

en

$$F^n = -(A_1 F^{n-1} + A_2 F^{n-2} G + \cdots + A_n G^{n-1}) G$$

en dus is G een deler van F^n. Dit kan enkel als een van de irreducibele factoren van G een deler is van F, m.a.w. als F en G een gemene factor hebben, en dit is strijdig met onze onderstelling. □

Algebraische en transcendente elementen

Onderstel dat $k \subset l$ lichamen zijn, en neem $v \in l$. We zeggen dat v *algebraisch* is over k als er een $F \neq 0 \in k[X]$ bestaat zodat $F(v) = 0$. Als F delen door de coëfficiënt van de term van de hoogste graad, dan krijgen we een monische veelterm, en dan volgt dat v integraal is over k. Als v niet algebraisch is over k, dan noemen we v *transcendent* over k. We geven nu karakterisaties van algebraische en transcendente elementen.

Stelling 1.3.6 *Onderstel dat $k \subset l$ lichamen zijn, en neem $v \in l$. Beschouw het unieke ringmorfisme $\tilde{v} : k[X] \to l$ waarvoor $\tilde{v}(X) = v$. Dan zijn de volgende uitspraken equivalent.*

1. $\mathrm{Ker}\,(\tilde{v}) = (0)$*;*
2. $\tilde{v} : k[X] \to \mathrm{Im}\,(\tilde{v}) = k[v]$ *is een isomorfisme;*
3. $k[v] \subsetneq k(v)$*;*
4. v *is transcendent over* k*.*

Bewijs. 1. $\Leftrightarrow$ 2. is evident.
2. $\Rightarrow$ 4. $k[v] \cong k[X]$ is niet eindig voortgebracht als een k-moduul, en dus is v niet algebraisch over k, door stelling 1.3.2.
4. $\Rightarrow$ 1. (uit het ongerijmde). Onderstel dat $\mathrm{Ker}\,(\tilde{v}) \neq (0)$. Neem $F \neq 0 \in \mathrm{Ker}\,(\tilde{v})$. Dan is $F(v) = \tilde{v}(F) = 0$, zodat v algebraisch is over k.
2. $\Rightarrow$ 3. $\tilde{v} : k[X] \to k[v]$ is een isomorfisme. Dan is $\tilde{v} : k(X) \to k(v)$, $\tilde{v}(F/G) = \tilde{v}(F)/\tilde{v}(G)$ ook een isomorfisme, en we hebben een commutatief diagram

$$\begin{array}{ccc} k[X] & \xrightarrow{\tilde{v}} & k[v] \\ \subsetneq\downarrow & & \downarrow\subset \\ k(X) & \xrightarrow{\tilde{v}} & k(v) \end{array}$$

Aangezien het linkse verticale morfisme een echte inclusie is, is het rechtse dat ook.
3. $\Rightarrow$ 1. (uit het ongerijmde). Onderstel dat $\mathrm{Ker}\,(\tilde{v}) \neq (0)$. Omdat $k[X]$ een hoofdideaalring is, is $\mathrm{Ker}\,(\tilde{v}) = (F)$, met $F \neq 0$. (F) is een priemideaal, en dus een maximaal ideaal (zie "Algebra I", stelling 1.7.5). Dit betekent dat $k[v] \cong k[X]/(F)$ een lichaam is, en dus is $k(v) = k[v]$. □

Gevolg 1.3.7 *Onderstel dat $k \subset l$ lichamen zijn, en neem $v \in l$. Beschouw het unieke ringmorfisme $\tilde{v} : k[X] \to l$ waarvoor $\tilde{v}(X) = v$. Dan zijn de volgende uitspraken equivalent.*

1. $\mathrm{Ker}\,(\tilde{v}) \neq (0)$*;*
2. $\tilde{v} : k[X] \to \mathrm{Im}\,(\tilde{v}) = k[v]$ *is geen isomorfisme;*
3. $k[v] = k(v)$*;*
4. v *is algebraisch over* k*.*

Stelling van Zariski

Stelling 1.3.8 *Onderstel dat $k \subset l$ lichamen. Als l eindig voortgebracht is als een k-algebra, dan ook als k-moduul. Met andere woorden, l is eindigdimensionaal als k-vectorruimte.*

Bewijs. Onderstel

$$l = k[v_1, \cdots, v_m]$$

We werken per inductie op m.
Onderstel eerst dat $m = 1$. $l = k[v_1]$ is een lichaam, zodat $k[v_1] = k(v_1)$. Uit gevolg 1.3.7 volgt dat v_1 algebraisch is over k, zodat $l = k[v_1]$ eindig voortgebracht is als een k-moduul.
Onderstel nu dat de eigenschap geldt voor $m = n - 1$. We zullen aantonen dat ze ook geldt voor $m = n$. Schrijf $k_1 = k(v_1)$. Dan is

$$l = k_1[v_2, \cdots, v_n]$$

eindig voortgebracht als k_1-moduul, door de inductiehypothese. Er zijn nu twee mogelijkheden:
1) v_1 is algebraisch over k, of $k_1 = k[v_1] = k(v_1)$. Dan is k_1 eindig voortgebracht als k-moduul, en dus is ook l voortgebracht als k-moduul.
2) v_1 is transcendent over k. $v_2, \cdots, v_n$ zijn algebraisch over k_1, en voldoen dus aan een vergelijking van de vorm

$$v_i^{n_i} + a_{1i}v_i^{n_i-1} + \cdots + a_{n_i i} = 0 \tag{1.11}$$

met $a_{ij} \in k_1$. Neem een gemeen veelvoud $a \in k[v_1]$ van alle noemers die voorkomen in de $a_{ij} \in k_1 = k(v_1)$, en vermenigvuldig (1.11) met a^{n_i}. We krijgen

$$(av_i)^{n_i} + aa_{1i}(av_i)^{n_i-1} + \cdots + a^{n_i}a_{n_i i} = 0$$

en dus is av_i integraal over $k[v_1]$. Een willekeurig element $z \in k[v_1, \cdots, v_n] = l$ is te schrijven als een eindige $k[v_1]$-lineaire combinatie van termen van de vorm

$$v_2^{j_2}v_3^{j_3} \cdots v_n^{j_n}$$

Na vermenigvuldiging met $a^{j_2+\cdots+j_n}$ is deze integraal over $k[v_1]$, en dus is er een $N \in \mathbb{N}$ zodat $a^N z$ integraal is over $k[v_1]$. In het bijzonder geldt:

$$\forall z \in k(v_1) : \ \exists N \in \mathbb{N} : \ a^N z \text{ integraal over } k[v_1] \tag{1.12}$$

waarbij $a \in k[v_1]$. $k[v_1] \cong k[X]$ is een UFD. Neem nu een irreducibel polynoom $b \in k[v_1]$ dat geen deler is van a. Uit (1.12) volgt dat er een $N \in \mathbb{N}$ bestaat zodat a^N/b integraal is over $k[v_1]$. Maar a^N/b is geen veelterm, en we hebben dus een contradictie met stelling 1.3.5. Het is dus onmogelijk dat v_1 transcendent is over k. □

Gevolg 1.3.9 *Zij $k \subset l$ lichamen, en onderstel dat k algebraisch gesloten is. Als l eindig voortgebracht is als k-algebra, dan is $k = l$.*

Bewijs. l is eindig voortgebracht als k-moduul (stelling 1.3.8), en dus is elke $a \in l$ algebraisch over k, en dus een wortel van een monische veelterm $F \in k[X]$. Omdat k algebraisch gesloten is,

is F te schrijven als een product van lineaire factoren in $k[X]$:

$$F(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$$

met $a_i \in k$. Dus is

$$F(a) = (a - a_1)(a - a_2) \cdots (a - a_n) = 0$$

en dus is $a = a_i$ voor een zekere i, en $a \in k$. □

1.4 Comaximale idealen

Zij R een commutatieve ring, en I en J idealen. Het is gemakkelijk om aan te tonen dat $IJ \subset I \cap J$. Het is mogelijk dat deze inclusie strikt is. Echter, als I en J *comaximaal* zijn, wat wil zeggen dat $I + J = R$, dan hebben we dat $IJ = I \cap J$ (zie "Algebra II", stelling 2.9.1). We formuleren nu enkele nieuwe eigenschappen van comaximale idealen.

Stelling 1.4.1 *Als I en J comaximaal zijn, dan zijn I^n en J^m het ook, voor alle $n, m \geq 1$.*

Bewijs. Neem $a \in I,\ b \in J$ zodat $a + b = 1$. Dan is

$$1 = (a + b)^{n+m} = \sum_{i=0}^{n+m} \binom{m+n}{i} a^i b^{n+m-i} \in I^n + J^m$$

Immers, voor elke $i \in \{0, 1, \cdots, n + m\}$ geldt $i \geq n$ (en dan is $a^i b^{n+m-i} \in I^n$) of $n + m - i \geq m$ (en dan is $a^i b^{n+m-i} \in J^m$). □

Lemma 1.4.2 *Neem idealen $I_1, I_2, \cdots, I_r$ en een priemideaal P.*

$$I_1 \cap I_2 \cap \cdots \cap I_r \subset P \implies \exists i :\ I_i \subset P$$

Bewijs. We bewijzen de eigenschap eerst voor $n = 2$. We onderstellen dus dat $I \cap J \subset P$.
Als $I \not\subset P$ en $J \not\subset P$, dan bestaan er $x \in I \setminus P$ en $y \in J \setminus P$. We hebben enerzijds

$$x, y \notin P \ \Rightarrow\ xy \notin P \ \Rightarrow\ xy \notin I \cap J,$$

en anderzijds

$$x \in I,\ y \in J \ \Rightarrow\ xy \in I \cap J,$$

en we hebben dus een contradictie. We kunnen besluiten dat $I \subset P$ of $J \subset P$.
Het algemene geval gaat via een eenvoudige inductie op n. □

Stelling 1.4.3 *Voor een stel idealen $I_1, \cdots, I_n$ zijn de volgende uitspraken equivalent:*
1) $I_1, \cdots, I_n$ zijn twee aan twee comaximaal;
2) voor elke i zijn de idealen I_i en $\cap_{j \neq i} I_j$ comaximaal.

Bewijs. $2) \Rightarrow 1)$ is duidelijk. Immers, voor $i \neq k$ hebben we

$$I_i + I_k \supset I_i + \cap_{j \neq i} I_j = R$$

$1) \Rightarrow 2)$. Onderstel dat I_i en $\cap_{j \neq i} I_j$ NIET comaximaal zijn. Dan is $I_i + \cap_{j \neq i} I_j$ een echt ideaal van R, en dus bevat in een maximaal ideaal M:

$$I_i + \cap_{j \neq i} I_j \subset M$$

en dus

$$I_i \subset M \text{ en } \cap_{j \neq i} I_j \subset M$$

Uit lemma 1.4.2 volgt dat $I_k \subset M$, voor een zekere $k \neq i$. Maar dan is $I_i + I_k \subset M$, en dit is een contradictie. □

Stelling 1.4.4 *Als $I_1, \cdots, I_n$ twee aan twee comaximaal, dan is*

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$$

Bewijs. We weten reeds dat de eigenschap geldt voor $n = 2$. Onderstel dat ze geldt voor $n - 1$. Voor elk stel twee aan twee comaximale idealen $I_1, I_2, \cdots, I_n$ hebben we dan

$$I_1 \cap \cdots \cap I_n = I_1 \cap (I_2 \cap \cdots \cap I_n) = I_1(I_2 \cap \cdots \cap I_n) = I_1(I_2 \cdots I_n) = I_1 I_2 \cdots I_n$$

en dit bewijst onze stelling. □

Tenslotte vermelden we de *Chinese reststelling*, die reeds bewezen werd in de cursus "Algebra II" (gevolg 2.9.3):

Stelling 1.4.5 (Chinese reststelling)
Als $I_1, \cdots, I_n$ twee aan twee comaximaal, dan is de afbeelding

$$R/\cap_{i=1}^n I_i \to \prod_{i=1}^n R/I_i : \ x \mapsto (x \mathrm{mod} I_1, \cdots, x \mathrm{mod} I_n)$$

een isomorfisme.

1.5 Exacte rijen

Neem een stel vectorruimten $V_1, V_2, \cdots, V_n$, en lineaire afbeeldingen $f_i : \ V_i \to V_{i+1}$, voor $i = 1, \cdots n-1$. We zeggen dat de rij

$$V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-2}} V_{n-1} \xrightarrow{f_{n-1}} V_n$$

een *complex* is als $f_i \circ f_{i-1} = 0$, voor elke $i = 1, \cdots n-2$, of equivalent, als $\mathrm{Im}\,(f_{i-1}) \subset \mathrm{Ker}\,(f_i)$. De rij is exact in V_i als $\mathrm{Im}\,(f_{i-1}) = \mathrm{Ker}\,(f_i)$. Als de rij exact is in $V_2, \cdots, V_{n-1}$, dan spreken we van een *exacte rij*.
0 stelt de nulruimte voor. Merk op dat er precies één lineaire afbeelding $0 \to V$ bestaat (degene die 0 afbeeldt op 0), en precies één lineaire afbeelding $V \to 0$ (degene die alle vectoren in V op 0 afbeeldt).

Stelling 1.5.1 *Neem twee vectorruimten V en W.*
De rij $0 \to V \xrightarrow{f} W$ is exact in V als en alleen als f injectief is.
De rij $V \xrightarrow{f} W \to 0$ is exact in W als en alleen als f surjectief is.

Bewijs. Het beeld van de afbeelding $0 \to V$ is 0. Dus $0 \to V \xrightarrow{f} W$ is exact in V als en alleen als $0 = \mathrm{Ker}\,(f)$, wat precies betekent dat f injectief is. De tweede formule wordt op analoge manier bewezen. □

Een exacte rij van het type

$$0 \to V \xrightarrow{f} W \xrightarrow{g} X \to 0$$

wordt een *korte exacte rij* genoemd. Voor elke lineaire afbeelding $f : V \to W$ hebben we een korte exacte rij

$$0 \to \mathrm{Ker}\,(f) \xrightarrow{i} V \xrightarrow{f} \mathrm{Im}\,(f) \to 0.$$

Als V eindigdimensionaal is, dan hebben we de tweede dimensieformule uit de lineaire algebra:

$$\mathrm{dim}V = \mathrm{dim}\mathrm{Ker}\,(f) + \mathrm{dim}\mathrm{Im}\,(f). \tag{1.13}$$

Stelling 1.5.2 *Onderstel dat*

$$0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-2}} V_{n-1} \xrightarrow{f_{n-1}} V_n \to 0$$

een exacte rij van eindigdimensionale vectorruimten is. Dan is

$$\sum_{i=1}^{n} (-1)^{i-1} \mathrm{dim}V_i = 0. \tag{1.14}$$

Bewijs. We schrijven (1.13) op voor $f_1, \cdots, f_{n-1}$:

$$\begin{aligned}
\mathrm{dim}V_1 &= \mathrm{dim}\mathrm{Im}\,(f_1) \\
-\mathrm{dim}V_2 &= -\mathrm{dim}\mathrm{Ker}\,(f_2) - \mathrm{dim}\mathrm{Im}\,(f_2) \\
\mathrm{dim}V_3 &= \mathrm{dim}\mathrm{Ker}\,(f_3) + \mathrm{dim}\mathrm{Im}\,(f_3) \\
&\cdots \\
(-1)^{n-1}\mathrm{dim}V_n &= (-1)^{n-1}\mathrm{dim}\mathrm{Ker}\,(f_n)
\end{aligned}$$

Omdat de rij exact is, hebben we dat $\mathrm{dim}\mathrm{Im}\,(f_{i-1}) = \mathrm{dim}\mathrm{Ker}\,(f_i)$. Als we dan de som nemen van de formules hierboven vinden we (1.14). □

1.6 Oefeningen

Tenzij anders vermeld gebruiken we in onderstaande oefeningen steeds volgende conventies :
R, R', S, T zijn domeinen, K, K', L lichamen, k, k', l algebraisch gesloten lichamen. I, J, M zijn idealen in R. F, G, H zijn veeltermen in $R[X], K[X], R[X_1, \cdots, X_n]$ of $K[X_1, \cdots, X_n]$, al naargelang de context.

Oefening 1.1

1. F en G vormen in $R[X_1, \cdots, X_n]$ van graad r en s respectievelijk, dan is FG een vorm van graad $r + s$.
2. elke factor van een vorm in $R[X_1, \cdots, X_n]$ is ook een vorm.

Oefening 1.2 Toon aan dat er in $K[X]$ een oneindig aantal irreducibele veeltermen zijn.
(HINT : Klassiek bewijs van Euclides)

Oefening 1.3 Toon aan dat een algebraisch gesloten lichaam k oneindig is.
(HINT : Wat zijn de irreducibelen van $k[X]$?)

Oefening 1.4 Toon aan

1. I priem $\Leftrightarrow$ R/I domein
2. I maximaal $\Leftrightarrow$ R/I lichaam

Oefening 1.5 Toon aan :
p is priem $\Leftrightarrow$ $(p) \subset R$ is priem $\Rightarrow$ p irreducibel.

Oefening 1.6 R UFD. Toon aan :
p irreducibel $\Leftrightarrow$ p priem.

Oefening 1.7 R PID en I eigenlijk priemideaal. Toon aan dat

1. I wordt voortgebracht door een irreducibel element.
2. I maximaal is.

Oefening 1.8 Toon aan dat $I = (X, Y) \subset k[X, Y]$ geen hoofdideaal is.

Oefening 1.9 $\phi : K \to R$ ringhomomorfisme dan $\phi = 0$ of ϕ injectief.

Oefening 1.10 Zij R DVR met breukenlichaam K. Toon aan voor $z, z' \in K$

1. **(a)** $\mathrm{Ord}(zz') = \mathrm{Ord}(z) + \mathrm{Ord}(z')$
   (b) $\mathrm{Ord}(z + z') \geq min(\mathrm{Ord}(z), \mathrm{Ord}(z'))$
2. $\|z\| := 2^{-\mathrm{Ord}(z)}$
   Toon aan
   (a) $d(z, z') = \|z - z'\|$ is een metriek.
   (b) $\|z\| \geq 0$
   (c) $\|z + z'\| \leq \|z\| + \|z'\|$
   (d) $\|z\|\|z'\| = \|zz'\|$
3. R is een topologische ring (optelling en vermenigvuldiging zijn continu). Toon aan dat $\|\cdot\|$ een niet-Archimedische metriek geeft.
4. Toon aan : $a \in K \Rightarrow a \in R$ of $a^{-1} \in R$

Oefening 1.11 I eigenlijk ideaal, dan bestaat er een $I \subseteq M$ maximaal ideaal.

Oefening 1.12 R Noetherse commutatieve ring.
Bewijs dat er een N bestaat zodat $\mathrm{rad}(I)^N \subseteq I$.

Oefening 1.13 K oneindig lichaam.
Veronderstel dat $F(a_1, \cdots, a_n) = 0$ voor alle $a_1, \cdots, a_n \in K$. Toon aan dat $F = 0$.

Oefening 1.14 R UFD.

1. Toon aan dat een monische veelterm van graad 2 of 3 in $R[X]$ irreducibel is als en slechts als hij geen wortel heeft in R.
2. Toon aan dat $X^2 - a$ irreducibel is als en slechts als a geen kwadraat is in R.

Oefening 1.15 $F \in K[X]$ van graad $n > 0$. Toon aan dat de residu-klassen $\overline{1}, \overline{X}, \overline{X^2}, \cdots, \overline{X^{n-1}}$ een basis vormen van $K[X]/(F)$.

Oefening 1.16 Bewijs de implicatie
S eindig voortgebracht over R als moduul $\Rightarrow$ S eindig voortgebracht over R als ring.
Toon ook aan dat $S = R[X]$ een tegenvoorbeeld is van de omgekeerde implicatie.

Oefening 1.17 Bewijs de implicatie
L eindig voortgebracht over K als ring $\Rightarrow$ L eindig voortgebracht over K als lichaam.
Toon ook aan dat $L = K(X)$ een tegenvoorbeeld is van de omgekeerde implicatie.

Oefening 1.18 1. Alle eindigheidscondities zijn transitief.

2. Integraliteit van ringen is transitief.

Oefening 1.19 Veronderstel S eindig voortgebracht over R als ring. Toon aan :
S eindig voortgebracht als moduul $\Leftrightarrow$ S integraal over R.

Oefening 1.20 Zij $k \subset L$.

1. elk element van L dat algebraisch is over k zit reeds in k.

2. Een algebraisch gesloten lichaam heeft, behalve zichzelf, geen lichaamsuitbreidingen die ook eindig voortgebracht zijn als moduul.

Hoofdstuk 2

Affiene algebraische verzamelingen

2.1 Algebraische verzamelingen

Beschouw een lichaam k. We noteren

$$\mathbb{A}^n = \mathbb{A}^n(k) = k^n = \{P = (a_1, \cdots, a_n) \mid a_i \in k\}$$

We noemen $\mathbb{A}^n(k)$ de *affiene n-dimensionale ruimte* . De elementen van $\mathbb{A}^n(k)$ noemen we punten. $\mathbb{A}^1(k)$ noemen we de affiene rechte, en $\mathbb{A}^2(k)$ het affiene vlak.
Neem $F \in k[X_1, \cdots, X_n]$. $P = (a_1, \cdots, a_n)$ wordt een nulpunt van F genoemd indien

$$F(a_1, \cdots, a_n) = 0$$

Als F een niet-constante veelterm is, dan noemen we

$$V(F) = \{P \in \mathbb{A}^n(k) \mid P \text{ een nulpunt van } F\}$$

het (affiene) *hyperoppervlak* gedefinieerd door F. Een hyperoppervlak in $\mathbb{A}^2(k)$ wordt *affiene vlakke kromme* genoemd. Als F van graad één is, dan noemen we $V(F)$ een *hypervlak*. Een *rechte* is een hypervlak in $\mathbb{A}^2(k)$.
Neem nu een willekeurige verzameling

$$S \subset k[X_1, \cdots, X_n]$$

van veeltermen in n veranderlijken. We schrijven nu

$$V(S) = \bigcap_{F \in S} V(F) = \{P \in \mathbb{A}^n(k) \mid P \text{ een nulpunt van } F, \text{ voor elke } F \in S\} \tag{2.1}$$

Als $\{F_1, \cdots, F_r\} \subset k[X_1, \cdots, X_n]$ eindig, dan schrijven we

$$V(F_1, \cdots, F_r) = V(\{F_1, \cdots, F_r\})$$

Definitie 2.1.1 *Een deelverzameling X van $\mathbb{A}^n(k)$ noemen we een algebraische verzameling als $X = V(S)$ voor een zekere $S \subset k[X_1, \cdots, X_n]$. Een algebraische verzameling is dus de oplossingsverzameling van een (mogelijk oneindig) stelsel veeltermvergelijkingen.*

Stelling 2.1.2 *Met dezelfde notaties als hierboven hebben we volgende eigenschappen:*
1) $S \subset S' \subset k[X_1, \cdots, X_n] \implies V(S') \subset V(S)$*;*
2) Als $I = (S)$ *het ideaal is voortgebracht door* $S \subset k[X_1, \cdots, X_n]$*, dan is*

$$V(I) = V(S) \tag{2.2}$$

Algebraische delen van $\mathbb{A}^n(k)$ kunnen dus ook gedefinieerd worden als deelverzamelingen van de vorm $V(I)$, waarbij I een ideaal van $k[X_1, \cdots, X_n]$ is.
3) Neem een verzameling idealen $\{I_\alpha \mid \alpha \in A\}$ van $k[X_1, \cdots, X_n]$. Dan is

$$V(\bigcup_{\alpha \in A} I_\alpha) = \bigcap_{\alpha \in A} V(I_\alpha) \tag{2.3}$$

Een willekeurige doorsnede van algebraische verzamelingen is dus opnieuw algebraisch.
4) Voor $F, G \in k[X_1, \cdots, X_n]$ geldt:

$$V(FG) = V(F) \cup V(G) \tag{2.4}$$

5) Voor twee idealen I, J in $k[X_1, \cdots, X_n]$ geldt:

$$V(I) \cup V(J) = V(\{FG \mid F \in I,\ G \in J\}) \tag{2.5}$$

Een eindige unie van algebraische verzamelingen is dus opnieuw algebraisch.
6) $V(0) = \mathbb{A}^n(k)$ *en* $V(1) = \emptyset$*.*
7) Neem $P = (a_1, \cdots, a_n) \in \mathbb{A}^n(k)$*. Dan is*

$$V(X_1 - a_1, \cdots, X_n - a_n) = \{P\}$$

Elke eindige deelverzameling van $\mathbb{A}^n(k)$ is dus algebraisch.

Bewijs. 1) is duidelijk.
2) Uit 1) volgt dat $V(I) \subset V(S)$. Neem $P \in V(S)$, en $G \in I$. Dan kan G geschreven worden onder de vorm

$$G = A_1F_1 + \cdots + A_kF_k$$

waarbij $F_i \in S$ en $A_i \in k[X_1, \cdots, X_n]$. Bijgevolg is

$$G(P) = A_1(P)F_1(P) + \cdots + A_k(P)F_k(P) = 0$$

en hieruit volgt dat $P \in V(G)$. Hiermee is bewezen dat $V(S) \subset V(I)$.
3) tonen we aan als volgt:

$$\begin{aligned} P \in V(\bigcup_{\alpha \in A} I_\alpha) &\iff \forall \alpha \in A,\ \forall F \in I_\alpha :\ F(P) = 0 \\ &\iff \forall \alpha \in A :\ P \in V(I_\alpha) \\ &\iff P \in \bigcap_{\alpha \in A} V(I_\alpha) \end{aligned}$$

4) op dezelfde manier:

$$\begin{aligned} P \in V(FG) &\iff F(P)G(P) = 0 \\ &\iff F(P) = 0 \text{ of } G(P) = 0 \\ &\iff P \in V(F) \text{ of } P \in V(G) \\ &\iff P \in V(F) \cup V(G) \end{aligned}$$

5) ditmaal redeneren we vanuit het ongerijmde:

$$\begin{aligned} P \notin V(I) \cup V(J) &\iff P \notin V(I) \text{ en } P \notin V(J) \\ &\iff \exists F \in I:\ F(P) \neq 0 \text{ en } \exists G \in J:\ G(P) \neq 0 \\ &\iff \exists F \in I,\ G \in J:\ F(P)G(P) \neq 0 \\ &\iff P \notin V(\{FG \mid F \in I,\ G \in J\}) \end{aligned}$$

6) en 7) zijn duidelijk. □

Een algebraische verzameling is de oplossingsverzameling van een - mogelijk oneindig - stelsel veeltermenvergelijkingen. Dank zij de Hilbert basis stelling (zie § 1.2) kunnen we het aantal vergelijkingen steeds beperken tot een eindig aantal:

Stelling 2.1.3 *Zij X een algebraische verzameling in $\mathbb{A}^n(k)$. Dan bestaan er veeltermen $F_1, F_2, \cdots, F_r \in k[X_1, \cdots, X_n]$ zodat*

$$X = V(F_1, \cdots, F_r)$$

Bewijs. Stel $X = X(I)$, waarbij I een ideaal in $k[X_1, \cdots, X_n]$. Uit de Hilbert basis stelling weten we dat I eindig voortgebracht is. Neem een eindig stel voortbrengers $F_1, F_2, \cdots, F_r$ voor I. Dan is $X = V(I) = V(F_1, \cdots, F_r)$. □

Als $F \in k[X_1, \cdots, X_n]$ niet constant is, dan noemen we $V(F)$ een *hyperoppervlak* $\mathbb{A}^n(k)$. Stelling 2.1.3 vertelt ons dat elke algebraische verzameling te schrijven is als een eindige doorsnede van hyperoppervlakken.

2.2 Het ideaal behorend bij een stel punten

Voor $X \subset \mathbb{A}^n(k)$ stellen we

$$I(X) = \{F \in k[X_1, \cdots, X_n] \mid F(P) = 0,\ \forall P \in X\}$$

Het is eenvoudig in te zien dat $I(X)$ een ideaal is, en we noemen dit het ideaal behorend bij X.

Stelling 2.2.1 *1) $X \subset Y \subset \mathbb{A}^n(k) \implies I(Y) \subset I(X)$;*
2) $I(\emptyset) = k[X_1, \cdots, X_n]$;
3) als k een oneindig lichaam is, dan is ook $I(\mathbb{A}^n(k)) = (0)$;
4) $I\{(a_1, \cdots, a_n)\} = (X_1 - a_1, X_2 - a_2, \cdots, X_n - a_n)$.

Bewijs. 1) en 2) zijn duidelijk;
3) te bewijzen is de volgende uitspraak:

$$F(P) = 0,\ \forall P \in \mathbb{A}^n(k) \implies F = 0 \tag{2.6}$$

Dit gaan we doen met behulp van volledige inductie op n, de dimensie van $\mathbb{A}^n(k)$.
a) $n = 1$. Als $0 \neq F \in k[X]$ van graad r, dan heeft F tenhoogste r nulpunten in k. Een veelterm die nul wordt in alle punten van k is dus noodzakelijk de nulveelterm, want k bevat een oneindig aantal elementen.
b) Onderstel dat (2.6) waar is voor $n-1$. We nemen $F \in k[X_1, \cdots, X_n]$, en onderstellen dat $F(P) = 0$, voor elke $P \in \mathbb{A}^n(k)$. We schrijven F onder de vorm

$$F = F_0 + F_1 X_n + F_2 X_n^2 + \cdots F_r X_n^r$$

waarbij $F_i \in k[X_1, \cdots, X_{n-1}]$. Neem $(a_1, \cdots, a_{n-1}) \in \mathbb{A}^{n-1}(k)$ willekeurig. Voor elke $a_n \in k$ geldt dan

$$\begin{aligned} 0 &= F(a_1, \cdots, a_n) \\ &= F_0(a_1, \cdots, a_{n-1}) + F_1(a_1, \cdots, a_{n-1})a_n + F_2(a_1, \cdots, a_{n-1})a_n^2 + \cdots F_r(a_1, \cdots, a_{n-1})a_n^r \end{aligned}$$

Dit betekent in feite dat de veelterm $F(a_1, \cdots, a_{n-1}, X) \in k[X_n]$ nul wordt in elke $a_n \in k$, en dus de nulveelterm is, vanwege het geval $n = 1$. Maar dan hebben we

$$F_i(a_1, \cdots, a_{n-1}) = 0$$

en dit voor elke $(a_1, \cdots, a_{n-1}) \in \mathbb{A}^{n-1}(k)$. Daarom is $F_i = 0$, vanwege de inductiehypothese, en dus is $F = 0$.
4) Het is duidelijk dat $(X_1 - a_1, X_2 - a_2, \cdots, X_n - a_n) \subset I\{(a_1, \cdots, a_n)\}$. Omgekeerd, onderstel dat $F \in I\{(a_1, \cdots, a_n)\}$, of $F(a_1, \cdots, a_n) = 0$. Schrijf

$$U_i = X_i - a_i \ \text{ en } \ X_i = U_i + a_i$$

en

$$G(U_1, \cdots, U_n) = F(a_1 + U_1, \cdots, a_n + U_n) = F(X_1, \cdots, X_n)$$

Dan is $G(0, 0, \cdots, 0) = 0$. Schrijf nu

$$G = G_0 + G_1 + \cdots + G_d$$

waarbij G_i een vorm is van graad i. Dan is $G_0 = 0$, en alle termen in $G_1, \cdots, G_d$ zijn deelbaar door tenminste een $U_i = X_i - a_i$. □

Stelling 2.2.2 *Zij $X \subset \mathbb{A}^n(k)$ en $S \subset k[X_1, \cdots, X_n]$. Dan*

$$S \subset I(V(S)) \quad \text{en} \quad V(S) = V(I(V(S))) \tag{2.7}$$
$$X \subset V(I(X)) \quad \text{en} \quad I(X) = I(V(I(X))) \tag{2.8}$$

Bewijs.

$$F \in S \implies F(P) = 0,\ \forall P \in V(S) \implies F \in I(V(S))$$

en dit bewijst de eerste helft van (2.7). De eerste helft van (2.8) gaat op analoge manier:

$$P \in X \implies F(P) = 0,\ \forall F \in I(X) \implies P \in V(I(X))$$

Als we V toepassen op beide leden van de eerste helft van (2.7), dan vinden we, rekening houdend met deel 1) van stelling 2.1.2

$$V(I(V(S))) \subset V(S)$$

Als we $X = V(S)$ nemen in de eerste helft van (2.8), dan vinden we

$$V(S) \subset V(I(V(S)))$$

en dit bewijst de tweede helft van (2.7). Op dezelfde manier bewijzen we de tweede helft van (2.8): I toepassen op de eerste helft geeft

$$I(V(I(X))) \subset I(X)$$

en de eerste helft van (2.7) geeft, voor $S = I(X)$:

$$I(X) \subset I(V(I(X)))$$

□

Zij X een algebraische verzameling, en $I = I(X)$. Dan hebben we volgende eigenschap:

$$F^r \in I,\ \text{met } r \in \mathbb{N} \implies F \in I$$

We zeggen dat I een *radicaal ideaal* is. De algemene definitie is de volgende:

Definitie 2.2.3 *Zij R een commutatieve ring, en I een ideaal. We noemen I een radicaal ideaal als*

$$a^n \in I,\ \text{met } n \in \mathbb{N}_0 \implies a \in I$$

Stelling 2.2.4 *Zij I een ideaal in een commutatieve ring R.*

$$\sqrt{I} = \text{rad}(I) = \{a \in R \mid \exists n \in \mathbb{N}_0 :\ a^n \in I\}$$

is een ideaal van R dat I bevat. We noemen dit nieuwe ideaal het radicaal van I.

Bewijs. Onderstel $a, b \in \sqrt{I}$. Dan bestaan er natuurlijke getallen n, m zodat $a^n \in I$, $b^m \in I$. Voor elke $x \in R$ geldt $(xa)^n \in I$, en $(a+b)^{n+m} \in I$, en dus $a + b, xa \in \sqrt{I}$, en $\sqrt{I}$ is een ideaal. □

Voorbeelden 2.2.5 1) $I = 64\mathbb{Z}$ is geen radicaal ideaal van $\mathbb{Z}$. Immers, $2^6 \in I$, terwijl $2 \notin I$. $\sqrt{64\mathbb{Z}} = 2\mathbb{Z}$.
2) Elk priemideaal is een radicaal ideaal.

Stelling 2.2.6 *Zij X een algebraische verzameling. Dan is $I(X)$ een radicaal ideaal.*

2.3 Irreducibele algebraische verzamelingen

We noemen een algebraische verzameling $V \subset \mathbb{A}^n(k)$ *reducibel* als V de unie is van twee andere algebraische verzamelingen V_1 en V_2 die echte delen zijn van V:

$$V = V_1 \cup V_2 \ ; \ V_1 \neq V \ ; \ V_2 \neq V$$

Anders noemen we V een *irreducibele algebraische verzameling* .

Voorbeeld 2.3.1 *Als de karakteristiek van k verschillend is van 2, dan is $V = V(X^2-1) \subset \mathbb{A}^2(k)$ reducibel. Immers,*

$$V = V(X+1) \cup V(X-1)$$

is de unie van twee evenwijdige rechten.

Stelling 2.3.2 *Voor een algebraische verzameling $V \subset \mathbb{A}^n(k)$ zijn volgende uitspraken equivalent:*
1) V is irreducibel;
2) $I(V)$ is een priemideaal.

Bewijs. We bewijzen beide implicaties uit het ongerijmde.
Onderstel eerst dat $I(V)$ geen priemideaal is. Dan bestaan er veeltermen F_1, F_2, zodat $F_1F_2 \in I(V)$ maar $F_1 \notin I(V)$, $F_2 \notin I(V)$.
Aangezien $F_1 \notin I(V)$ bestaat er een $P \in V$ zodat $F_1(P) \neq 0$. Dus is $P \in V \setminus V(F_1)$, en $V \cap V(F_1) \subsetneq V$. Op dezelfde manier is $V \cap V(F_2) \subsetneq V$. Bovendien is

$$V = \Big(V \cap V(F_1)\Big) \cup \Big(V \cap V(F_2)\Big)$$

Een inclusie is triviaal. De omgekeerde wordt bewezen alsvolgt: neem $P \in V$. Dan is $F_1(P)F_2(P) = 0$, want $F_1F_2 \in I(V)$. Als $F_1(P) = 0$, dan is

$$P \in V \cap V(F_1) \subset \Big(V \cap V(F_1)\Big) \cup \Big(V \cap V(F_2)\Big)$$

Analoog indien $F_2(P) = 0$. Hiermee hebben we aangetoond dat V de unie is van twee echte algebraische delen, en dus is V reducibel.
Omgekeerd, onderstel V reducibel:

$$V = V_1 \cup V_2 \ ; \ V_1 \subsetneq V \ ; \ V_2 \subsetneq V$$

Dan is

$$I(V_1) \supsetneq I(V) \ \text{ en } \ I(V_2) \supsetneq I(V)$$

Neem $F_1 \in I(V_1) \setminus I(V)$ en $F_2 \in I(V_1) \setminus I(V)$. Neem $P \in V$ willekeurig. Als $P \in V_1$, dan is $F_1(P) = 0$, en als $P \in V_2$, dan is $F_2(P) = 0$. In beide gevallen is $F_1F_2(P) = 0$, en dus is $F_1F_2 \in I(V)$. Dus is $I(V)$ geen priemideaal. □

Herinner dat elke ideaal I bevat is in een maximaal ideaal M. Voor een noetherse ring R hebben we een iets sterkere eigenschap.

Lemma 2.3.3 *Zij R een noetherse ring, en $\mathcal{A}$ een verzameling idealen van R. Dan bestaat er in $\mathcal{A}$ een maximaal element, dit is een ideaal van $\mathcal{A}$ dat van geen enkel ander ideaal van $\mathcal{A}$ een echt deel is.*

Bewijs. Voor elke niet-lege deelverzameling van $\mathcal{A}$ kiezen we een ideaal $I \in \mathcal{A}$ uit deze deelverzameling (met behulp van het keuzeaxioma). Stel $\mathcal{A}_0 = \mathcal{A}$, en I_0 het ideaal dat bij $\mathcal{A}_0 = \mathcal{A}$ hoort. Per inductie definiëren we

$$\mathcal{A}_n = \{I \in \mathcal{A} \mid I_{n-1} \subsetneq I\}$$

en I_n het ideaal dat hoort bij $\mathcal{A}_n$. Als $\mathcal{A}_n = \emptyset$ voor een index n, dan betekent dit dat I_{n-1} maximaal is in $\mathcal{A}$, en dan is het lemma bewezen. Anders hebben we een strikt stijgende keten idealen

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

en dit is onmogelijk in een noetherse ring. □

Gevolg 2.3.4 *Elke verzameling $\mathcal{V}$ bestaande uit algebraische delen van $\mathbb{A}^n(k)$ heeft een minimaal element.*

Bewijs. $\{I(V) \mid V \in \mathcal{V}\}$ is een verzameling idealen in de noetherse ring $k[X_1, \cdots, X_n]$, en heeft dus een maximaal element $I(W)$. Dit betekent:

$$\forall V \in \mathcal{V} : \ I(W) \subset I(V) \ \ \Rightarrow \ \ I(W) = I(V).$$

Als nu $V \subset W$ in $\mathcal{V}$, dan is $I(W) \subset I(V)$, en dus $I(W) = I(V)$, en, tenslotte, $V = V(I(V)) = V(I(W)) = W$, en dus is W een minimaal element van $\mathcal{V}$. □

Stelling 2.3.5 *Zij $V \subset \mathbb{A}^n(k)$ een algebraische verzameling. Er bestaat een uniek stel irreducibele algebraische verzamelingen $V_1, \cdots, V_m$ zodat*

$$V = V_1 \cup V_2 \cup \cdots \cup V_m \tag{2.9}$$

waarbij $V_i \not\subset V_j$ als $i \neq j$. We noemen (2.9) de ontbinding van V in irreducibele componenten. De V_i worden de irreducibele componenten van V genoemd.

Bewijs. We stellen $\mathcal{V}$ de verzameling van alle algebraische delen van $\mathbb{A}^n(k)$ die NIET te schrijven zijn als een eindige unie van irreducibele algebraische delen. Als $\mathcal{V} \neq \emptyset$, dan kunnen we een minimaal element V van $\mathcal{V}$ beschouwen, door gevolg 2.3.4. Bij onderstelling is V niet irreducibel (anders is het de unie van irreducibelen), en dus is

$$V = V_1 \cup V_2$$

met $V_1 \neq V$, $V_2 \neq V$. Omdat V minimaal is in $\mathcal{V}$, behoren V_1 en V_2 niet tot $\mathcal{V}$, en zijn dus te schrijven als de eindige unie van irreducibele algebraische delen. Maar dan is ook $V = V_1 \cup V_2$ de eindige unie van irreducibelen, wat een contradictie is.
We concluderen dat $\mathcal{V} = \emptyset$, en elk algebraisch deel V is de eindige unie van irreducibelen:

$$V = V_1 \cup V_2 \cup \cdots \cup V_m$$

Als $V_i \subset V_j$ voor $i \neq j$, dan schrappen we gewoon V_i; aldus verkrijgen we een ontbinding die aan de gewenste eigenschappen voldoet.
De uniciteit wordt bewezen alsvolgt. Onderstel dat

$$V = W_1 \cup W_2 \cup \cdots \cup W_r$$

een andere ontbinding van V is in irreducibele componenten. Dan is

$$V_i = V \cap V_i = (W_1 \cap V_i) \cup (W_2 \cap V_i) \cup \cdots \cup (W_r \cap V_i)$$

Omdat V_i irreducibel is bestaat er een index j zodat

$$V_i = W_j \cap V_i$$

en dus $W_j \supset V_i$. Op dezelfde manier bestaat er een index k zodat $V_k \supset W_j$. Maar dan is $V_i \subset W_j \subset V_k$, en dit kan alleen maar als $i = k$. We concluderen dat er voor elke i een index j bestaat zodat $V_i = W_j$. De V_i's en W_j's zijn dus aan mekaar gelijk, op de volgorde na. □

2.4 Algebraische delen van het vlak

Door stelling 2.3.5 kennen we alle algebraische delen van het vlak $\mathbb{A}^2(k)$ als we de irreducibele delen kennen.

Stelling 2.4.1 *Neem twee veeltermen $F, G \in k[X, Y]$ zonder gemene factoren. Dan is de doorsnede $V(F, G) = V(F) \cap V(G)$ van de krommen $V(F)$ en $V(G)$ een eindige verzameling.*

Bewijs. F en G hebben geen gemene factoren in $k[X, Y]$, en dus ook niet in $k(X)[Y]$ (zie § 1.2). Maar $k(X)[Y]$ is een PID, en dus hebben we

$$(F, G) = 1 \text{ in } k(X)[Y]$$

en er bestaan dus $R, S \in k(X)[Y]$ zodat $RF + SG = 1$. We schrijven

$$R = \frac{A}{D} \; ; \; S = \frac{B}{D}$$

waarbij $A, B \in k[X, Y]$, $D \in k[X]$. Dan is

$$AF + BG = D$$

in $k[X, Y]$. Als $(a, b) \in V(F, G)$, dan is $D(a) = 0$. Deze vergelijking heeft slechts een eindig aantal oplossingen, zodat er slechts een eindig aantal mogelijkheden voor a zijn. Op dezelfde manier zijn er slechts een eindig aantal mogelijkheden voor b, en is dus $V(F, G)$ eindig. □

Gevolg 2.4.2 *Als $F \in k[X, Y]$ irreducibel, en $V(F)$ een oneindige verzameling, dan is $V(F)$ irreducibel, $I(V(F)) = (F)$.*

Bewijs. We weten al dat $(F) \subset I(V(F))$. Omgekeerd,

$$\begin{aligned} G \in I(V(F)) &\implies V(G,F) = V(F) \text{ oneindig} \\ &\implies G \text{ en } F \text{ hebben gemene factoren} \\ &\implies G \in (F) \end{aligned}$$

want F is irreducibel. Omdat $I(V(F)) = (F)$ een priemideaal is, is $V(F)$ irreducibel. □

Gevolg 2.4.3 *Onderstel k algebraisch gesloten, en neem $F \in k[X,Y] \setminus k$ irreducibel. Dan is $V(F)$ een oneindige irreducibele verzameling en $I(V(F)) = F$.*

Bewijs. We bewijzen dat $V(F)$ oneindig is. Omdat F geen constante veelterm is, hebben we

$$\frac{\partial F}{\partial X} \neq 0 \text{ of } \frac{\partial F}{\partial Y} \neq 0$$

Laten we onderstellen dat de partiële afgeleide naar X niet nul is, met andere woorden dat F afhangt van X. Voor elke $b \neq 0 \in k$ is dan $F(X,b)$ een niet constante veelterm, en heeft de vergelijking $F(x,b) = 0$ tenminste 1 oplossing $a(b)$, omdat k algebraisch gesloten is. We vinden een oneindige familie oplossingen $\{(a(b),b) \mid b \neq 0 \in k\}$ van de vergelijking $F(x,y) = 0$. Uit gevolg 2.4.2 volgt nu dat $V(F)$ irreducibel is, en dat $I(V(F)) = F$. □

Gevolg 2.4.4 *Onderstel dat k een oneindig lichaam is. De enige irreducibele algebraische delen van het vlak $\mathbb{A}^2(k)$ zijn dan:*
1) het vlak $\mathbb{A}^2(k)$;
2) de lege verzameling $\emptyset$;
3) de singletons $\{(a,b)\}$, waarbij $a,b \in k$;
4) de irreducibele vlakke krommen $V(F)$, waarbij $F \in k[X,Y]$ irreducibel, en $V(F)$ een oneindige verzameling.

Bewijs. Neem een irreducibele algebraische verzameling $V \subset \mathbb{A}^2(k)$.
Als $V = \emptyset$, dan is $I(V) = k[X,Y]$.
Als $V \neq \emptyset$ eindig, dan is $V = \{(a,b)\}$ een singleton.
Als $V = \mathbb{A}^2(k)$, dan is $I(V) = (0)$.
In alle andere gevallen kunnen we dus onderstellen dat V oneindig is, en $I(V) \neq (0)$ een echt ideaal. Neem $F \neq 0 \in I(V)$. Dan is F niet constant, want $I(V)$ is een echt ideaal. Omdat $I(V)$ een priemideaal is (V is irreducibel) zit tenminste 1 irreducibele factor van F ook in $I(V)$, en dus kunnen we onderstellen dat F irreducibel is.
Neem nu $G \in I(V)$ willekeurig. Als $G \notin (F)$, dan bevatten F en G geen gemene factoren, en is $V \subset V(F,G)$ eindig. Dus moet $G \in (F)$, en $I(V) = (F)$. □

Gevolg 2.4.5 *Onderstel k algebraisch gesloten, en neem $F \in k[X,Y] \setminus k$, en de ontbinding*

$$F = F_1^{n_1} F_2^{n_2} \cdots F_r^{n_r}$$

in irreducibele factoren. Dan is de ontbinding van $V(F)$ in irreducibele componenten

$$V(F) = V(F_1) \cup V(F_2) \cup \cdots \cup V(F_r) \tag{2.10}$$

en $I(V(F))$ is het ideaal voortgebracht door $F_1 \cdots F_r$.

Bewijs. Uit gevolg 2.4.3 volgt dat $V(F_j)$ een oneindige irreducibele verzameling is, en dat $(F_j) = I(V(F_j))$. Als $i \neq j$, dan is F_i geen deler van F_j, en dus is $V(F_j) \not\subset V(F_i)$. We kunnen dus besluiten dat (2.10) de irreducibele ontbinding is van $V(F)$.
Nu is

$$\begin{aligned} I(V(F)) &= I(V(F_1) \cup \cdots \cup V(F_r)) \\ &= I(V(F_1)) \cap \cdots \cap I(V(F_r)) \\ &= (F_1) \cap \cdots \cap (F_r) \\ &\supset (F_1) \cdots (F_r) = (F_1 \cdots F_r) \end{aligned}$$

en onze eigenschap is bewezen als we deze laatste inclusie ook kunnen omkeren (herhaal dat, voor twee idealen I en J, we steeds hebben dat $IJ \subset I \cap J$, met mogelijk een strikte inclusie). Neem

$$G \in (F_1) \cap \cdots \cap (F_r)$$

Dan zijn $F_1, F_2, \cdots, F_r$ allen factoren van G, en, omdat de F_i allen irreducibel, is ook $F_1 \cdots F_r$ een factor van G, en dus $G \in (F_1 \cdots F_r)$, wat de omgekeerde inclusie bewijst. □

2.5 De Hilbert Nullstellensatz

Voor de resultaten uit deze paragraaf is de onderstelling dat k algebraisch gesloten is essentieel.

Stelling 2.5.1 (zwakke Nullstellensatz)
Zij k algebraisch gesloten. Voor elk echt ideaal I van $k[X_1, \cdots, X_n]$ geldt dat $V(I)$ niet leeg is.

Bewijs. Neem een maximaal ideaal M dat I bevat. Dan is $V(M) \subset V(I)$, en het volstaat dus om te bewijzen dat $V(M)$ niet leeg is.
Omdat M maximaal is, is $l = k[X_1, \cdots, X_n]/M$ een lichaam, en als k-algebra is l eindig voortgebracht. Uit gevolg 1.3.9 halen we dat $l = k$, of met andere woorden, de kanonieke afbeelding

$$k \to k[X_1, \cdots, X_n]/M$$

is een isomorfisme. Neem het invers beeld a_i van de klasse bepaald door X_i. Dan is $X_i - a_i \in M$, en dus

$$(X_1 - a_1, \cdots, X_n - a_n) \subset M$$

Maar $(X_1 - a_1, \cdots, X_n - a_n)$ is zelf een maximaal ideaal, en dus is $(X_1 - a_1, \cdots, X_n - a_n) = M$, en

$$V(M) = \{(a_1, \cdots, a_n)\} \neq \emptyset$$

□

Stelling 2.5.2 (sterke Nullstellensatz)
Zij k algebraisch gesloten. Voor elk ideaal I van $k[X_1, \cdots, X_n]$ hebben we

$$I(V(I)) = \mathrm{rad}(I)$$

Bewijs. We weten al dat $\mathrm{rad}(I) \subset I(V(I))$, want $I(V(I))$ is een radicaal ideaal dat I bevat. Onderstel $I = (F_1, F_2, \cdots, F_r)$. Om de omgekeerde inclusie te bewijzen moeten we aantonen dat

$$G \in I(V(I)) \implies G \in \mathrm{rad}(I)$$

$G \in I(V(I))$ betekent

$$F_1(P) = \cdots = F_r(P) = 0 \implies G(P) = 0$$

en $G \in \mathrm{rad}(I)$ betekent dat er een $N \in \mathbb{N}$ bestaat zodat $G^N \in I$ of

$$G^N = A_1F_1 + \cdots + A_rF_r$$

waarbij $A_i \in k[X_1, \cdots, X_n]$. Stel

$$J = (F_1, \cdots, F_r, X_{n+1}G - 1) \subset k[X_1, \cdots, X_n, X_{n+1}]$$

Dan is $V(J) \subset \mathbb{A}^{n+1}(k)$ leeg. Door de zwakke Nullstellensatz is

$$J = k[X_1, \cdots, X_n, X_{n+1}]$$

Dit betekent dat er $B, B_1, \cdots, B_r \in k[X_1, \cdots, X_n, X_{n+1}]$ bestaan zodat

$$\sum_{i=1}^{r} B_iF_i + (X_{n+1}G - 1)B = 1$$

Bekijk deze identiteit in $k(X_{n+1})[X_1, \cdots, X_n]$. Stel nu $Y = 1/X_{n+1}$, en vermenigvuldig beide leden met een hoge macht van Y, zodat alle noemers uit het linkerlid verdwijnen. We vinden dan

$$\sum_{i=1}^{r} C_i(X_1, \cdots, X_n, Y)F_i + (G - Y)D(X_1, \cdots, X_n, Y) = Y^N$$

Als we nu $Y = G(X_1, \cdots, X_n)$ stellen, vinden we

$$\sum_{i=1}^{r} C_i(X_1, \cdots, X_n, G(X_1, \cdots, X_n))F_i = G^N$$

en dit is net wat we nodig hebben. □

Opmerking 2.5.3 De zwakke Nullstellensatz geldt niet als k niet algebraisch gesloten is. Neem bijvoorbeeld $k = \mathbb{R}$. Dan is $(X^2 + Y^2 + 1)$ een echt ideaal in $\mathbb{R}[X, Y]$, maar $V(X^2 + Y^2 + 1) = \emptyset$. Merk ook op dat

$$\mathbb{R}[X, Y]/(X^2 + Y^2 + 1) \cong \mathbb{C}$$

een echte lichaamsuitbreiding van $\mathbb{R}$ is.

Gevolg 2.5.4 *Als I een radicaal ideaal is, dan is*

$$I(V(I)) = I$$

Als V een algebraische verzameling is, dan is $I(V)$ een radicaal ideaal (zie stelling 2.2.6). Bovendien geldt dan $V(I(V)) = V$ (zie stelling 2.2.6). Als we dit nog combineren met gevolg 2.5.4 vinden we

Gevolg 2.5.5 *I definieert een bijectie van de verzameling der algebraische deelverzamelingen van $\mathbb{A}^n(k)$ naar de verzameling van de radicaal idealen van $k[X_1, \cdots, X_n]$, en de inverse wordt gegeven door V.*

Als V een irreducibel algebraisch deel is, dan is $I(V)$ een priemideaal. Elk priemideaal I is automatisch een radicaal ideaal. $V(I)$ is dan weer een irreducibel algebraisch deel. We hebben dus ook

Gevolg 2.5.6 *I definieert ook een bijectie van de verzameling der irreducibele algebraische delen van $\mathbb{A}^n(k)$ naar de verzameling der priemidealen van $k[X_1, \cdots, X_n]$.*

Een singleton $\{P\}$ is een minimaal niet-leeg irreducibel algebraisch deel van $\mathbb{A}^n(k)$. Het hiermee corresponderend maximaal ideaal $I(P)$ is daarom een maximaal ideaal van $k[X_1, \cdots, X_n]$, en we hebben

Gevolg 2.5.7 *I definieert ook een bijectie van $\mathbb{A}^n(k)$ naar de verzameling der maximale idealen van $k[X_1, \cdots, X_n]$.*

Neem $F \in k[X_1, \cdots, X_n]$, en de ontbinding

$$F = F_1^{n_1} \cdots F_r^{n_r}$$

in irreducibele factoren. We hebben

$$V(F) = V(F_1^{n_1}) \cup \cdots \cup V(F_r^{n_r}) = V(F_1) \cup \cdots \cup V(F_r)$$

en

$$I(V(F)) = \mathrm{rad}(F) = (F_1 \cdots F_r)$$

Als $V(F)$ irreducibel is, dan is noodzakelijk $r = 1$, $F = F_1^{n_1}$, en dus

$$V(F) = V(F_1^{n_1}) = V(F_1),$$

en $I(V(F)) = (F_1)$, met F_1 irreducibel.
Als F irreducibel is, dan is (F) een priemideaal, en $V(F)$ een irreducibel hyperoppervlak.

Gevolg 2.5.8 *I definieert ook een bijectie van de irreducibele hyperoppervlakken van $\mathbb{A}^n(k)$ naar de verzameling der irreducibele veeltermen van $k[X_1, \cdots, X_n]$.*

Samengevat hebben we dus volgende 1-1 correspondenties (als k algebraisch gesloten is):

$$\begin{aligned} \text{Algebraische delen} &\longleftrightarrow \text{radicaal idealen} \\ \text{Irreducibele algebraische delen} &\longleftrightarrow \text{priemidealen} \\ \text{Punten} &\longleftrightarrow \text{maximale idealen} \\ \text{Irreducibele hyperoppervlakken} &\longleftrightarrow \text{Irreducibele veeltermen} \end{aligned}$$

Gevolg 2.5.9 *Als I een ideaal in $k[X_1, \cdots, X_n]$, en $V(I) = \emptyset$, dan is $I = k[X_1, \cdots, X_n]$.*

Bewijs. Uit de Nullstellensatz weten we dat

$$I(V(I)) = \mathrm{rad}(I) = k[X_1, \cdots, X_n]$$

Indien I een echt ideaal is, dan bestaat er een maximaal ideaal M dat I bevat, en dan is $\mathrm{rad}(I) \subset \mathrm{rad}(M) = M$ ook een echt ideaal, en dit is contradictie. □

2.6 Oefeningen

Oefening 2.1 De algebraische delen van $\mathbb{A}^1(K)$ zijn juist de eindige delen en $\mathbb{A}^1(K)$ zelf.

Oefening 2.2 K eindig, dan is elke deelverzameling van $\mathbb{A}^n(K)$ algebraisch.

Oefening 2.3 Geef een voorbeeld van een aftelbare verzameling algebraische delen waarvan de unie niet algebraisch is.

Oefening 2.4 C een affiene vlakke kromme en L een rechte in $\mathbb{A}^2(K), L \nsubseteq C$. Veronderstel $C = V(F)$ met F van graad n. Toon aan dat $L \cap C$ ten hoogste n punten bevat.

Oefening 2.5 Toon aan dat de volgende veramelingen niet algebraisch zijn :

1. $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | \quad y = \sin(x)\}$
2. $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) | \quad |z|^2 + |w|^2 = 1\}$

Oefening 2.6 $F \in k[X_1, \cdots, X_n] \setminus k$. Dan is $\mathbb{A}^n(k) - V(F)$ oneindig als $n \geq 1$, en $V(F)$ is oneindig als $n \geq 2$. Besluit hieruit dat het complement van elk algebraisch deel oneindig is.

Oefening 2.7 $V \subset \mathbb{A}^n(K), W \subset \mathbb{A}^m(K)$ algebraische verzamelingen. Toon aan dat $V \times W$ een algebraisch deel is van $\mathbb{A}^{n+m}(K)$.

Oefening 2.8 V, W algebraische verzamelingen in $\mathbb{A}^n(K)$. Toon aan

$$V = W \Leftrightarrow I(V) = I(W)$$

Oefening 2.9

1. V algebraische verzameling in $\mathbb{A}^n(K), P \notin V$. Toon aan dat er een veelterm $F \in I(V)$ bestaat waarvoor geldt dat $F(P) \neq 0$.
2. $\{P_1, \cdots, P_r\} \subset \mathbb{A}^n(K)$. Toon aan dat er veeltermen $F_1, \cdots, F_n$ bestaan waarvoor geldt dat $F_i(P_j) = 0$ als $i \neq j$ en $F_i(P_i) \neq 0$.
3. V algebraische verzameling in $\mathbb{A}^n(K), P_1, P_2 \notin V$. Toon aan dat er een veelterm F bestaat waarvoor geldt dat $F(P_i) \neq 0, i = 1, 2$ maar $F \in I(V)$.

Oefening 2.10 Toon aan dat $I = (X^2 + 1) \subset \mathbb{R}[X]$ een radicaal, zelfs een priem-, ideaal is, maar geen ideaal behorend bij een deelverzameling van $\mathbb{A}^1(\mathbb{R})$.

Oefening 2.11 $I \subset K[X_1, \cdots, X_n]$. Bewijs dat $V(I) = V(\mathrm{rad}(I))$ en $\mathrm{rad}(I) \subset I(V(I))$.

Oefening 2.12 Toon aan dat $I = (X_1 - a_1, \cdots, X_n - a_n) \subset k[X_1, \cdots, X_n]$ een maximaal ideaal is, en het natuurlijk homomorfisme van k naar $k[X_1, \cdots, X_n]/I$ een isomorfisme.

Oefening 2.13 V irreducibel

$$V = \bigcup_{i=1}^{n} V_i \qquad V_i \text{ algebraisch}$$

Toon aan dat een i bestaat zodat $V_i = V$.

Oefening 2.14

1. Toon aan dat $X^2 + Y^2 - 1 \in \mathbb{C}[X, Y]$ irreducibel is.
2. $I = (Y - Z, X^2 + Y^2 - 1)$. Toon aan dat
$$\mathbb{C}[X, Y, Z]/I \cong \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$$
3. Leid hieruit af dat I priem is.

Oefening 2.15

1. Ontbind $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ in irreducibele delen.
2. Ontbind $V(X^2 + Y^2 - 1, X^2 + Z^2 - 1) \subset \mathbb{A}^3(\mathbb{C})$ in irreducibele componenten.

Oefening 2.16 V, W algebraische delen van $\mathbb{A}^n(K), V \subset W$. Toon aan dat elke irreducibele component van V bevat is in een irreducibele component van W.

Oefening 2.17 Als $V = V_1 \cup V_2 \cup \cdots \cup V_r$ de decompositie is van een algebraische verzameling in irreducibele componenten, toon aan dat $V_i \nsubseteq \bigcup_{j \neq i} V_j$.

Oefening 2.18 Als K oneindig is, toon aan dat $\mathbb{A}^n(K)$ irreducibel is.

Oefening 2.19 Zij $I = (Y^2 - X^2, Y^2 + X^2) \subset \mathbb{C}[X, Y]$. Zoek $V(I)$ en $\dim_{\mathbb{C}}(\mathbb{C}[X, Y]/I)$.

Oefening 2.20

1. R UFD, en $P = (p)$ eigenlijk, priem hoofdideaal. Toon aan dat er geen priemideaal Q bestaat zodat $0 \subsetneq Q \subsetneq P$.
2. $V = V(F)$ irreducibel hyperoppervlak in $\mathbb{A}^n$. Toon aan dat er geen irreducibel deel W bestaat zodat $V \subsetneq W \subsetneq \mathbb{A}^n$.

Hoofdstuk 3

Affiene variëteiten

In dit hoofdstuk onderstellen we steeds dat het lichaam k algebraisch gesloten is.

3.1 Affiene variëteiten en veeltermafbeeldingen

Variëteiten en coördinatenringen

Een irreducibele algebraische verzameling $V \subset \mathbb{A}^n(k)$ noemen we een *affiene variëteit*. Als V een affiene variëteit is, dan is $I(V)$ een priemideaal, en dus is

$$\Gamma(V) = k[X_1, \cdots, X_n]/I(V)$$

een domein. We noemen $\Gamma(V)$ de *coördinatenring* van V. We schrijven

$$\pi_V : \ k[X_1, \cdots, X_n] \to \Gamma(V)$$

voor de kanonieke surjectie die elke veelterm F afbeeldt op zijn klasse

$$\pi_V(F) = [F]$$

Zij nu $\mathcal{F}(V, k)$ de verzameling van alle afbeeldingen van V naar k. Dan is $\mathcal{F}(V, k)$ een k-algebra. Een afbeelding $f : \ V \to k$ noemen we een *veeltermafbeelding* indien er een veelterm $F \in k[X_1, \cdots, X_n]$ bestaat zodanig dat

$$f(a_1, \cdots, a_n) = F(a_1, \cdots, a_n)$$

voor alle $(a_1, \cdots, a_n) \in V$. De verzameling van alle veeltermafbeeldingen $V \to k$ vormt een deelalgebra van $\mathcal{F}(V, k)$. Merk ook op dat twee veeltermen $F, G \in k[X_1, \cdots, X_n]$ dezelfde veeltermafbeelding $V \to k$ bepalen indien deze samenvallen op V, wat betekent

$$F(a_1, \cdots, a_n) = G(a_1, \cdots, a_n)$$

voor alle $(a_1, \cdots, a_n) \in V$, of met andere woorden

$$F - G \in I(V)$$

Dit betekent in feite dat de deelalgebra van $\mathcal{F}(V, k)$ die bestaat uit alle veeltermafbeeldingen gegeven wordt door de coördinatenring $\Gamma(V)$:

$$\Gamma(V) \cong \{f : V \to k \mid f \text{ is een veeltermafbeelding}\}$$

Merk ook op dat

$$\Gamma(\mathbb{A}^n(k)) = k[X_1, \cdots, X_n]$$

Immers, $I(\mathbb{A}^n(k)) = \{0\}$.

Zij $V \subset \mathbb{A}^n(k)$ een variëteit. Uit de Nullstellensatz volgt dat er een bijectie bestaat tussen de verzameling der algebraische verzamelingen $X \subset V$ en de verzameling der radicale idealen $J \subset k[X_1, \cdots, X_n]$ die $I = I(V)$ bevatten.
Er is ook een bijectie tussen de idealen J van $k[X_1, \cdots, X_n]$ die $I(V)$ bevatten, en de idealen van $\Gamma(V)$: het ideaal dat correspondeert met J is $\pi_V(J)$, en, voor een ideaal $J' \subset \Gamma(V)$ is het corresponderend ideaal $\pi_V^{-1}(J') \subset k[X_1, \cdots, X_n]$. Bewijs zelf als oefening dat deze bijectie en haar inverse radicale idealen stuurt naar radicale idealen, priemidealen naar priemidealen en maximale idealen naar maximale idealen. We krijgen daarom bijecties tussen de volgende verzamelingen:

$$\begin{aligned} \text{algebraische delen van } V &\longleftrightarrow \text{radicale idealen van } \Gamma(V) \\ \text{deelvariëteiten van } V &\longleftrightarrow \text{priemidealen van } \Gamma(V) \\ \text{punten van } V &\longleftrightarrow \text{maximale idealen van } \Gamma(V) \end{aligned}$$

Veeltermafbeeldingen en algebramorfismen

Beschouw veeltermen $T_1, \cdots, T_m \in k[X_1, \cdots, X_n]$. De afbeelding

$$T = (T_1, \cdots, T_m) : \mathbb{A}^n(k) \to \mathbb{A}^m(k) : (a_1, \cdots, a_n) \mapsto \Big(T_1(a_1, \cdots, a_n), \cdots, T_m(a_1, \cdots, a_n)\Big)$$

noemen we een *veeltermafbeelding*. De verzameling van de veeltermafbeeldingen $\mathbb{A}^n(k) \to \mathbb{A}^m(k)$ noteren we door $\mathrm{Pol}_k(\mathbb{A}^n(k), \mathbb{A}^m(k)) \cong k[X_1, \cdots, X_n]^m$. Uit stelling 1.1.2 weten we dat we een bijectie

$$\Gamma : \mathrm{Pol}_k(\mathbb{A}^n(k), \mathbb{A}^m(k)) \to \mathrm{Alg}_k(k[Y_1, \cdots, Y_m), k[X_1, \cdots, X_n]) \tag{3.1}$$

hebben. We noteren (zie § 1.1)

$$\Gamma(T) = \Gamma(T_1, \cdots, T_m) = \tilde{T}.$$

Beschouw veeltermafbeeldingen $T = (T_1, \cdots, T_m) : \mathbb{A}^n(k) \to \mathbb{A}^m(k)$ en $S = (S_1, \cdots, S_p) : \mathbb{A}^m(k) \to \mathbb{A}^p(k)$. Uit stelling 1.1.3 volgt, rekening houden met gevolg 1.1.4, dat

$$\widetilde{S \circ T} = \tilde{T} \circ \tilde{S}.$$

Neem nu variëteiten $V \subset \mathbb{A}^n(k)$ en $W \subset \mathbb{A}^m(k)$. We noemen $\varphi : V \to W$ een *veeltermafbeelding* als er een veeltermafbeelding $T : A^n(k) \to \mathbb{A}^m(k)$ bestaat zodat

$$\varphi = T_{|V}$$

Het is duidelijk dat de samenstelling van twee veeltermafbeeldingen opnieuw een veeltermafbeelding is. Voor twee variëteiten V en W noteren we

$$\mathrm{Pol}_k(V, W) = \{\varphi : V \to W \mid \varphi \text{ veeltermafbeelding}\}$$

Stel $\underline{\underline{\mathrm{Var}}}_k$ de categorie met de k-variëteiten als objecten en veeltermafbeeldingen als morfismen. Voor twee k-algebras A en B noteren we

$$\mathrm{Alg}_k(A, B) = \{f : A \to B \mid f \; k\text{-algebra homomorfisme}\}$$

Stel $\underline{\underline{\mathrm{Alg}}}_k$ de categorie met als objecten k-algebras en als morfismen k-algebra homomorfismen.
We hebben hierboven gezien dat we voor elke variëteit V een k-algebra $\Gamma(V)$ kunnen definiëren. We zullen nu aantonen dat Γ een functor is. Eerst bewijzen we een lemma.

Lemma 3.1.1 *Beschouw een veeltermafbeelding $\varphi : V \to W$ tussen twee variëteiten, en onderstel dat $\varphi = T_{|V}$, waarbij $T : A^n(k) \to \mathbb{A}^m(k)$. Dan bestaat er een uniek k-algebra homomorfisme $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$ zodat het diagram (3.2) commutatief is:*

$$\begin{array}{ccc} k[Y_1, \cdots, Y_m] & \xrightarrow{\widetilde{T}} & k[X_1, \cdots, X_n] \\ {\scriptstyle \pi_W}\downarrow & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(W) & \xrightarrow{\widetilde{\varphi}} & \Gamma(V) \end{array} \tag{3.2}$$

Bewijs. $\widetilde{\varphi}$ is uniek bepaald door (3.2), aangezien

$$\widetilde{\varphi}([G]) = [\widetilde{T}(G)] = [G(T_1, \cdots, T_m)]$$

voor elke $G \in k[Y_1, \cdots, Y_m]$.
$\widetilde{\varphi}$ is ook welgedefinieerd: als $[G] = 0$ in $\Gamma(W)$, dan is $G \in I(W)$, en dus $G(Q) = 0$ voor elke $Q \in W$. Dan geldt voor elke $P \in V$ dat $\widetilde{T}(G)(P) = G(T(P)) = 0$ en dus is $\widetilde{T}(G) \in I(V)$, en $[\widetilde{T}(G)] = 0$ in $\Gamma(V)$. □

Voorbeeld 3.1.2 Zij $V \subset \mathbb{A}^n(k)$ een variëteit, en noteer $i : V \to \mathbb{A}^n(k)$ voor de kanonieke inclusie. Dan is $\Gamma(i) = \pi_V : k[X_1, \cdots, X_n] \to \Gamma(V)$.

Stelling 3.1.3 *We hebben een contravariante functor*

$$\Gamma : \underline{\underline{\mathrm{Var}}}_k \to \underline{\underline{\mathrm{Alg}}}_k$$

Voor een variëteit $V \subset \mathbb{A}^n(k)$ definiëren we $\Gamma(V) = k[X_1, \cdots, X_n]/I(V)$, en voor een veeltermafbeelding $\varphi : V \to W$ stellen we $\Gamma(\varphi) = \widetilde{\varphi}$.

Bewijs. Onderstel $\varphi = T_{|V}$, $\psi = S_{|W}$, waarbij

$$\mathbb{A}^n(k) \xrightarrow{T} \mathbb{A}^m(k) \xrightarrow{S} \mathbb{A}^p(k)$$

veeltermafbeeldingen. Dan is

$$\Gamma(S \circ T)(X_i) = S_i(T_1, \cdots, T_m) = \Gamma(T)(S_i) = \Gamma(T)(\Gamma(S)(X_i))$$

en dus is $\Gamma(S \circ T) = \Gamma(T) \circ \Gamma(S)$. Het commutatieve diagram

$$\begin{array}{ccccc} k[Z_1, \cdots, Y_p] & \xrightarrow{\Gamma(S)} & k[Y_1, \cdots, Y_m] & \xrightarrow{\Gamma(T)} & k[X_1, \cdots, X_n] \\ \downarrow{\scriptstyle \pi_X} & & \downarrow{\scriptstyle \pi_W} & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(X) & \xrightarrow{\Gamma(\psi)} & \Gamma(W) & \xrightarrow{\Gamma(\varphi)} & \Gamma(V) \end{array}$$

bepaalt op unieke wijze $\Gamma(\psi)$, $\Gamma(\varphi)$ en dus $\Gamma(\varphi) \circ \Gamma(\psi)$. Als we dit vergelijken met het diagram

$$\begin{array}{ccc} k[Z_1, \cdots, Y_p] & \xrightarrow{\Gamma(S \circ T)} & k[X_1, \cdots, X_n] \\ \downarrow{\scriptstyle \pi_X} & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(X) & \xrightarrow{\Gamma(\psi \circ \varphi)} & \Gamma(V) \end{array}$$

dat $\Gamma(\psi \circ \varphi)$ uniek bepaalt, dan vinden we

$$\Gamma(\psi \circ \varphi) = \Gamma(\varphi) \circ \Gamma(\psi)$$

hetgeen net is wat we wilden bewijzen. □

Een contravariante functor $F : \mathcal{C} \to \mathcal{D}$ heet *trouw* als voor elke $M, N \in \mathcal{C}$ de afbeelding

$$F : \operatorname{Hom}_{\mathcal{C}}(M, N) \to \operatorname{Hom}_{\mathcal{D}}(N, M)$$

injectief is. Indien deze afbeelding steeds surjectief is, dan spreken we van een *volle functor*, en indien ze steeds bijectief is van een *voltrouwe functor* (Eng. faithful, full, fully faithful).

Stelling 3.1.4 *De contravariante functor* $\Gamma : \underline{\underline{\mathrm{Var}}}_k \to \underline{\underline{\mathrm{Alg}}}_k$ *is voltrouw; m.a.w., voor elk tweetal variëteiten* V *en* W *is*

$$\Gamma : \operatorname{Pol}_k(V, W) \to \operatorname{Alg}_k(\Gamma(W), \Gamma(V))$$

bijectief.

Bewijs. We weten dat

$$\Gamma : \operatorname{Pol}_k(\mathbb{A}^n(k), \mathbb{A}^m(k)) \to \operatorname{Alg}_k(k[Y_1, \cdots, Y_m], k[X_1, \cdots, X_m])$$

bijectief is, zie (3.1). Neem nu twee variëteiten $V \subset \mathbb{A}^n(k)$, $W \subset \mathbb{A}^m(k)$, en beschouw

$$\Gamma : \operatorname{Pol}_k(V, W) \to \operatorname{Alg}_k(\Gamma(W), \Gamma(V)).$$

1) Γ is surjectief. Neem een k-algebra homomorfisme

$$f:\ \Gamma(W) \to \Gamma(V)$$

en schrijf $f([Y_i]) = [T_i]$, met $T_i \in k[X_1, \cdots, X_n]$, voor $i = 1, \cdots, m$. Dan is

$$T = (T_1, \cdots, T_m):\ \mathbb{A}^n(k) \to \mathbb{A}^m(k)$$

een veeltermafbeelding, en we hebben een commutatief diagram

$$\begin{array}{ccc} k[Y_1, \cdots, Y_m] & \xrightarrow{\widetilde{T}} & k[X_1, \cdots, X_n] \\ {\scriptstyle \pi_W}\downarrow & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(W) & \xrightarrow{f} & \Gamma(V) \end{array} \tag{3.3}$$

Bekijk nu de veeltermafbeelding

$$T_{|V}:\ V \to \mathbb{A}^m(k)$$

We beweren dat het beeld van $T_{|V}$ bevat is in W, m.a.w. $T(P) \in W$ voor elke $P \in V$.
Neem $G \in I(W)$. Dan is $\pi_W(G) = 0$ in $\Gamma(W)$, en dus

$$0 = f(\pi_W(G)) = \pi_V(\widetilde{T}(G)) \text{ in } \Gamma(V)$$

en dus is $\widetilde{T}(G) \in I(V)$. Voor elke $P \in V$ en $G \in I(W)$ hebben we dus

$$G(T(P)) = (\widetilde{T}(G))(P) = 0$$

hetgeen betekent dat $T(P) \in W$.
We hebben nu een veeltermafbeelding

$$\varphi = T_{|V}:\ V \to W$$

$\Gamma(\varphi) = \widetilde{\varphi}$ wordt eenduidig bepaald door het commutatieve diagram (3.2); ook het diagram (3.3), en dus is $f = \Gamma(\varphi) \in \mathrm{Im}\,(\Gamma)$.
2) Γ is injectief. Neem twee veeltermafbeeldingen $\varphi, \psi:\ V \to W$, respectievelijk beperkingen van $T, S:\ \mathbb{A}^n(k) \to \mathbb{A}^m(k)$, en onderstel dat

$$\Gamma(\varphi) = \Gamma(\psi)$$

Dit betekent dat

$$[T_i] = \Gamma(\varphi)[Y_i] = \Gamma(\psi)[Y_i] = [S_i]$$

in $\Gamma(V) = k[X_1, \cdots, X_n]/I(V)$, of

$$T_i - S_i \in I(V)$$

of

$$T_i(P) = S_i(P), \text{ voor elke } P \in V$$

en dus

$$\varphi = T_{|V} = S_{|V} = \psi$$

en dit bewijst dat Γ injectief is. $\square$

Voorbeeld 3.1.5 Onderstel dat V een deelvariëteit is van de variëteit W:

$$V \subset W \subset \mathbb{A}^n(k) \tag{3.4}$$

en noteer $i : V \to W$ voor de inclusieafbeelding. Duidelijk is i een veeltermafbeelding, aangezien i de beperking is van de identieke afbeelding $I = (X_1, \cdots, X_n) : \mathbb{A}^n(k) \to \mathbb{A}^n(k)$ tot V. (3.2) neemt nu volgende vorm aan:

$$\begin{array}{ccc} k[X_1, \cdots, X_n] & \xrightarrow{\widetilde{I}} & k[X_1, \cdots, X_n] \\ \downarrow{\scriptstyle \pi_W} & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(W) & \xrightarrow{\widetilde{i}} & \Gamma(V) \end{array}$$

waarbij $\widetilde{i}([F]) = [F]$. Merk op dat uit (3.4) volgt dat $I(W) \subset I(V)$. Het is ook duidelijk dat

$$\mathrm{Ker}\,(\widetilde{i} \circ \pi_W) = I(V)$$

Schrijf nu $I_W(V) = \pi_W(I(V))$, het beeld van $I(V)$ in $\Gamma(W)$. Omdat π_W surjectief is, is

$$\ker(\widetilde{i}) = I_W(V)$$

en dus vinden we

$$\Gamma(V) \cong \Gamma(W)/I_W(V) \tag{3.5}$$

Een veeltermafbeelding $\varphi : V \to W$ noemen we een *isomorfisme van variëteiten* indien er een veeltermafbeelding $\psi : W \to V$ bestaat zodat

$$\varphi \circ \psi = I_W \ \text{ en } \ \psi \circ \varphi = I_V$$

Uit de functorialiteit van Γ volgt nu onmiddellijk:

Stelling 3.1.6 *Twee variëteiten V en W zijn isomorf als en alleen als hun coördinatenringen $\Gamma(V)$ en $\Gamma(W)$ isomorf zijn (als k-algebras).*

3.2 Rationale functies en locale ringen

Beschouw weer een variëteit $V \subset \mathbb{A}^n(k)$. We hebben gezien dat $\Gamma(V)$ een domein is, en we kunnen hiervan het breukenlichaam $k(V)$ nemen. We noemen $k(V)$ het *functielichaam* van V:

$$k(V) = \left\{ \frac{a}{b} \mid a, b \in \Gamma(V),\ b \neq 0 \right\}$$

We zeggen dat f gedefinieerd is in $P \in V$ indien $f = a/b$ waarbij $b(P) \neq 0$. We schrijven dan

$$f(P) = \frac{a(P)}{b(P)}$$

Laten we aantonen dat $f(P)$ welgedefinieerd is. Onderstel

$$f = \frac{a}{b} = \frac{c}{d}$$

in $k(V)$, waarbij $a, b, c, d \in \Gamma(V)$, $a = \pi_V(A)$, $b = \pi_V(B)$, $c = \pi_V(C)$ en $d = \pi_V(D)$, met $A, B, C, D \in k[X_1, \cdots, X_n]$. Dan is

$$ad = bc \text{ in } \Gamma(V)$$

en dus

$$AD - BC \in I(V)$$

en voor elke $P \in V$:

$$A(P)D(P) = B(P)C(P)$$

waaruit

$$\frac{A(P)}{B(P)} = \frac{C(P)}{D(P)}$$

Opmerking 3.2.1 Onderstel dat $\Gamma(V)$ een UFD is; dit is ondermeer het geval als $V = \mathbb{A}^n(k)$ en $\Gamma(V) = k[X_1, \cdots, X_n]$. Elke $f \in k(V)$ kan dan geschreven worden onder de vorm $f = a/b$, waarbij a en b onderling ondeelbaar zijn, d.w.z. dat ze geen gemeenschappelijke irreducibele factoren hebben. f is dan gedefinieerd in $P \in V$ als $b(P) \neq 0$. Om te controleren dat f gedefinieerd is in P volstaat het dus om $b(P)$ uit te rekenen voor één enkele b.
In het algemeen is het echter mogelijk dat $\Gamma(V)$ geen UFD, en dan is alles ingewikkelder. Neem bijvoorbeeld

$$V = V(XW - YZ) \subset \mathbb{A}^4(k)$$

en beschouw

$$f = \frac{x}{y} = \frac{z}{w} \in k(V)$$

Neem een willekeurig punt $P = (a, b, c, d) \in V$.
Als $b \neq 0$ of $d \neq 0$, dan is f gedefinieerd in P. Neem daarom $b = d = 0$. Dan weten we dat $P = (a, 0, c, 0) \in V$. Onderstel dat f gedefinieerd is in P. Dit betekent dat er veeltermen $G, G' \in k[X, Y, Z, W]$ bestaan zodat

$$f = \frac{g}{g'} \text{ met } G'(a, 0, c, 0) \neq 0$$

We vinden dat $XG' - YG, ZG' - WG \in (XW - YZ)$, en dus

$$XG' = YG + (XW - YZ)H_1 \tag{3.6}$$
$$ZG' = WG + (XW - YZ)H_2 \tag{3.7}$$

Als we beide betrekkingen toepassen op P vinden we

$$aG'(a, 0, c, 0) = cG'(a, 0, c, 0) = 0$$

en dus $a = c = 0$. Dus $P = (0, 0, 0, 0)$ is de enige overblijvende mogelijkheid. Leid (3.6) af naar X, en vul $P = (0, 0, 0, 0)$ in. Dit geeft $G'(0, 0, 0, 0) = 0$, hetgeen strijdig is met de onderstelling. We kunnen besluiten dat f gedefinieerd is in $P = (a, b, c, d) \in V$ als en alleen als $b \neq 0$ of $d \neq 0$. Hieruit volgt ook dat $\Gamma(V)$ geen UFD is.

Beschouw nu

$$\mathcal{O}_P(V) = \{f \in k(V) \mid f \text{ is gedefinieerd in } P\}$$

Bewijs zelf dat $\mathcal{O}_P(V)$ een deelring is van het lichaam $k(V)$ (en zelfs een k-algebra). Uiteraard is elk element van $\Gamma(V)$ gedefinieerd in P, en dus hebben we

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V) \tag{3.8}$$

We noemen

$$\text{poolset}(f) = \{P \in V \mid f \text{ is niet gedefinieerd in } P\}$$

de *poolverzameling* van f. We hebben onmiddellijk dat

$$P \notin \text{poolset}(f) \iff f \in \mathcal{O}_P(V) \tag{3.9}$$

Stelling 3.2.2 *Neem $f \in k(V)$, waarbij V een variëteit. Dan is de poolverzameling van f een algebraische verzameling, en*

$$\Gamma(V) = \cap_{P \in V} \mathcal{O}_P(V) \tag{3.10}$$

Bewijs. Stel

$$J_f = \{G \in k[X_1, \cdots, X_n] \mid gf \in \Gamma(V)\}$$

(hierbij noteren we, zoals steeds, $\pi_V(G) = g$). Het is makkelijk in te zien dat J_f een ideaal is, en $I(V) \subset J_f$ (immers, als $G \in I(V)$, dan is $g = 0$, en $gf \in \Gamma(V)$). We beweren nu dat

$$\text{poolset}(f) = V(J_f)$$

Als $P \in \text{poolset}(f)$, dan is f niet gedefinieerd in P. Neem $G \in J_f$. Dan is $gf = g' \in \Gamma(V)$, en dus $f = g'/g$. Omdat f niet gedefinieerd is in P betekent dit dat $g(P) = 0$, en dus $G(P) = 0$. Dus $P \in V(J_f)$.
Omgekeerd, onderstel $P \in V(J_f)$, of $G(P) = 0$, voor alle $G \in J_f$. Als $f = [G']/[G]$, dan is $[G]f \in \Gamma(V)$, en dus $G(P) = 0$, zodat f niet gedefinieerd is in P, en $P \in \text{poolset}(f)$.
Uit (3.8) volgt onmiddellijk dat

$$\Gamma(V) \subset \cap_{P \in V} \mathcal{O}_P(V)$$

Omgekeerd, als

$$f \in \cap_{P \in V} \mathcal{O}_P(V)$$

dan hebben we

$$\forall P \in V : \ f \in \mathcal{O}_P(V)$$

en, gebruik makend van (3.9)

$$\forall P \in V : \ P \notin \text{poolset}(f)$$

en dus

$$\text{poolset}(f) = V(J_f) = \emptyset$$

Uit de Nullstellensatz volgt dan dat $J_f = k[X_1, \cdots, X_n]$ (zie gevolg 2.5.9). Dus is $1 \in J_f$, en dit betekent niets anders dan $f \in \Gamma(V)$. □

Stel nu

$$\begin{aligned} M_P(V) &= \{f \in \mathcal{O}_P(V) \mid f(P) = 0\} \\ &= \text{Ker}\left(\mathcal{O}_P(V) \to k : \ f \mapsto f(P)\right) \end{aligned}$$

We zien onmiddellijk dat $\mathcal{O}_P(V)/M_P(V) \cong k$ een lichaam is, en dus is $M_P(V)$ een maximaal ideaal van $\mathcal{O}_P(V)$.
Onderstel nu dat $f \in \mathcal{O}_P(V) \setminus M_P(V)$ niet in dit maximaal ideaal ligt. We kunnen dan schrijven

$$f = \frac{a}{b}$$

met $a, b \in \Gamma(V)$, $a(P) \neq 0$ en $b(P) \neq 0$. Maar dan is

$$f' = \frac{b}{a} \in \mathcal{O}_P(V)$$

en duidelijk is $ff' = 1$. Alle elementen buiten $M_P(V)$ zijn dus inverteerbaar in $\mathcal{O}_P(V)$, en dit betekent dat $\mathcal{O}_P(V)$ een *locale ring* is (zie "Algebra I", stelling 1.6.5).

Stelling 3.2.3 *$\mathcal{O}_P(V)$ is een noethers locaal domein.*

Bewijs. We weten reeds dat $\mathcal{O}_P(V)$ locaal is. Het is een domein, omdat het een deelring is van het lichaam $k(V)$.
$\Gamma(V)$ is noethers, want het is een quotiënt van de noetherse ring $k[X_1, \cdots, X_n]$ (zie § 1.2). Neem een ideaal $I \subset \mathcal{O}_P(V)$, en generatoren $f_1, \cdots, f_r$ van het ideaal $I \cap \Gamma(V) \subset \Gamma(V)$. Neem $f \in I$, en schrijf

$$f = \frac{a}{b}$$

waarbij $b(P) \neq 0$. Dan is $bf = a \in I \cap \Gamma(V)$, en dus

$$bf = \sum_{i=1}^{r} a_i f_i$$

met $a_i \in \Gamma(V)$. Hieruit volgt dat

$$f = \sum_{i=1}^{r} \frac{a_i}{b} f_i$$

en dus zijn $f_1, \cdots, f_r$ ook een eindig stel generatoren voor I. □

Voorbeeld 3.2.4 Stel $V = \mathbb{A}^n(k)$, en $P = (0, \cdots, 0)$. Dan is

$$\Gamma(V) = k[X_1, \cdots, X_n]$$

en

$$\mathcal{O}_P(\mathbb{A}^n(k)) = \{\frac{F}{G} \mid F, G \in k[X_1, \cdots, X_n], \ G(0, \cdots, 0) \neq 0\}$$

Als we G schrijven als een som van vormen

$$G = G_0 + \cdots + G_d$$

dan moet dus $G_0 \neq 0$, m.a.w. $G \notin I = (X_1, \cdots, X_n)$. We kunnen ook besluiten

$$M_P(\mathbb{A}^n(k)) = \{\frac{F}{G} \mid F \in I,\ G \notin I\} = I\mathcal{O}_P(\mathbb{A}^n(k))$$

en, voor elke $r \geq 0$:

$$M_P(\mathbb{A}^n(k))^r = I^r\mathcal{O}_P(\mathbb{A}^n(k))$$

Zij $V \subset \mathbb{A}^n(k)$ een variëteit, en $P \in V$. Schrijf

$$I = I(V) \subset k[X_1, \cdots, X_n]$$

We hebben al gezien dat er een bijectief verband is tussen de idealen J van $k[X_1, \cdots, X_n]$ die I bevatten, en de idealen J' van $\Gamma(V)$. Dit verband wordt gegeven door

$$J' = \pi_V(J) \ \text{ en } \ J = \pi_V^{-1}(J')$$

Stelling 3.2.5 *We hebben een k-algebra isomorfisme*

$$\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$$

In het bijzonder is (neem $J = I$):

$$\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V)$$

Bewijs. We definiëren

$$\varphi :\ \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$$

door

$$\varphi\left[\frac{F}{G}\right] = \left[\frac{\pi_V(F)}{\pi_V(G)}\right]$$

1) φ is welgedefinieerd. Neem $x \in J\mathcal{O}_P(\mathbb{A}^n)$. We kunnen schrijven:

$$x = \sum_i F_i \frac{A_i}{G}$$

waarbij $F_i \in J$, en A_i en G veeltermen, met $G(P) \neq 0$. Als we dit uitwerken vinden we

$$x = \frac{\sum_i F_i A_i}{G} = \frac{F}{G}$$

met $F \in J$ en $G(P) \neq 0$. Dan is $\pi_V(F) \in J'$ en $\pi_V(F)/\pi_V(G) \in J'\mathcal{O}_P(V)$, zodat

$$\varphi[x] = \left[\frac{\pi_V(F)}{\pi_V(G)}\right] = 0 \ \text{ in } \ \mathcal{O}_P(V)/J'\mathcal{O}_P(V).$$

2) φ is injectief. Als

$$\varphi\left[\frac{F}{G}\right] = \left[\frac{\pi_V(F)}{\pi_V(G)}\right] = 0$$

dan is

$$\frac{\pi_V(F)}{\pi_V(G)} \in J'\mathcal{O}_P(V),$$

We kunnen dus schrijven:

$$\frac{\pi_V(F)}{\pi_V(G)} = \frac{\pi_V(F')}{\pi_V(G')},$$

waarbij $F' \in J$ en $G'(P) \neq 0$. Hieruit volgt dat

$$\pi_V(FG') = \pi_V(F)\pi_V(G') = \pi_V(G)\pi_V(F') = \pi_V(GF')$$

en

$$FG' = GF' + H$$

met $H \in I(V) \subset J$. Omdat $G(P)$ en $G(P')$ allebei verschillend van nul hebben we in $\mathcal{O}_P(\mathbb{A}^n)$:

$$\frac{F}{G} = \frac{F'}{G'} + \frac{H}{GG'}.$$

Aangezien

$$\frac{F'}{G'},\ \frac{H}{GG'} \in J\mathcal{O}_P(\mathbb{A}^n)$$

volgt nu dat

$$\frac{F}{G} \in J\mathcal{O}_P(\mathbb{A}^n)$$

en $[F/G] = 0$ in $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n)$.
3) φ is surjectief: duidelijk. □

3.3 Idealen met een eindig aantal nulpunten

In deze paragraaf bestuderen we idealen $I \subset k[X_1, \cdots, X_n]$ waarvoor geldt dat $V(I)$ eindig is. Ook hier beperken we ons tot de situatie waarin k algebraisch gesloten is. We beginnen met het volgende onmiddellijke gevolg van de Nullstellensatz.

Stelling 3.3.1 *Zij $I \subset k[X_1, \cdots, X_n]$. Dan is $V(I)$ eindig als en alleen als $k[X_1, \cdots, X_n]/I$ eindigdimensionaal is als k-vectorruimte. In dit geval is*

$$\#V(I) \leq \dim_k(k[X_1, \cdots, X_n]/I)$$

Bewijs. Neem $P_1, \cdots, P_r \in V(I)$ allen verschillend, en kies $F_1, \cdots, F_r \in k[X_1, \cdots, X_n]$ zodat

$$F_i(P_j) = \delta_{ij}$$

(zie lemma 3.3.2). We beweren nu dat $\{[F_1], [F_2], \cdots, [F_r]\}$ een linear onafhankelijk stel is in $k[X_1, \cdots, X_n]/I$. Immers,

$$\begin{aligned} \sum_{i=1}^{r} \lambda_i [F_i] = 0 \implies F = \sum_{i=1}^{r} \lambda_i F_i \in I \\ \implies \forall j \in \{1, \cdots, r\} : \ 0 = F(P_j) = \sum_{i=1}^{r} \lambda_i F_i(P_j) = \lambda_j \end{aligned}$$

Hieruit volgt dat $r \leq \dim_k(k[X_1, \cdots, X_n]/I)$. Dus als $k[X_1, \cdots, X_n]/I$ eindigdimensionaal, dan is $V(I)$ noodzakelijk eindig. Het tweede deel van de stelling is meteen ook bewezen.
Omgekeerd, onderstel dat $V(I) = \{P_1, \cdots, P_r\}$ eindig. Schrijf $P_i = (a_{i1}, \cdots, a_{in})$, en stel

$$G_j(X_1, \cdots, X_n) = \prod_{i=1}^{r} (X_j - a_{ij})$$

voor $j = 1, \cdots, n$. Voor elke i geldt $G_j(P_i) = 0$, en dus is

$$G_j \in I(V(I))$$

Gebruik makende van de Nullstellensatz:

$$\exists N : \ G_j^N \in I$$

en dit betekent dat $[G_j]^N = 0$ in $k[X_1, \cdots, X_n]/I$. Als we N groot genoeg nemen, kunnen we ervoor zorgen dat eenzelfde N goed is voor elke j. G_j^N is een monische veelterm in x_j van graad Nr, en we vinden dat $[X_j]^{rN}$ een lineaire combinatie is van $\{[1], [X_j], \cdots, [X_j]^{rN-1}\}$. Hetzelfde geldt dan voor alle hogere machten van $[X_j]$, en we hebben daarom bewezen dat de eindige verzameling

$$\{[X_1^{m_1} \cdots X_n^{m_n}] \mid m_i < rN\}$$

de vectorruimte $k[X_1, \cdots, X_n]/I$ voortbrengt. Deze vectorruimte is dus eindigdimensionaal. □

We gebruikten volgende veralgemening van de interpolerende veeltermen van Lagrange.

Lemma 3.3.2 *We nemen r verschillende punten $P_1, \cdots, P_r \in \mathbb{A}^n(k)$. Dan bestaan er veeltermen $F_1, \cdots, F_r \in k[X_1, \cdots, X_n]$ zodat*

$$F_i(P_j) = \delta_{ij}$$

voor elke $i, j \in \{1, \cdots, r\}$.

Bewijs. Schrijf $P_i = (a_{i1}, \cdots, a_{in})$. Voor elke $i \neq j$ kiezen we een index c_{ij} zodat $a_{ic_{ij}} \neq a_{jc_{ij}}$. Dit kan omdat de P_i twee aan twee verschillend zijn. Stel nu

$$F_j(X_1, \cdots, X_n) = \prod_{i=1, i\neq j}^{r} \frac{X_{c_{ij}} - a_{ic_{ij}}}{a_{jc_{ij}} - a_{ic_{ij}}}$$

Dan is duidelijk $F_i(P_j) = \delta_{ij}$. □

In het geval waarin $V(I)$ een singleton is, hebben we volgende beschrijving van $k[X_1, \cdots, X_n]/I$:

Stelling 3.3.3 *Onderstel $V(I) = \{P\}$, en schrijf $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n(k))$. Dan hebben we een k-algebra isomorfisme*

$$k[X_1, \cdots, X_n]/I \cong \mathcal{O}/I\mathcal{O}$$

Bewijs. We bewijzen eerst de volgende eigenschap:
$(*)$: Neem $F \in k[X_1, \cdots, X_n]$. Als $F(P) \neq 0$, dan bestaat er een veelterm $G \in k[X_1, \cdots, X_n]$ zodat $FG - 1 \in I$, met andere woorden $[F]$ is inverteerbaar in $k[X_1, \cdots, X_n]/I$.
Schrijf $F(P) = a$. Dan is $1 - F/a \in I(P) = \mathrm{rad}(I)$, en dus bestaat er een q zodat

$$(1 - F/a)^q \in I$$

Als we deze q-de macht uitwerken met behulp van het binomium van Newton, dan vinden we iets van de vorm $1 - FG$, en dit bewijst $(*)$.

We definiëren nu

$$\phi : \ k[X_1, \cdots, X_n]/I \to \mathcal{O}/I\mathcal{O}$$

door

$$\phi([F]) = [F]$$

(de vierkante haakjes hebben hierin natuurlijk verschillende betekenissen). Het is duidelijk dat ϕ welgedefinieerd is.
a) ϕ is injectief. Neem een veelterm $A \in k[X_1, \cdots, X_n]$, en onderstel dat $[A] \in \mathrm{Ker}\,(\phi)$, dit wil zeggen dat $A \in I\mathcal{O}$, of nog:

$$A = \frac{B}{C} \ \text{ met } \ B \in I, \ C \in k[X_1, \cdots, X_n], \ C(P) \neq 0$$

Dan is $B = AC$ in $k[X_1, \cdots, X_n]$, en

$$0 = [B] = [A][C] \ \text{ in } \ k[X_1, \cdots, X_n]/I$$

Uit $(*)$ weten we dat $[C]$ inverteerbaar is in $k[X_1, \cdots, X_n]/I$, en dus is $[A] = 0$ in $k[X_1, \cdots, X_n]/I$.
b) ϕ is surjectief. Neem $[f] \in \mathcal{O}/I\mathcal{O}$, gerepresenteerd door $f \in \mathcal{O}$, dwz $f = A/B$ met $A, B \in k[X_1, \cdots, X_n]$ en $B(P) \neq 0$. Gebruik makend van $(*)$ kiezen we een veelterm C zodat $BC - 1 \in I$. We vinden achtereenvolgens

$$BCA - A \in I$$

$$CA - \frac{A}{B} \in I\mathcal{O}$$
$$\phi([CA]) = \left[\frac{A}{B}\right] = [f]$$

□

We willen nu stelling 3.3.3 uitbreiden tot het geval waarin $V(I)$ een eindige verzameling is. Om dit te doen moeten we eerst enkele lemma's bewijzen.

Lemma 3.3.4 *Zij R een noetherse commutatieve ring, I een ideaal, en $\mathrm{rad}(I) = J$. Dan bestaat er een $q \in \mathbb{N}$ zodat $J^q \subset I$.*

Bewijs. Zij $x_1, \cdots, x_r$ een stel voortbrengers voor J. Voor elke i bestaat een m_i zodat $x_i^{m_i} \in I$. Een willekeurige $y \in J$ kan geschreven worden onder de vorm

$$y = \sum_{i=1}^{r} \alpha_i x_i$$

Stel $q = m_1 + \cdots + m_r$, en neem $y_1, \cdots, y_q \in J$, en schrijf

$$y_j = \sum_{i=1}^{r} \alpha_{ij} x_i$$

Dan is

$$y_1 y_2 \cdots y_q = \prod_{j=1}^{q} \Big(\sum_{i=1}^{r} \alpha_{ij} x_i \Big) \in I$$

want als we het product uitwerken, dan is elk van de r^q termen een veelvoud van een product van q van de x_i, en dus gelegen in I. □

Vanaf nu onderstellen we $V(I) = \{P_1, \cdots, P_N\}$, en schrijven $P_i = (a_{i1}, \cdots, a_{in})$. We stellen ook

$$I_i = I(P_i) = (X_1 - a_{i1}, X_2 - a_{i2}, \cdots, X_n - a_{in})$$

Dan zijn de I_i verschillende maximale idealen, die dus twee aan twee comaximaal zijn. Dit kunnen we ook rechtstreeks inzien op de volgende manier: voor $i \neq j$ nemen we een index k zodat $a_{ik} \neq a_{jk}$. Dan is

$$0 \neq a_{ik} - a_{jk} = (X_k - a_{jk}) - (X_k - a_{ik}) \in I_j + I_i$$

en dus $1 \in I_j + I_k$. Merk ook op dat

$$I \subset I(V(I)) = I(\{P_1, \cdots, P_N\}) \subset I(P_i) = I_i$$

Lemma 3.3.5 *Er bestaan idealen $J_1, \cdots, J_N \subset k[X_1, \cdots, X_n]$ zodat*
a) $J_1, \cdots, J_N$ twee aan twee comaximaal;
b) $\mathrm{rad}(J_i) = I_i$, en dus $V(J_i) = V(I_i) = \{P_i\}$;
c) $J_1 \cap \cdots \cap J_N = I$.

Bewijs. Merk eerst op dat

$$\mathrm{rad}(I) = I(\{P_1, \cdots, P_N\}) = I(\{P_1\} \cup \cdots \cup \{P_N\}) = I_1 \cap \cdots \cap I_N$$

Uit lemma 3.3.4 en het feit dat $k[X_1, \cdots, X_n]$ noethers is volgt dat er een q bestaat zodat

$$(I_1 \cap \cdots \cap I_N)^q \subset I \tag{3.11}$$

We stellen nu $J_i = I + I_i^q$. Hieruit volgt onmiddellijk dat $I \subset J_i$, en $I \subset J_1 \cap \cdots \cap J_N$, wat een van de twee inclusies in c) bewijst. Verder is ook $I_i^q \subset J_i$, en $J_i \subset I_i$ omdat $I \subset I_i$ en $I_i^q \subset I_i$. Dus

$$I_i^q \subset J_i \subset I_i$$

Hieruit volgt b):

$$\begin{aligned} x \in \mathrm{rad}(J_i) &\implies \exists m : \ x^m \in J_i \subset I_i \\ &\implies x \in \mathrm{rad}(I_i) = I_i \end{aligned}$$

en

$$\begin{aligned} x \in I_i &\implies x^q \in I_i^q \subset J_i \\ &\implies x \in \mathrm{rad}(J_i) \end{aligned}$$

Omdat $I_1, I_2, \cdots, I_N$ twee aan twee comaximaal zijn, zijn $I_1^q, I_2^q, \cdots, I_N^q$ het ook (stelling 1.4.1), en $J_1, J_2, \cdots, J_N$ ook (want $R = I_i^q + I_j^q \subset J_i + J_j$ voor $i \neq j$). Hiermee is ook a) bewezen.
We moeten nog een van de twee inclusies van c) bewijzen:

$$\begin{aligned} J_1 \cap \cdots \cap J_N &= J_1 \cdots J_N \\ &= (I_1^q + I) \cdots (I_N^q + I) \\ &\subset I_1^q \cdots I_N^q + I \\ &= (I_1 \cdots I_N)^q + I \\ &= (I_1 \cap \cdots \cap I_N)^q + I = I \end{aligned}$$

In de laatste stap gebruikten we (3.11). □

Schrijf nu $\mathcal{O}_j = \mathcal{O}_{P_j}(\mathbb{A}^n)$. Deze locale ring bestaat uit alle rationale vormen in $k(X_1, \cdots, X_n)$ waarvan de noemer geen som is van veelvouden van $X_k - a_{jk}$ (en dus niet verdwijnt in P_j).

Lemma 3.3.6 *Met notaties zoals hierboven hebben we*

$$J_i\mathcal{O}_j = \begin{cases} I\mathcal{O}_j & \textit{als } i = j; \\ \mathcal{O}_j & \textit{als } i \neq j. \end{cases}$$

Bewijs. Neem eerst het geval $i \neq j$, en neem $F \in k[X_1, \cdots, X_n]$ zodat

$$F(P_i) = 0 \ \text{ en } \ F(P_j) = 1$$

Dan is $F \in I_i$ (omdat $F(P_i) = 0$), en $1/F \in \mathcal{O}_j$ (omdat $F(P_j) \neq 0$). Dus voor elke $f = G/H \in \mathcal{O}_j$ kunnen we schrijven

$$f = F^q \frac{G}{F^q H} \in I_i^q \mathcal{O}_j \subset J_i \mathcal{O}_j$$

en hieruit volgt dat $\mathcal{O}_j \subset J_i \mathcal{O}_j$. De omgekeerde inclusie is triviaal.
Voor $i = j$ vinden we

$$\begin{aligned} I\mathcal{O}_j &= (J_1 \cap \cdots \cap J_N)\mathcal{O}_j \\ &= (J_1 \cdots J_N)\mathcal{O}_j \\ &= (J_1\mathcal{O}_j) \cdots (J_j\mathcal{O}_j) \cdots (J_N\mathcal{O}_j) \\ &= \mathcal{O}_j \cdots (J_j\mathcal{O}_j) \cdots \mathcal{O}_j \\ &= J_j\mathcal{O}_j \end{aligned}$$

waarbij we het geval $i \neq j$ gebruikten. □

We hebben nu genoeg voorbereidende resultaten om de volgende belangrijke stelling te bewijzen.

Stelling 3.3.7 *Onderstel nu $V(I) = \{P_1, \cdots, P_N\}$ eindig, en schrijf $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n(k))$. Dan hebben we een k-algebra isomorfisme*

$$k[X_1, \cdots, X_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_i/I\mathcal{O}_i$$

Bewijs.

$$\begin{aligned} k[X_1, \cdots, X_n]/I &= k[X_1, \cdots, X_n]/(J_1 \cap \cdots \cap J_N) \quad \text{(lemma 3.3.5)} \\ &\cong \prod_{i=1}^{N} k[X_1, \cdots, X_n]/J_i \quad \text{(stelling 1.4.5 : Chinese reststelling)} \\ &\cong \prod_{i=1}^{N} \mathcal{O}_i/J_i\mathcal{O}_i \quad \text{(stelling 3.3.3)} \\ &\cong \prod_{i=1}^{N} \mathcal{O}_i/I\mathcal{O}_i \quad \text{(lemma 3.3.6)} \end{aligned}$$

□

3.4 Affiene coördinatentransformaties

Neem een veeltermafbeelding

$$T = (T_1, \cdots, T_n) : \ \mathbb{A}^n(k) \to \mathbb{A}^n(k)$$

en veronderstel dat elke T_i van graad 1 is:

$$T_i = \sum_{j=1}^{n} a_{ij} X_j + b_i$$

waarbij $a_{ij}, b_i \in k$. Als de matrix $A = (a_{ij})$ regulier is, dan noemen we T een *affiene coördinatentransformatie* . T is dan een isomorfisme van variëteiten. De inverse afbeelding $T^{-1} = (T'_1, \cdots, T'_n)$ wordt beschreven als volgt: schrijf

$$A^{-1} = (a'_{ij})$$

voor de inverse van de matrix A. Dan is

$$T'_j = \sum_{k=1}^{n} a'_{jk}(X_k - b_k)$$

(verifieer zelf). T^{-1} is dus ook een affiene coördinatentransformatie.
Neem nu een variëteit $W \subset \mathbb{A}^n(k)$, en schrijf $V = T(W)$. We hebben dan een isomorfisme van variëteiten

$$\varphi = T_{|W} : \ W \to V$$

en bijgevolg een k-algebra isomorfisme

$$\widetilde{\varphi} : \ \Gamma(V) \to \Gamma(W) \tag{3.12}$$

en we hebben dus ook een isomorfisme tussen de functielichamen

$$\widetilde{\varphi} : \ k(V) \to k(W)$$

waarbij $\widetilde{\varphi}(f/g) = \widetilde{\varphi}(f)/\widetilde{\varphi}(g)$. Als $Q \in W$, en $T(Q) = P$, dan beperkt dit isomorfisme zich tot een isomorfisme

$$\widetilde{\varphi} : \ \mathcal{O}_P(V) \xrightarrow{\cong} \mathcal{O}_Q(W) \tag{3.13}$$

en we hebben dus ook dat

$$\widetilde{\varphi} : \ M_P(V) \xrightarrow{\cong} M_Q(W) \tag{3.14}$$

Stelling 3.4.1 *Neem twee rechten L_1 en L_2 in $\mathbb{A}^2(k)$ die mekaar snijden in een punt P, en twee andere rechten M_1 en M_2 die mekaar snijden in Q. Dan bestaat er een affiene coördinatentransformatie T van $\mathbb{A}^2(k)$ die Q afbeeldt op P en $V(M_i)$ op $V(L_i)$. Dit betekent ook dat $\widetilde{T}(L_i) = M_i$.*

Bewijs. Schrijf $P = (a_1, a_2)$, en neem een punt $P' = (a_1 + b_1, a_2 + b_2) \neq P$ op L_1 en $P'' = (a_1 + c_1, a_2 + c_2) \neq P$ op L_2. Het is voldoende de stelling te bewijzen voor $Q = (0, 0)$, M_1 de x-as, en M_2 de y-as. De gevraagde transformatie is dan

$$\begin{cases} T_1 = a_1 + b_1 X + c_1 Y \\ T_2 = a_2 + b_2 X + c_2 Y \end{cases}$$

Het is duidelijk dat $T(0,0) = P$, $T(1,0) = P'$ en $T(0,1) = P''$, zodat $T(V(M_i)) = V(L_i)$. Laten we rechtstreeks verifiëren dat $\widetilde{T}(L_i) = M_i$. We zien makkelijk in dat

$$L_1 = b_2X - b_1Y - b_2a_1 + b_1a_2$$

(P en P' liggen erop), en dus

$$\begin{aligned}\widetilde{T}(L_1) &= b_2T_1 - b_1T_2 - b_2a_1 + b_1a_2 \\ &= b_2(a_1 + b_1X + c_1Y) - b_1(a_2 + b_2X + c_2Y) - b_2a_1 + b_1a_2 \\ &= (b_2c_1 - b_1c_2)Y\end{aligned}$$

en dit is juist de x-as. □

3.5 Oefeningen

Oefening 3.1 Zij W een deelvariëteit van een variëteit V, en zij $I_V(W)$ het ideaal van $\Gamma(V)$ dat overeenkomt met W.

1. Toon aan dat je elke veeltermafbeelding op V kan beperken tot een veeltermafbeelding op W.
2. Toon aan dat de hierboven vermelde afbeelding van $\Gamma(V)$ naar $\Gamma(W)$ een homomorfisme is met kern $I_V(W)$, zodat $\Gamma(W)$ isomorf is met $\Gamma(V)/I_V(W)$.

Oefening 3.2 Voor een variëteit V zijn de volgende eigenschappen equivalent.

1. V is een punt.
2. $\Gamma(V) = k$.
3. $\dim_k \Gamma(V) < \infty$

Oefening 3.3 $F \in k[X,Y]$ irreducibel en monisch in Y, d.w.z. $F = Y^n + a_1(X)Y^{n-1} + \cdots$. $V = V(F) \subset \mathbb{A}^2$. Toon aan dat het natuurlijk homomorfisme van $k[X]$ naar $\Gamma(V) = k[X,Y]/(F)$ injectief is. Toon tevens aan dat $\Gamma(V)$ een moduul is over $k[X]$ met voortbrengers $\overline{1}, \ldots, \overline{Y^{n-1}}$.

Oefening 3.4 De samenstelling van twee polynomiale afbeeldingen is een polynomiale afbeelding.

Oefening 3.5 De projectie $pr : \mathbb{A}^n \to \mathbb{A}^r, n \geq r$, gedefinieerd door $pr(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$ is een polynomiale afbeelding.

Oefening 3.6 Zij $k = \mathbb{C}$. Zet op $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ de gewone topologie.

1. Toon aan dat $\mathbb{C} \setminus S$ wegsamenhangend is met S een eindig deel van $\mathbb{C}$.
2. Toon aan dat $\mathbb{A}^n(\mathbb{C}) \setminus V$ wegsamenhangend is met V een eigenlijk algebraisch deel van $\mathbb{A}^n(\mathbb{C})$.

Oefening 3.7 Er is een natuurlijke bijectieve correspondentie tussen de priemidealen van $O_P(V)$ en de deelvariëteiten die P bevatten.

Oefening 3.8 Zij f een rationale functie op een variëteit V. Zij

$$U = \{P \in V | f \text{ is gedefinieerd in } P\}$$

Dan definieert f een functie van U naar k. Toon aan dat deze functie de functie f eenduidig bepaalt. Een rationale functie kan dus beschouwd worden als een soort functie, maar enkel op het complement van een algebraisch deel van V, niet op V zelf.

Oefening 3.9 Zij $\phi : V \to W$ een veeltermafbeelding van affiene variëteiten, $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ de geïnduceerde afbeelding op de coördinaatringen. Veronderstel verder $P \in V, \phi(P) = Q$. Toon aan dat je $\tilde{\phi}$ op een unieke manier kan uitbreiden tot een ringhomomorfisme van $\mathcal{O}_Q(W)$ naar $\mathcal{O}_P(V)$. Toon ook aan dat dan $\tilde{\phi}(M_Q(W) \subset M_P(V)$.

Oefening 3.10 $P = (0, \ldots, 0) \in \mathbb{A}^n, \mathcal{O} = \mathcal{O}_P(\mathbb{A}^n), M = M_P(\mathbb{A}^n)$. $I = (X_1, \ldots, X_n) \subset k[X_1, \ldots, X_n]$. Toon aan dat $I\mathcal{O} = M$ en dus $I^r\mathcal{O} = M^r$ voor alle r.

Oefening 3.11 $I, J \subset k[X_1, \ldots, X_n]$ zijn comaximaal $\Leftrightarrow V(I) \cap V(J) = \emptyset$.

Oefening 3.12 $I = (X, Y) \subset k[X, Y]$. Toon aan dat

$$\dim_k(k[X, Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Oefening 3.13 $\mathcal{O}$ een lokale ring met maximaal ideaal M.

$$0 \longrightarrow M^n/M^{n+1} \longrightarrow \mathcal{O}/M^{n+1} \longrightarrow \mathcal{O}/M^n \longrightarrow 0$$

is een natuurlijke exacte rij.

Oefening 3.14 R DVR met maximaal ideaal M en veronderstel verder dat $k \subset R$ en de samenstelling $k \longrightarrow R \longrightarrow R/M$ een isomorfisme.

1. $\dim_k(M^n/M^{n+1}) = 1$ voor alle $n \geq 0$.
2. $\dim_k(R/M^n) = n$ voor alle $n > 0$.
3. als $(z) = M^n$ dan is $\mathrm{Ord}(z) = n$.
4. $\mathrm{Ord}(z) = \dim_k(R/(z))$.

Oefening 3.15 Toon aan dat $k[[X]]$, de ring der formele machtreeksen, een DVR is met uniformiserende parameter X. Zijn quotiëntlichaam wordt $K((X))$ genoteerd.

Oefening 3.16 $W = V_1 \cup V_2$ algebraische delen van $\mathbb{A}^n$. $P \in V_1 \setminus V_2$.
Toon aan dat het ringhomomorfisme

$$\mathcal{O}_P(W) \longrightarrow \mathcal{O}_P(V_1) : \frac{a}{b} \mapsto \frac{\overline{a}}{\overline{b}}$$

een isomorfisme is.

Oefening 3.17 $V = V(XW - YT) \subseteq \mathbb{A}^4(\mathbb{C})$, V een variëteit.
$\overline{X} = x \in \Gamma(V), \overline{Y} = y \in \Gamma(V), \overline{W} = w \in \Gamma(V), \overline{T} = t \in \Gamma(V)$, dus $xw - yt = 0$.
Wat is de poolverzameling van $f = \frac{x}{y}$?

Oefening 3.18 $V = V_1 \cup \ldots \cup V_n$ decompositie in irreducibele componenten, $P \in V_1, \ldots, V_m$; $P \notin V_{m+1}, \ldots, V_n$.

1. $I_V(V_1, \ldots, V_m)$ is de kern van

$$\Gamma(V) \longrightarrow \mathcal{O}_P(V) : f \mapsto \frac{f}{1}$$

2. $\mathcal{O}_P(V)$ is een domein $\Leftrightarrow m = 1$.

Oefening 3.19 $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ algebraisch.
Polynomiale afbeeldingen $V \to W$ zijn continu (voor de Zariski-topologie).

Oefening 3.20 V, W algebraische delen, $\phi : V \to W$ surjectieve polynomiale afbeelding. Toon aan V irreducibel $\Leftrightarrow$ W irreducibel.

Hoofdstuk 4

Vlakke krommen

4.1 Raaklijnen

Zij k een algebraisch gesloten lichaam. Uit gevolg 2.4.5 weten we dat een vlakke kromme correspondeert met een veelterm $F \in k[X,Y]$ waarvan al de irreducibele factoren enkelvoudig zijn. Om redenen die verderop duidelijk worden is het nuttig om ook meervoudige factoren toe te laten, en vandaar volgende definitie.

Definitie 4.1.1 *Twee niet-constante veeltermen $F, G \in k[X,Y]$ worden equivalent genoemd, indien $F = \lambda G$, waarbij $\lambda \in k \setminus \{0\}$. Een affiene vlakke kromme is per definitie een equivalentieklasse van zulke veeltermen.*

De graad van een kromme is de graad van de veelterm die de kromme definieert; een kromme van graad 1 noemen we een rechte. Beschouw een kromme F, en de ontbinding van F in irreducibele factoren:

$$F = F_1^{e_1} \cdots F_k^{e_k}$$

De F_i worden de componenten van F genoemd, en e_i de multipliciteit van de component F_i. Als $e_i = 1$, dan noemen we F_i een enkelvoudige component. Als de algebraische verzameling $V(F)$ gekend is, dan ook de componenten van F, maar niet hun multipliciteiten.
Als $F \in k[X,Y]$ irreducibel is, dan is $V(F)$ een variëteit, en we noteren

$$\Gamma(F) = \Gamma(V(F)) \ ; \ k(F) = k(V(F)) \ ; \ \mathcal{O}_P(F) = \mathcal{O}_P(V(F))$$

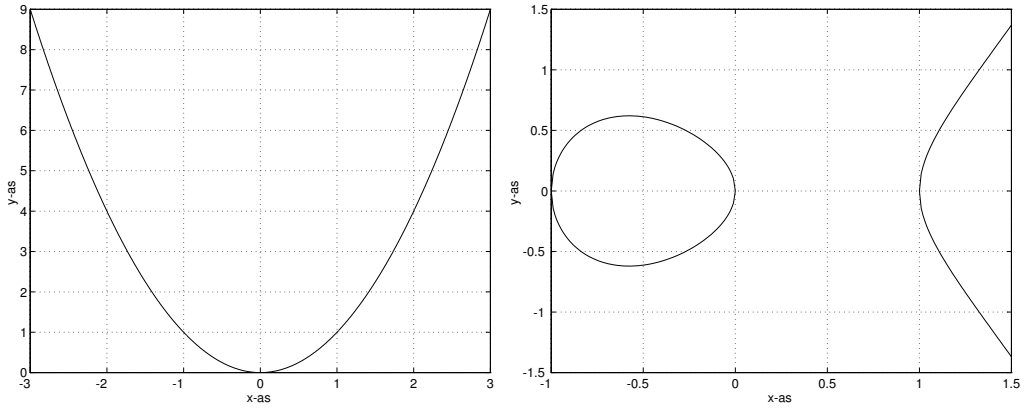
Neem een kromme F, en $P = (a,b) \in V(F)$, m.a.w. $F(a,b) = 0$. We noemen P een *enkelvoudig punt* van F indien

$$\frac{\partial F}{\partial X}(P) \neq 0 \ \text{ of } \ \frac{\partial F}{\partial Y}(P) \neq 0$$

De rechte

$$\frac{\partial F}{\partial X}(P)(X-a) + \frac{\partial F}{\partial Y}(P)(Y-b)$$

noemen we dan de *raaklijn* aan F in P.
Een punt $P \in V(F)$ dat niet enkelvoudig is noemen we *meervoudig* of *singulier*. Een kromme waarvan alle punten enkelvoudig zijn noemen we een *reguliere kromme*. Ga zelf na dat de krommen $Y - X^2$ en $Y^2 - X^3 + X$ regulier zijn.



Figuur 4.1: $A(X,Y) = Y - X^2$ en $B(X,Y) = Y^2 - X^3 + 1$

Neem een kromme F, en schrijf F als een som van vormen

$$F = F_m + F_{m+1} + \cdots + F_n$$

waarbij F_i een vorm van graad i, en $F_m \neq 0$. We noemen m de *multipliciteit* van F in het punt $P = (0,0)$, en noteren

$$m = m_F(P)$$

Merk op dat

$$\begin{aligned} m_F(P) > 0 &\implies P \in V(F) \\ m_F(P) = 1 &\implies P \text{ is een enkelvoudig punt op } F \end{aligned}$$

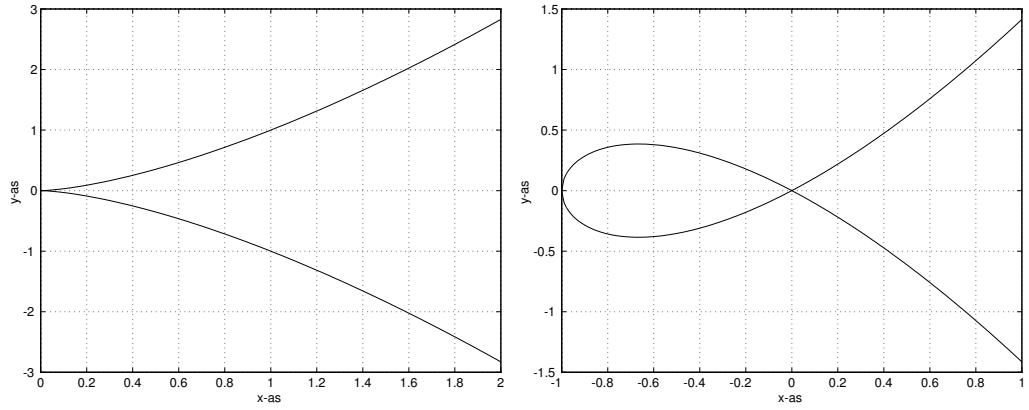
en in dit laatste geval is F_1 de raaklijn aan F in P. Als $m_P(F) = 2$, dan noemen we P een *dubbelpunt*. Als $m_P(F) \geq 1$, dan kunnen we F_m ontbinden in homogene lineaire factoren (zie gevolg 1.1.6):

$$F_m = \prod_i L_i^{r_i}$$

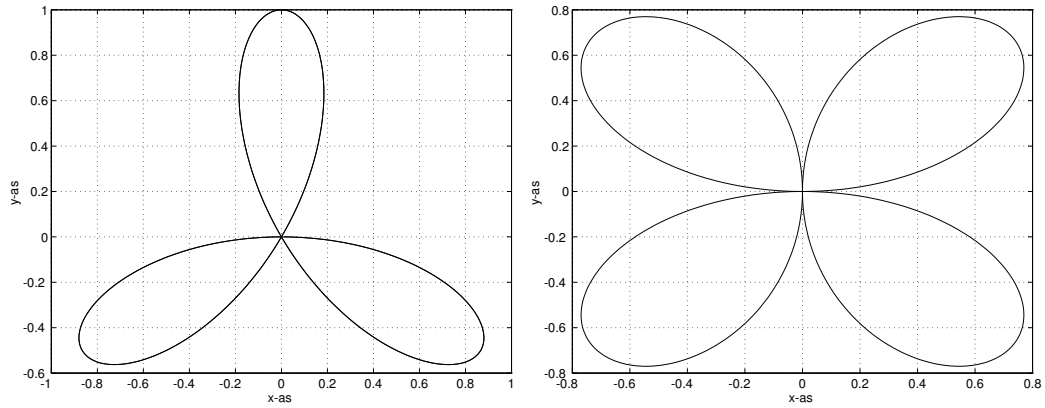
waarbij de L_i rechten zijn, en $\sum_i r_i = m_P(F)$. We noemen de rechten L_i de *raaklijnen* aan F in P.
Als $r_i = 1$, dan noemen we L_i een *enkelvoudige raaklijn*; als $r_i = 2$, dan spreken we van een *dubbele raaklijn*. Als alle raaklijnen enkelvoudig zijn, dan noemen we P een *gewoon meervoudig punt*. Een gewoon dubbelpunt noemen we een *knooppunt*. Een rechte door P die niet aan F raakt noemen we een raaklijn van multipliciteit nul.
Volgende eigenschap is duidelijk:

$$F = \prod_i F_i^{e_i} \implies m_P(F) = \sum_i e_i m_P(F_i) \tag{4.1}$$

en als L raakt aan F_i met multipliciteit r_i, voor elke i, dan raakt L aan F met multipliciteit $\sum_i e_i r_i$. Dus P is een enkelvoudig punt van F als en alleen als P behoort tot juist 1 component F_i, P een enkelvoudig punt is van die component F_i, en die component F_i zelf een enkelvoudige component van F is.



Figuur 4.2: $C(X,Y) = Y^2 - X^3$ en $D(X,Y) = Y^2 - X^3 - X^2$



Figuur 4.3: $E(X,Y) = (X^2+Y^2)^2 + 3X^2Y - Y^3$ en $F(X,Y) = (X^2+Y^2)^3 - 4X^2Y^2$

Als $P = (a,b) \neq (0,0)$, dan worden alle bovenstaande definities als volgt veralgemeend. Stel

$$T(X,Y) = (X+a, Y+b)$$

en, zoals voorheen,

$$F^T = F \circ T = \tilde{T}(F)$$

Het is duidelijk dat $P = (a,b) \in V(F)$ als en alleen als $(0,0) \in V(F^T)$, en we definiëren daarom

$$m_P(F) = m_{(0,0)}(F^T)$$

Voorbeelden 4.1.2 $P = (0,0)$ is een dubbelpunt op de kromme $C(X,Y) = Y^2 - X^3$. We hebben in P de x-as als dubbele raaklijn.

$P = (0,0)$ is een knooppunt op de kromme $D(X,Y) = Y^2 - X^3 - X^2$. Er zijn namelijk twee enkelvoudige raaklijnen, namelijk de bissectrices $Y + X$ en $Y - X$. De oorsprong is een gewoon drievoudig punt op de kromme $E(X,Y) = (X^2 + Y^2)^2 + 3X^2Y - Y^3$. De raaklijnen zijn Y, $\sqrt{3}X - Y$ en $\sqrt{3}X + Y$.
$(0,0)$ is een viervoudig punt op $F(X,Y) = (X^2 + Y^2)^3 - 4X^2Y^2$. De twee coördinaatassen zijn dubbele raaklijnen.
De grafieken in Figuur 4.2 en Figuur 4.3 geven hiervan een idee; wel moeten we deze tekeningen relativeren: de grafieken geven enkel de reële oplossingen van de bijhorende vergelijkingen, terwijl onze theorie enkel geldig is over algebraisch gesloten lichamen (bijvoorbeeld $\mathbb{C}$).

4.2 Locale ringen

Stelling 4.2.1 *Zij F een irreducibele vlakke kromme. Dan is P een enkelvoudig punt op F als en alleen als $\mathcal{O}_P(F)$ een DVR is.*
Als L een rechte door P is die geen raaklijn is, dan is het beeld l van L in $\mathcal{O}_P(F)$ een uniformiserende parameter.

Bewijs. Onderstel eerst dat P een enkelvoudig punt is. Zij R de raaklijn aan F in P. Gebruik makend van stelling 3.4.1 vinden we een affiene coördinatentransformatie T zodat

$$T(0,0) = P \ ; \ \widetilde{T}(R) = Y \ ; \ \widetilde{T}(L) = X$$

T beperkt zich tot een isomorfisme van variëteiten

$$T_{|V(F^T)} = \varphi : \ V(F^T) \to V(F)$$

en we hebben dus een ringisomorfisme (zie (3.13))

$$\widetilde{\varphi} : \ \mathcal{O}_P(F) \to \mathcal{O}_{(0,0)}(F^T)$$

Bovendien is $\widetilde{\varphi}(r) = y$ en $\widetilde{\varphi}(l) = x$, en het volstaat dus om de stelling te bewijzen in het geval waarin $P = (0,0)$, Y de raaklijn, en X de rechte die geen raaklijn is.
We moeten aantonen dat het maximaal ideaal $M_P(F)$ een hoofdideaal is. We tonen aan dat $M_P(F) = (x)$ (en dan is x een uniformiserende parameter). We weten in elk geval dat

$$M_P(F) = (x, y)$$

(zie voorbeeld 3.2.4). Omdat Y de raaklijn aan F in P is, kunnen we schrijven

$$\begin{aligned} F &= Y + F_2 + \cdots + F_d \\ &= YG - X^2H \end{aligned}$$

waarbij $G = 1 + \cdots \in k[X,Y]$. In $\Gamma(F) \subset \mathcal{O}_P(F)$ hebben we dus

$$yg = x^2h$$

Maar g is inverteerbaar in $\mathcal{O}_P(F)$ (omdat $G(P) \neq 0$). Dus in $\mathcal{O}_P(F)$ hebben we

$$y = x^2 h g^{-1} \in (x)$$

Dit bewijst een implicatie van onze stelling. De andere bewijzen we verderop. □

Onderstel dat P een enkelvoudig punt is op de irreducibele kromme F, en beschouw

$$\mathrm{ord}_P^F : \ k(F) \setminus \{0\} \to \mathbb{Z}$$

Als L een rechte is door P, dan hebben we dus

$$\begin{aligned} L \text{ geen raaklijn} &\implies \mathrm{ord}_P^F(l) = 1 \\ L \text{ een raaklijn} &\implies \mathrm{ord}_P^F(l) > 1 \end{aligned}$$

Immers, in het bewijs van stelling 4.2.1 hebben we gezien dat

$$\mathrm{ord}_P^F(y) = \mathrm{ord}_P^F(x^2 h g^{-1}) \geq 2$$

Stelling 4.2.2 *Zij P een punt op een irreducibele kromme F. Voor n voldoende groot (met name $n \geq m_P(F)$) hebben we*

$$m_P(F) = \dim_k(M_P(F)^n / M_P(F)^{n+1}) \tag{4.2}$$

Dit betekent ondermeer dat de multipliciteit $m_P(F)$ volledig bepaald wordt door de locale ring $\mathcal{O}_P(F)$.

Bewijs. Schrijf $\mathcal{O} = \mathcal{O}_P(F)$ en $M = M_P(F)$. Net zoals in stelling 4.2.1 kunnen we ons beperken tot het geval $P = (0,0)$. We hebben een exacte rij

$$0 \longrightarrow M^n/M^{n+1} \longrightarrow \mathcal{O}/M^{n+1} \longrightarrow \mathcal{O}/M^n \longrightarrow 0 \tag{4.3}$$

Als we kunnen bewijzen dat

$$\dim_k(\mathcal{O}/M^n) = n m_P(F) + s \tag{4.4}$$

voor $n \geq m_P(F)$, met s een constante, dan volgt (4.2) door toepassing van de dimensieformule op (4.3).
Herhaal (voorbeeld 3.2.4) dat $M^n = I^n \mathcal{O}$, met $I = (X, Y)$. Omdat $V(I^n) = \{P\}$ is ook $V(I^n, F) = \{P\}$, en dus

$$\begin{aligned} k[X,Y]/(I^n, F) &\cong \mathcal{O}_P(\mathbb{A}^2)/(I^n, F)\mathcal{O}_P(\mathbb{A}^2) \quad (\text{stelling } 3.3.3) \\ &\cong \mathcal{O}_P(F)/I^n \mathcal{O}_P(F) \quad (\text{stelling } 3.2.5) \\ &\cong \mathcal{O}/M^n \end{aligned} \tag{4.5}$$

en het volstaat dus om $\dim_k(k[X,Y]/(I^n, F))$ te berekenen.
Vanaf nu onderstellen we dat $n \geq m$. Schrijf $m = m_P(F)$, dan is $F \in I^m$. Als $G \in I^{n-m}$, dan is $FG \in I^n$, en dus is

$$\psi : \ k[X,Y]/I^{n-m} \to k[X,Y]/I^n : \ [G] \mapsto [FG]$$

welgedefinieerd. Toon zelf aan dat we een exacte rij hebben

$$0 \longrightarrow k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/(I^n,F) \longrightarrow 0 \tag{4.6}$$

waarbij φ de kanonieke surjectie is. Bovendien is (ga zelf na!)

$$\dim_k(k[X,Y]/I^n) = \frac{n(n+1)}{2}$$

en dus levert de dimensieformule, toegepast op (4.6):

$$\dim_k(k[X,Y]/(I^n,F)) = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = nm - \frac{m(m-1)}{2}$$

en dit bewijst (4.4). □

Bewijs van het omgekeerde van stelling 4.2.1. Onderstel dat $\mathcal{O} = \mathcal{O}_P(F)$ een DVR is, met maximaal ideaal $M = (t)$. Als we (4.5) toepassen in het geval $n = 1$ vinden we

$$\mathcal{O}/M = k[X,Y]/(I,F) \cong k. \tag{4.7}$$

Definieer nu $\varphi:\ M^n/M^{n+1} \to \mathcal{O}/M$ door

$$\varphi([z]) = [zt^{-n}]$$

Het is eenvoudig aan te tonen dat φ welgedefinieerd, injectief en surjectief is. Dus

$$\dim_k(M^n/M^{n+1}) = 1$$

en uit stelling 4.2.2 volgt dat $m_P(F) = 1$. □

4.3 Intersectiegetallen

Neem twee vlakke krommen F, G en een punt $P \in \mathbb{A}^2(k)$. We zullen het *intersectiegetal*

$$I(P, F \cap G)$$

definiëren. We wensen dat dit een getal in $\mathbb{N} \cup \{\infty\}$ is dat voldoet aan de volgende zeven axioma's:
A1 $I(P, F \cap G) = \infty \iff P$ ligt op een gemeenschappelijke component van F en G;
A2 $I(P, F \cap G) = 0 \iff P \notin V(F) \cap V(G)$;
$I(P, F \cap G)$ hangt enkel af van de componenten van F en G waar P opligt;
A3 als T een affiene coördinatentransformatie is, en $T(Q) = P$, dan is $I(Q, F^T \cap G^T) = I(P, F \cap G)$;
A4 $I(P, F \cap G) = I(P, G \cap F)$;
A5 $I(P, F \cap G) \geq m_P(F) m_P(G)$;

$I(P, F \cap G) = m_P(F)m_P(G) \iff F$ en G hebben geen gemeenschappelijke raaklijnen in P;
A6 als $F = \prod_i F_i^{r_i}$ en $G = \prod_j G_j^{s_j}$, dan is

$$I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$$

A7 voor elke $A \in k[X, Y]$:

$$I(P, F \cap G) = I(P, F \cap (G + AF))$$

Stelling 4.3.1 *Er bestaat een uniek intersectiegetal $I(P, F \cap G)$ dat aan de axioma's A1-A7 voldoet, en dit wordt gegeven door de formule*

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)) \tag{4.8}$$

Bewijs. uniciteit Onderstel dat I en J aan de zeven axioma's voldoen. We moeten aantonen dat $I = J$, of

$$I(P, F \cap G) = x \iff J(P, F \cap G) = x, \tag{4.9}$$

voor alle $x \in \mathbb{N} \cup \{\infty\}$, $P \in \mathbb{A}^2(k)$ en $F, G \in k[X, Y] \setminus k$.
Uit **A3** volgt dat het voldoende is om (4.9) aan te tonen voor $P = (0, 0)$.
Uit **A1** en **A2** volgt dat (4.9) geldt voor $x = 0$ en $x = \infty$. Per inductie zullen we nu bewijzen dat (4.9) geldt voor $P = (0, 0)$ en $x = n \in \mathbb{N}_0$.
Inductiehypothese: we onderstellen dat (4.9) geldt voor $x = 0, 1, \cdots, n - 1$.
We bewijzen dat

$$I(P, F \cap G) = n \implies J(P, F \cap G) = n.$$

De omgekeerde implicatie volgt door de rollen van I en J om te wisselen. Onderstel dus dat $I(P, F \cap G) = n$. Bekijk de veeltermen $F(X, 0), G(X, 0) \in k[X]$, en onderstel (zie **A4**)

$$\deg(F(X, 0)) = r \leq \deg(G(X, 0)) = s$$

We kunnen er altijd voor zorgen dat $F(X, 0)$ en $G(X, 0)$ monisch zijn, omdat een kromme maar op een veelvoud na bepaald is.
Onderstel eerst dat $r > 0$. Dan stellen we

$$H = G - X^{s-r}F$$

Merk op dat P ook op H ligt, aangezien $H(0, 0) = 0$. Uit **A7** volgt dat

$$I(P, F \cap G) = I(P, F \cap H) \text{ en } J(P, F \cap G) = J(P, F \cap H)$$

Hierbij is $\deg H(X, 0) < s$. We herhalen deze redenering, tot we uiteindelijk krommen K en L vinden zodanig dat

$$I(P, F \cap G) = I(P, K \cap L), \quad J(P, F \cap G) = J(P, K \cap L)$$

en

$$\deg(K(X, 0)) = 0 \leq \deg(L(X, 0)) = u$$

Omdat $K(0,0) = 0$ en $K(X,0)$ constant is, hebben we dat $K(X,0) = 0$. Hieruit volgt dat $Y \mid K(X,Y)$. Schrijf $K(X,Y) = YM(X,Y)$. Uit **A6** volgt nu dat

$$I(P, K \cap L) = I(P, Y \cap L) + I(P, M \cap L) \text{ en } J(P, K \cap L) = J(P, Y \cap L) + J(P, M \cap L) \quad (4.10)$$

Schrijf nu

$$L(X,0) = X^m(a_0 + a_1X + \cdots + a_{u-m}X^{u-m}),$$

waarbij $a_0 \neq 0$. Omdat $L(0,0) = 0$ is $m > 0$. $L(X,Y) - L(X,0)$ is deelbaar door Y, het quotiënt noemen we $N(X,Y)$:

$$L(X,Y) = L(X,0) + YN(X,Y).$$

Nu berekenen we

$$\begin{aligned} I(P, Y \cap L) &= I(P, Y \cap (L - YN(X,Y))) \quad (\mathbf{A7}) \\ &= I(P, Y \cap L(X,0)) \\ &= I(P, Y \cap X^m) + I(P, Y \cap (a_0 + a_1X + \cdots + a_{s-m}X^{s-m})) \quad (\mathbf{A6}) \\ &= I(P, Y \cap X^m) \quad (\mathbf{A2}) \\ &= m \quad (\mathbf{A5}) \end{aligned}$$

Op dezelfde wijze zien we dat $J(P, Y \cap L) = m$. Omdat $I(P, Y \cap L) = n$ volgt uit (4.10) dat $I(P, M \cap L) = n - m < n$, en uit de inductiehypothese besluiten we dat ook $J(P, M \cap L) = n - m$. We kunnen nu besluiten dat

$$\begin{aligned} n &= I(P, F \cap G) = I(P, K \cap L) \\ &= I(P, Y \cap L) + I(P, M \cap L) \\ &= J(P, Y \cap L) + J(P, M \cap L) \\ &= J(P, K \cap L) = J(P, F \cap G) \end{aligned}$$

<u>existentie</u> We zullen aantonen dat (4.8) aan de zeven axioma's voldoet.
A4 triviaal.

A3 Een affiene coördinatentransformatie $T : \mathbb{A}^2(k) \to \mathbb{A}^2(k)$ induceert een isomorfisme $\widetilde{T} : k[X,Y] \to k[X,Y]$. als $T(Q) = P$, dan geeft dit ook een ringisomorfisme (zie (3.13))

$$\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_Q(\mathbb{A}^2)$$

en dus

$$\mathcal{O}_P(\mathbb{A}^2)/(F,G) \cong \mathcal{O}_Q(\mathbb{A}^2)/(F^T, G^T)$$

en **A3** volgt nadat we de dimensies nemen van beide leden.
Voor het bewijs van al de overige axioma's kunnen we ons dus beperken tot het geval $P = (0,0)$.

A7 volgt uit $(F, G + AF) = (F, G)$.

A2 Onderstel dat $P \notin V(F)$. Dan is $F(P) \neq 0$, en F is inverteerbaar in $\mathcal{O}_P(\mathbb{A}^2)$. Dus is $(F,G) = (1)$ in $\mathcal{O}_P(\mathbb{A}^2)$, en

$$\dim(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = \dim(\mathcal{O}_P(\mathbb{A}^2)/\mathcal{O}_P(\mathbb{A}^2)) = 0$$

Omgekeerd, als $\dim(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = 0$, dan is $(F,G) = 1$, en dus bestaan er $A/C, B/C \in \mathcal{O}_P(\mathbb{A}^2)$ zodat $AF + BG = C$. Dan is $(AF + BG)(P) = C(P) \neq 0$. Maar dan is $F(P) \neq 0$ of $G(P) \neq 0$ en dus ligt P niet op de doorsnede van F en G.
Als $F = F_1F_2$ met $F_2(P) \neq 0$, dan is F_2 inverteerbaar in $\mathcal{O}_P(\mathbb{A}^2)$, en $(F,G) = (F_1,G)$. We kunnen dus onderstellen dat P op alle componenten van F en G ligt.

A1 Onderstel dat F en G geen gemene componenten hebben. Dan is $V(F,G) = \{P_1 = P, \cdots, P_N\}$ eindig, en

$$k[X,Y]/(F,G) = \prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^2)/(F,G)$$

(zie stelling 3.3.7). $k[X,Y]/(F,G)$ is eindigdimensionaal (zie stelling 3.3.1), en dus is ook $\mathcal{O}_{P_i}(\mathbb{A}^2)/(F,G)$ eindigdimensionaal.
Omgekeerd, onderstel dat F en G een gemene irreducibele component H hebben, waarop B ligt. Dan is $(F,G) \subset (H)$, en we kunnen de kanonieke surjectie

$$\mathcal{O}_P(\mathbb{A}^2)/(F,G) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/(H)$$

beschouwen. Dit impliceert dat

$$\dim(\mathcal{O}_P(\mathbb{A}^2)/(H)) \leq \dim(\mathcal{O}_P(\mathbb{A}^2)/(F,G))$$

Bovendien is

$$\mathcal{O}_P(\mathbb{A}^2)/(H) \cong \mathcal{O}_P(H) \supset \Gamma(H)$$

Als $\Gamma(H) = k[X,Y]/(H)$ eindigdimensionaal, dan is $V(H)$ eindig (stelling 3.3.1), en dus is $V(H)$ een punt (want H is irreducibel). Dit is strijdig met het feit dat H een gemene irreducibele component is van F en G. A fortiori is $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$ oneindigdimensionaal.

A6 Het volstaat te bewijzen dat

$$I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H) \tag{4.11}$$

Hierbij mogen we onderstellen dat F en GH geen gemene componenten hebben (anders zijn beide leden ∞). Omdat $(F,GH) \subset (F,G)$ hebben we de kanonieke surjectie

$$\varphi : \mathcal{O}_P(\mathbb{A}^2)/(F,GH) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/(F,G)$$

Definieer nu

$$\psi : \mathcal{O}_P(\mathbb{A}^2)/(F,H) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/(F,GH)$$

via de formule

$$\psi([z]) = [Gz]$$

Het is duidelijk dat ψ welgedefinieerd is: als $[z] = [A/B] = 0$ in $\mathcal{O}_P(\mathbb{A}^2)/(F,H)$, dan is $A \in (F,H)$, en dus $AG \in (GF, GH) \subset (F, GH)$ en $[AG/B] = 0$ in $\mathcal{O}_P(\mathbb{A}^2)/(F,GH)$. (4.11) volgt nu uit de dimensieformule als we kunnen aantonen dat de rij

$$0 \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/(F,H) \xrightarrow{\psi} \mathcal{O}_P(\mathbb{A}^2)/(F,GH) \xrightarrow{\varphi} \mathcal{O}_P(\mathbb{A}^2)/(F,G) \longrightarrow 0$$

exact is. We weten al dat φ surjectief is. Bewijs zelf dat

$$\mathrm{Im}\,(\psi) = \mathrm{Ker}\,(\varphi)$$

We bewijzen dat ψ injectief is. Onderstel $\psi([z]) = 0$. Dan is $Gz = uF + vGH$, met $u, v \in \mathcal{O}_P(\mathbb{A}^2)$. Stel

$$u = \frac{A}{S} \;\; ; \;\; v = \frac{B}{S} \;\; ; \;\; z = \frac{C}{S}$$

met $S(P) \neq 0$ (we kunnen u, v en z steeds op gelijke noemer brengen). Dan volgt

$$\frac{GC}{S} = \frac{AF}{S} + \frac{BGH}{S}$$

en

$$GC = AF + BGH$$

en

$$G(C - BH) = AF$$

Omdat F en G geen gemene factoren hebben volgt hieruit dat F een deler is van $C - BH$, en dus

$$C - BH = DF$$

en

$$z = \frac{C}{S} = \frac{D}{S}F + \frac{B}{S}H \in (F,H)$$

en $[z] = 0$ in $\mathcal{O}_P(\mathbb{A}^2)/(F,H)$.

A5 Schrijf $m = m_P(F)$, $n = m_P(G)$, en $I = (X,Y) \subset k[X,Y]$, en beschouw het diagram

$$\begin{array}{ccccccc} k[X,Y]/I^n \times k[X,Y]/I^m & \xrightarrow{\psi} & k[X,Y]/I^{n+m} & \xrightarrow{\varphi} & k[X,Y]/(I^{n+m},F,G) & \longrightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & \mathcal{O}_P(\mathbb{A}^2)/(F,G) & \xrightarrow{\pi} & \mathcal{O}_P(\mathbb{A}^2)/(I^{n+m},F,G) & \longrightarrow & 0 \end{array}$$

Hierin zijn φ, α en π de kanonieke afbeeldingen. φ en π zijn surjectief, en α is een isomorfisme, vanwege het feit dat $V(I^{n+m}, F, G) = \{P\}$ en stelling 3.3.3. De afbeelding ψ definiëren we met de formule

$$\psi([A],[B]) = [AF + BG]$$

Het is duidelijk dat ψ welgedefinieerd is, en dat de bovenste rij van het diagram exact is. Uit dit laatste volgt

$$\begin{aligned} \dim_k(k[X,Y]/I^n \times k[X,Y]/I^m) &\geq \dim(\mathrm{Im}\,(\psi)) \\ &= \dim_k(k[X,Y]/I^{n+m}) - \dim_k(k[X,Y]/(I^{n+m},F,G)) \end{aligned}$$

en we vinden

$$\begin{aligned} I(P, F \cap G) &= \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) \\ &\geq \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(I^{n+m}, F, G)) \\ &= \dim_k(k[X,Y]/(I^{n+m}, F, G)) \\ &\geq \dim_k(k[X,Y]/I^{n+m}) - \dim_k(k[X,Y]/I^n) - \dim_k(k[X,Y]/I^m) \\ &= \frac{(m+n)(m+n+1)}{2} - \frac{n(n+1)}{2} - \frac{m(m+1)}{2} \\ &= mn \end{aligned}$$

en dit bewijst het eerste deel van **A5**. Dit bewijst tevens dat

$$I(P, F \cap G) = mn$$

als en alleen als de twee ongelijkheden in bovenstaande redenering gelijkheden zijn.
De eerste ongelijkheid is een gelijkheid als en alleen als π ook injectief is, d.w.z. dat $I^{n+m} \subset (F,G)\mathcal{O}_P(\mathbb{A}^2)$.
De tweede ongelijkheid is een gelijkheid als en alleen als ψ injectief is.
Uit lemma 4.3.2 volgt dat beide ongelijkheden gelijkheden zijn als en alleen als F en G geen gemene raaklijnen hebben in P, en dit beëindigt het bewijs. □

Lemma 4.3.2 *a) Als F en G geen gemene raaklijnen hebben in P, dan is*

$$I^t \subset (F,G)\mathcal{O}_P(\mathbb{A}^2) \tag{4.12}$$

zodra $t \geq m+n-1$.
b) ψ is injectief als en alleen als F en G geen gemene raaklijnen hebben in P.

Bewijs. a) Stap 1 Merk eerst op dat als (4.12) geldt voor $t = s$, dan automatisch ook voor $t = s' > s$, omdat dan $I^{s'} \subset I^s$.

Stap 2 Er bestaat een M zodat (4.12) geldt voor $t = M$.
Stel $V(F,G) = \{P, Q_1, \cdots, Q_s\}$ (F en G hebben geen gemene componenten). Kies H zo dat $H(Q_i) = 0$ en $H(P) \neq 0$. Vanwege de Nullstellensatz hebben we

$$HX, HY \in I(V(F,G)) = \mathrm{rad}(F,G)$$

en dus bestaat er een N zodat

$$(HX)^N, (HY)^N \in (F,G) \subset k[X,Y]$$

In $\mathcal{O}_P(\mathbb{A}^2)$ is H inverteerbaar (omdat $H(P) \neq 0$), en dus

$$X^N, Y^N \in (F,G)\mathcal{O}_P(\mathbb{A}^2)$$

en

$$I^{2N} \subset (F,G)\mathcal{O}_P(\mathbb{A}^2)$$

Stap 3 Neem $s \geq n + m - 1$ en onderstel dat

$$I^{s+1} \subset (F, G)\mathcal{O}_P(\mathbb{A}^2). \tag{4.13}$$

m.a.w. (4.12) geldt voor $t = s + 1$. Dan geldt (4.12) ook voor $t = s$.
(4.13) betekent dat alle vormen van graad $s + 1$ en hoger in $(F, G)\mathcal{O}_P(\mathbb{A}^2)$ liggen. Het volstaat nu om te bewijzen dat ook alle vormen van graad s in $(F, G)\mathcal{O}_P(\mathbb{A}^2)$ liggen, of

$$V(s, 2) \subset (F, G)\mathcal{O}_P(\mathbb{A}^2).$$

Schrijf $L_1, \cdots, L_m$ voor de raaklijnen aan F in P, en $M_1, \cdots, M_n$ voor de raaklijnen aan G in P. Als $i > m$, dan stellen we $L_i = L_m$, en als $j > n$ stellen we $M_j = M_n$. Schrijf

$$A_{ij} = L_1 \cdots L_i M_1 \cdots M_j$$

Dan is A_{ij} een vorm van graad $i + j$, en uit lemma 4.3.3 volgt dat

$$\{A_{ij} \mid i + j = s\}$$

een basis is van $V(s, 2)$, de vectorruimte die bestaat uit alle vormen van graad s in twee veranderlijken. Het volstaat dus om te bewijzen dat

$$A_{ij} \in (F, G)\mathcal{O}_P(\mathbb{A}^2)$$

zodra $i + j = s$. Omdat $i + j = s \geq m + n - 1$ is $i \geq m$ of $j \geq n$. Onderstel bijvoorbeeld dat $i \geq m$. Dan is

$$A_{ij} = A_{m0}B = F_m B$$

met B een vorm van graad $s - m$. Bovendien is

$$F = F_m + F_{m+1} + \cdots + F_d$$

waarbij $F_{m+1} + \cdots + F_d \in I^{m+1}$. We zien dat

$$A_{ij} = BF - B(F_{m+1} + \cdots + F_d) \in (F, G)\mathcal{O}_P(\mathbb{A}^2),$$

aangezien $BF \in (F, G)$ en $B(F_{m+1} + \cdots + F_d) \in I^{s-m}I^{m+1} = I^{s+1} \subset (F, G)\mathcal{O}_P(\mathbb{A}^2)$ (vanwege (4.13)).

Stap 4 Er bestaat een M zodat (4.12) geldt voor $t = M$ (Stap 2). Als $M \leq s$, dan geldt (4.12) ook voor $t = s$ (Stap 1). Als $M > s$, dan volgt, na herhaaldelijk toepassen van (Stap 3) dat (4.12) ook geldt voor $t = M - 1, M - 2, \cdots, s$. Dit bewijst het gestelde.

b) Onderstel dat er geen gemeenschappelijke raaklijnen zijn in P, en dat

$$\psi([A], [B]) = [AF + BG] = 0$$

Dit betekent dat

$$AF + BG \in I^{n+m} \tag{4.14}$$

een som is van vormen van graad tenminste $m+n$. Schrijf

$$A = A_r + \cdots \ ; \ B = B_s + \cdots$$

zodat

$$AF + BG = A_r F_m + B_s G_n + \cdots$$

Als $r \geq n$ en $s \geq m$, dan is $A \in I^n$ en $B \in I^m$, en dus $[A] = 0$ in $k[X,Y]/I^n$ en $[B] = 0$ in $k[X,Y]/I^m$.
We zullen bewijzen dat het onmogelijk is dat $r < n$ of $s < m$. Onderstel bijvoorbeeld dat $r < n$. Er zijn dat drie mogelijke gevallen: $r+m < s+n$, $r+m > s+n$ en $r+m = s+n$. We tonen dat die alle drie tot een tegenstrijdigheid leiden.
1) $r+m < s+n$. De homogene component van $AF+BG$ van laagste graad is dan $A_r F_m$, van graad $r+m < n+m$. Dit is strijdig met (4.14), dat zegt dat alle homogene componenten van $AF+BG$ van tenminste graad $m+n$ zijn.
2) $r+m > s+n$. De homogene component van $AF+BG$ van laagste graad is dan $B_s G_n$, van graad $s+n < r+m < n+m$. Dit is strijdig met (4.14), dat zegt dat alle homogene componenten van $AF+BG$ van tenminste graad $m+n$ zijn.
3) $r+m = s+n$. Als $A_r F_m + B_s G_n \neq 0$, dan is de homogene component van $AF+BG$ van laagste graad $A_r F_m + B_s G_n$, en deze heeft graad $r+m < n+m$, wat weer strijdig is (4.14). Dus moet $A_r F_m + B_s G_n = 0$. Omdat F_m en G_n geen gemene factoren hebben, volgt hieruit dat $F_m | B_s$ en $G_n | A_r$, waaruit volgt dat $s \geq m$ en $r \geq n$, wat weer een tegenstrijdigheid is.
Omgekeerd, als L een gemeenschappelijke raaklijn is aan F en G in P, dan kunnen we schrijven

$$F_m = LF'_{m-1} \ \text{ en } \ G_n = LG'_{n-1}$$

Dan is

$$\begin{aligned} \psi([G'_{n-1}, -F'_{m-1}]) &= [FG'_{n-1} - GF'_{m-1}] \\ &= [LF'_{m-1}G'_{n-1} - LG'_{n-1}F'_{m-1} + \cdots] \\ &= 0 \ \text{ in } \ k[X,Y]/I^{n+m} \end{aligned}$$

en ψ is niet injectief. □

Lemma 4.3.3 *In $k[X,Y]$ nemen we twee stellen rechten $L_1, L_2, \cdots$ en $M_1, M_2, \cdots$, waarbij we onderstellen dat geen enkel van de L_i samenvalt met een der M_j:*

$$\lambda M_i \neq L_j$$

voor alle $i, j \in \mathbb{Z}$ en $\lambda \in k$. Schrijf

$$A_{ij} = L_1 \cdots L_i M_1 \cdots M_j$$

dan is

$$\{A_{ij} \mid i+j = d\}$$

een basis voor $V(d,2)$, de vectorruimte die bestaat uit alle vormen van graad d.

Bewijs. We bewijzen het lemma per inductie op d. Voor $d = 1$ is het lemma waar, want $\{L_1, M_1\}$ is een basis voor $V(1, 2)$. Onderstel dat het lemma geldt voor $V(d-1, 2)$.
We weten dat $\dim_k(V(d, 2)) = d + 1$, aangezien

$$\{X^d, X^{d-1}Y, \cdots, XY^{d-1}, Y^d\}$$

duidelijk een basis is. Het volstaat dus om aan te tonen dat de A_{ij} lineair onafhankelijk zijn. Onderstel dat

$$\sum_{i=0}^{d} \alpha_i A_{d-i,i} = 0 \tag{4.15}$$

Merk op dat A_{ij} deelbaar is door M_1 zodra $j > 0$. Kies $(a, b) \neq (0, 0)$, zodat $M_1(a, b) = 0$. Als we (a, b) invullen in (4.15), dan vinden we

$$\sum_{i=0}^{d} \alpha_i A_{d-i,i} = \alpha_0 A_{d,0}(a, b) = 0$$

Omdat $A_{d,0}(a, b) = L_1(a, b) \cdots L_d(a, b) \neq 0$ volgt hieruit dat $\alpha_0 = 0$. In (4.15) zijn alle overblijvende termen deelbaar door M_1. Omdat het lemma waar is voor $d - 1$, volgt dat ook $\alpha_1 = \cdots = \alpha_d = 0$. □

Voorbeeld 4.3.4 Bekijk de vlakke krommen $E = (X^2 + Y^2)^2 + 3X^2Y - Y^3$ en $F = (X^2 + Y^2)^3 - 4X^2Y^2$. We zullen het intersectiegetal $I(P, E \cap F)$ bepalen in het punt $P = (0, 0)$. Hiervoor gebruiken we uitsluitend de zeven axioma's.
Merk eerst op dat

$$\begin{aligned} F - (X^2 + Y^2)E &= -4X^2Y^2 - (X^2 + Y^2)3X^2Y + (X^2 + Y^2)Y^3 \\ &= Y\Big((X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y\Big) \\ &= YG \end{aligned}$$

Gebruik makend van achtereenvolgens **A7** en **A6** vinden we

$$\begin{aligned} I(P, E \cap F) &= I(P, E \cap YG) \\ &= I(P, E \cap Y) + I(P, E \cap G) \end{aligned}$$

Hierbij is

$$G = -3(X^2 + Y^2)^2 + 4Y^2(X^2 + Y^2) - 4X^2Y$$

en dus

$$\begin{aligned} G + 3E &= 4Y^2(X^2 + Y^2) + 5X^2Y - 3Y^3 \\ &= Y(5X^2 - 3Y^2 + 4Y^3 + 4X^2Y) \\ &= YH \end{aligned}$$

en dus, weerom gebruik makend van **A7** en **A6**:

$$I(P, E \cap F) = 2I(P, E \cap Y) + I(P, E \cap H)$$

Omdat $E = X^4 + YE_1$ vinden we, via **A7** en **A5**:

$$I(P, E \cap Y) = I(P, X^4 \cap Y) = 4 \times 1 = 4$$

en, omdat E en H geen gemene raaklijnen hebben:

$$I(P, E \cap H) = m_P(E)m_P(H) = 3 \times 2 = 6$$

en tenslotte

$$I(P, E \cap F) = 8 + 6 = 14$$

We zullen nu aantonen dat het intersectiegetal nog aan twee bijkomende eigenschappen (**A8** en **A9**) voldoet. Onderstel dat F een irreducibele kromme is, en P een enkelvoudig punt. Dan is $\mathcal{O} = \mathcal{O}_P(F)$ een DVR (zie stelling 4.2.1), met maximaal ideaal $M = (t)$.
In het bewijs van stelling 4.2.1 hebben we al gezien dat $M^n/M^{n+1} \cong \mathcal{O}/M \cong k$, zie (4.7). Bekijk nu de exacte rij

$$0 \longrightarrow M^{k+1}/M^{k+l} \longrightarrow M^k/M^{k+l} \longrightarrow M^k/M^{k+1} \longrightarrow 0$$

Hieruit volgt, met de dimensieformule

$$\dim_k(M^{k+1}/M^{k+l}) + 1 = \dim_k(M^k/M^{k+l})$$

en dus

$$\dim_k(M^k/M^{k+l}) = l$$

en, in het bijzonder

$$\dim_k(\mathcal{O}/M^n) = n$$

Als $\mathrm{ord}_P^F(G) = n$, dan is $M^n = ([G])$, en dus

$$\dim_k(\mathcal{O}/([G])) = n$$

Merk nu op dat (zie stelling 3.2.5)

$$\mathcal{O}_P(\mathbb{A}^2)/(F, G) \cong \mathcal{O}_P(F)/([G])$$

en we hebben bewezen:

Stelling 4.3.5 *Zij P een enkelvoudig punt op de irreducibele kromme F. Voor elke andere kromme G geldt dan*
A8 $I(P, F \cap G) = \mathrm{ord}_P^F(G)$.

Onderstel nu dat F en G geen gemene componenten hebben. Dan is $V(F, G) = \{P_1, \cdots, P_N\}$ eindig, en uit stelling 3.3.7 vinden we

$$k[X, Y]/(F, G) \cong \prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^2)/(F, G)$$

Als we de dimensies van beide leden nemen, dan vinden we volgend resultaat.

Stelling 4.3.6 *Als* $V(F,G) = \{P_1, \cdots, P_N\}$*, dan is*

A9 $\displaystyle\sum_{i=1}^{N} I(P_i, F \cap G) = \dim_k(k[X,Y]/(F,G))$

Voorbeeld 4.3.7 Stel $F = Y - X^2$ en $G = Y - 1$. F en G snijden elkaar in $(-1,1)$ en $(1,1)$, met intersectiegetal 1. Het linkerlid van **A9** is dus 2. Het rechterlid is ook 2, want

$$k[X,Y]/(Y - X^2, Y - 1) \cong k[X]/(1 - X^2)$$

heeft als basis $\{[1], [X]\}$.

4.4 Oefeningen

Oefening 4.1 Zoek de raaklijnen in de meervoudige punten voor de volgende krommen :

1. $F = Y^3 - Y^2 + X^3 - X^2 + 3Y^2X + 3X^2Y + 2XY$
2. $F = X^4 + Y^4 - X^2Y^2$
3. $F = X^3 + Y^3 - 3X^2 - 3Y^2 + 3XY + 1$
4. $F = X^3 + X^2 + Y^2$

Oefening 4.2 Als een kromme F van graad n een punt P heeft van multipliciteit n, toon dan aan dat F bestaat uit n lijnen door P.

Oefening 4.3 Toon aan dat een irreducibele vlakke kromme slechts een eindig aantal singuliere punten heeft.

Oefening 4.4 F vlakke kromme. Als F geen meervoudige componenten heeft dan heeft F slechts een eindig aantal singuliere punten.

Oefening 4.5 $F = F_1 \dots F_m$ met F_i irreducibel.
Toon aan : $P \in F$ singulier $\Leftrightarrow \exists i$ zodat P een singulier punt is van F_i of $\exists i \neq j$ zodat $P \in F_i \cap F_j$.

Oefening 4.6 Zij $F \in k[X_1, \dots, X_n]$ een veelterm die een hyperoppervlak $V(F) \subset \mathbb{A}^n$ definieert. Zij $P \in \mathbb{A}^n$.

1. Zoek een definitie van de multipliciteit $m_P(F)$ in P van F.
2. Als $m_P(F) = 1$, zoek dan een definitie voor het raakhypervlak aan F in P.
3. Bestudeer $F = X^2 + Y^2 - Z^2, P = (0,0,0)$. Is het mogelijk om raakhypervlakken te definiëren in meervoudige punten?

Oefening 4.7 Zij P een dubbelpunt op een kromme F. Toon aan dat P een knoop is als en slechts als $F_{XY}(P)^2 \neq F_{XX}(P)F_{YY}(P)$.

Oefening 4.8 Zij k van karakteristiek 0. Toon aan dat $m_P(F)$ het kleinste geheel getal is, zodat er i, j bestaan waarvoor geldt dat $i + j = m$ en

$$\frac{\partial^m F}{\partial X^i \partial Y^j}(P) \neq 0$$

Vind een uitdrukking voor de vorm van F met de kleinste graad in termen van deze afgeleiden.

Oefening 4.9 Toon aan dat

$$\phi : \mathbb{A}^1 \longrightarrow V(Y^2 - X^3) : t \mapsto (t^2, t^3)$$

een bijectie is maar geen isomorfisme.

Oefening 4.10 Zij $T : \mathbb{A}^2 \to \mathbb{A}^2$ een polynomiale afbeelding, $T(Q) = P$.

1. Toon aan dat $m_Q(F^T) \geq m_P(F)$.
2. Zij $T = (T_1, T_2)$, dan noemen we $J_Q T = (T_{iX_j}(Q))$ de Jacobiaanse matrix van T in Q. Toon aan dat $m_Q(F^T) = m_P(F)$ als $J_Q T$ inverteerbaar is.
3. Toon dat de omgekeerde implicatie van het voorgaande vals is: neem $T = (X^2, Y), F = Y - X^2, P = Q = (0, 0)$.

Oefening 4.11 P is een punt op een irreducibele kromme F, en $M = M_P(F)$. Bespreek de functie

$$\psi : \mathbb{N} \longrightarrow \mathbb{N} : n \mapsto \dim_k(M^n/M^{n+1})$$

Besluit hieruit dat P een enkelvoudig punt is $\Leftrightarrow \dim_k(M/M^2) = 1$.

Oefening 4.12 Een enkelvoudig punt P op een kromme F wordt een flex genoemd als $\text{ord}_P^F(L) \geq 3$, waar L de raaklijn is aan F in P. Een flex heet gewoon als $\text{ord}_P^F(L) = 3$, anders is het een hogere flex.

1. Zij $F = Y - X^n$. Voor welke waarde(n) van n heeft F een flex in $P = (0, 0)$, en wat voor een?
2. Veronderstel dat $P = (0, 0), L = Y$ is de raaklijn, $F = Y + aX^2 + \cdots$. Toon aan dat P een flex van F is als en slechts als $a = 0$. Zoek een eenvoudig criterium om $\text{ord}_P^F(Y)$ te berekenen en dus ook om te bepalen of P een (hogere) flex is.

Oefening 4.13 Vind het intersectiegetal in het punt $P = (0, 0)$ van

1. $F = Y - X^2, \quad G = Y^2 - X^3$

2. $F = Y^2 - X^3 - X^2 \quad G = (X^2 + Y^2)^2 + 3X^2Y - Y^3$

Oefening 4.14 Een rechte L raakt aan een kromme F in een punt $P \Leftrightarrow I(P, F \cap L) > m_P(F)$.

Oefening 4.15 P een dubbelpunt op een kromme F, en veronderstel verder dat F slechts een raaklijn L heeft in P.

1. Toon aan dat $I(P, F \cap L) \geq 3$. In het geval dat $I(P, F \cap L) = 3$ zeggen we dat F in P een cusp heeft.
2. Neem $P = (0, 0)$ en $L = Y$. Toon aan dat P een cusp is $\Leftrightarrow F_{XXX}(P) \neq 0$. Geef hiervan een voorbeeld.
3. Als P een cusp is van F, dan gaat slechts een component van F door P.

Oefening 4.16 Een punt P op een kromme F wordt een hypercusp genoemd als $M_P(F) > 1$, F slechts één raaklijn L heeft in P en $I(P, L \cup F) = m_P(F) + 1$. Veralgemeen de resultaten van de voorgaande oefening voor hypercusps.

Oefening 4.17

1. $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^2)$ voor een zekere $P \in \mathbb{A}^2, M = M_P(\mathbb{A}^2)$.
   Bereken $\chi(n) = \dim_k(\mathcal{O}/M^n)$.
2. $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^r)$ voor een zekere $P \in \mathbb{A}^r, M = M_P(\mathbb{A}^r)$.
   Toon aan dat $\chi(n)$ een veelterm is van graad r in n, met hoogstemachtscoëfficiënt $1/r!$

Oefening 4.18 $F \in k[X_1, \ldots, X_r]$ irreducibel definieert een hyperoppervlak in $\mathbb{A}^r$. $\mathcal{O} = \mathcal{O}_P(V(F))$ voor $P = (0, \ldots, 0) \in \mathbb{A}^r, M = M_P(V(F))$.
Toon aan dat $\chi(n)$ een veelterm is van graad $r-1$ voor voldoende grote n, met hoogstemachtscoëfficiënt $m_P(F)/(r-1)!$

Oefening 4.19 Als P een enkelvoudig punt is van F, dan

$$I(P, F \cap (G + H)) \geq \min(I(P, F \cap G), I(P, F \cap H))$$

Geef een tegenvoorbeeld om aan te tonen dat dit niet geldt als P geen enkelvoudig punt is.

Oefening 4.20 Het doel van deze oefening is om een eigenschap van de lokale ring $\mathcal{O}_P(F)$ te vinden waarmee men kan bepalen of P al dan niet een enkelvoudig punt van F is. Zij F een irreducibele vlakke kromme, $P = (0, 0), m = m_P(F) > 1$. Zij $M = M_P(F)$. De klasse van $G \in k[X, Y]$ in $\Gamma(F)$ noteren we met g. De klasse van $g \in M$ in M/M^2 noteren we met $\overline{g}$.

1. Toon aan dat de afbeelding van de vectorruimte van de vormen van $k[X, Y]$ van graad 1 naar M/M^2 die $aX + bY$ afbeeldt op $\overline{aX + BY}$ een isomorfisme van vectorruimten is.
2. Veronderstel dat P een gewoon meervoudig punt is met raaklijnen $L_1, \ldots, L_m$. Toon dan aan dat $I(P, F \cap L_i) > m$ en $\overline{l_i} \neq \lambda \overline{l_j}$ voor alle $i \neq j$ en alle $\lambda \in k$.

3. Veronderstel dat er $G_1, \ldots, G_m \in k[X, Y]$ bestaan zodat $I(P, F \cap G_i) > m$ en $\overline{g_i} \neq \lambda \overline{g_j}$ voor alle $i \neq j$ en alle $\lambda \in k$. Toon aan dat P een gewoon meervoudig punt is van F.

4. Toon aan dat P een gewoon meervoudig punt is van F als en slechts als er $g_1, \ldots, g_m \in M$ bestaan zodat $\overline{g_i} \neq \lambda \overline{g_j}$ voor alle $i \neq j$ en alle $\lambda \in k$, en $\dim \mathcal{O}_P(F)/(g_i) > m$.

Hoofdstuk 5

Projectieve variëteiten

5.1 De projectieve ruimte

Op $\mathbb{A}^{n+1}(k) \setminus \{0\}$ bekijken we de volgende equivalentierelatie:

$$(x_1, \cdots, x_{n+1}) \sim (y_1, \cdots, y_{n+1}) \iff \exists \lambda \in k : \forall i : x_i = \lambda y_i$$

De verzameling van de equivalentieklassen noteren we $\mathbb{P}^n(k)$ en we noemen deze de *projectieve n-dimensionale ruimte* . De equivalentieklassen noemen we punten in de projectieve ruimte. Er is een bijectieve correspondentie tussen de punten in $\mathbb{P}^n(k)$ en de verzameling van de rechten door de oorsprong in $\mathbb{A}^{n+1}(k)$. Als $P \in \mathbb{P}^n(k)$ gerepresenteerd wordt door $(x_1, \cdots, x_{n+1})$, dan noemen we $(x_1, \cdots, x_{n+1})$ een stel *homogene coördinaten* van P. Merk op dat de homogene coördinaten niet uniek zijn: elke representant van de equivalentieklasse bepaalt een stel homogene coördinaten. Wel is steeds bepaald of de i-de coördinaat van een punt P nul is of niet: indien de i-de coördinaat nul (niet nul) is voor een bepaald stel homogene coördinaten, dan is hij nul (niet nul) voor elk stel homogene coördinaten. Indien $x_i \neq 0$, dan is x_j/x_i onafhankelijk van het gekozen stel coördinaten. We stellen nu

$$U_i = \{(x_1, \cdots, x_{n+1}) \in \mathbb{P}^n(k) \mid x_i \neq 0\}$$

Elke $P \in U_i$ heeft dan een uniek stel coördinaten van de vorm

$$(x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)$$

We noemen $(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n)$ de *niet-homogene coördinaten* van P met betrekking tot U_i (of i, of X_i). De afbeelding

$$\varphi_i : \mathbb{A}^n(k) \to U_i : (x_1, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) \mapsto (x_1, \cdots, x_{i-1}, 1, x_i, x_{i+1}, \cdots, x_n)$$

is duidelijk een bijectie. Bovendien hebben we

$$\mathbb{P}^n(k) = \cup_{i=1}^{n+1} U_i$$

en dus wordt $\mathbb{P}^n(k)$ overdekt door $n+1$ verzamelingen die eruitzien als $\mathbb{A}^n(k)$. We noemen

$$H_\infty = \mathbb{P}^n(k) \setminus U_{n+1} = \{(x_1, \cdots, x_{n+1}) \in \mathbb{P}^n(k) \mid x_{n+1} = 0\}$$

het *hypervlak op oneindig*. De afbeelding

$$\mathbb{P}^{n-1}(k) \to H_\infty : \ (x_1, \cdots, x_n) \mapsto (x_1, \cdots, x_n, 0)$$

is een bijectie, en we kunnen $\mathbb{P}^n(k) = U_{n+1} \cup H_\infty$ beschouwen als de disjuncte unie van $\mathbb{A}^n(k)$ en $\mathbb{P}^{n-1}(k)$.

Voorbeelden 5.1.1 1) $\mathbb{P}^0(k)$ bestaat uit 1 punt.
2) $\mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{(1,0)\}$ noemen we de *projectieve rechte* . Deze ontstaat dus door aan de gewone affiene rechte 1 punt (het punt op oneindig) toe te voegen.
3) $\mathbb{P}^2(k) = \mathbb{A}^2(k) \cup \{(x,y,0) \mid (x,y) \in \mathbb{P}^1(k)\}$ noemen we het *projectief vlak*. H_∞ is nu de *rechte op oneindig*.
4) Bekijk de affiene rechte $Y = mX + b$ in het vlak $\mathbb{A}^2(k)$. We identificeren $\mathbb{A}^2(k)$ met $U_3 \subset \mathbb{P}^3(k)$, gebruik makend van de afbeelding φ_3. De punten van de rechte voldoen dan allen aan de vergelijking

$$Y = mX + bZ$$

In $\mathbb{P}^3(k)$ bestaat er nog 1 oplossing meer van deze vergelijking, namelijk het punt $\{(1,m,0)\}$, gelegen op de rechte op oneindig.
5) Bekijk de orthogonale hyperbool $Y^2 = X^2 + 1$ in het vlak $\mathbb{A}^2(k)$. Als we het vlak weer identificeren met U_3, dan voldoen de punten van de orthogonale hyperbool aan de vergelijking

$$Y^2 = X^2 + Z^2$$

Op de rechte op oneindig zijn er nog twee extra oplossingen van deze vergelijking gelegen, namelijk $(1,1,0)$ en $(1,-1,0)$.

5.2 Projectieve algebraische verzamelingen

Neem $F \in k[X_1, \cdots, X_{n+1}]$. We noemen $P \in \mathbb{P}^n(k)$ een nulpunt van F indien $F(x_1, \cdots, x_{n+1}) = 0$ voor elk stel homogene coördinaten $(x_1, \cdots, x_{n+1})$ van P. Schrijf F als een som van vormen:

$$F = \sum_{i=0}^{d} F_i$$

en neem een vast stel coördinaten $(x_1, \cdots, x_{n+1})$ van P. Voor elke $\lambda \neq 0$ geldt dan

$$0 = F(\lambda x_1, \cdots, \lambda x_{n+1}) = \sum_{i=0}^{d} \lambda^i F_i(x_1, \cdots, x_{n+1})$$

Als k een oneindig lichaam is (bijvoorbeeld k algebraisch gesloten), dan hebben we dus een veelterm van graad d met meer dan d wortels. Bijgevolg zijn alle coëfficiënten nul, en hebben we

$$F_i(x_1, \cdots, x_{n+1}) = 0$$

voor elke i. Het volstaat dus om nulpunten van vormen te bekijken.
Neem nu een willekeurig deel $S \subset k[X_1, \cdots, X_{n+1}]$. We noemen

$$V(S) = \{P \in \mathbb{P}^n(k) \mid P \text{ nulpunt van elke } F \in S\}$$

een *projectieve algebraische verzameling* . Als I het ideaal is dat voortgebracht wordt door S, dan is $V(I) = V(S)$.
Voor $X \subset \mathbb{P}^n(k)$ noteren we

$$I(X) = I_p(X) = \{F \in k[X_1, \cdots, X_{n+1}] \mid \forall P \in X : \ P \text{ nulpunt van } F\}$$

Definitie 5.2.1 *Een ideaal $I \subset k[X_1, \cdots, X_{n+1}]$ wordt homogeen genoemd indien*

$$F = \sum_{i=0}^{d} F_i \in I \implies \forall i : \ F_i \in I$$

met andere woorden, als $F \in I$, dan behoren ook alle homogene componenten van F tot I.

Stelling 5.2.2 *Voor elke $X \subset \mathbb{P}^n(k)$ is $I_p(X)$ een homogeen ideaal.*

Bewijs. We hebben hierboven gezien dat als P een nulpunt is van F, dan ook van alle homogene componenten van F. □

Stelling 5.2.3 *Een ideaal $I \subset k[X_1, \cdots, X_{n+1}]$ is homogeen als en alleen als het wordt voortgebracht door een (eindig) stel vormen.*

Bewijs. Onderstel eerst dat $I = (F^{(1)}, \cdots, F^{(N)})$ homogeen. Dan is ook $I = (\{F_j^{(i)} \mid i = 1, \cdots, N, \ j \in \mathbb{N}\})$ voortgebracht door een eindig stel vormen.
Omgekeerd, onderstel dat I wordt voortgebracht door een stel vormen:

$$I = (\{F^{(\alpha)} \mid \alpha \in X\})$$

waarbij X een indexverzameling, en $F^{(\alpha)}$ een vorm van graad d_α. Neem nu

$$F = \sum_{i=0}^{d} F_i \in I$$

We moeten aantonen dat elke $F_i \in I$. Schrijf

$$F = \sum_{\alpha} A^{(\alpha)} F^{(\alpha)}$$

en neem in beide leden de homogene termen van graad i. Dit geeft

$$F_i = \sum_\alpha A_{i-d_\alpha}^{(\alpha)} F^{(\alpha)} \in I$$

□

Als we van een ideaal weten dat het homogeen is, dan bestaat er een eenvoudiger criterium om te testen dat het een priemideaal is:

Stelling 5.2.4 *Neem een homogeen ideaal $I \subset k[X_1, \cdots, X_{n+1}]$. Dan is I een priemideaal als en alleen als*

$$\forall F, G \text{ vormen}: \ FG \in I \implies F \in I \text{ of } G \in I \tag{5.1}$$

Bewijs. Een implicatie is triviaal: indien I een priemideaal is, dan geldt (5.1) voor alle veeltermen, en a fortiori voor alle vormen.
Omgekeerd moeten we bewijzen dat als (5.1) geldt voor alle vormen, dan voor alle veeltermen. Onderstel dat

$$F = F_0 + \cdots + F_d, \ G = G_0 + \cdots + G_d \in k[X_1, \cdots, X_{n+1}] \setminus I$$

terwijl $FG \in I$. Dan ligt tenminste een homogene component van F en G buiten I. We nemen i en j minimaal zodat

$$F_i, G_j \in k[X_1, \cdots, X_{n+1}] \setminus I$$

Dan geldt uiteraard dat

$$\widetilde{F} = F_0 + \cdots + F_{i-1}, \ \widetilde{G} = G_0 + \cdots + G_{j-1} \in I$$

en

$$(F - \widetilde{F})(G - \widetilde{G}) = FG - \widetilde{F}G - F\widetilde{G} + \widetilde{F}\widetilde{G} \in I$$

De component van $(F - \widetilde{F})(G - \widetilde{G})$ van graad $i + j$ is $F_i G_j$, en $F_i G_j \notin I$, vanwege (5.1). Maar dit betekent dat $(F - \widetilde{F})(G - \widetilde{G}) \notin I$, een contradictie. □

Een algebraische verzameling $V \subset \mathbb{P}^n(k)$ noemen we irreducibel als ze niet kan geschreven worden als de unie van twee echte algebraische deelverzamelingen: als $V = V_1 \cup V_2$, met V_1 en V_2 algebraisch, dan is $V = V_1$ of $V = V_2$.

Stelling 5.2.5 *Een algebraische verzameling $V \subset \mathbb{P}^n(k)$ is irreducibel als en alleen als $I_p(V)$ een (homogeen) priemideaal is in $k[X_1, \cdots, X_{n+1}]$.*

Bewijs. Het bewijs is analoog met dat van stelling 2.3.2, waarbij we rekening houden met stelling 5.2.4. Merk eerst op dat, voor twee vormen F en G,

$$V_p(FG) = V_p(F) \cup V_p(G)$$

Onderstel dat $I_p(V)$ geen priemideaal is. Dan bestaan er vormen F en G zodat $F,\ G \notin I_p(V)$, terwijl $FG \in I_p(V)$. Dan is

$$V = V(FG) \cap V = (V(F) \cap V) \cup (V(G) \cap V)$$

Omdat $F,\ G \notin I_p(V)$, vinden we

$$V(F) \cap V \neq V \ \text{ en } \ V(G) \cap V \neq V$$

zodat V reducibel is.
Omgekeerd, onderstel dat V reducibel is: $V = V_1 \cup V_2$, met $V_1, V_2 \neq V$. Dan is $I_p(V_i) \supset I_p(V)$, en $I_p(V_i) \neq I_p(V)$, neem vormen

$$F \in I_p(V_1) \setminus I_p(V) \ \text{ en } \ G \in I_p(V_2) \setminus I_p(V)$$

Dan is $FG \in I_p(V)$, zodat $I_p(V)$ geen priemideaal is. □

Een irreducibel algebraisch deel van $\mathbb{P}^n(k)$ noemen we een *projectieve variëteit*. Net zoals in het affiene geval bewijzen we dat elke projectieve algebraische verzameling op unieke manier te schrijven is als de unie van een eindig aantal projectieve variëteiten.
Vanaf nu onderstellen we dat k algebraisch gesloten is. We kunnen dan een projectieve versie van de Nullstellensatz opschrijven. We hebben afbeeldingen

$$\left\{ \begin{array}{c} \text{homogene idealen} \\ \text{van } k[X_1, \cdots, X_{n+1}] \end{array} \right\} \quad \begin{array}{c} \xrightarrow{V_p} \\ \xleftarrow[I_p]{} \end{array} \quad \left\{ \begin{array}{c} \text{projectieve algebraische} \\ \text{verzamelingen in } \mathbb{P}^n(k) \end{array} \right\}$$

en $V_p(I_p(X)) = X$, voor elke algebraische verzameling X (bewijs zelf, zie stelling 2.2.2). Voor een algebraisch deel $V \subset \mathbb{P}^n(k)$ noemen we

$$C(V) = \{(x_1, \cdots, x_{n+1}) \in \mathbb{A}^{n+1}(k) \mid (x_1, \cdots, x_{n+1}) \in V\} \cup \{(0, \cdots, 0)\}$$

de kegel van V (C staat voor "cone"). Merk op

$$V \neq \emptyset \implies I_a(C(V)) = I_p(V)$$

$$I \text{ homogeen},\ V_p(I) \neq \emptyset \implies C(V_p(I)) = V_a(I)$$

Stelling 5.2.6 (projectieve Nullstellensatz) *Onderstel dat k algebraisch gesloten is, en neem een homogeen ideaal $I \subset k[X_1, \cdots, X_{n+1}]$.*
1) $V_p(I) = \emptyset$ als en alleen als er een $N \in \mathbb{N}$ bestaat zodat I alle vormen van graad minstens N bevat.
2) Als $V_p(I) \neq \emptyset$, dan is

$$I_p(V_p(I)) = \mathrm{rad}(I)$$

Bewijs.

$$V_p(I) = \emptyset$$

als en alleen als

$$V_a(I) \subset \{(0, \cdots, 0)\}$$

als en alleen als

$$\mathrm{rad}(I) = I_a(V_a(I)) \supset (X_1, \cdots, X_{n+1}) = I_a\{(0, 0, \cdots, 0)\}$$

(hier gebruikten we de affiene Nullstellensatz). Voor elke i bestaat er dan een N_i zodat $X_i^{N_i} \in I$. Stel $N = N_1 + \cdots + N_{n+1}$. Dan is $(X_1, \cdots, X_{n+1})^N \subset I$, en I bevat alle vormen van graad tenminste N. Omgekeerd, als I alle vormen van graad minstens N bevat, dan is $(X_1, \cdots, X_{n+1}) \subset \mathrm{rad}(I)$.
Als $V_p(I) \neq \emptyset$, dan is

$$I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \mathrm{rad}(I)$$

waarbij we weer gebuik maakten van de affiene Nullstellensatz. □

Als I alle vormen van graad tenminste N bevat, dan is $\mathrm{rad}(I) = (X_1, \cdots, X_{n+1}) = M$. M is een maximaal homogeen ideaal in $k[X_1, \cdots, X_{n+1}]$. Net zoals in het affiene geval definiëren V_p en I_p daarom bijecties tussen volgende verzamelingen.

$$\begin{array}{rcl} \text{Algebraische delen van } \mathbb{P}^n(k) & \longleftrightarrow & \text{homogene radicaal idealen} \neq M \\ \text{Irreducibele algebraische delen van } \mathbb{P}^n(k) & \longleftrightarrow & \text{homogene priemidealen} \neq M \\ \text{Irreducibele hyperoppervlakken} & \longleftrightarrow & \text{Irreducibele vormen} \end{array}$$

Een projectief hypervlak is een hyperoppervlak gedefinieerd door een vorm van graad 1. $V(X_i)$ noemen we een coördinaathypervlak. Het is het hypervlak op ∞ tenopzichte van U_i.

5.3 Affiene en projectieve variëteiten

Zij $F \in k[X_1, \cdots, X_{n+1}]$ een vorm. Herhaal (§ 1.1) dat de gedehomogenizeerde $F_* \in k[X_1, \cdots, X_n]$ gedefinieerd wordt door

$$F_*(X_1, \cdots, X_n) = F(X_1, \cdots, X_n, 1)$$

Omgekeerd, als $F \in k[X_1, \cdots, X_n]$ een veelterm is van graad d, dan definiëren we de gehomogenizeerde $F^* \in k[X_1, \cdots, X_{n+1}]$ door

$$F^*(X_1, \cdots, X_{n+1}) = X_{n+1}^{d+1} F\Big(\frac{X_1}{X_{n+1}}, \cdots, \frac{X_n}{X_{n+1}}\Big)$$

We identificeren $\mathbb{A}^n(k)$ en $U_{n+1} \subset \mathbb{P}^n(k)$ met behulp van de afbeelding

$$\varphi_{n+1} : \mathbb{A}^n(k) \to \mathbb{P}^n(k) : (a_1, \cdots, a_n) \mapsto (a_1, \cdots, a_n, 1)$$

Neem een algebraische verzameling $V \subset \mathbb{A}^n(k)$ en bekijk

$$I = I_a(V) \subset k[X_1, \cdots, X_n]$$

Stel

$$I^* = (\{F^* \mid F \in I\}) \subset k[X_1, \cdots, X_{n+1}]$$

I^* is een homogeen ideaal (want het wordt voortgebracht door vormen), en we stellen

$$V^* = V_p(I^*) \subset \mathbb{P}^n(k) \text{ zodat ook } I_p(V^*) = \mathrm{rad}(I^*) \tag{5.2}$$

vanwege de projectieve Nullstellensatz.
Neem nu een algebraische verzameling $V \subset \mathbb{P}^n(k)$ en bekijk

$$I = I_p(V) \subset k[X_1, \cdots, X_{n+1}]$$

Dit keer stellen we

$$I_* = (\{F_* \mid F \in I \text{ vorm}\}) \subset k[X_1, \cdots, X_n]$$

en

$$V_* = V_a(I_*) \subset \mathbb{A}^n(k) \tag{5.3}$$

Stelling 5.3.1 *Voor $V \subset \mathbb{A}^n(k)$ algebraisch hebben we (na identificatie van $\mathbb{A}^n(k)$ en U_{n+1} via φ_{n+1}):*

$$V = V^* \cap \mathbb{A}^n(k) \text{ en } (V^*)_* = V$$

Bewijs.

$$\begin{aligned}
(x_1, \cdots, x_n) \in V &\iff \forall F \in I_a(V) : F(x_1, \cdots, x_n) = 0 \\
&\iff \forall F \in I_a(V) : F^*(x_1, \cdots, x_n, 1) = 0 \\
&\iff (x_1, \cdots, x_n, 1) \in V^* \cap U_{n+1}
\end{aligned}$$

en dit bewijst de eerste bewering. Neem nu $V \subset \mathbb{A}^n(k)$ algebraisch, en stel $I = I_a(V)$. Voor $X = (x_1, \cdots, x_n) \in \mathbb{A}^n(k)$ hebben we

$$\begin{aligned}
X \in (V^*)_* &\iff \forall F \in I_p(V^*) = I_p(V_p(I^*)) = \mathrm{rad}(I^*) : F_*(X) = 0 \\
&\iff \forall F \in I^* : F_*(X) = 0 \\
&\iff \forall F \in I : (F^*)_*(X) = 0 \\
&\iff \forall F \in I : F(X) = 0 \\
&\iff X \in V
\end{aligned}$$

waarbij we gebruik maakten van het feit dat $I^* = (\{F^* \mid F \in I\})$. □

Stelling 5.3.2 *Als $V \subset W \subset \mathbb{A}^n(k)$ algebraische verzamelingen, dan is ook $V^* \subset W^* \subset \mathbb{P}^n(k)$. Als $V \subset W \subset \mathbb{P}^n(k)$ algebraische verzamelingen, dan is ook $V_* \subset W_* \subset \mathbb{A}^n(k)$.*

Bewijs. De eerste bewering wordt als volgt bewezen:

$$\begin{aligned} V \subset W &\implies I_a(W) \subset I_a(V) \\ &\implies I_a(W)^* \subset I_a(V)^* \\ &\implies V^* = V_p(I_a(V)^*) \subset W^* = V_p(I_a(W)^*) \end{aligned}$$

Het bewijs van de tweede bewering is volledig analoog. □

Stelling 5.3.3 *Als $V \subset \mathbb{A}^n(k)$ irreducibel, dan is ook $V^* \subset \mathbb{P}^n(k)$ irreducibel.*

Bewijs. We bewijzen eerst de volgende hulpeigenschap: voor een vorm $F \in k[X_1, \cdots, X_{n+1}]$, en een ideaal $I \subset k[X_1, \cdots, X_n]$ hebben we

$$F \in I^* \iff F_* \in I \tag{5.4}$$

Onderstel eerst dat $F \in I^*$. Dan bestaan er vormen A_i, en $F_i \in I$ zodat

$$F = \sum_i A_i F_i^*$$

en dan is

$$F_* = \sum_i (A_i)_* (F_i^*)_* = \sum_i (A_i)_* F_i \in I$$

Omgekeerd, onderstel dat $F_* \in I$, en schrijf $F = X_{n+1}^r G$, met r maximaal. Dan is $F_* = G_* \in I$, en $(G_*)^* = G \in I^*$, en $F = X_{n+1}^r G = X_{n+1}^r (G_*)^* \in I^*$.
Als $V \subset \mathbb{A}^n(k)$ irreducibel is, dan is $I = I_a(V)$ een priemideaal. Neem twee vormen $F, G \in k[X_1, \cdots, X_{n+1}]$.

$$\begin{aligned} FG \in I^* &\implies (FG)_* = F_* G_* \in I \\ &\implies F_* \in I \text{ of } G_* \in I \\ &\implies F \in I^* \text{ of } G \in I^* \end{aligned}$$

waarmee bewezen is dat I^* een (homogeen) priemideaal is, en dus is $V^* = V_p(I^*)$ irreducibel. □

Stelling 5.3.4 *Neem een algebraische verzameling $V \subset \mathbb{A}^n(k)$. Dan is V^* het kleinste algebraisch deel van $\mathbb{P}^n(k)$ dat V (in feite $\varphi_{n+1}(V)$) bevat.*

Bewijs. Onderstel dat $V \subset W$ waarbij W een algebraisch deel van $\mathbb{P}^n(k)$ is. Neem een vorm $F \in I_p(W)$. Dan geldt voor alle $(x_1, \cdots, x_n) \in V$ dat $(x_1, \cdots, x_n, 1) \in W$, zodat

$$0 = F(x_1, \cdots, x_n, 1) = F_*(x_1, \cdots, x_n),$$

hetgeen betekent dat $F_* \in I_a(V)$. Dit impliceert dat $F = X_{n+1}^r (F_*)^* \in I_a(V)^*$. Hiermee is aangetoond dat

$$I_p(W) \subset I_a(V)^*$$

en dus

$$W = V_p(I_p(W)) \supset V^* = V_p(I_a(V)^*)$$

en dit bewijst onze stelling. □

Stelling 5.3.5 *Voor twee algebraische delen $V, W \subset \mathbb{A}^n(k)$ geldt*

$$(V \cup W)^* = V^* \cup W^*$$

Als $V = V_1 \cup \cdots \cup V_n$ de irreducibele ontbinding is van een algebraische verzameling V in $\mathbb{A}^n(k)$, dan is $V^* = V_1^* \cup \cdots \cup V_n^*$ de irreducibele ontbinding van V^* in $\mathbb{P}^n(k)$.

Bewijs. Schrijf $I_a(V) = I$, $I_a(W) = J$. Dan is $V \cup W = V_a(IJ)$, en

$$I_a(V \cup W) = I_a(V_a(IJ))) = \mathrm{rad}(IJ).$$

Dus:

$$P \in (V \cup W)^* \iff \forall F \in \mathrm{rad}(IJ) : \ F^*(P) = 0.$$

Dit is ook equivalent met

$$\forall F \in IJ : \ F^*(P) = 0 \tag{5.5}$$

Een implicatie is duidelijk, omdat $IJ \subset \mathrm{rad}(IJ)$. Omgekeerd, onderstel dat (5.5) geldt, en neem $F \in \mathrm{rad}(IJ)$. Dan is $F^N \in IJ$ voor een zekere N, en $(F^*)^N(P) = (F^N)^*(P) = 0$, en dus $F^*(P) = 0$. (5.5) is equivalent met

$$\forall F \in I, \ \forall G \in J : \ (F^*G^*)(P) = 0$$

Omdat het ideaal I^*J^* wordt voortgebracht door $\{F^*G^* \mid F \in I, \ G \in J\}$ is dit equivalent met

$$\forall H \in I^*J^* : \ H(P) = 0.$$

of

$$P \in V_p(I^*J^*) = V_p(I^*) \cup V_p(J^*) = V^* \cup W^*.$$

Onderstel nu dat $V = V_1 \cup \cdots \cup V_n$ de irreducibele ontbinding is van V. Uit het eerste deel van de stelling weten we dat $V^* = V_1^* \cup \cdots \cup V_n^*$, en uit stelling 5.3.3 volgt dat de V_i^* irreducibel zijn. Als $V_i^* \subset V_j^*$, dan is $V_i = \mathbb{A}^n(k) \cap V_i^* \subset V_j = \mathbb{A}^n(k) \cap V_j^*$ (stelling 5.3.1) en dus is $i = j$.
$V^* = V_1^* \cup \cdots \cup V_n^*$ de irreducibele ontbinding van V^* □

Stelling 5.3.6 *Neem een algebraische verzameling $V \subset \mathbb{A}^n(k)$, en onderstel dat $V \neq \emptyset$ en $V \neq \mathbb{A}^n(k)$. Dan ligt geen enkele irreducibele component van V^* in H_∞, en bevat ook geen enkele irreducibele component H_∞.*

Bewijs. Gebruik makend van stelling 5.3.5 kunnen we onderstellen dat V irreducibel is. V^* is dan ook irreducibel, en dus de enige irreducibele component van V^*.
Als $V^* \subset H_\infty$, dan volgt uit stelling 5.3.1 dat

$$V = V^* \cap \mathbb{A}^n(k) = \emptyset$$

en dit is een contradictie.
Als $H_\infty \subset V^*$, dan is

$$I_a(V)^* \subset I_p(V_p(I_a(V)^*)) = I_p(V^*) \subset I_p(H_\infty) = (X_{n+1})$$

Omdat $V \neq \mathbb{A}^n(k)$ bestaat er een $F \in I_a(V) \setminus \{0\}$. $F^* \in I_a(V)^*$ is dan geen veelvoud van X_{n+1}, en dit is weer een contradictie. □

Stelling 5.3.7 *Neem een algebraische verzameling $V \subset \mathbb{P}^n(k)$, en onderstel dat geen enkele irreducibele component van V een deel is van H_∞, en dat geen enkele irreducibele component H_∞ bevat. Dan is V_* een echt deel van $\mathbb{A}^n(k)$, en $(V_*)^* = V$.*

Bewijs. We mogen veronderstellen dat V irreducibel is.
Om te beginnen tonen we aan dat $\varphi_{n+1}(V_*) \subset V$. Immers

$$\begin{aligned}(x_1, \cdots, x_n) \in V_* &\implies \forall F \in I_p(V) : \ F_*(x_1, \cdots, x_n) = F(x_1, \cdots, x_n, 1) = 0 \\ &\implies (x_1, \cdots, x_n, 1) = \varphi_{n+1}(x_1, \cdots, x_n) \in V\end{aligned}$$

Uit stelling 5.3.4 volgt dat $(V_*)^*$ de kleinste algebraische deelverzameling van $\mathbb{P}^n(k)$ is die V_* bevat. Omdat ook V $V_* = \varphi_{n+1}(V_*)$ bevat, volgt hieruit dat $(V_*)^* \subset V$.
Om aan te tonen dat $V \subset (V_*)^*$ volstaat het om aan te tonen dat

$$I_p((V_*)^*) = I_p(V_p(I_a(V_*)^*)) = \mathrm{rad}((I_a(V_*))^*) \subset I_p(V)$$

of

$$(I_a(V_*))^* \subset I_p(V)$$

want $I_p(V)$ is een radicaal ideaal. Neem $F \in I_a(V_*) = I_a(V_a(I_p(V)_*)) = \mathrm{rad}(I_p(V)_*)$. Dan bestaat er een natuurlijk getal N zodat $F^N \in I_p(V)_*$, en dit betekent dat

$$F^N = \sum_i A_i (F_i)_*$$

waarbij $F_i \in I_p(V)$, en $A_i \in k[X_1, \cdots, X_n]$. Als we herhaaldelijk (1.8) toepassen, dan vinden we natuurlijke getallen r_i en t zodat

$$X_{n+1}^t (F^N)^* = \sum_i X_{n+1}^{r_i} A_i^* ((F_i)_*)^*$$

Gebruik makend van (1.6) vinden we dan, na eventueel beide leden met een geschikte macht van X_{n+1} te vermenigvuldigen, dat er natuurlijke getallen r_i en t zijn zodat

$$X_{n+1}^t (F^N)^* = \sum_i X_{n+1}^{r_i} A_i^* F_i \in I_p(V)$$

$I_p(V)$ is priem, en $X_{n+1} \notin I_p(V)$ (anders is $V \subset H_\infty$), en dus is $(F^N)^* = (F^*)^N \in I_p(V)$, en $F^* \in I_p(V)$, want $I_p(V)$ is een radicaal ideaal.
Tenslotte, als $V_* = \mathbb{A}^n(k)$, dan is $(V_*)^* = \mathbb{P}^n(k) \subset V$. □

Voor $V \subset \mathbb{A}^n(k)$ noemen we V^* de *projectieve sluiting* van V. Stellingen 5.3.6 en 5.3.7 vertellen ons dat er een 1-1 correspondentie bestaat tussen affiene variëteiten, en projectieve variëteiten die geen deel zijn van H_∞.

5.4 Functielichamen en locale ringen

Neem een projectieve variëteit $V \subset \mathbb{P}^n(k)$. Dan is $I = I_p(V)$ een homogeen priemideaal, en $\Gamma_h(V) = k[X_1, \cdots, X_{n+1}]/I$ is dus een domein, genaamd de *homogene coördinatenring* van V. $\Gamma_h(V)$ heeft ook nog de eigenschap dat elk element op unieke wijze te schrijven is als een som van vormen.
Onderstel dat I een willekeurig ideaal van $k[X_1, \cdots, X_{n+1}]$ is, en stel $\Gamma = k[X_1, \cdots, X_{n+1}]/I$. Een element $f \in \Gamma$ noemen we een vorm van graad d als f kan gerepresenteerd worden door een vorm van graad d in $k[X_1, \cdots, X_{n+1}]$:

$$f = [F], \text{ met } F \in k[X_1, \cdots, X_{n+1}], \deg(F) = d$$

Stelling 5.4.1 *Zij $I \subset k[X_1, \cdots, X_{n+1}]$ een homogeen ideaal, en $\Gamma = k[X_1, \cdots, X_{n+1}]/I$. Dan is elke $f \in \Gamma$ op unieke manier te schrijven als een som*

$$f = f_0 + f_1 + \cdots + f_m$$

waarbij f_i een vorm is van graad i.

Bewijs. De existentie is duidelijk: als $f = [F]$, waarbij $F \in k[X_1, \cdots, X_{n+1}]$, dan kunnen we F schrijven als een som van vormen

$$F = F_0 + \cdots + F_d$$

Als we dan $f_i = [F_i]$ stellen, dan is

$$f = f_0 + f_1 + \cdots + f_d$$

zoals gewenst.
Uniciteit: onderstel dat

$$f = \sum_{i=0}^{d} f_i = \sum_{i=0}^{d} g_i$$

waarbij $f_i = [F_i]$, $g_i = [G_i]$, en F_i en G_i vormen van graad i. Dan is $\sum_{i=0}^{d} F_i - \sum_{i=0}^{d} G_i = \sum_{i=0}^{d}(F_i - G_i) \in I$. Omdat I een homogeen ideaal is, is $F_i - G_i \in I$, en dus $f_i = g_i$, voor elke i. □

Het quotiëntlichaam $k_h(V)$ van $\Gamma_h(V)$ noemen we het *homogeen functielichaam*. Let wel op: de elementen van $\Gamma_h(V)$ definiëren geen functies op V, zoals in het affiene geval. Het is zelfs zo dat $k[X_1, \cdots, X_{n+1}]$ geen functies definieert op $\mathbb{P}^n(k)$. Dit komt omdat een punt P geen uniek stel coördinaten heeft, en de functiewaarde in een veelterm afhangt van de keuze van deze coördinaten. Neem twee vormen f, g in $\Gamma_h(V)$ van dezelfde graad d. Dan bepaalt het quotiënt f/g wel een functie

$$V \setminus \{P \mid g(P) = 0\} \to k$$

Immers, als $(x_1, \cdots, x_{n+1})$ een stel coördinaten voor P, dan is een ander stel coördinaten van de vorm $(\lambda x_1, \cdots, \lambda x_{n+1})$, en

$$\frac{f(\lambda x_1, \cdots, \lambda x_{n+1})}{g(\lambda x_1, \cdots, \lambda x_{n+1})} = \frac{\lambda^d f(x_1, \cdots, x_{n+1})}{\lambda^d g(x_1, \cdots, x_{n+1})} = \frac{f(x_1, \cdots, x_{n+1})}{g(x_1, \cdots, x_{n+1})}$$

is onafhankelijk van de keuze van de coördinaten. Stel daarom

$$k(V) = \{z \in k_h(V) \mid z = f/g \text{ met } f \text{ en } g \text{ vormen van dezelfde graad}\}$$

Ga zelf na dat $k(V)$ een deellichaam is van $k_h(V)$. We noemen $k(V)$ het *functielichaam* van V. Merk op dat

$$k \subset k(V) \subset k_h(V)$$

maar

$$\Gamma_h(V) \not\subset k(V)$$

De elementen van $k(V)$ noemen we rationale functies op V. Neem een rationale functie $z = f/g$. Dan is z gedefinieerd in $P \in V$ als $g(P) \neq 0$. We stellen

$$\mathcal{O}_P(V) = \{z \in k(V) \mid z \text{ is gedefinieerd in } P\}$$

$\mathcal{O}_P(V)$ is dan een deelring van $k(V)$, en is een locale ring met maximaal ideaal

$$M_P(V) = \{z = \frac{f}{g} \in \mathcal{O}_P(V) \mid f(P) = 0 \text{ en } g(P) \neq 0\}$$

Immers, alle elementen $z = f/g \in \mathcal{O}_P(V) \setminus M_P(V)$ zijn inverteerbaar, met inverse $z^{-1} = g/f$.

Affiene en projectieve locale ringen

Zij $V \subset \mathbb{A}^n(k)$ een affiene variëteit, en $P \in V$. We kunnen dan de locale ring $\mathcal{O}_P(V)$ beschouwen. Als we de projectieve sluiting V^* van V in $\mathbb{P}^n(k)$ bekijken, dan hebben we

$$P \in V \subset V^*$$

en we kunnen ook de locale ring $\mathcal{O}_P(V^*)$ beschouwen. Wat is het verband tussen deze twee? Neem een vorm $f = [F] \in \Gamma_h(V^*)$ van graad d, en stel $f_* = [F_*] \in \Gamma(V)$. De afbeelding

$$\Gamma_h(V^*) \to \Gamma(V) : \ f \mapsto f_*$$

is dan een ringhomomorfisme. We tonen aan dat de afbeelding welgedefinieerd is. Immers, als $F \in I_p(V)$, dan is $F_* \in I_a(V_*)$. We hebben dan ook een homomorfisme van lichamen

$$\alpha : \ k(V^*) \to k(V) \tag{5.6}$$

gegeven door

$$\alpha\Big(\frac{f}{g}\Big) = \frac{f_*}{g_*}$$

Definieer nu

$$\beta : \ k(V) \to k(V^*)$$

als volgt: vooreerst stellen we, voor $f = [F] \in \Gamma(V)$,

$$f^* = [F^*] \in \Gamma_h(V^*)$$

Als $f, g \in \Gamma(V)$, $\deg(f^*) = d$ en $\deg(g^*) = e$, dan schrijven we

$$\beta\Big(\frac{f}{g}\Big) = \frac{X_{n+1}^{e-d} f^*}{g^*}$$

Ook β is een welgedefinieerd homomorfisme van lichamen, en het is een eenvoudige oefening om te verifiëren dat α en β mekaars inversen zijn.
$\alpha :\ k(V^*) \to k(V)$ is dus een isomorfisme van lichamen. Neem nu $P \in V \subset V^*$. Dan beperkt α zich tot een ringisomorfisme

$$\alpha :\ \mathcal{O}_P(V) \xrightarrow{\cong} \mathcal{O}_P(V^*) \tag{5.7}$$

Voorbeeld 5.4.2 Neem $V = \mathbb{A}^n(k)$, zodat $V^* = \mathbb{P}^n(k)$. Dan is $k(V) = k(X_1, \cdots, X_n)$, en

$$k(V^*) = \{F/G \in k(X_1, \cdots, X_{n+1}) \mid \deg(F) = \deg(G)\}$$

5.5 Projectieve coördinatentransformaties

Neem een lineaire coördinatentransformatie

$$T = (T_1, \cdots, T_{n+1}) :\ \mathbb{A}^{n+1}(k) \to \mathbb{A}^{n+1}(k)$$

dus

$$T_i = \sum_{j=1}^{n+1} a_{ij} X_j$$

waarbij de matrix $A = (a_{ij})$ regulier. T beeldt rechten door de oorsprong af op rechten door de oorsprong, en dus induceert T een afbeelding

$$T :\ \mathbb{P}^n(k) \to \mathbb{P}^n(k)$$

die we een *projectieve coördinatenverandering* noemen. Als $V \subset \mathbb{P}^n(k)$ een algebraische verzameling is, dan is ook $V^T = T^{-1}(V)$ een algebraische verzameling. Immers, als $V = V_p(I)$, dan

$$\begin{aligned} P \in V_p(I) &\iff \forall F \in I \text{ vorm } :\ F(P) = 0 \\ &\iff \forall F \in I \text{ vorm } :\ (F \circ T)(T^{-1}(P)) = 0 \\ &\iff T^{-1}(P) \in V_p(\{F^T \mid F \in I\}) \end{aligned}$$

Merk op dat $F^T = F \circ T$ een vorm is van dezelfde graad als F. Als V een projectieve variëteit is, dan is ook V^T een projectieve variëteit, en omgekeerd.
We hebben een ringisomorfisme

$$\widetilde{T} :\ k[X_1, \cdots, X_{n+1}] \to k[X_1, \cdots, X_{n+1}]$$

gedefinieerd door

$$\widetilde{T}(F) = F^T = F \circ T$$

Als V een projectieve variëteit, en $I_p(V) = (F_1, \cdots, F_m)$ waarbij de F_i vormen zijn, dan hebben we hierboven aangetoond dat

$$I(V^T) = (F_1^T, \cdots, F_m^T) = (\widetilde{T}(F_1), \cdots, \widetilde{T}(F_m))$$

en dus beperkt $\widetilde{T}$ zich tot een isomorfisme van idealen

$$\widetilde{T}: \ I(V) \xrightarrow{\cong} I(V^T)$$

en

$$\widetilde{T}: \ \Gamma_h(V) \xrightarrow{\cong} \Gamma_h(V^T): \ [F] \mapsto [F^T]$$

en

$$\widetilde{T}: \ k_h(V) \xrightarrow{\cong} k_h(V^T): \ [F]/[G] \mapsto [F^T]/[G^T]$$

Neem nu $P \in V$, en stel $T^{-1}(P) = Q$. Als $G(P) \neq 0$, dan is $G^T(T^{-1}(P)) = G^T(Q) \neq 0$, zodat $\widetilde{T}$ zich beperkt tot een isomorfisme van ringen

$$\widetilde{T}: \ \mathcal{O}_P(V) \xrightarrow{\cong} \mathcal{O}_Q(V^T) \tag{5.8}$$

5.6 Oefeningen

Oefening 5.1 Toon aan $(F)^* = (F^*)$.

Oefening 5.2 $F \in k[X_1, \ldots, X_{n+1}]$ en $P \in \mathbb{P}^n(k)$. Schrijf $F = \sum F_i$ met F_i een vorm van graad i. Veronderstel dat $F(X_1, \ldots, X_{n+1}) = 0$ voor elke keuze van homogene coördinaten van P. Toon dat elke $F_i(X_1, \ldots, X_{n+1}) = 0$ voor elke keuze van homogene coördinaten van P.

Oefening 5.3 Zij I een homogeen ideaal in $k[X_1, \ldots, X_{n+1}], \Gamma = k[X_1, \ldots, X_{n+1}]/I$. Toon aan dat de vormen van graad d in Γ een eindigdimensionale vectorruimte over k vormen.

Oefening 5.4 $I \subset k[X_1, \ldots, X_{n+1}]$ homogeen ideaal.
I is priem $\Leftrightarrow (FG \in I \Rightarrow F \in I \mathrm{o} f G \in I, \ \ \forall F, G$ homogeen)

Oefening 5.5 Het radicaal van een homogeen ideaal is opnieuw homogeen.

Oefening 5.6 Zij P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) drie niet-collineaire punten in $\mathbb{P}^n$. Toon aan dat er een projectieve coördinatentransformatie $T : \mathbb{P}^2 \to \mathbb{P}^2$ bestaat zodat $T(P_i) = Q_i$. Wat in het geval van 4 punten?

Oefening 5.7 Zij L_1, L_2, L_3 (resp. M_1, M_2, M_3) drie niet-collineaire punten in $\mathbb{P}^n$. Toon aan dat er een projectieve coördinatentransformatie $T : \mathbb{P}^2 \to \mathbb{P}^2$ bestaat zodat $T(L_i) = M_i$.

Oefening 5.8 $I = (Y - X^2, Z - X^3)$ en homogenisatie gebeurt in $k[X, Y, Z, W]$.
Toon aan dat $ZW - YX \in I^*$ maar $ZW - YX \notin ((Y - X^2)^*, (Z - X^3)^*)$.

Oefening 5.9 $V(F) = V \subset W \subset \mathbb{P}^n$ irreducibel met F een niet-constante, irreducibele vorm. Toon aan $W = V$ of $W = \mathbb{P}^n$.

Oefening 5.10 Zij z een rationale functie op een projectieve variëteit V. Toon aan dat de poolverzameling van z een algebraïsch deel is van V.

Hoofdstuk 6

Projectieve vlakke krommen

6.1 Projectieve vlakke krommen

Een *projectieve vlakke kromme* is een hyperoppervlak in $\mathbb{P}^2(k)$. Net zoals in het affiene geval laten we meervoudige componenten toe. Er is dus een één-één correspondentie tussen projectieve vlakke krommen en equivalentieklassen $[F]$ van vormen in $k[X,Y,Z]$ ($F \neq 0$). Hierbij zijn twee vormen F en G equivalent als en alleen als F een veelvoud is van G: $F = \lambda G$ met $\lambda \in k$.
De graad van een kromme is de graad van een van de definiërende vormen. We gebruiken dezelfde notaties en conventies als voor affiene vlakke krommen, bijvoorbeeld

$$\mathcal{O}_P(F) = \mathcal{O}_P(V(F))$$

Voor $P = (x, y, 1)$ gelegen op de kromme F hebben we (zie (5.7))

$$\mathcal{O}_P(F) \cong \mathcal{O}_{(x,y)}(F_*)$$

Herhaal ook dat de multipliciteit van een punt P enkel afhangt van de locale ring $\mathcal{O}_P(F)$, aangezien

$$m_P(F) = \dim_k(M_P(F)^n / M_P(F)^{n+1})$$

zodra $n \geq m_P(F)$, en ook omdat $\mathcal{O}_P(F) \cong \mathcal{O}_Q(F^T)$ als T een projectieve verandering van coördinaten is, en $T(Q) = P$ (zie (5.8)).
Onderstel dat een eindig stel punten $P_1, P_2, \cdots, P_n \in \mathbb{P}^2(k)$ gegeven zijn. Dan bestaat er steeds een rechte L die geen enkel van de punten P_i bevat. Als F een vorm is van graad d, dan stellen we

$$F_* = \frac{F}{L^d} \in k(\mathbb{P}^2(k))$$

We zullen verderop zien wat het verband is met de vroeger gedefinieerde F_*. Maar om te beginnen merken we op dat F_* afhankelijk is van de keuze van de rechte L. Dit is echter niet belangrijk, want als L' een andere rechte is die geen enkel van de punten P_i bevat, dan is

$$\frac{F}{L'^d} = \frac{L^d}{L'^d} F_*$$

en de nieuwe F_* is gelijk aan de oude F_* op een inverteerbaar element in elk van de $\mathcal{O}_{P_i}$ na. Het enige waarin we zullen geïnteresseerd zijn is de orde van F_* in elk van deze locale ringen.
Door een projectieve coördinaatverandering kunnen we er steeds voor zorgen dat $L = Z$ de rechte op oneindig is. Dan is

$$F_* = F(\frac{X}{Z}, \frac{Y}{Z}, 1)$$

en als we $k(\mathbb{A}^2(k)) = k(X, Y)$ identificeren met

$$k(\mathbb{P}^2(k)) = \{F/G \mid F, G \in k[X, Y, Z] \text{ vormen van dezelfde graad}\}$$

via (5.6), dan stemt F_* overeen met de F_* die we vroeger definieerden.
Als $m_P(F) = 1$, dan is $\mathcal{O}_P(F)$ een DVR, en we noteren ord_P^F voor de bijhorende valuatie op $k(F)$.
Voor twee projectieve vlakke krommen F en G en $P \in \mathbb{P}^2(k)$ definiëren we het intersectiegetal

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{P}^2(k))/(F_*, G_*))$$

Deze definitie is onafhankelijk van de keuze van de rechte L (die niet door P mag gaan, en de eigenschappen van het intersectiegetal uit § 4.3 blijven geldig, als we **A3** en **A7** als volgt aanpassen. In **A3** laten we ook projectieve coördinaatsveranderingen toe.
A7 wordt: $I(P, F \cap G) = I(P, F \cap (G + AF))$ als A, F en G vormen zijn met $\deg(A) = \deg(G) - \deg(F)$.

Definitie 6.1.1 *Een rechte L raakt aan de kromme F in het punt P als*

$$I(P, F \cap L) > m_P(F)$$

We noemen P een gewoon meervoudig punt op F als F in P $m_P(F)$ verschillende raaklijnen heeft. Twee krommen F en G worden projectief equivalent genoemd als er een projectieve verandering van coördinaten T bestaat zodat $G = F^T$.

6.2 Lineaire systemen van krommen

De bedoeling is om projectieve krommen van een gegeven graad $d \geq 1$ te bestuderen. Een projectieve kromme van graad d wordt gegeven door een vorm van graad d. Zulk een vorm is op unieke wijze te schrijven als een lineaire combinatie van monomen $X^i Y^j Z^k$ van graad d. Het totaal aantal monomen van graad d is

$$N = \frac{(d+1)(d+2)}{2} = \binom{d+2}{2}$$

Schrijf $M_1, \cdots, M_N$ voor deze N monomen. Een vorm F van graad d is dan te schrijven als

$$F = \sum_{i=1}^{N} a_i M_i$$

Omdat F en λF dezelfde vlakke kromme bepalen, hebben we daarom een bijectie van de verzameling van de krommen van graad d naar $\mathbb{P}^{N-1}(k)$, door $F = \sum_{i=1}^{N} a_i M_i$ af te beelden op

het punten met coördinaten $(a_1, \cdots, a_N)$. We identificeren F met het overeenstemmend punt in $\mathbb{P}^{N-1}(k) = \mathbb{P}^{d(d+3)/2}(k)$. Zo vinden we

$$\begin{aligned} \text{krommen van graad } d = 1 &\cong \mathbb{P}^2(k) \\ \text{krommen van graad } d = 2 &\cong \mathbb{P}^5(k) \\ \text{krommen van graad } d = 3 &\cong \mathbb{P}^9(k) \\ \text{krommen van graad } d = 4 &\cong \mathbb{P}^{14}(k) \end{aligned}$$

Een *lineair systeem van krommen* is per definitie een lineaire deelvariëteit van $\mathbb{P}^{N-1}(k)$.

Lemma 6.2.1 *Neem $P \in \mathbb{P}^2(k)$. De verzameling van de krommen van graad d die P bevatten vormen een hypervlak in $\mathbb{P}^{N-1}(k)$.*

Bewijs. $P = (x, y, z)$ ligt op de kromme $F = \sum a_i M_i$ als en alleen als

$$\sum_{i=1}^{N} a_i M_i(x, y, z) = 0 \tag{6.1}$$

Aangezien niet alle $M_i(x, y, z) = 0$ (anders is $x = y = z = 0$), bepaalt (6.1) een hypervlak in $\mathbb{P}^{N-1}(k)$. □

Lemma 6.2.2 *Neem een projectieve verandering van coördinaten $T : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$. De afbeelding $F \mapsto F^T$ bepaalt dan een projectieve verandering van coördinaten in $\mathbb{P}^{N-1}(k)$.*

Bewijs. Schrijf

$$M_i^T = \sum_{j=1}^{N} b_{ij} M_j$$

Dan is, voor $F = \sum_{i=1}^{N} a_i M_i$,

$$F^T = \sum_{j=1}^{N} (\sum_{i=1}^{N} a_i b_{ij}) M_j$$

en de afbeelding $F \to F^T$ is de lineaire afbeelding die bepaald wordt door de matrix met elementen b_{ij}. De inverse afbeelding is de afbeelding die F afbeeldt op $F^{T^{-1}}$. □

Om te besluiten geven we een eenvoudige meetkundige toepassing: de verzameling van alle krommen van graad d die een gegeven stel punten bevat, is een doorsnede van hypervlakken in $\mathbb{P}^{N-1}(k)$ en dus een lineaire variëteit in $\mathbb{P}^{N-1}(k)$.
In $\mathbb{P}^{N-1}(k)$ is de doorsnede van $N - 1$ hypervlakken nooit leeg (immers, we hebben een lineair stelsel van $N - 1$ homogene vergelijkingen in N veranderlijken op te lossen, en er is steeds een oplossing verschillend van nul).
We kunnen dus besluiten dat door $d(d + 3)/2$ gegeven punten in het projectieve vlak minstens één kromme van graad d gaat.
Door 2 gegeven punten loopt er steeds een rechte.
Door 5 gegeven punten loopt er steeds een kegelsnede.

6.3 De stelling van Bezout

Lemma 6.3.1 *F, G, H zijn vormen in $k[X, Y, Z]$. We onderstellen dat F en G geen gemeenschappelijke factoren hebben, en geen snijpunten op oneindig. Als er vormen A en B bestaan zodat*

$$ZH = AF + BG$$

dan bestaan er ook vormen A' en B' zodat

$$H = A'F + B'G$$

Anders geformuleerd, de afbeelding

$$\alpha : \ k[X, Y, Z]/(F, G) \to k[X, Y, Z]/(F, G) : \ [H] \mapsto [ZH]$$

is injectief.

Bewijs. Voor $J(X, Y, Z) \in k[X, Y, Z]$ schrijven we

$$J_0(X, Y) = J(X, Y, 0)$$

F en G hebben geen snijpunten op oneindig, en dus hebben F, G en Z geen gemeenschappelijke nulpunten.
F_0 en G_0 zijn vormen in $k[X, Y]$, en zijn dus te schrijven als producten van lineaire vormen (we onderstellen nog steeds dat k algebraisch gesloten is). Indien $aX + bY$ een gemene factor is van F_0 en G_0, dan is $(b, -a, 0)$ een gemeenschappelijk nulpunt van F, G en Z, en dit kan niet. F_0 en G_0 zijn dus relatief priem in $k[X, Y]$.
Uit $ZH = AF + BG$ volgt $A_0F_0 + B_0G_0 = 0$, en dus bestaat er een $C \in k[X, Y]$ zodat

$$B_0 = F_0C \ \text{ en } \ A_0 = -G_0C$$

Schrijf nu

$$A_1 = A + CG \ \text{ en } \ B_1 = B - CF$$

Dan is

$$(A_1)_0 = (B_1)_0 = 0$$

en dus

$$A_1 = ZA' \ \text{ en } \ B_1 = ZB'$$

waarbij $A', B' \in k[X, Y, Z]$. We rekenen nu gemakkelijk uit dat

$$\begin{aligned} ZH &= AF + BG \\ &= (A_1 - CG)F + (B_1 + CF)G \\ &= Z(A'F + B'G) \end{aligned}$$

en dus $H = A'F + B'G$. We weten niet of A' en B' wel vormen zijn. Stel $s = \deg(H) - \deg(F)$ en $t = \deg(H) - \deg(G)$, en neem in beide leden het homogene stuk van graad $\deg(H)$. Dan vinden we

$$H = A'_sF + B'_tG$$

en dit bewijst onze stelling. □

Stelling 6.3.2 (Bezout)
Neem twee projectieve vlakke krommen F en G, waarbij $\deg(F) = m$ en $\deg(G) = n$. Onderstel dat F en G geen gemeenschappelijke componenten hebben. Dan is

$$\sum_P I(P, F \cap G) = mn$$

warbij P loopt over alle snijpunten P van F en G.

Bewijs. $F \cap G$ is eindig. Er is dus een rechte die door geen enkel van de snijpunten gaat. Door een projectieve coördinatentransformatie leggen we deze rechte op oneindig. We kunnen dus onderstellen dat F en G geen snijpunten hebben op oneindig, en, gebruik makend van eigenschap **A9** van intersectiegetallen

$$\sum_P I(P, F \cap G) = \sum_P I(P, F_* \cap G_*) = \dim_k(k[X, Y]/(F_*, G_*)$$

Stel nu

$$\begin{aligned} \Gamma &= k[X, Y, Z]/(F, G) \\ \Gamma_* &= k[X, Y]/(F_*, G_*) \\ R &= k[X, Y, Z] \end{aligned}$$

We schrijven Γ_d en R_d voor de verzameling van alle vormen van graad d in Γ en R.
We zullen bewijzen dat

$$\dim_k(\Gamma_*) = \dim_k(\Gamma_d) = mn$$

zodra d voldoende groot.
Stap 1: $d \geq m + n \implies \dim_k(\Gamma_d) = mn$.
Bekijk de volgende afbeeldingen:

$$\begin{aligned} \pi: &\quad R \to \Gamma: \ A \mapsto [A] \\ \varphi: &\quad R \times R \to R: \ (A, B) \mapsto AF + BG \\ \psi: &\quad R \to R \times R: \ C \mapsto (GC, -FC) \end{aligned}$$

We hebben dan een exacte rij

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0 \tag{6.2}$$

Het is duidelijk dat ψ injectief is, en π surjectief.
Verder is $(\varphi \circ \psi)(C) = GCF - FCG = 0$, zodat $\mathrm{Im}\,(\psi) \subset \mathrm{Ker}\,(\pi)$. We bewijzen de omgekeerde inclusie: onderstel dat

$$\varphi(A, B) = AF + BG = 0, \ \text{ of } \ AF = -BG$$

Stel C gelijk aan de grootste gemene deler van A en B, en $A = CA'$, $B = CB'$. Dan is

$$A'F = -B'G$$

Elke irreducibele component van B' is deler van $A'F$, en dus van F. Daarom is B' een deler van F, en kunnen we schrijven dat $F = B'B''$. Op dezelfde manier vinden we $G = A'A''$. Maar dan is

$$A'B'B'' = -B'A'A'', \text{ en dus } B'' = -A''$$

een gemene component van F en G. Omdat F en G geen gemene componenten hebben, is $B'' = -A'' = -a \in k$, en

$$A = CA' = \frac{CG}{a} \text{ en } B = CB' = -\frac{CF}{a}$$

en tenslotte

$$(A, B) = \psi\Big(\frac{C}{a}\Big) \in \mathrm{Im}\,(\psi)$$

De exactheid in R is duidelijk: $(\pi \circ \varphi)(A, B) = [AF + BG] = 0$ in Γ, en als $\pi(H) = [H] = 0$ in Γ, Dan is $H \in (F, G)$, en $H = AF + BG \in \mathrm{Im}\,(\varphi)$.
Als $d \geq m + n$, dan beperken $\psi,\ \varphi$ en π zich tot afbeeldingen

$$\begin{array}{ll} \pi: & R_d \to \Gamma_d \\ \varphi: & R_{d-m} \times R_{d-n} \to R_d \\ \psi: & R_{d-n-m} \to R_{d-m} \times R_{d-n} \end{array}$$

en we vinden een nieuwe exacte rij

$$0 \longrightarrow R_{d-n-m} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0 \tag{6.3}$$

en we vinden met behulp van de dimensieformule

$$\begin{array}{rcl} \dim_k(\Gamma_d) & = & \dim_k(R_d) - \dim_k(R_{d-m} \times R_{d-n}) + \dim_k(R_{d-n-m}) \\ & = & \dfrac{(d+1)(d+2)}{2} - \dfrac{(d-m+1)(d-m+2)}{2} - \dfrac{(d-n+1)(d-n+2)}{2} \\ & + & \dfrac{(d-m-n+1)(d-m-n+2)}{2} = mn \end{array}$$

Stap 2: neem weer $d \geq m + n$. We weten uit stap 1 dat $\dim_k(\Gamma_d) = mn$. We kiezen vormen $A_1, \cdots, A_{mn} \in k[X, Y, Z]$ zodanig dat

$$\{[A_1], \cdots, [A_{mn}]\}$$

een basis is voor Γ_d. Stel nu

$$a_i = [A_{i*}] \in \Gamma_* = k[X, Y]/(F_*, G_*)$$

Onze stelling is bewezen als we kunnen aantonen dat

$$\{a_1, \cdots, a_{mn}\}$$

een basis is voor Γ_*.
We bekijken opnieuw het monomorfisme

$$\alpha:\ \Gamma = k[X, Y, Z]/(F, G) \to \Gamma = k[X, Y, Z]/(F, G):\ [H] \mapsto [ZH]$$

uit lemma 6.3.1. Deze beperkt zich tot een monomorfisme

$$\alpha : \Gamma_d \to \Gamma_{d+1}$$

Omdat Γ_d en Γ_{d+1} beiden dimensie mn hebben, is dit monomorfisme automatisch ook surjectief, en dus een isomorfisme. We kunnen hieruit concluderen dat

$$\{[Z^r A_1], \cdots, [Z^r A_{mn}]\}$$

een basis is voor Γ_{d+r}, en dit voor elke $r \geq 0$.
a $\{a_1, \cdots, a_{mn}\}$ is een voortbrengend stel.
Neem $h = [H] \in \Gamma_*$. Voor N voldoende groot is $Z^N H^*$ een vorm van graad $d + r$, en dus kunnen we schrijven

$$Z^N H^* = \sum_{i=1}^{mn} \lambda_i Z^r A_i + BF + CG$$

waarbij $\lambda_i \in k$, en $B, C \in k[X, Y, Z]$ vormen. Hieruit volgt dat

$$H = (Z^N H^*)_* = \sum_{i=1}^{mn} \lambda_i (A_i)_* + B_* F_* + C_* G_*$$

en

$$h = \sum_{i=1}^{mn} \lambda_i a_i$$

b $\{a_1, \cdots, a_{mn}\}$ is lineair onafhankelijk.
Onderstel

$$\sum_{i=1}^{mn} \lambda_i a_i = 0$$

of

$$\sum_{i=1}^{mn} \lambda_i (A_i)_* = BF_* + CG_*$$

Omdat de A_i allen vormen van dezelfde graad zijn, vinden we

$$\sum_{i=1}^{mn} \lambda_i A_i = (\sum_{i=1}^{mn} \lambda_i (A_i)_*)^* = (BF_* + CG_*)^*$$

Er bestaan $r, s, t \in \mathbb{N}$ zodat (zie (1.8)):

$$Z^r (BF_* + CG_*)^* = Z^s (BF_*)^* + Z^t (CG_*)^*$$

Omdat F en G geen componenten op oneindig hebben (en dus niet deelbaar zijn door Z) is $(F_*)^* = F$ en $(G_*)^* = G$. We krijgen dus

$$Z^r \sum_{i=1}^{mn} \lambda_i A_i = Z^s B^* F + Z^t C^* G$$

en dit betekent dat

$$\sum_{i=1}^{mn} \lambda_i [Z^r A_i] = 0 \text{ in } \Gamma_{d+r}$$

en hieruit volgt dat $\lambda_i = 0$, voor elke i. □

We formuleren enkele onmiddellijke meetkundige gevolgen.

Gevolg 6.3.3 *F en G zijn twee projectieve vlakke krommen zonder gemeenschappelijke componenten.*

$$\sum_P m_P(F) m_P(G) \leq \deg(F)\deg(G)$$

Bewijs. Dit volgt onmiddellijk door de stelling van Bezout te combineren met eigenschap **A5** van intersectiegetallen. □

Gevolg 6.3.4 *Als twee projectieve vlakke krommen van graad respectievelijk m en n juist mn snijpunten hebben, dan zijn dit allemaal enkelvoudige snijpunten, en alle intersectiegetallen zijn gelijk aan* 1.

Gevolg 6.3.5 *Als twee projectieve vlakke krommen van graad respectievelijk m en n meer dan mn punten gemeen hebben, dan hebben ze een gemene component.*

6.4 Grondstelling van Max Noether

Een "zero cycle" op $\mathbb{P}^2(k)$ is per definitie een som van de vorm

$$\sum_{P \in \mathbb{P}^2(k)} n_P P$$

waarbij $n_P \in \mathbb{Z}$, en waarbij we onderstellen dat alle $n_P = 0$, op een eindig aantal na. De verzameling van alle "zero cycles"vormen een abelse groep voor de optelling, dit is in feite de *vrije abelse groep* op $\mathbb{P}^2(k)$. De graad van een "zero cycle"wordt gedefinieerd door de formule

$$\deg(\sum_{P \in \mathbb{P}^2(k)} n_P P) = \sum_{P \in \mathbb{P}^2(k)} n_P$$

Verder stellen we

$$\sum_{P \in \mathbb{P}^2(k)} n_P P \leq \sum_{P \in \mathbb{P}^2(k)} m_P P \iff n_P \leq m_P, \ \forall P \in \mathbb{P}^2(k)$$

Als $\sum_{P \in \mathbb{P}^2(k)} n_P P \geq 0$, dan zeggen we dat de "zero cycle"positief is.
Voor twee projectieve vlakke krommen F en G zonder gemene componenten voeren we nu volgende notatie in

$$F \cdot G = \sum_{P \in \mathbb{P}^2(k)} I(P, F \cap G) P \tag{6.4}$$

(6.4) laat toe om sommige van de eigenschappen van intersectiegetallen bondig te herformuleren, bijvoorbeeld

$$\deg(F \cdot G) = \deg(F)\deg(G) \ \text{(Bezout)}$$
$$F \cdot G = G \cdot F$$
$$F \cdot (GH) = F \cdot G + F \cdot H$$
$$F \cdot (G + AF) = F \cdot G$$

Het probleem dat we in deze paragraaf willen bespreken is het volgende: onderstel dat drie projectieve vlakke krommen $F,\ G,\ H$ gegeven zijn zodat

$$H \cdot F \geq G \cdot F$$

Kunnen we een kromme B vinden zodat

$$H \cdot F - G \cdot F = B \cdot F \ ?$$

Als dit het geval is, dan hebben we door de stelling van Bezout dat

$$\deg(H)\deg(F) - \deg(G)\deg(F) = \deg(B)\deg(F)$$

en

$$\deg(H) - \deg(G) = \deg(B)$$

Het probleem is opgelost als we krommen A en B vinden zodat

$$H = AF + BG$$

want dan is

$$H \cdot F = (AF + BG) \cdot F = (BG) \cdot F = B \cdot F + G \cdot F$$

Definitie 6.4.1 *Onderstel dat $F,\ G$ en H vlakke krommen zijn, en dat F en G geen gemene componenten hebben. We zeggen dat de voorwaarde van Noether voldaan is in een punt P ten opzichte van de krommen $F,\ G$ en H als H_* ligt in het ideaal van $\mathcal{O}_P(\mathbb{P}^2(k))$ voortgebracht door F_* en G_*:*

$$H_* \in (F_*, G_*) \subset \mathcal{O}_P(\mathbb{P}^2(k))$$

Dit betekent dat er $a, b \in \mathcal{O}_P(\mathbb{P}^2(k))$ bestaan zodat

$$H_* = aF_* + bG_*$$

Merk op dat aan de voorwaarde van Noether automatisch voldaan is als P geen snijpunt is van F en G. Immers, als P niet op de kromme F gelegen is, dan is $F(P) \neq 0$, en dan is F_* inverteerbaar in $\mathcal{O}_P(\mathbb{P}^2(k))$, en dan is $(F_*, G_*) = \mathcal{O}_P(\mathbb{P}^2(k))$. De voorwaarde is dus enkel relevant in de snijpunten. De grondstelling van Max Noether kan beschouwd worden als een locaal-globaal eigenschap:

Stelling 6.4.2 (grondstelling van Max Noether)
Onderstel dat $F,\ G$ en H vlakke krommen zijn, en dat F en G geen gemene componenten hebben. Er bestaan krommen A en B zodat

$$H = AF + BG$$

als en alleen als de voorwaarde van Noether voldaan is in elk snijpunt P van F en G.

Bewijs. Een implicatie is triviaal: als $H = AF + BG$, dan geldt voor elke $P \in \mathbb{P}^2(k)$ dat

$$H_* = A_*F_* + B_*G_* \in (F_*, G_*)$$

Omgekeerd, onderstel dat in elk snijpunt P aan de voorwaarde van Noether voldaan is. Door een projectieve verandering van coördinaten kunnen we onderstellen dat geen enkel van de snijpunten van F en G op oneindig ligt. We kunnen dan schrijven

$$F_* = F(X, Y, 1) \ ; \ G_* = G(X, Y, 1) \ ; \ H_* = H(X, Y, 1)$$

Uit de voorwaarde van Noether volgt dat

$$[H_*] = 0 \text{ in } \mathcal{O}_P(\mathbb{P}^2(k))/(F_*, G_*)$$

Uit stelling 3.3.7 (over idealen met een eindig aantal nulpunten) weten we

$$k[X, Y]/(F_*, G_*) \cong \prod_P \mathcal{O}_P(\mathbb{P}^2(k))/(F_*, G_*)$$

en hieruit volgt dat

$$[H_*] = 0 \text{ in } k[X, Y]/(F_*, G_*)$$

en er bestaan dus $a, b \in k[X, Y]$ zodat

$$H_* = aF_* + bG_*$$

Gebruik makend van (1.8) vinden we $r, s, t \in \mathbb{N}$ zodat

$$Z^t(H_*)^* = Z^r a^*(F_*)^* + Z^s b^*(G_*)^* \tag{6.5}$$

Uit (1.6) weten we dat er een natuurlijk getal m bestaat zodat $Z^m(H_*)^* = H$, en analoge eigenschappen gelden voor F en G. Als we (6.5) vermenigvuldigen met een geschikte macht van Z, dan vinden we dus $A, B \in k[X, Y, Z]$ en $r \in \mathbb{N}$ zodat

$$Z^r H = AF + BG$$

Pas nu lemma 6.3.1 r maal toe. Dit levert vormen $A', B' \in k[X, Y, Z]$ zodat

$$H = A'F + B'G$$

□

In de volgende stelling geven we voldoende voorwaarden opdat de voorwaarde van Noether voldaan zou zijn.

Stelling 6.4.3 *Onderstel F, G en H als in vorige stelling, en neem een snijpunt P van F en G. In elk van de volgende gevallen is in P voldaan aan de voorwaarde van Noether:*
1) F en G snijden transversaal in P (dit betekent dat $I(P, F \cap G) = 1$, of, equivalent, dat P een enkelvoudig punt is van F en G en dat de raaklijnen aan F en G in P verschillend zijn), en P ligt

op H.
2) P is een enkelvoudig punt op F, en

$$I(P, H \cap F) \geq I(P, G \cap F)$$

3) F en G hebben verschillende raaklijnen in P en

$$m_P(H) \geq m_P(F) + m_P(G) - 1$$

Bewijs. 2) Omdat P een enkelvoudig punt is op F, ligt P maar op een irreducibele component van F. De andere componenten kunnen we weglaten, want die spelen geen rol bij de berekening van intersectiegetallen in P. We kunnen dus onderstellen dat F irreducibel is.
Uit eigenschap **A8** van intersectiegetallen weten we

$$\mathrm{ord}_P^F(H) = I(P, H \cap F) \geq I(P, G \cap F) = \mathrm{ord}_P^F(G)$$

Dit kunnen we als volgt herschrijven: neem een uniformiserend element van de DVR $\mathcal{O}_P(F)$. We hebben

$$[G_*] = ut^n \text{ en } [H_*] = vt^m$$

waarbij $u, v \in \mathcal{O}_P(F)$ inverteerbaar, en $n \leq m$. Hieruit volgt dat $[H_*] \in ([G_*]) \subset \mathcal{O}_P(F)$, en

$$[H_*] = 0 \text{ in } \mathcal{O}_P(F)/([G_*]) \cong \mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)$$

en dit is juist de voorwaarde van Noether.
3) Na een projectieve coördinatentransformatie kunnen we ervoor zorgen dat $P = (0, 0, 1)$. Uit eigenschap **A5** van intersectiegetallen volgt

$$I(P, F \cap G) = m_P(F) m_P(G)$$

Stel $m = m_P(F) = m_P(F_*)$ en $n = m_P(G) = m_P(G_*)$. Omdat $m_P(H_*) \geq m + n - 1$, hebben we dat $H_* \in I^{m+n-1}$, waarbij $I = (X, Y)$. Een van de stappen in het bewijs van eigenschap **A5** van intersectiegetallen bestond erin om te bewijzen dat

$$I^t \subset (F_*, G_*) \subset \mathcal{O}_P(\mathbb{P}^2)$$

zodra $t \geq m + n - 1$. Dit hebben we hier ook, en in het bijzonder volgt dat $H_* \in (F_*, G_*) \subset \mathcal{O}_P(\mathbb{P}^2)$. Dit is weer de voorwaarde van Noether.
1) is een speciaal geval van zowel 2) als 3). □

Gevolg 6.4.4 *Onderstel dat F, G en H zijn zoals in de voorgaande stellingen, en dat aan een van de twee volgende eigenschappen voldaan is:*
1) F en G snijden elkaar in $\deg(F)\deg(G)$ verschillende punten, en H gaat door al die snijpunten;
2) alle snijpunten van F en G zijn enkelvoudige punten op F, en $H \cdot F \geq G \cdot F$.
Dan bestaat er een kromme B zodat

$$B \cdot F = H \cdot F - G \cdot F$$

Bewijs. 1) Uit gevolg 6.3.4 volgt dat $I(P, F \cap G) = 1$, voor elk snijpunt P van F en G. Omdat elk snijpunt P ook op H ligt, kunnen we uit voorwaarde 1) van stelling 6.4.3 besluiten dat de voorwaarde van Noether geldt in elk snijpunt P, en het gewenste besluit volgt uit de grondstelling van Noether.
2) Aan voorwaarde 2) van stelling 6.4.3 is voldaan in elk snijpunt P, en dus is de voorwaarde van Noether geldig in elk snijpunt. We passen weer de grondstelling toe. □

6.5 Enkele meetkundige toepassingen

Stelling 6.5.1 *Neem twee projectieve krommen C en C' van graad 3, en een kegelsnede Q (Q is dus van graad 2). Onderstel*

$$C \cdot C' = \sum_{i=1}^{9} P_i$$

(zie de stelling van Bezout), en onderstel dat $P_1, \cdots, P_6$ enkelvoudige punten zijn op de kromme C. De P_i hoeven niet noodzakelijk te verschillen. Als bovendien

$$Q \cdot C = \sum_{i=1}^{6} P_i$$

dan liggen P_7, P_8 en P_9 op een rechte.

Bewijs. Alle snijpunten van C en Q zijn enkelvoudige punten op C, en

$$C \cdot C' = \sum_{i=1}^{9} P_i \geq \sum_{i=1}^{6} P_i = Q \cdot C$$

We kunnen dus deel 2) van gevolg 6.4.4 toepassen, met F, G en H vervangen door C, Q en C', en we vinden een kromme B van graad 1 (dus een rechte) zodat

$$B \cdot C = C \cdot C' - Q \cdot C = P_7 + P_8 + P_9$$

P_7, P_8 en P_9 liggen dus op de rechte B. □

Gevolg 6.5.2 (Pascal)
Als we een zeshoek inschrijven in een irreducibele kegelsnede, dan snijden de tegenoverliggende zijden elkaar in collineaire punten.

Gevolg 6.5.3 (Pappus)
Neem twee niet-samenvallende rechten L_1 en L_2, en punten P_1, P_2, P_3 op L_1 en Q_1, Q_2, Q_3 op L_2, waarbij geen van de punten op het snijpunt van L_1 en L_2 ligt. L_{ij} is de rechte die P_i en Q_j verbindt, en $R_k = L_{ij} \cdot L_{ji}$ (met $\{i, j, k\} = \{1, 2, 3\}$). Dan zijn R_1, R_2 en R_3 collineair.

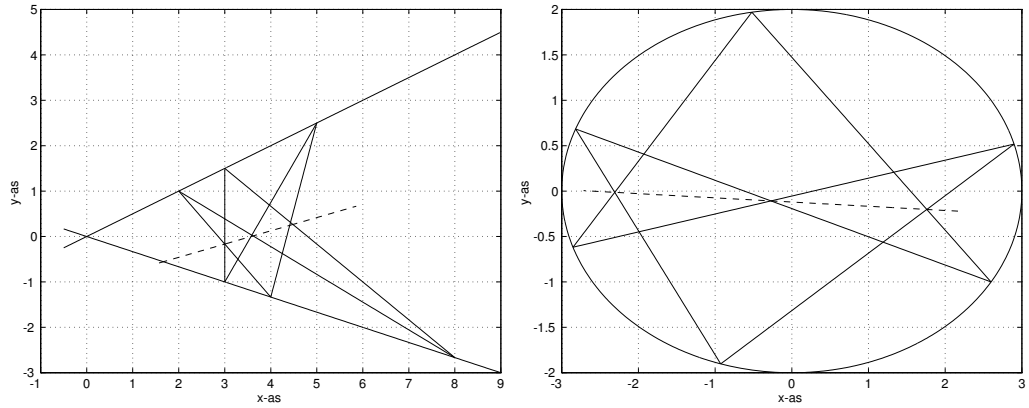
Bewijs. Stel $Q = L_1L_2$, $C = L_{12}L_{23}L_{31}$ en $C' = L_{21}L_{13}L_{32}$. Dan is

$$C \cdot C' = P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3 + R_1 + R_2 + R_3$$

en

$$C \cdot Q = P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3$$

en de stelling van Pappus volgt onmiddellijk uit stelling 6.5.1. Pascal volgt op analoge manier, maar we nemen voor Q een irreducibele kegelsnede in plaats van twee niet-samenvallende rechten. □



Figuur 6.1: De stellingen van Pappus en Pascal

Stelling 6.5.4 *Neem derdegraadskrommen C, C' en C''. We onderstellen dat C regulier is. Als*

$$C' \cdot C = \sum_{i=1}^{9} P_i$$

en

$$C'' \cdot C = \sum_{i=1}^{8} P_i + Q$$

waarbij de P_i enkelvoudige punten zijn op C, maar niet noodzakelijk van elkaar verschillend, dan is

$$P_9 = Q$$

Bewijs. Onderstel dat $P_9 \neq Q$. Dan bestaat er een rechte L die door P_9 gaat, maar niet door Q. Uit de stelling van Bezout volgt:

$$L \cdot C = P_9 + R + S$$

We becijferen gemakkelijk dat

$$\begin{aligned} LC'' \cdot C &= L \cdot C + C'' \cdot C \\ &= P_9 + R + S + \sum_{i=1}^{8} P_i + Q \\ &= C' \cdot C + Q + R + S \end{aligned}$$

en dus

$$LC'' \cdot C - C' \cdot C = Q + R + S$$

Neem $F = C$, $G = C'$ en $H = LC''$ in de grondstelling van Noether. Aan de tweede voorwaarde van gevolg 6.4.4 is voldaan, en dus vinden we een rechte L' zodat

$$L' \cdot C = LC'' \cdot C - C' \cdot C = Q + R + S$$

De rechten L en L' gaan allebei door R en S, en zijn dus aan elkaar gelijk. Bijgevolg ligt Q op L. Dit is strijdig met onze onderstelling, en dus moet $P_9 = Q$. □

Stelling 6.5.4 laat toe om op een reguliere kromme C van graad 3 een abelse groepsstructuur te definiëren. Neem $P, Q \in C$. Als $P \neq Q$, dan stellen we L de rechte die P en Q verbindt. Als $P = Q$, dan nemen we voor L de unieke raaklijn aan C in P. Gebruik makend van de stelling van Bezout vinden we

$$L \cdot C = P + Q + R$$

en we definiëren $\varphi : \ C \times C \to C$ door

$$\varphi(P, Q) = R$$

We fixeren een vast punt O op C, en definiëren

$$P \oplus Q = \varphi(0, \varphi(P, Q)) \tag{6.6}$$

Stelling 6.5.5 *Neem een reguliere kromme C van graad 3. Dan is $C, \oplus$ een abelse groep, met neutraal element O.*

Bewijs. De associativiteit is het moeilijkste om te bewijzen. Neem $P, Q, R \in C$, en rechten L_i en M_i zodat

$$\begin{aligned}
L_1 \cdot C &= P + Q + S' \\
M_1 \cdot C &= O + S' + S \\
L_2 \cdot C &= S + R + T' \\
M_2 \cdot C &= Q + R + U' \\
L_3 \cdot C &= O + U' + U \\
M_3 \cdot C &= P + U + T''
\end{aligned}$$

Uit de eerste twee vergelijkingen volgt dat $P \oplus Q = S$, en uit de derde dat $(P \oplus Q) \oplus R = S \oplus R = \varphi(O, T')$.
De vierde en vijfde vergelijking geven $Q \oplus R = U$, en uit de zesde volgt dat $P \oplus (Q \oplus R) = P \oplus U = \varphi(O, T'')$.
Het volstaat dus om aan te tonen dat $T' = T''$. We stellen $C' = L_1 L_2 L_3$ en $C'' = M_1 M_2 M_3$. Dan is

$$\begin{aligned}
C' \cdot C &= (L_1 L_2 L_3) \cdot C \\
&= L_1 \cdot C + L_2 \cdot C + L_3 \cdot C \\
&= P + Q + S' + S + R + T' + O + U' + U
\end{aligned}$$

en

$$\begin{aligned} C'' \cdot C &= (M_1 M_2 M_3) \cdot C \\ &= M_1 \cdot C + M_2 \cdot C + M_3 \cdot C \\ &= O + S' + S + Q + R + U' + P + U + T'' \end{aligned}$$

en uit stelling 6.5.4 volgt dat $T' = T''$.
We tonen nu aan dat O het neutraal element is. Neem $P \in C$, en onderstel dat $\varphi(O, P) = R$. Dit betekent dat er een rechte L_1 is zodat

$$L_1 \cdot C = O + P + R$$

Dit laatste betekent echter ook dat $\varphi(O, R) = P$, en dus

$$O \oplus P = \varphi(O, R) = P$$

We zoeken nu het tegengestelde element van P:
$P \oplus Q = \varphi(O, \varphi(P, Q)) = O$ als en alleen als de rechte die O en $\varphi(P, Q)$ verbindt aan C raakt in O. Dit is ook nog equivalent met te zeggen

$$\varphi(O, O) = \varphi(P, Q)$$

of met

$$Q = \varphi(P, \varphi(O, O))$$

en hiermee is het tegengestelde element gevonden. De commutativiteit is evident. □

6.6 Oefeningen

Oefening 6.1 $F \subset \mathbb{P}^2$ vlakke kromme.
$P \in \mathbb{P}^2$ meervoudig punt van $F \Leftrightarrow F_X(P) = F_Y(P) = F_Z(P) = 0$

Oefening 6.2 $F \subset \mathbb{P}^2, P \in F$ glad punt.
De raaklijn in P aan F is

$$XF_X(P) + YF_Y(P) + ZF_Z(P)$$

Oefening 6.3 Toon aan dat de volgende krommen irreducibel zijn. Zoek ook de meervoudige punten, met hun multipliciteiten en raaklijnen.

1. $XY^4 + YZ^4 + XZ^4$.
2. $X^n + Y^n + Z^n, n > 0$.

Oefening 6.4 Zoek alle snijpunten, en de intersectiegetallen in deze snijpunten, van de volgende paren van krommen.

1. $Y^2Z - X(X-2Z)(X+Z)$ en $Y^2 + X^2 - 2XZ$.
2. $(X^2+Y^2)Z + X^3 + Y^3$ en $X^3 + Y^3 - 2XYZ$.

Oefening 6.5 Voor elke F en $P \in F$, toon aan

$$m_P(F_X) \geq m_P(F) - 1$$

Oefening 6.6 Twee vlakke krommen F, F' heten projectief equivalent als er een projectieve coördinatentransformatie $T : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$ bestaat zodat $F' = F^T$. Toon aan dat elke irreducibele kegelsnede projectief equivalent is met $X^2 + YZ$. Classificeer de tweedegraadskrommen.

Oefening 6.7 Classificeer de derdegraadskrommen.

Oefening 6.8 Zij F een projectieve vlakke kromme van graad n met c enkelvoudige componenten en geen meervoudige componenten. Toon aan dat

$$\sum_P \frac{m_P(F)(m_P(F)-1)}{2} \leq \frac{(n-1)(n-2)}{2} + c - 1 \leq \frac{n(n-1)}{2}$$

Oefening 6.9 Zij F een irreducibele projectieve vlakke kromme en veronderstel dat $z \in k(F)$ overal gedefinieerd is. Toon aan dat $z \in k$.

Index

affiene n-dimensionale ruimte 23
affiene coördinatentransformatie 53
affiene variëteit 38
affiene vlakke kromme 23
algebra 3
algebraisch element 15
algebraische verzameling 24
Chinese reststelling 18
comaximale idealen 17
complex 18
discrete valuatiering 10
dubbele raaklijn 59
dubbelpunt 59
DVR 10
eindig voortgebracht moduul 12
eindig voortgebrachte algebra 13
eindige lichaamsuitbreiding 13
enkelvoudig punt 58
enkelvoudige raaklijn 59
exacte rij 18
formule van Euler 7
formule van Taylor 7
functielichaam 43
functielichaam 88
gewoon meervoudig punt 59
Hilbert basis stelling 10
homogeen functielichaam 87
homogeen ideaal 79
homogene coördinaten 77
homogene coördinatenring 87
homogene veelterm 4
hoofdideaaldomein 9
hyperoppervlak 23, 25
hypervlak 23
hypervlak op oneindig 78
integraal element 13
integrale sluiting 14
intersectiegetal 63
irreducibel element 9
irreducibele algebraische verzameling 28
kettingregel 7
knooppunt 59
korte exacte rij 19
lineair systeem van krommen 94
meervoudig punt 59
monische veelterm 6
monoom 4
multipliciteit 59
Noetherse ring 10
partiële afgeleide 7
PID 9
poolverzameling 45
projectief vlak 78
projectieve algebraische verzameling 79
projectieve coördinatenverandering 89
projectieve rechte 78
projectieve ruimte 77
projectieve sluiting 86
projectieve variëteit 81
projectieve vlakke kromme 92
raaklijn 59
radicaal 27
radicaal ideaal 27
rechte 23
reducibele algebraische verzameling 28
reguliere kromme 59
singulier punt 59
transcendent element 15
trouwe functor 41
UFD 9
uniek factorizatie domein 9
uniformiserende parameter 12
veeltermafbeelding 38, 39
vermenigvuldigingsregel 7

volle functor 41
voltrouwe functor 41
vorm 4
vrije groep 99