Chapter 1

Affiene en Projectieve Variëteiten

0 Inleiding

0.1 Algebraïsche meetkunde

Algebraïsche meetkunde gaat over figuren gegeven door polynomische vergelijkingen; anders gezegd: over nulpuntsverzamelingen van stelsels polynomen in twee of meer onbepaalden.
De cirkel C met straal 2 gelegen in de ruimte in het vlak op hoogte 2 evenwijdig met het (x, y)-vlak kun je algebraïsch beschrijven als de verzameling van de punten (x, y, z) in de ruimte die aan de volgende twee vergelijkingen voldoen:

$$x^2 + y^2 - 4 = 0 \ , \ z - 2 = 0. \tag{1}$$

Dus C is de verzameling van de gemeenschappelijke nulpunten van de polynomen

$$X^2 + Y^2 - 4 \ , \ Z - 2.$$

De vergelijkingen (1) beschrijven C als de doorsnijding van de cirkelcylinder $x^2 + y^2 - 4 = 0$ en een vlak. Maar C kan evengoed worden weergegeven als de snijkromme van een bol met een vlak, b.v. door de simultane vergelijkingen

$$x^2 + y^2 + z^2 - 8 = 0 \ , \ z - 2 = 0. \tag{2}$$

Of ook door de vergelijkingen $x^2 + y^2 - 4 = 0$, $x^2 + y^2 - 2z = 0$; deze geven de cirkel als snijkromme van een cirkelcylinder en een omwentelingsparaboloïde.
Er is een meer neutrale manier om C te beschrijven: je geeft *alle* polynomische vergelijkingen waaraan z'n punten voldoen. Om hier greep op te krijgen constateren we eerst: als $f = f(X, Y, Z)$ en $g = g(X, Y, Z)$ polynomen zijn waarvan de waarden $f(x, y, z)$ en $g(x, y, z)$ identiek nul zijn op C, dan geldt hetzelfde voor $f - g$ en voor elk polynoom van de vorm $af = a(X, Y, Z)f(X, Y, Z)$. Dit betekent:

> de verzameling van alle polynomen waarvan de waarden identiek nul zijn op C is een ideaal in de ring van alle X, Y, Z-polynomen.

Dit ideaal nu, en niet een speciaal paar elementen ervan, is de uiteindelijke beschrijving van C. Elk polynoom dat uit de twee polynomen van de vergelijkingen (1) door lineaire combinatie (met *polynomen* als "scalairen"!) kan worden verkregen behoort tot dit ideaal. Omgekeerd kun je laten zien dat elke polynomische vergelijking $h(x, y, z) = 0$ welke een oppervlak dat door de kromme C gaat voorstelt, kan worden geschreven in de vorm $h = a(X, Y, Z) \cdot (X^2 + Y^2 - 4) + b(X, Y, Z) \cdot (Z - 2)$.

Dus het ideaal van alle polynomen die nul zijn op C is niets anders dan $(X^2+Y^2-4, Z-2)$, d.i. het ideaal voortgebracht door $f = X^2+Y^2-4$ en $g = Z-2$ in de polynoomring $\mathbb{R}[X,Y,Z]$.
De polynomen uit (2) genereren hetzelfde ideaal, want het zijn lineaire combinaties van f en g en omgekeerd zijn f en g lineaire combinaties van de polynoom uit (2). Het bij C behorend ideaal heeft dus verschillende "bases": $(X^2+Y^2-4, Z-2) = (X^2+Y^2+Z^2-8, Z-2) = (X^2+Y^2-4, X^2+Y^2-2Z) = \cdots$.
Een ander voorbeeld: Als t de verzameling $\mathbb{R}$ doorloopt, dan doorloopt het punt (t, t^2, t^3) een kromme in de ruimte $\mathbb{R}^3$, de zogeheten "twisted cubic", C_3. Het ideaal van deze kromme bestaat uit alle polynomen $f(X,Y,Z)$ die 0 worden wanneer voor X, Y, Z resp. $t, t^2 t^3$ wordt ingevuld. Dit zijn dus de polynomen die onder het homomorfisme

$$f \in \mathbb{R}[X,Y,Z] \mapsto f(T, T^2, T^3) \in \mathbb{R}[T]$$

in het nulpolynoom overgaan. Zoals gemakkelijk na te rekenen is vormen deze het ideaal M, voortgebracht door $Y - X^2$ en $Z - X^3$. Er geldt dat de factorring $\mathbb{R}[X,Y,Z]/M$ isomorf is met $\mathbb{R}[T]$. Deze factorring speelt in het algemeen bij het bestuderen van een kromme, oppervlak, etc. ("algebraïsche verzameling") een zeer belangrijke rol.
In dimensie n verstaat men onder een algebraïsche verzameling de verzameling Z van alle punten $(x_1, \cdots, x_n)$ die voldoen aan een gegeven (eindig) stelsel polynomische vergelijkingen

$$f_1(x_1, \cdots, x_n) = 0, \cdots, f_t(x_1, \cdots, x_n) = 0$$

De verzameling van alle polynomen die nul zijn op Z omvat in elk geval het ideaal $(f_1, \cdots, f_t)$, maar het kan groter zijn. Elk ideaal I in de ring van polynomen in de onbepaalden $X_1, \cdots, X_n$ bepaalt een verzameling Z, die uit alle punten $(x_1, \cdots, x_n)$ bestaat zodat $f(x_1, \cdots, x_n) = 0$ voor ieder polynoom $f \in I$. Hilbert's basisstelling zegt dat I door eindig veel polynomen wordt voortgebracht. Dus elk ideaal bepaalt een algebraïsche verzameling.

0.2 Eén vergelijking, één onbekende

We beginnen onze bestudering van algebraïsche verzamelingen met het eenvoudigste geval: *één vergelijking met één onbekende.*
Zij $f = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ een polynoom in één onbepaalde X. Hoe ziet de *nulpuntsverzameling* $Z(f)$[1] van f eruit? Het antwoord hangt nogal af van de ring R waarin de coëfficienten $a_0, \ldots, a_{d-1}$ van f liggen en waarin de nulpunten van f moeten liggen. Ter illustratie:

(i) $f = X^2 + 3$: als $R = \mathbb{R}$, dan $Z(f) = \emptyset$, als $R = \mathbb{C}$, dan $Z(f) = \{\pm i\sqrt{3}\}$.

(ii) $f = 3X^2 + 5$: als $R = \mathbb{Q}$, dan $Z(f) = \emptyset$, als $R = \mathbb{Z}/8\mathbb{Z}$, dan $Z(f) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

(iii) $f = X^2 + 1$, $R = \mathbb{H}$ (de quaternionen van Hamilton). Nu is $Z(f)$ een oneindige verzameling. Inderdaad, als $a, b, c \in \mathbb{R}$ voldoen aan $a^2 + b^2 + c^2 = 1$ dan voldoet $x = ai + bj + ck$ aan $x^2 = -1$.

Om algemene uitspraken te kunnen doen over het aantal nulpunten van een polynoom van graad n moeten we op z'n minst aannemen dat R commutatief is en geen nuldelers heeft, d.w.z. een domein is. Dan heeft zo'n polynoom hoogstens n nulpunten. Maar een domein is deelring van z'n quotientenlichaam en, zoals ieder lichaam, is dit bevat in een groter lichaam k dat algebraïsch gesloten is (d.w.z. dat elk polynoom $\neq 0$ over k minstens één nulpunt in k heeft). In het vervolg zullen we steeds over zo'n lichaam k werken, dus we nemen steeds aan:

[1] Z van 'zero'.

k is een commutatief lichaam dat algebraïsch gesloten is .

(een enkele maal zullen we $k = \mathbb{R}$ nemen, maar dat zullen we expliciet vermelden). Vaak zullen we $k = \mathbb{C}$ kiezen. In dat geval is $\mathrm{kar}(k)$, de karakteristiek van k, gelijk aan 0. Maar we laten ook lichamen toe met karakteristiek $p > 0$ (in dit geval is het priemlichaam van k isomorf met $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ en we schrijven $\mathbb{F}_p \subset k$).
Voor een (commutatief en algebraïsch gesloten) lichaam k geldt: elk niet-constant polynoom

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in k[X]$$

ontbindt in lineaire factoren, d.w.z.

$$f = (X - \alpha_1)^{n_1} \cdots (X - \alpha_t)^{n_t}$$

met $\alpha_1, \ldots, \alpha_t$ verschillende elementen van k en $n_1, \cdots, n_t \geq 1$. Dan is $Z(f) = \{\alpha_1, \ldots, \alpha_t\}$ en n_i heet de orde of multipliciteit van het nulpunt α_i. Natuurlijk is $n_1 + \cdots + n_t = n =$ graad van f.
Dank zij onze aanname over k is de situatie "één polynoom in één onbepaalde" duidelijk. We doen nu de voor de hand liggende stap: één polynoom met twee onbepaalden. Eerst herinneren we nog aan iets dat we dikwijls zullen gebruiken.

Een algebraïsch gesloten lichaam k is oneindig.

(bij elk n-tal elementen $\alpha_1, \ldots, \alpha_n \in k$ is immers wel een hiervan verschillend element van k te vinden, b.v. een nulpunt van $1 + (X - \alpha_1) \cdots (X - \alpha_n)$).

1 Vlakke affiene krommen.

1.1 Definities.

De *nulpuntsverzameling* van een polynoom

$$f = a_{00} + a_{10}X_1 + a_{01}X_2 + a_{20}X_1^2 + \cdots + a_{\ell m}X_1^\ell X_2^m \in k[X_1, X_2]$$

geven we aan met $Z(f)$. Een *nulpunt van* f is een paar (a, b) met $a, b \in k$ en $f(a, b) = 0$.
De verzameling $\{(a, b) \mid a, b \in k\}$ geven we aan met $\mathbb{A}^2$ of $\mathbb{A}^2(k)$ en we noemen deze verzameling het *affiene vlak* (over k).
Als $f \in k$, d.w.z. als f een constant polynoom is, dan is $Z(f) = \emptyset$ of $Z(f) = \mathbb{A}^2$. We beschouwen nu niet-constante f:

Definitie 1.1.1 Een *(vlakke) affiene kromme* is de nulpuntsverzameling $Z(f)$ van een niet-constant polynoom $f \in k[X_1, X_2]$.

In plaats van X_1, X_2 zullen we meestal de letters X, Y voor de onbepaalden gebruiken: $f = \sum_{i,j} a_{ij}X^iY^j$. De graad van een term $a_{ij}X^iY^j$ (met $a_{ij} \neq 0$) is per definitie gelijk aan $i + j$ en de graad van f, $gr(f)$, is de maximale graad die "echt voorkomt":

$$gr(f) = \max\{i + j \mid a_{ij} \neq 0\}.$$

Een affiene kromme heeft dus altijd een graad ≥ 1. Een *rechte (lijn)* is een kromme van graad 1: $Z(aX + bY + c)$ met $(a, b) \neq (0, 0)$. Een *kwadriek* is een kromme van graad 2. Als $gr(f) = 3$ dan spreekt men van een *kubische kromme*.

Verschillende polynomen kunnen dezelfde kromme opleveren. Zeer triviaal is: $Z(f) = Z(af)$ als $0 \neq a \in k$. Polynomen f en $af (0 \neq a \in k)$ noemen we *equivalent*. Iets minder flauw is

$$Z(2(X + Y)^3) = Z(X + Y) \text{ als } \mathrm{kar}(k) \neq 2.$$

1.2 Splitsing in irreducibele krommen.

Een kromme kan een vereniging zijn van meerdere krommen:

$$Z(X^2 - Y^2) = Z(X - Y) \cup Z(X + Y)$$

(merk evenwel op $X^2 - Y^2 = (X + Y)^2$ als $\mathrm{kar}(k) = 2$). Algemeen:

$$\text{als } f = gh, \text{ dan } Z(f) = Z(g) \cup Z(h).$$

Definitie 1.2.1 Een vlakke kromme heet *irreducibel* als hij van de vorm $Z(f)$ is met f een irreducibel polynoom.

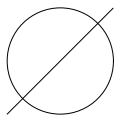
Zoals bekend is $k[X, Y]$ een ontbindingsdomein [Algebra 5.4.2]: iedere niet-constante $f \in k[X, Y]$ kan men uniek (op constanten na) ontbinden als $f = f_1^{n_1} \cdots f_t^{n_t}$ met $f_1, \ldots, f_t$ niet-equivalente irreducibele polynomen en $n_1, \ldots, n_t \geq 1$. De nulpuntsverzameling van f voldoet dan aan

$$Z(f) = Z(f_1) \cup \cdots \cup Z(f_t).$$

In woorden

Stelling 1.2.2 *Elke kromme is een eindige vereniging van irreducibele krommen.*

Ter illustratie: als $f = (X^2 + Y^2 - 1)(X - Y)$ dan is $Z(f) = Z(X^2+Y^2-1) \cup Z(X-Y)$ de vereniging van een rechte met een kwadriek. De kwadriek $X^2 + Y^2 - 1$ is irreducibel als $\mathrm{kar}(k) \neq 2$; men rekent namelijk gemakkelijk na dat $X^2 + Y^2 - 1$ niet het product is van twee lineaire factoren of men ziet $X^2 + Y^2 - 1$ als een polynoom in Y met coëfficienten in $k[X]$ en constateert dat het een Eisenstein-polynoom (met $p = X \pm 1$) is [Algebra 5.5.3].



De ontbinding van een *polynoom* f in irreducibele factoren is uniek. Hetzelfde geldt voor de splitsing van de *kromme* $Z(f)$ in irreducibele krommen. Maar het één volgt niet onmiddellijk uit het ander. Het is immers à priori niet ondenkbaar dat er nog een splitsing $Z(f) = Z(g_1) \cup \cdots \cup Z(g_s)$ bestaat waarbij de g_i geen factoren van f zijn. Dat zoiets tóch niet mogelijk is volgt gemakkelijk uit de volgende twee beweringen:

1. $Z(f)$ is een oneindige verzameling.
2. als g irreducibel en geen deler van f is, dan is $Z(f) \cap Z(g)$ eindig.

Bewering 1. is een gevolg van het feit dat k oneindig (want algebraïsch gesloten) is. Dit ziet men door de kromme $Z(f)$ te snijden met alle lijnen evenwijdig aan de y-as en per lijn het aantal snijpunten te "tellen". Algebraïsch betekent dit dat men, voor elke $\lambda \in k$, kijkt naar het aantal oplossingen van de vergelijking $f(\lambda, y) = 0$. Hiervoor is het handig om f te schrijven als $f = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n$. De details laten we aan de lezer over. We kunnen nog iets meer concluderen:

Stelling 1.2.3 *Voor een niet-constant polynoom f zijn $Z(f)$ en $\mathbb{A}^2 - Z(f)$ oneindig.*

Voor het bewijs van 2. kijken we eerst naar de doorsnede van krommen in het algemeen. Om deze te bepalen moet een simultaan stelsel vergelijkingen

$$f(x,y)=0\ ,\ g(x,y)=0$$

opgelost worden. Net zo als bij lineaire vergelijkingen probeer je dit te doen door een onbekende te elimineren met behulp van een "veegproces": door telkens bij één van de vergelijkingen een (polynoom-) veelvoud van de andere vergelijking op te tellen probeer je een niet triviale vergelijking te produceren waarin maar één onbekende voorkomt. Een eventuele gemeenschappelijke factor h in f en g blijft bij het 'vegen' altijd aanwezig; die moet er dus eerst uitgehaald worden. Stel $f=f_1h, g=g_1h$ met f_1 en g_1 onderling ondeelbaar. Dan is $Z(f)=Z(h)\cup\{Z(g_1)\cap Z(h_1)\}$. Het volgend lemma zegt dat voor onderling ondeelbare polynomen succes gegarandeerd is en het bewijs geeft aan hoe je dit kunt bereiken.

Lemma 1.2.4 *Als f en g ondeelbaar zijn, dan is er een polynoom $b(X)\neq 0$ van de vorm $uf+vg$ met $u,v\in k[X,Y]$. M.a.w. dan bevat het ideaal (f,g) een polynoom $\neq 0$ dat alleen van X afhangt (eventueel constant).*

Bewijs: We vatten f en g op als polynomen in Y : $f,g\in R[Y]$ met $R=k[X]$. We willen de delingsalgoritme (delen met rest) toepassen. Maar dit wil i.h.a. alleen met polynomen over een lichaam. Dus we zien f en g als polynomen in $K[Y]$, waarbij K het breukenlichaam van $R=k[X]$ is:

$$K=k(X):=\{\frac{a}{b}\mid a,b\in k[X],b\neq 0\}.$$

Men gaat gemakkelijk na dat ook in $K[Y]$ geldt g.g.d.$(f,g)=1$ (zie Algebra 5.4). Met de Euclidische delingsalgoritme vinden we $u,v\in K[Y]$ zó dat

$$uf+vg=1\qquad(u,v\in K[Y]).$$

De coëfficienten in de polynomen $u=u(Y)$ en $v=v(Y)$ zijn breuken van de vorm $\dfrac{a(X)}{b(X)}$. Door noemers te verdrijven vinden we nu polynomen $\tilde{u},\tilde{v}\in R[Y]=k[X,Y]$ en een $b(X)\in k[X]$ met $b(X)\neq 0$ zódat

$$\tilde{u}f+\tilde{v}g=b.$$

Hiermee is het lemma bewezen.

Stelling 1.2.5 *Als f en g onderling ondeelbare polynomen zijn dan is $Z(f)\cap Z(g)$ eindig.*

Bewijs: Volgens het lemma zijn er polynomen $u,v\in k[X,Y]$ en een polynoom $b(X)\in k[X]$ met $b(X)\neq 0$, zó dat $uf+vg=b(X)$. Als $(\lambda,\mu)\in Z(f)\cap Z(g)$, dan is $f(\lambda,\mu)=g(\lambda,\mu)=0$, dus $b(\lambda)=0$. Wegens $b(X)\neq 0$ zijn er slechts eindig veel λ's met $b(\lambda)=0$. Voor zo'n λ zijn f en g niet beide deelbaar door $X-\lambda$ (want $g.g.d(f,g)=1$), dus is minstens één van de polynomen $f(\lambda,Y)$ en $g(\lambda,Y)$ (de 'rest' bij deling door het monische polynoom $X-\lambda$) ongelijk aan 0. Bijgevolg heeft de vergelijking $f(\lambda,y)=0$ of $g(\lambda,y)=0$ eindig veel oplossingen $y=\mu$. Er zijn dus eindig veel λ's en bij elk van deze maar eindig veel μ's zodat $(\lambda,\mu)\in Z(f)\cap Z(g)$.

Gevolgen 1.2.6 (van de voorgaande twee stellingen):

1. Als g irreducibel is en geen deler van f, dan is $Z(f)\cap Z(g)$ eindig.

2. Voor irreducibele f_1 en f_2 geldt:

$$Z(f_1) = Z(f_2) \Leftrightarrow f_1 \text{ en } f_2 \text{ zijn equivalent.}$$

3. De splitsing van een kromme in irreducibele krommen is uniek.

De details van de bewijzen hiervan laten we aan de lezer over. We formuleren nóg een gevolg. Dit heeft te maken met het ideaal van een kromme en is een speciaal geval van *Hilbert's Nullstellensatz* die we later in dimensie n zullen geven. Eerst een definitie:

Definitie 1.2.7 De polynomen g die *nul zijn op* $Z(f)$, d.w.z. die voldoen aan

$$g(\lambda, \mu) = 0 \text{ voor alle } (\lambda, \mu) \in Z(f),$$

vormen (zoals onmiddellijk te verifiëren) een ideaal in $k[X, Y]$. Dit zullen we het *ideaal van* $Z(f)$ noemen.

Stelling 1.2.8 *Stel f is een irreducibel polynoom. Dan geldt:*
als $g \in k[X, Y]$ nul is op $Z(f)$, dan is er een polynoom $h \in k[X, Y]$ met $g = hf$.
m.a.w.:
als f irreducibel is, dan is het ideaal van $Z(f)$ gelijk aan (f), d.i. het ideaal in $k[X, Y]$ voortgebracht door f.

Bewijs: Als $g \in (f)$, d.w.z. als $g = hf$ voor een $h \in k[X, Y]$, dan is g uiteraard nul op $Z(f)$. Omgekeerd: Als g nul is op $Z(f)$, dan is $Z(f) \subset Z(g)$ en dus $Z(f) \cap Z(g) = Z(f)$, oneindig. Als g niet deelbaar is door f dan is $\text{ggd}(f, g) = 1$ daar f irreducibel is, dus $Z(f) \cap Z(g)$ eindig. Dus als g nul is op $Z(f)$ dan is g deelbaar door f, d.w.z. dan geldt $g \in (f)$.

1.3 Affiene transformaties

Gegeven een kromme $Z(f)$ van graad n is er altijd een richting aan te geven zodat alle lijnen in deze richting k snijpunten, met $1 \leq k \leq n$, met $Z(f)$ hebben. Dit geldt zelfs voor "bijna alle" richtingen: alle, uitgezonderd hoogstens n richtingen. Dit is het eenvoudigst te zien als we een geschikt coördinatenstelsel (oorsprong, x- en y-as) gebruiken of, wat op hetzelfde neerkomt, een affiene transformatie uitvoeren.

Definitie 1.3.1 Een *affiene transformatie* is een afbeelding $\mathbb{A}^2 \to \mathbb{A}^2$ van de soort $(\lambda, \mu) \mapsto (\lambda', \mu') = (a\lambda + b\mu + e_1, c\lambda + d\mu + e_2)$ met $a, b, c, d, e_1, e_2 \in k$ en $ad - bc \neq 0$.

Een affiene transformatie is dus een samenstelling van een lineaire afbeelding met determinant $\neq 0$ en een verschuiving. Zo'n transformatie is bijectief en de inverse afbeelding heeft weer dezelfde vorm:

$$(\lambda', \mu') = (a\lambda + b\mu + e_1, c\lambda + d\mu + e_2) \Rightarrow (\lambda, \mu) = (A\lambda' + B\mu' + E_1, C\lambda' + D\mu' + E_2),$$

waarbij $\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$. Een kromme $Z(f)$ wordt afgebeeld op een kromme $Z(g)$. Het verband tussen f en g is:

$$g(X, Y) = f(AX + BY + E_1, CX + DY + E_2) \ , \ f(X, Y) = g(aX + bY + e_1, cX + dY + e_2),$$

want

$$(\lambda,\mu) \in Z(f) \Leftrightarrow$$
$$0 = f(\lambda,\mu) = f(A\lambda' + B\mu' + E_1, C\lambda' + D\mu' + E_2) = g(\lambda',\mu') \Leftrightarrow (\lambda',\mu') \in Z(g).$$

Het toepassen van een affiene transformatie komt dus neer op het uitvoeren van een substitutie $X \to AX + BY + E_1, Y \to CX + DY + E_2$ met $AD - BC \neq 0$.
Omdat hierbij evenals bij de inverse substitutie de graad zeker niet groter wordt kunnen we vaststellen:

affiene transformaties behouden de graad van een kromme.

Door affiene transformaties kan men de vergelijking van een kromme vaak in eenvoudige(r) vorm brengen (het is aan te bevelen om tijdens de berekening andere letters zoals X_1, Y_1 of S, T voor de onbepaalden te gebruiken ten einde de 'oude' en 'nieuwe' onbepaalden uit elkaar te houden; na afloop kan men weer X en Y gebruiken).
Een lijn kan men in de vorm X (of $x = 0$) schrijven. Voor krommen van graad 2 vindt men vijf "standaardvormen":

Stelling 1.3.2 *Ieder polynoom van graad 2 is na affiene transformatie equivalent met precies één van de volgende vijf polynomen:*

i) X^2 *("dubbellijn")*

ii) XY *(twee snijdende rechten)*

iii) $X(X-1)$ *(twee evenwijdige rechten)*

iv) $X^2 + Y$ *(parabool)*

v) $XY - 1$ *(hyperbool).*

Bewijs: We kijken eerst alleen naar de kwadratische termen van het polynoom f van de graad 2:

$$f_2 := a_{20}X^2 + a_{11}XY + a_{02}Y^2.$$

Daar k algebraïsch gesloten is kan men f_2 in lineaire factoren ontbinden. Dit is duidelijk als $a_{20} = 0$; als $a_{20} \neq 0$ dan hebben we

$$f_2(X,1) = a_{20}(X-\lambda)(X-\mu), \text{ dus } f_2(X,Y) = a_{20}(X-\lambda Y)(X-\mu Y) \text{ met } \lambda,\mu \in k.$$

De twee mogelijkheden

1. f_2 is een kwadraat
2. f_2 is geen kwadraat

geven resp. voor f_2 de vormen X_1^2 en X_1Y_1. In het schema hieronder gaan we na wat dit voor f oplevert na eventueel nog een substitutie.

1. $f = X_1^2 + aX_1 + bY_2 + c$	$(b = 0)$	X_2^2	(f is een kwadraat)
		$X_2(X_2 - 1)$	(f is geen kwadraat)
	$(b \neq 0)$	$X_2^2 + Y_2$	

2. $f = X_1Y_1 + aX_1 + bY_1 + c = (X_1 + b)(Y_1 + a) + c'$ $\quad \begin{matrix} X_2Y_2 & (c' = 0) \\ X_2Y_2 - 1 & (c' \neq 0) \end{matrix}$

De vijf polynomen kunnen niet door affiene transformaties in elkaar overgevoerd worden. Dat komt omdat eigenschappen als "f_2 is een kwadraat" en "f is (ir-)reducibel" behouden blijven onder affiene transformaties.

Opmerking. Als $k = \mathbb{C}$ dan is de vergelijking van de 'cirkel' $x^2 + y^2 = 1$ te schrijven als $(x + iy)(x - iy) = 1$ en dit wordt na de affiene transformatie $X + iY \to X$, $X - iY \to Y$ de hyperbool $XY - 1$. Als we over $k = \mathbb{R}$ (niet algebraïsch gesloten!) werken, dan kunnen we alleen reële affiene transformaties gebruiken: over $\mathbb{R}$ is de cirkel niet affien equivalent met een hyperbool. In het reële geval heb je dus meer "standaardkwadrieken".

1.4 Het snijden van lijnen en krommen.

1.4.1 Met affiene transformaties is het eenvoudig om voor een gegeven kromme $Z(f)$ van graad n een richting te vinden zodat alle lijnen in deze richting een niet lege doorsnede met $Z(f)$ hebben.

Je kiest n.l. $a, b, c, d \in k$ met $ad - bc \neq 0$ zó dat in het polynoom

$$g(X, Y) := f(aX + bY, cX + dY)$$

de term Y^n voorkomt. De snijpunten van $Z(g)$ met een rechte $x = \lambda$ zijn dan (λ, μ_j) $(j = 1, \cdots n)$ waarbij $\mu_1, \ldots, \mu_n$ de oplossingen zijn van de n-de graadsvergelijking $g(\lambda, y) = y^n + \cdots = 0$ (de μ_j hoeven uiteraard niet alle verschillend te zijn).
De keuze van a, b, c, d kan als volgt gebeuren. Zij f_n resp. g_n de som van de n-de graads termen in f resp. g. De coëfficient van Y^n in $g_n(X, Y) = f_n(aX + bY, cX + dY)$ is gelijk aan $g_n(0, 1) = f_n(b, d)$. We nemen $b = 1$ en voor d een oplossing van de vergelijking $f_n(1, y) = 1$. Zo'n oplossing bestaat als Y echt in $f_n(X, Y)$ voorkomt, want k is algebraïsch gesloten. Als Y niet in $f_n(X, Y)$ voorkomt, dan is $f_n = a_{n0}X^n$ met $a_{n0} \neq 0$. Dan kiezen we $d = 0$ en voor b een oplossing van $a_{n0}x^n = 1$. Nemen we nog $a = 0$, $c = 1$, dan is $ad - bc = -b \neq 0$.
Als we aan elk snijpunt (λ, μ_j) een multipliciteit toekennen, dan zijn er met multipliciteit geteld precies n snijpunten. We definiëren in het algemeen:

Definitie 1.4.2 De *multipliciteit* van een snijpunt P van een rechte $Z(\ell)$ met een kromme $Z(f)$ wordt als volgt gedefinieerd: we nemen een parametervoorstelling van $\ell : (x, y) = (a, b) + t(c, d), t \in k$. De snijpunten van $Z(\ell)$ en $Z(f)$ vinden we uit de vergelijking

$$f(a + ct, b + dt) = 0.$$

Als nu $t = \tau$ een m-voudige wortel van deze vergelijking is, dan is per definitie $P = (a, b) + \tau(c, d)$ een *snijpunt van multipliciteit* m. ($m = \infty$ als $f(a + ct), b + dt) = 0$ voor alle t).

Men gaat na: deze multipliciteit is onafhankelijk van de gekozen parametervoorstelling van $Z(\ell)$ en blijft behouden onder affiene transformaties.

Om nog wat meer over de snijpunten van lijnen en krommen te kunnen zeggen hebben we nog een definitie nodig.

Definitie 1.4.3 Een polynoom $f \in k[X,Y]$ heet *homogeen van graad d* als er in f uitsluitend termen van graad d voorkomen:

$$f = \sum_{i+j=d} a_{ij} X^i Y^j.$$

Iedere $f \in k[X,Y]$ kunnen we schrijven als $f = f_0 + \cdots + f_n$ met f_i homogeen van graad i of $f_i = 0$. Deze schrijfwijze is uniek: f_i is de som van alle termen van graad i in f($f_i = 0$ als er in f geen termen van graad i voorkomen). De f_i heten de *homogene componenten* van f.

Het is duidelijk dat voor een homogeen polynoom f_d van graad d in twee onbepaalden geldt

1. f_d is te ontbinden in d lineaire factoren,
2. $f_d(tX, tY) = t^d f(X,Y)$.

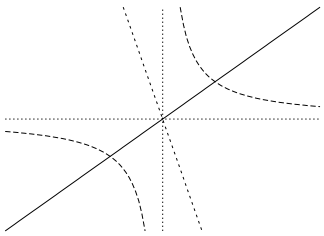
1.4.4 Laat een kromme van graad n en een lijn gegeven zijn. Met een verschuiving kunnen we ervoor zorgen dat de lijn door de oorsprong gaat. B.v. als de lijn is: $(x,y) = (1,2) + t(c,d)$ $(t \in k)$ en de kromme: $X^2 - 2X + Y$, dan substitueren we $x = 1 + x_1$, $y = 2 + y_1$, en nu moeten we de lijn $(x_1, y_1) = t(c,d)$ snijden met $X_1^2 - 2X_1 + Y_1 + 1$. Stel f is de vergelijking van de kromme na de verschuiving. We splitsen f in homogene componenten f_i en krijgen de vergelijking

$$0 = f(ct, dt) = \sum_{i=0}^{n} f_i(c,d) t^i.$$

Dit is een vergelijking van graad n als $f_n(c,d) \neq 0$; dan zijn er n snijpunten, geteld met multipliciteit. Alleen voor de uitzonderlijke richtingen (c,d) met $f_n(c,d) = 0$ zijn er minder dan n snijpunten. Deze richtingen vinden we door f_n in lineaire factoren te ontbinden. Dus we hebben

> **Afgezien van k richtingen $(1 \leq k \leq n)$ hebben alle lijnen precies n snijpunten (geteld met multipliciteit) met een kromme van graad n.**

Voorbeeld. Voor de hyperbool $XY - 1$ zijn de uitzonderlijke richtingen precies die van de asymptoten $x = 0$, $y = 0$. Elke lijn in een andere richting heeft twee snijpunten met de hyperbool (in de figuur zijn alleen de reële snijpunten zichtbaar!). Voor een raaklijn telt het raakpunt dubbel. We moeten nog een algebraïsche definitie van 'raaklijn' geven.



1.5 Raaklijnen en singuliere punten.

Stel P is een punt van de kromme $Z(f)$ van graad n. We nemen aan $P = (0,0)$ (dit is door een verschuiving te bereiken). We snijden de lijnen door $(0,0)$ met $Z(f)$ en onderzoeken de mogelijke snij-multipliciteiten. We splitsen f weer in homogene componenten

$$f = f_1 + \cdots + f_n \qquad (f_0 = f(0,0) = 0)$$

en een lijn door $(0,0)$ geven we in parametervoorstelling: $(x,y) = t(c,d), t \in k$; $(c,d) \neq (0,0)$ is de richting van de lijn. De snijpunten vindt men uit:

$$f_1(c,d)t + \cdots + f_n(c,d)t^n = 0.$$

We nemen eerst aan dat $f_1 \neq 0$; dus $f_1 = aX + bY$ met $(a, b) \neq (0, 0)$.
In dit geval heet $P = (0, 0)$ een *gewoon punt* van $Z(f)$.
Als $f_1(c, d) \neq 0$, dan is $P = (0, 0)$ een enkelvoudig snijpunt. Als $f_1(c, d) = 0$, dan is $(0, 0)$ een m-voudig snijpunt met $2 \leq m \leq \infty$ en de lijn heet een *raaklijn* in $(0, 0)$ aan de kromme. De voorwaarde $f_1(c, d) = 0$ betekent dat de raaklijn gelijk is aan $f_1 = aX + bY$. In een gewoon punt is er dus één raaklijn. Met gebruik van partiële afgeleiden (deze kunnen op de bekende wijze algebraïsch worden ingevoerd) en de notatie f_X, f_{XY} voor $\frac{\partial f}{\partial X}$, $\frac{\partial^2 f}{\partial X \partial Y}$ etc. vinden we zo de bekende formule uit de analyse voor de raaklijn:

> de raaklijn in een gewoon punt $P = (\lambda, \mu)$, d.w.z. een punt met $f(P) = 0$, $f_X(P)$ en $f_Y(P)$ niet beide nul, wordt gegeven door de vergelijking:
>
> $$f_X(P)(x - \lambda) + f_Y(P)(y - \mu) = 0.$$

Een punt met $f(P) = f_X(P) = f_Y(P) = 0$ heet een *singulier punt* van $Z(f)$. We nemen weer $P = (0, 0)$. Als $(0, 0)$ singulier is en $f_0 = \cdots = f_{d-1} = 0$, $f_d \neq 0$ dan heet $(0, 0)$ een *d-voudig punt*. Door f_d in lineaire factoren te ontbinden vindt men: 'bijna alle' lijnen door een d-voudig punt P hebben een d-voudig snijpunt in P met de kromme. Alleen voor de lineaire factoren van f_d is deze snij-multipliciteit groter dan d. Dit zijn per definitie de raaklijnen in P aan $Z(f)$. In een singulier punt zijn er dus meerdere (of meervoudig getelde) raaklijnen. B.v. $Z(X^2 + XY + Y^2 + Y^3)$ heeft in $(0, 0)$ de raaklijnen $X + \omega Y$ en $X + \omega^2 Y$ waarbij $\omega \in k$ een oplossing is van $x^2 + x + 1 = 0$.

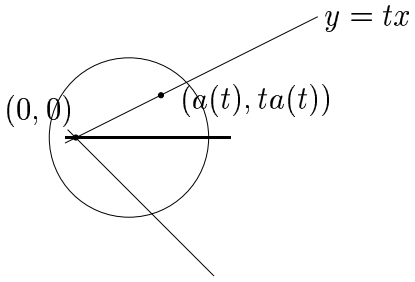
1.6 Het parametriseren van krommen.

1.6.1 We hebben reeds parametervoorstellingen (parametriseringen) van rechten gebruikt. Uit de analyse is de parametrisering $(x, y) = (\cos\varphi, \sin\varphi)$ van de (reële) cirkel $x^2 + y^2 = 1$ overbekend. Maar $\sin\varphi$ en $\cos\varphi$ zijn *transcendente*, geen *algebraïsche* functies; dit houdt in dat je om x, y uit φ te krijgen of omgekeerd, niet kan volstaan met het oplossen van door polynomen gegeven vergelijkingen. Met een bekende truc (zie ook 1.6.3) vindt men evenwel de volgende rationale parametrisering van de cirkel: $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Dit betekent: als de parameter t de verzameling $\mathbb{R}$ doorloopt, dan doorloopt het genoemde punt alle punten van de cirkel. Eén punt $(-1, 0)$ ontbreekt, dit korrespondeert met $t \to \pm\infty$. We hebben metéén een parametrisering van de 'cirkel' $x^2 + y^2 = 1$ in het complexe affiene vlak; nu mag t niet de waarde $\pm i$ aannemen.
Omdat we geen last van uitzonderingen willen hebben, zien we t verder als een onbepaalde in de polynoomring $k[t]$ en een rationale functie als een element van het breukenlichaam $k(t)$ en we definiëren:

Definitie 1.6.2 Zij $f \in k[X, Y]$ een irreducibel polynoom. Een (rationale) parametrisering van $Z(f)$ is een paar $(a(t), b(t))$ met $a(t), b(t) \in k(t)$ en $f(a(t), b(t)) = 0 \in k(t)$, a en b niet beide constant.

1.6.3 Niet alleen rechten, maar ook irreducibele kwadrieken kunnen geparametriseerd worden: zo'n kwadriek is namelijk, na een affiene transformatie, de hyperbool $XY - 1$ of de parabool $X^2 + Y$ met resp. de parametriseringen $(t, \frac{1}{t})$ en $(t, -t^2)$ (om een parametrisering van de oorspronkelijke kwadriek te krijgen moet men natuurlijk wel weer 'terugtransformeren').
Handiger wellicht is de volgende methode. Deze gebruikt alleen een translatie die ervoor zorgt dat $(0, 0) \in Z(f)$; f is de vergelijking van de kwadriek na de verschuiving.

De lijnen door $(0,0)$ korresponderen $1-1$ met de punten van $Z(f)$ omdat ze behalve $(0,0)$ nog maar één snijpunt met $Z(f)$ hebben. Deze lijnen parametriseren we met $t \in k$: $y = tx$ (eigenlijk moeten we hier voor t een andere letter b.v. λ gebruiken; maar na afloop wordt de 'variabele' λ vervangen door de 'onbepaalde' t; om dezelfde reden is het ook niet erg dat we een lijn overgeslagen hebben).

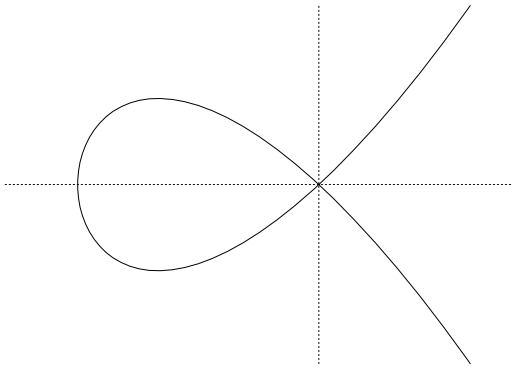


De rechte $y = tx$ snijden we met $Z(f)$. Dat levert voor x een tweedegraads vergelijking op, waarvan we al één oplossing kennen, n.l. $x = 0$. De andere is een rationale functie $a(t)$ en dan is $(a(t), ta(t))$ een parametrisering. De $a(t)$ kan men gemakkelijk vinden. Schrijf f in homogene componenten: $f = f_0 + f_1 + f_2$. Dan $f_0 = f(0,0) = 0$ en $f(x, tx) = f_1(1,t)x + f_2(1,t)x^2$, dus $a(t) = \frac{-f_1(1,t)}{f_2(1,t)}$.

Men kan gemakkelijk nagaan dat de afbeelding $\tau \mapsto (a(\tau), \tau a(\tau))$ een "bijna bijectieve" afbeelding van k naar $Z(f)$ is. De "bijna inverse" voegt aan een punt $(\lambda, \mu) \neq (0,0)$ van $Z(f)$ toe $\frac{\mu}{\lambda} = \tau \in k$. Het "bijna" betekent dat men eindig veel τ-waarden en eindig veel punten van $Z(f)$ moet weglaten (dus $\tau \mapsto (a(\tau), \tau a(\tau))$ is een bijectie van $k - T$ op $Z(f) - A$ voor zekere eindige deelverzamelingen T van k en A van $Z(f)$). In bovenstaand voorbeeld moet men de waarden $\tau \in k$ met $f_2(1,\tau) = 0$ uitsluiten en van $Z(f)$ het punt $(0,0)$ in het geval dat de vergelijking $f_1(1,t) = 0$ geen oplossing heeft.

1.6.4 Parametrisering van de derdegraadskromme $Y^2 - X^2(X+1) = 0$.

Een tekening van de reële punten van de kromme staat hiernaast. Het punt $(0,0)$ is wat afwijkend van de andere punten. Inderdaad is het een singulier punt (zie 1.5). In het algemeen zal een lijn de kromme in drie punten snijden. Voor een lijn door $(0,0)$ telt $(0,0)$ als een meervoudig snijpunt en verwachten we (hoogstens) nog maar één ander snijpunt. Inderdaad als we $Y - tX$ met de kromme snijden krijgen we de vergelijking $t^2x^2 = x^2(x+1)$ met dubbele wortel $x = 0$ en nog de wortel $x = t^2 - 1$. Dit levert de parametrisering $(t^2 - 1, t(t^2 - 1))$.



1.6.5 Niet elke kromme kan geparametriseerd worden:

> **De derde-graads-kromme $Y^2 - X(X-1)(X-\lambda)$ met $\lambda \neq 0, 1$ over een lichaam k met kar$(k) \neq 2$ laat geen parametrisering toe.**

Bewijs. Veronderstel dat er wel een parametrisering is. Schrijf dan $x = \frac{a(t)}{b(t)}$, $y = \frac{c(t)}{d(t)}$ met $a, b, c, d \in k[t]$, waarbij

$$(1) \qquad \begin{cases} b, d \neq 0 \text{ en monisch, } \mathrm{ggd}(a,b) = \mathrm{ggd}(c,d) = 1, \\ a, b, c, d \text{ niet alle constant.} \end{cases}$$

Invullen in de vergelijking geeft, na wegwerken van de noemers

$$(2) \qquad b^3c^2 = a(a-b)(a-\lambda b)d^2.$$

We gebruiken nu dat $k[t]$ een ontbindingsring is en merken op:

(i) geen van de factoren in (2) is 0.
B.v. $a = 0$ zou geven $b = 1$ (wegens $\text{ggd}(a, b) = 1$, b monisch) en vervolgens $c = 0$, $d = 1$, in strijd met (1).

(ii) er geldt $b^3 = d^2$. Immers, $\text{ggd}(a, b) = \text{ggd}(a - b, b) = \text{ggd}(a - \lambda b, b) = 1$ en $\text{ggd}(c, d) = 1$; bovendien zijn b en d monisch.

(iii) uit $b^3 = d^2$ volgt: b is een kwadraat en uit $c^2 = a(a-b)(a-\lambda b)$ volgt dat a, $a-b$ en $a-\lambda b$ ook kwadraten zijn. Dus als we schrijven $a = f^2$, $b = g^2$, dan zijn $f^2 - g^2$ en $f^2 - \lambda g^2$ kwadraten. Maar dan zijn f en g constant volgens het lemma hieronder. Dan zijn a en b en dus ook c en d constant. Tegenspraak.

Lemma 1.6.6 *Stel $f, g \in k[t]$ zijn polynomen met $ggd(f, g) = 1$ en stel dat $f^2 - g^2$ en $f^2 - \lambda g^2$ kwadraten zijn voor zekere $\lambda \in k$ met $\lambda \neq 0, 1$. Dan zijn f en g constant. We nemen hier aan dat $kar(k) \neq 2$.*

Bewijs. Zo niet, dan kiezen we f en g die aan de voorwaarden voldoen, en wel zo dat $\max(\text{gr}(f), \text{gr}(g)) > 0$ zo klein mogelijk is. We schrijven $\lambda = \mu^2$. Nu zijn $(f + g)(f - g)$ en $(f - \mu g)(f + \mu g)$ kwadraten. Uit $\text{ggd}(f, g) = 1$ volgt dat $\text{ggd}(f + g, f - g) = 1$ en evenzo $\text{ggd}(f + \mu g, f - \mu g) = 1$ (hier gebruik je $kar(k) \neq 2$). Dus $f \pm g$ en $f \pm \mu g$ zijn alle kwadraten.
Stel $f + g = f_1^2$, $f - g = g_1^2$. Dan blijkt (na een kleine berekening waarbij $kar(k) \neq 2$ weer een rol speelt) dat ook f_1 en ρg_1, met $\rho^2 = \frac{\mu-1}{\mu+1}$, aan de voorwaarden van het lemma voldoen, terwijl $0 < \max(gr(f_1), gr(\rho g_1)) < \max(gr(f), gr(g))$. Dit is in strijd met de keuze van f en g en bewijst dus het lemma. □

1.6.7 Toepassing: het berekenen van integralen.
De integraal $\int \frac{dx}{y}$ met $y = \sqrt{x^2(x+1)}$ is te berekenen door de parametrisering $x = t^2 - 1$, $y = t(t^2 - 1)$ van de kromme $y^2 = x^2(x + 1)$ te gebruiken: onder de substitutie $x = t^2 - 1$, $y = t(t^2 - 1)$ gaat de integraal over in $\int \frac{2tdt}{t(t^2-1)}$ welke op de bekende manier uit te rekenen is en na afloop kan men de parameter t weer door $\frac{y}{x}$ vervangen. Deze methode werkt voor elke integraal $\int R(x, y)dx$, met $R(x, y)$ een rationale functie van x en y, als $y = y(x)$ een functie van x is die voldoet aan een parametriseerbare vergelijking $f(x, y) = 0$ (we zullen nog zien (1.7.8) dat in zo'n geval de parameter t als een rationale functie van x en y te kiezen is).
De integraal $\int \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$ met $\lambda \neq 0, 1$ is niet te parametriseren. Deze integraal heet een *elliptische integraal* omdat hij optreedt bij de berekening van de booglengte van de ellips. Uit de studie van deze integraal is de elliptische functietheorie ontstaan. De kromme $y^2 = x(x-1)(x-\lambda)$ ($\lambda \neq 0, 1$ en $kar(k) \neq 2$) heet een *elliptische kromme in Legendre's normaalvorm.* Elliptische functies vervullen voor elliptische krommen dezelfde rol als de sinus en cosinus in het geval van de cirkel.

1.7 Het functielichaam van een irreducibele kromme.

Een breuk $\frac{a(X)}{b(X)} \in k(X)$ noemt men een rationale "functie" omdat hiermee een (niet overal gedefinieerde!) functie $k \to k$ is geassocieerd, n.l. $\lambda \mapsto \frac{a(\lambda)}{b(\lambda)}$. Punten $\lambda \in k$ met $a(\lambda) \neq 0$, $b(\lambda) = 0$ noemt men *polen* van de functie. Hier is de functie niet gedefinieerd. Alle andere punten heten *reguliere punten.* Omdat k algebraïsch gesloten is geldt: een rationale functie die overal op k regulier is, is van de vorm $\lambda \mapsto a(\lambda)$ met $a(X)$ een polynoom. Voor polynoomfuncties gebruikt men om deze reden ook de term *reguliere functies.* We gaan nu rationale functies op $\mathbb{A}^2$ en op krommen in $\mathbb{A}^2$ bekijken.

Definitie 1.7.1 Een functie $\mathbb{A}^2 \to k$ van de vorm

$$(\lambda, \mu) \mapsto f(\lambda, \mu) \quad \text{waarbij } f = f(X, Y) \in k[X, Y]$$

heet een polynoomfunctie of *reguliere functie*. Deze reguliere functies op $\mathbb{A}^2$ vormen (onder de gebruikelijke optelling en vermenigvuldiging van functies) een ring die we aangeven met $\mathcal{O}(\mathbb{A}^2)$. We schrijven ook wel $k[X, Y]$ voor deze ring, want $k[X, Y] \cong \mathcal{O}(\mathbb{A}^2)$ (dit komt omdat k oneindig is). Een functie $\varphi : Z = Z(f) \to k$ heet regulier als er een polynoomfunctie $g \in k[X, Y] = \mathcal{O}(\mathbb{A}^2)$ is zodat φ gelijk is aan de restrictie van g tot Z. De *ring van reguliere functies* op Z geven we aan met $\mathcal{O}(Z)$.

De restrictieafbeelding $\tau : k[X, Y] \to \mathcal{O}(Z)$, met $\tau(g) =$ restrictie van g tot Z, is een surjectief ringhomomorfisme. De kern van τ bestaat uit de polynomen die nul zijn op Z en is dus gelijk aan het ideaal van Z (zie 1.2.7). De eerste isomorfiestelling [Algebra 2.2.9] geeft nu:

Stelling 1.7.2 *$\mathcal{O}(Z) \cong k[X, Y]/I$, waarbij $I = I(Z)$ het ideaal van Z is.*

Als we aannemen dat f irreducibel is, dan weten we uit Stelling 1.2.8: $I(Z) = (f) =$ het ideaal voortgebracht door f. Algemeen leidt men uit 1.2.8 en 1.2.6 zonder veel moeite af:

Stelling 1.7.3 *Veronderstel dat $Z = Z(f)$ en dat $f = f_1^{n_1} \cdots f_t^{n_t}$ waarbij de f_i irreducibele, niet-equivalente polynomen zijn en $n_i \geq 1$. Dan is*

$$\mathcal{O}(Z) \cong k[X, Y]/(\hat{f}) \text{ met } \hat{f} = f_1 \cdots f_t.$$

1.7.4 Rekenen met reguliere functies op een kromme is kennelijk hetzelfde als rekenen met polynomen modulo het ideaal I van de kromme. Men gebruikt vaak de volgende *notatie*: voor de polynomen X en Y schrijft men:

$$x := X + I \ , \ y := Y + I$$

en dit geeft voor een polynoom $g \in k[X, Y]$:

$$g(x, y) = g + I.$$

Immers, als $g = \sum a_{ij} X^i Y^j$, dan is $g + I = \sum (a_{ij} + I)(X + I)^i (Y + I)^j$ en we mogen $a_{ij} + I$ wel vervangen door a_{ij} omdat beperkt tot constante polynomen $a \in k$ het homomorfisme $a \mapsto a + I$ injectief is.
Bij $g(x, y)$ mogen we ook denken aan de reguliere functie $(\lambda, \mu) \mapsto g(\lambda, \mu)$ op Z, want twee reguliere functies $(\lambda, \mu) \mapsto g(\lambda, \mu)$ en $(\lambda, \mu) \mapsto h(\lambda, \mu)$ zijn gelijk op Z precies dan als $g(x, y) = h(x, y)$. Bijvoorbeeld als Z de cirkel $Z(X^2 + Y^2 - 1)$ is, dan is $I = (X^2 + Y^2 - 1)$ en "$X^2 + Y^2 - 1 \in I$" wordt vertaald in "$x^2 + y^2 - 1 = 0$".
Op de cirkel geldt dus o.a. ook $x^2 + y^3 = x^2 + y(1 - x^2)$ en $x^2 - y^2 = 2x^2 - 1$. Als $Z = Z(X^2 - Y^2)$, dan is $I = (X^2 - Y^2)$ en nu geldt, met $x = X + I$, $y = Y + I$, $(x - y)(x + y) = 0$, dus $\mathcal{O}(Z)$ heeft nuldelers. Als $Z = Z(f)$ met f irreducibel, dan heeft $\mathcal{O}(Z)$ geen nuldelers (ga na). Dus we hebben:

Stelling 1.7.5 *$\mathcal{O}(Z)$ is een domein precies dan als Z irreducibel is.* □

Definitie 1.7.6 Het breukenlichaam $k(X, Y)$ van $\mathcal{O}(\mathbb{A}^2) = k[X, Y]$ heet het *lichaam van de rationale functies op* $\mathbb{A}^2$. Voor een irreducibele kromme Z heet het breukenlichaam van $\mathcal{O}(Z)$ het *lichaam van de rationale functies op Z*. Men gebruikt hiervoor wel de notatie $k(Z)$ en noemt $k(Z)$ ook het *functielichaam van Z*.

Een rationale functie op $Z(f)$, met f irreducibel, is dus een breuk $\frac{a(x,y)}{b(x,y)}$ met $b(x,y) \neq 0$; hierbij is, zoals afgesproken $x := X + (f), y := Y + (f)$. Deze voorstelling is niet uniek, want men kan de relatie $f(x,y) = 0$ gebruiken om de breuk om te vormen. Op de cirkel $Z(X^2 + Y^2 - 1)$ geldt b.v. $\frac{x}{1-y} = \frac{1+y}{x}$. Algemeen: $\frac{a(x,y)}{b(x,y)} = \frac{c(x,y)}{d(x,y)} \Leftrightarrow ad - bc \in (f)$, $b, d \notin (f)$.

Voorbeelden 1.7.7 (i) Neem de kwadriek $Z := Z(X^2 + Y)$. Dan is $\mathcal{O}(Z) \cong k[X]$, want $\mathcal{O}(Z) = k[X,Y]/(Y + X^2) \cong k[X]$. Derhalve is ook $k(Z) \cong k(X)$.

(ii) Beschouw vervolgens $Z = Z(Y^2 - X^2(X-1))$. Het polynoom $Y^2 - X^2(X-1)$ is irreducibel (ga na) en $\mathcal{O}(Z) = k[X,Y]/(Y^2 - X^2(X-1))$ heeft geen nuldelers. De parametrisering $(t^2+1, t(t^2+1))$ geeft een homomorfisme

$$k[X,Y] \to k[t] \ , \ X \mapsto t^2 + 1 \ , \ Y \mapsto t(t^2+1)$$

en met de homomorfiestelling [Algebra 2.2.8] geeft dit weer een homomorfisme

$$\tau : \mathcal{O}(Z) \to k[t] \ , \ x \mapsto t^2 + 1, y \mapsto t(t^2+1)$$

(zoals steeds is $x = X+I$, $y = Y+I$ met $I = (Y^2 - X^2(X-1))$). Dit laatste ringhomomorfisme is injectief. Dat kan men als volgt zien. Elk element van $\mathcal{O}(Z)$ is van de vorm $g(x,y) = a(x) + b(x)y$, waarbij $a, b \in k[X]$. Het τ-beeld van $g(x,y)$ is dan $a(1+t^2) + b(1+t^2) \cdot t(1+t^2)$. Als dit τ-beeld nul is dan moeten a en b nul zijn, want $a(1+t^2)$ gebruikt alleen even machten van t en $t(1+t^2)b(1+t^2)$ alleen oneven machten. Dus τ is injectief en identificeert $\mathcal{O}(Z)$ met een deelring van $k[t]$. Deze deelring bevat t niet! Het breukenlichaam ervan bevat t wél, want $t = \frac{\tau(y)}{\tau(x)}$. Derhalve is het functielichaam isomorf met $k(t)$.

1.7.8 Aan het tweede voorbeeld ziet men dat het parametriseren van een irreducibele kromme Z iets te maken heeft met het lichaam van de rationale functies van Z. Een nauwkeurige uitspraak hierover kunnen we niet doen zonder de stelling van Lüroth. Voor het bewijs hiervan verwijzen we naar "B.L. van der Waerden – Algebra".

Stelling van Lüroth. Zij ℓ een deellichaam van $k(t)$ dat k omvat en ongelijk aan k is. Dan is er een element $s \in k(t) - k$ met $\ell = k(s)$.

Stelling 1.7.9 *Een irreducibele kromme kan geparametriseerd worden precies dan als zijn functielichaam isomorf met $k(t)$ is.*

Bewijs. $\mathcal{O}(Z) = k[X,Y]/(f)$ waarbij f een irreducibel polynoom is. Als het breukenlichaam van $\mathcal{O}(Z)$ gelijk aan $k(t)$ is dan zijn de beelden van $x := X + (f)$ en $y := Y + (f)$ rationale functies $\frac{a(t)}{b(t)}$ en $\frac{c(t)}{d(t)}$ in $k(t)$. Dus we vinden een parametrisering.
Vervolgens, bij een parametrisering $\left(\frac{a(t)}{b(t)}, \frac{c(t)}{d(t)}\right)$ van $Z = Z(f)$ maken we het ringhomomorfisme

$$\tau : k[X,Y] \to k(t) \text{ met } X \mapsto \frac{a(t)}{b(t)} \ , \ Y \mapsto \frac{c(t)}{d(t)}.$$

Volgens de definitie van parametrisering zit f in de kern van τ dus het ideaal $I = (f)$ van Z is bevat in $ker(\tau)$. We gaan nu eerst aantonen dat $ker(\tau) = (f)$. Zo niet, dan bevat $ker(\tau)$ een $g \in k[X,Y]$ met $g \notin (f)$. Voor elke $\lambda \in k$ waarvoor $b(\lambda) \neq 0$ en $d(\lambda) \neq 0$ geldt nu $\left(\frac{a(\lambda)}{b(\lambda)}, \frac{c(\lambda)}{d(\lambda)}\right) \in Z(f) \cap Z(g)$.

Volgens 1.2.5 is $Z(f) \cap Z(g)$ eindig. Dus de rationale functies $\lambda \mapsto \frac{a(\lambda)}{b(\lambda)}$ en $\lambda \mapsto \frac{c(\lambda)}{d(\lambda)}$ nemen op hun gemeenschappelijke definitiegebied maar eindig veel waarden aan. Maar dit impliceert dat ze beide constant zijn (het bewijs hiervan laten we aan de lezer over), in strijd met de definitie van parametrisering. Dus $ker(\tau) = (f)$ en τ induceert een injectief homomorfisme

$$\bar{\tau} : \mathcal{O}(Z) = k[X, Y]/(f) \to k(t).$$

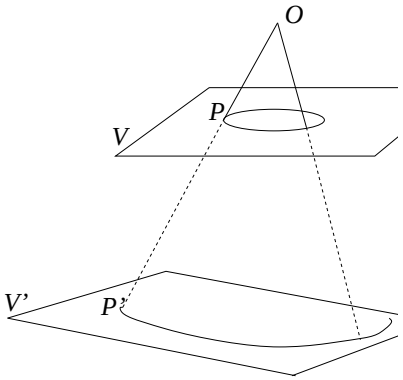
Het breukenlichaam van $\mathcal{O}(Z)$ is dan isomorf met een deellichaam ℓ van $k(t)$ dat k strict omvat. Volgens de stelling van Lüroth is het functielichaam van Z dan isomorf met een $k(s)$. Tenslotte moet nog opgemerkt: voor elke $s \in k(t) - k$ geldt, dat $k(s) \cong k(t)$, want zoals gemakkelijk te zien is elke $s \in k(t) - k$ transcendent over k [Algebra 7.2.1]. Dus $k(Z) \cong k(t)$.

Opmerking. De isomorfie $k(Z) \cong k(s)$ uit bovenstaand bewijs houdt óók in dat de parameter s als rationale functie van x en y te schrijven is. Dit is handig om te weten i.v.m. het berekenen van integralen, zie 1.6.7.

2 Vlakke Projectieve krommen.

2.1 Het projectieve vlak $\mathbb{P}^2$.

Bij het snijden van een n-de graads kromme met rechte lijnen hebben we geconstateerd dat er richtingen zijn waarvoor er "te weinig" snijpunten zijn. Hiermee samenhangend deed zich bij het parametriseren het verschijnsel voor dat de kromme soms punten "mist" t.a.v. de mogelijke waarden van t. Dit "defect" van het affiene vlak is te repareren door het affiene vlak op te vatten als een deel van een wat "groter" vlak, namelijk $\mathbb{P}^2$, het *projectieve vlak*.
Zoals de naam al aangeeft is het idee "projectief vlak" afkomstig uit een onderdeel van de meetkunde dat gaat over projecties en projecteren. Bij centrale projectie vanuit een punt O kan men een vlak V projecteren op een vlak V': de projectie van een punt P van V is het snijpunt P' van de lijn OP met V'. Punten van V waarvoor OP evenwijdig is met V' hebben geen projectie en een punt P' van V', waarvoor OP' evenwijdig met V is, heeft geen origineel in V.



Deze uitzonderingen verdwijnen als we de vlakken uitbreiden met "ideale" of "oneigenlijke" punten zó dat de oneigenlijke punten van ieder vlak $1-1$ korresponderen met de lijnen door O evenwijdig aan het vlak en afspreken dat zo'n lijn het vlak snijdt in het korresponderende oneigenlijke punt. De punten van dit uitgebreide vlak korresponderen nu bijectief met alle lijnen door O. Als een punt P in V via een lijn ℓ "naar oneindig gaat" dan is de limietstand van de lijn OP de rechte door O evenwijdig met ℓ en het met deze rechte korresponderende oneigenlijke punt noemt men daarom ook het *punt op oneindig* van ℓ. Dus evenwijdige rechten in V hebben hetzelfde punt op oneindig en de oneigenlijke punten van V korresponderen $1-1$ met de mogelijke richtingen in V.
We kunnen dit alles in algebra vertalen door te gebruiken dat een lijn door O bepaald is door z'n richtingsvector (a, b, c), waarbij we moeten opmerken dat (a, b, c) en $(\rho a, \rho b, \rho c)$ voor $\rho \neq 0$ dezelfde richting dus dezelfde lijn door O opleveren en dus ook hetzelfde punt (eigenlijk of oneigenlijk) van het projectieve vlak:

Definitie 2.1.1 $\mathbb{P}^2$, of nauwkeuriger $\mathbb{P}^2(k)$, bestaat uit de verzameling van de equivalentieklassen van drietallen $(a_0, a_1, a_2) \in k^3 \setminus \{(0,0,0)\}$. Twee drietallen $(a_0, a_1, a_2), (b_0, b_1, b_2) \in k^3 \setminus \{(0,0,0)\}$ heten equivalent als er een $\lambda \in k, \lambda \neq 0$, is met $(a_0, a_1, a_2) = \lambda(b_0, b_1, b_2)$. De equivalentieklasse van (a_0, a_1, a_2) noteren we voorlopig met

$$(a_0 : a_1 : a_2).$$

Voor een punt $P = (a_0 : a_1 : a_2) \in \mathbb{P}^2$ heten (a_0, a_1, a_2) *homogene coördinaten van* P.

2.1.2 Er is een natuurlijke bijectie tussen $\mathbb{P}^2(k)$ en de verzameling bestaande uit de lijnen in k^3 door $(0,0,0)$. Die bijectie τ geeft men door:

$$P = (a_0 : a_1 : a_2) \overset{\tau}{\mapsto} \text{ de lijn } k(a_0, a_1, a_2) \text{ in } k^3 \text{ door } (0,0,0).$$

Deze bijectie gebruikt men bij de definitie van "rechte lijn" in $\mathbb{P}^2$:

> Een deelverzameling L van $\mathbb{P}^2$ heet een rechte (lijn) als $\tau(L)$ bestaat uit alle lijnen door $(0,0,0)$ in een vlak V in k^3 door $(0,0,0)$.

Men ziet gemakkelijk:

(i) door twee punten P_1, P_2 van $\mathbb{P}^2$ met $P_1 \neq P_2$ gaat precies één rechte,

(ii) twee verschillende rechten L_1, L_2 in $\mathbb{P}^2$ snijden in één punt.

2.1.3 Het affiene vlak $\mathbb{A}^2$ kan men met een deelverzameling U_0 van $\mathbb{P}^2$ identificeren via de afbeelding

$$(a_1, a_2) \mapsto (1 : a_1 : a_2).$$

Het beeld van $\mathbb{A}^2$ onder deze afbeelding is

$$U_0 := \{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid a_0 \neq 0\}$$

en de inverse afbeelding $U_0 \to \mathbb{A}^2$ wordt gegeven door

$$(a_0 : a_1 : a_2) \mapsto \left(\frac{a_1}{a_0}, \frac{a_2}{a_0}\right),$$

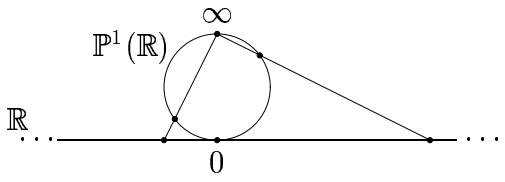
want $(a_0 : a_1 : a_2) = (1 : \frac{a_1}{a_0} : \frac{a_2}{a_0})$ als $a_0 \neq 0$.

2.1.4 *De projectieve rechte* $\mathbb{P}^1$ (of $\mathbb{P}^1(k)$) wordt geheel analoog gedefinieerd. De verzameling $\mathbb{P}^1$ bestaat uit de equivalentieklassen, genoteerd als $(a_0 : a_1)$, van paren $(a_0, a_1) \in k^2 \setminus \{(0,0)\}$, waarbij de equivalentierelatie gegeven is door:

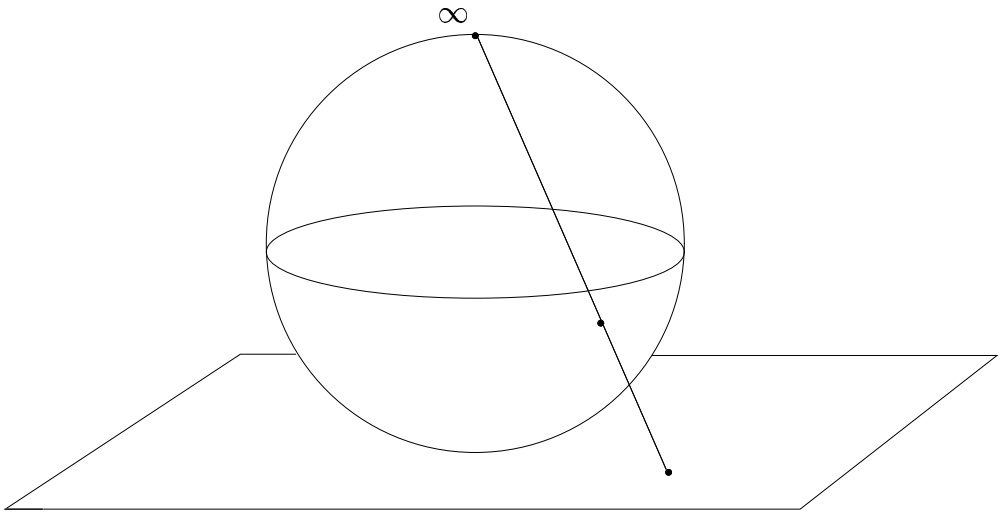
$$(a_0, a_1) \sim (b_0, b_1) \Leftrightarrow \text{ er is een } \lambda \in k \text{ met } \lambda \neq 0 \text{ zodat } (a_0, a_1) = \lambda(b_0, b_1)$$

Zoals boven kan men de $\mathbb{P}^1$ zien als de collectie van alle lijnen in k^2 door $(0,0)$. De afbeelding $a_1 \in \mathbb{A}^1(k) = k \mapsto (1 : a_1) \in \mathbb{P}^1$ geeft een inbedding van $\mathbb{A}^1$ in $\mathbb{P}^1$. Nu bestaat $\mathbb{P}^1 \setminus \mathbb{A}^1$ uit precies één punt namelijk $(0 : 1)$. Dit punt noemt men het "*punt op oneindig*". Er zijn natuurlijk andere inbeddingen van $\mathbb{A}^1$ in $\mathbb{P}^1$, bijvoorbeeld $a_1 \mapsto (a_1 : 1)$. Voor een andere inbedding vindt men in het algemeen een ander punt op oneindig. Voor de standaard inbedding $a_1 \mapsto (1 : a_1)$ schrijft men vaak ∞ voor het punt $(0 : 1)$. Met die notatie is $\mathbb{P}^1 = k \cup \{\infty\}$.

2.1.5 Voor de speciale gevallen $k = \mathbb{R}$ (niet algebraïsch gesloten) en $k = \mathbb{C}$ kan men zich een topologische voorstelling maken van de projectieve rechten $\mathbb{P}^1(\mathbb{R})$ en $\mathbb{P}^1(\mathbb{C})$. Bij $\mathbb{P}^1(\mathbb{R})$ stelt men zich vaak een cirkel voor, die door projectie uit het punt ∞ met $\mathbb{R}$ verbonden wordt:



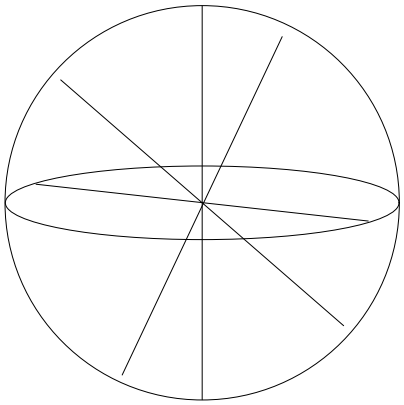
De $\mathbb{A}^1(\mathbb{C})$ is in feite het gewone, reële vlak. De complexe projectieve rechte $\mathbb{P}^1(\mathbb{C})$ ontstaat hieruit door één punt op oneindig toe te voegen. Men kan hierbij denken aan een bol waarop een punt ∞ gekozen is en waarvan de punten $\neq \infty$ door *stereografische projectie* met de punten van $\mathbb{C}$ worden geïdentificeerd. $\mathbb{P}^1(\mathbb{C})$ heet daarom ook de *complexe bol*.

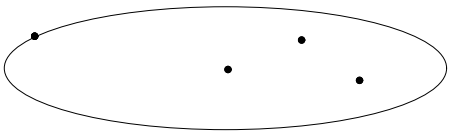


2.1.6 *De oneigenlijke rechte in* $\mathbb{P}^2$. De verzameling $\mathbb{P}^2 \setminus \mathbb{A}^2$ is $\{(a_0 : a_1 : a_2) \mid a_0 = 0\}$. Dit is een rechte van $\mathbb{P}^2$, genaamd de oneigenlijke rechte of ook de rechte op oneindig. Die rechte is een $\mathbb{P}^1$, want er is een bijectie $\mathbb{P}^1 \to \mathbb{P}^2 \setminus \mathbb{A}^2 = \mathbb{P}^2 \setminus U_0$ gegeven door $(a : b) \mapsto (0 : a : b)$.

2.1.7 Het beeldend voorstellen van $\mathbb{P}^2(\mathbb{R})$ en $\mathbb{P}^2(\mathbb{C})$ is nogal moeilijk. De $\mathbb{P}^2(\mathbb{C})$ is reëel gezien 4-dimensionaal en we doen geen poging om daar wat van te maken. De $\mathbb{P}^2(\mathbb{R})$ is 2-dimensionaal en "reëel gezien" een oppervlak. Volgens het voorgaande bestaat $\mathbb{P}^2(\mathbb{R})$ uit de lijnen door $(0, 0, 0)$ in de $\mathbb{R}^3$. We leggen in de $\mathbb{R}^3$ een halve bol met middelpunt $(0, 0, 0)$. Een lijn ℓ door $(0, 0, 0)$ snijdt dit halve boloppervlak in het algemeen in één punt. Uitzondering daarop maken de lijnen ℓ die de randcirkel C (de begrenzing van het halve boloppervlak) snijden. Zo'n lijn snijdt C in twee diametrale punten.

Een meetkundig beeld van $\mathbb{P}^2(\mathbb{R})$ krijgt men door het halve boloppervlak op de cirkelschijf met rand C te projecteren en daarna diametrale punten van C te identificeren.





Dus:

> $\mathbb{P}^2(\mathbb{R})$ wordt topologisch gerepresenteerd door een cirkelschijf in het vlak waarbij diametrale punten van de rand geïdentificeerd worden.

Het identificeren van die diametrale punten zou men kunnen proberen te doen door de rand C op zichzelf te plakken. Dat kan echter niet in $\mathbb{R}^3$! Men kan bewijzen dat het boven beschreven model van $\mathbb{P}^2(\mathbb{R})$ wél in $\mathbb{R}^4$ past. De moeilijkheden bij de meetkundige voorstelling van $\mathbb{P}^2(\mathbb{R})$ en $\mathbb{P}^2(\mathbb{C})$ storen natuurlijk niet bij het werken met deze ruimten evenmin als dat het geval is met $\mathbb{R}^n$ voor $n > 3$.

2.2 Projectieve krommen.

2.2.1 Bij iedere kromme $Z = Z(f)$ in het affiene vlak $\mathbb{A}^2$ hoort, via de inbedding $(a_1, a_2) \mapsto (1 : a_1 : a_2)$ van $\mathbb{A}^2$ in $\mathbb{P}^2$, een zogenaamde *projectieve afsluiting* in $\mathbb{P}^2$. Als voorbeeld nemen we de hyperbool Z met vergelijking

$$x^2 - y^2 + x + 1 = 0.$$

Onder de genoemde inbedding gaat deze over in de verzameling van de punten

$$(u : x : y) = \left(1 : \frac{x}{u} : \frac{y}{u}\right) \quad (u \neq 0)$$

die voldoen aan

$$\left(\frac{x}{u}\right)^2 - \left(\frac{y}{u}\right)^2 + \left(\frac{x}{u}\right) + 1 = 0 \quad (u \neq 0).$$

Na wegwerken van de noemers wordt dit

$$(*) \qquad x^2 - y^2 + ux + u^2 = 0.$$

Aan de laatste vergelijking voldoen, behalve de 'gewone' punten $(x, y) = (1 : x : y)$ (met $u = 1$) ook nog de 'oneigenlijke' punten $(0 : 1 : 1)$ en $(0 : 1 : -1)$. Deze vinden we door in $(*)$ $u = 0$ te nemen. Ze korresponderen met de asymptoot-richtingen $x - y = 0$ en $x + y = 0$ van de hyperbool in $\mathbb{A}^2$. We merken nog op dat bij de oplossing $(0, 0, 0)$ van $(*)$ geen projectief punt hoort. Bovendien is van essentieel belang: als (u, x, y) een oplossing van $(*)$ is, dan voldoet voor elke $\rho \neq 0$ ook $(\rho u, \rho x, \rho y)$ en omgekeerd. Dit komt doordat elke term van het polynoom $f^* = X^2 - Y^2 + UX + U^2$ in het linkerlid van $(*)$ graad 2 heeft; dus $f^*(\rho u, \rho x, \rho y) = \rho^2 f^*(u, x, y)$. We kunnen dus spreken over de projectieve punten $(u : x : y)$ die aan $(*)$ voldoen. Deze vormen per definitie de projectieve afsluiting van de hyperbool. Dit geeft aanleiding tot wat definities.

Definitie 2.2.2 Een polynoom $f = \sum a_{i_1} \cdots a_{i_n} X_1^{i_1} \cdots X_n^{i_n}$ in n onbepaalden $X_1, \ldots, X_n$ heet *homogeen van graad d* als f alleen termen van graad d, d.w.z. met $i_1 + \cdots + i_n = d$, bezit. Elke $f \in k[X_1, \ldots, X_n]$ van graad n is uniek te schrijven als een som $f = \sum_{i=0}^{n} f_i$ met f_i = som van alle termen van graad i in f of $f_i = 0$. Deze f_i noemen we de *homogene componenten* van f.

Definitie 2.2.3 Zij f een homogeen polynoom in X_0, X_1, X_2 met graad $d \geq 1$. Dan is $Z(f) = \{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid f(a_0, a_1, a_2) = 0\}$ een kromme in $\mathbb{P}^2$ en wel een *kromme van graad d.*

Het homogene polynoom f van graad d voldoet aan $f(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^d f(a_0, a_1, a_2)$. Dit maakt de definitie van $Z(f)$ zinvol, want dit heeft tot gevolg: als (a_0, a_1, a_2), $(b_0, b_1, b_2) \in k^3 \setminus \{(0,0,0)\}$ equivalent zijn, dan geldt $f(a_0, a_1, a_2) = 0 \Leftrightarrow f(b_0, b_1, b_2) = 0$.

2.2.4 De rechte lijnen in $\mathbb{P}^2$ die in 2.1.2 zijn ingevoerd zijn precies de krommen Z met $Z = Z(f)$ en graad $f = 1$. Verder: *kwadriek* = 2^{de}-graads kromme, *kubische kromme* = 3^{de}-graads kromme. Een kromme $Z(f)$ heet *irreducibel* als f irreducibel is. We hebben weer:

Stelling 2.2.5 *Iedere kromme in* $\mathbb{P}^2$ *is een eindige vereniging van irreducibele krommen.*

Bewijs. Een homogeen polynoom f met graad $(f) \geq 1$ is uniek te ontbinden in irreducibele factoren: $f = f_1^{n_1} \cdots f_t^{n_t}$. Dus als we kunnen aantonen dat elke factor f_i noodzakelijkerwijs homogeen is, dan zijn we klaar. Het volgende lemma zegt dat er zelfs nog iets meer geldt.

Lemma 2.2.6 *Als het product van twee (of meer) polynomen homogeen is, dan is elke factor homogeen.*

Bewijs. We splitsen $f, g \in k[X_1, \ldots, X_n]$ in homogene componenten:

$$f = \sum_{i=a}^{m} f_i \quad , \quad g = \sum_{j=b}^{n} g_j \text{ met } a \leq m, b \leq n; f_a, g_b, f_m, g_n \text{ alle } \neq 0.$$

Daar een product $f_i g_j$ homogeen van graad $i + j$ is (of gelijk 0) heeft het product fg de volgende splitsing in homogene componenten:

$$fg = \sum_{k=a+b}^{m+n} \left(\sum_{i+j=k} f_i g_j \right)$$

Hieruit zien we: als fg homogeen is, dan is $a + b = m + n$, dus $a = m, b = n$, d.w.z. dan zijn f en g beide homogeen.

In 3.4 zullen we zien dat de splitsing van een kromme in irreducibele krommen ook in de $\mathbb{P}^2$ uniek is.

2.3 Projectieve transformaties.

2.3.1 Ook op $\mathbb{P}^2$ laten we transformaties toe. Voor een 3×3-matrix $A = (\lambda_{ij})_{i,j=0,1,2}$ met $\det A \neq 0$ beschouwen we de afbeelding $\varphi_A : \mathbb{P}^2 \to \mathbb{P}^2$, gegeven door

$$\varphi_A(a_0 : a_1 : a_2) = \left(\sum_i \lambda_{0i} a_i : \sum_i \lambda_{1i} a_i : \sum_i \lambda_{2i} a_i \right)$$

Merk op dat dit een zinvolle definitie is. Het is natuurlijk hetzelfde als A werkend op de vector $(a_0, a_1, a_2) \in k^3$.
Er geldt:

$$\varphi_{AB} = \varphi_A \circ \varphi_B, \quad \varphi_{\lambda I} = \text{ identiteit } (\lambda \neq 0), \quad \varphi_A \text{ is bijectief.}$$

De groep van al deze transformaties wordt $PG\ell(3,k)$ genoemd, de *projektieve lineaire groep.*
Het homomorfisme $\varphi : G\ell(3,k) \to PG\ell(3,k)$ met $A \mapsto \varphi_A$ is surjectief. Z'n kern bestaat uit de matrices A met $\varphi_A =$ identiteit. Het laatste betekent dat elke $a \in k^3 \setminus \{(0,0,0)\}$ een eigenvector van A is; met een beetje lineaire algebra leidt men hieruit af dat $A = \lambda I$ met $0 \neq \lambda \in k$. De eerste isomorfie stelling (voor groepen) geeft

$$PG\ell(3,k) \cong G\ell(3,k)/\{\lambda I \mid 0 \neq \lambda \in k\}.$$

Bovenstaande klopt mooi met de interpretatie: de punten van $\mathbb{P}^2$ zijn de lijnen in k^3 door $(0,0,0)$. De gewone werking van de matrix A op k^3 levert een werking van A vop de lijnen door $(0,0,0)$ in k^3; die werking is juist de φ_A. De transformaties φ_A noemen we ook wel *projectieve transformaties* of *automorfismen* en $PG\ell(3,k)$ de *automorfismengroep* van $\mathbb{P}^2$.

2.3.2 De kwadrieken in $\mathbb{P}^2$.

Door automorfismen te gebruiken kan men krommen in $\mathbb{P}^2$ vaak op eenvoudige gedaante brengen. Zo'n automorfisme komt op hetzelfde neer als een substitutie $X_i \to X_i' := \sum_j a_{ij} X_j$ met $\det(a_{ij}) \neq 0$.

In het volgende gebruiken we de letters U, X, Y voor X_0, X_1, X_2 (en U_1, X_1, Y_1 etc. voor "nieuwe" variabelen). Voor 2-de graads krommen vindt men na toepassing van de transformaties de volgende "standaard-vergelijkingen"

(i) X^2 (dubbele lijn)

(ii) XY (twee lijnen)

(iii) $XY + U^2$ (irreducibele kwadriek).

Men ziet: ten opzichte van de affiene situatie is het aantal mogelijkheden verminderd. We komen hier nog op terug (2.4.2).

Bewijs.
Het homogene 2-de graadspolynoom $f = f(U,X,Y)$ kan reducibel zijn. Dan is het een kwadraat van een homogeen polynoom $X_1 = aU + bX + cY$ of een product van twee niet-equivalente dergelijke polynomen $X_1 = aU + bX + cY$ en $Y_1 = a'U + b'X + c'Y$; dit geeft, na geschikte keuze van Y_1 en U_1 resp. U_1, de vorm (i) resp. (ii). Stel vervolgens dat f irreducibel is. We kunnen schrijven

$$f = g(X,Y) + \ell(U,X,Y)U$$

met $g \neq 0$ en $\ell \neq 0$ omdat f irreducibel is, g en ℓ homogeen van graad 2 resp. 1.

Er zijn twee mogelijkheden
1) g is een kwadraat
2) g is een product van twee niet-equivalente lineare polynomen (in X, Y). Na een transformatie van de vorm $X_1 = aX + bY$, $Y_1 = cX + dY$, $U_1 = U$ krijgt f resp. de vorm
1) $f = X_1^2 + (\lambda U_1 + \mu X_1 + \nu Y_1)U_1$,
2) $f = X_1 Y_1 + (\lambda U_1 + \mu X_1 + \nu Y_1)U_1$.
In geval 1) is $\nu \neq 0$ (want f is irreducibel). We voeren nu in $U_2 = X_1, X_2 = \lambda U_1 + \mu X_1 + \nu Y_1, Y_2 = U_1$. Dit geeft de vorm (iii) voor f. In geval 2) schrijven we $f = (X_1 + \nu U_1)(Y_1 + \mu U_1) + (\lambda - \mu\nu)U_1^2 = X_2 Y_2 + U_2^2$, weer de vorm (iii), $(\lambda - \mu\nu \neq 0$ omdat f irreducibel is).

2.3.3 Met een beetje lineaire algebra is te zien, bij welke van de drie standaardvergelijkingen een gegeven kwadriek in $\mathbb{P}^2$ hoort. Dit gaat bijvoorbeeld als volgt.

We werken over een (algebraïsch afgesloten) lichaam k van karakteristiek $\neq 2$. Op de lineaire ruimte $V = K^3$ hebben we een niet-ontaarde bilineaire vorm $\langle \cdot, \cdot \rangle : V \times V \to K$, gegeven door

$$\langle \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \rangle = v_1 w_1 + v_2 w_2 + v_3 w_3.$$

Een homogeen tweedegraads polynoom $F(X, Y, U)$ is dan te schrijven als $\langle Av, v \rangle$, met $v = \begin{pmatrix} X \\ Y \\ U \end{pmatrix}$ en A een symmetrische 3×3 matrix. De coördinatentransformatie met een matrix B komt dan neer op het vervangen van A door $B^t \cdot A \cdot B$, waar B^t de gespiegelde is van B (eigenlijk stelt deze de geadjungeerde voor ten opzichte van $\langle \cdot, \cdot \rangle$ van de door B gegeven lineaire afbeelding).
Komen we na substitutie zo uit op de kwadratische vorm X^2, dan is kennelijk

$$B^t \cdot A \cdot B = \begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix}.$$

Komen we uit op XY, dan

$$B^t \cdot A \cdot B = \begin{pmatrix} 0 & \frac{1}{2} & \\ \frac{1}{2} & 0 & \\ & & 0 \end{pmatrix}$$

en bij $XY + U^2$ hadden we

$$B^t \cdot A \cdot B = \begin{pmatrix} 0 & \frac{1}{2} & \\ \frac{1}{2} & 0 & \\ & & 1 \end{pmatrix}.$$

Omdat geldt $\text{rang}(A) = \text{rang}(B^t \cdot A \cdot B)$ volgt dus:

Stelling 2.3.4 *Zij $A \neq 0$ een symmetrische 3×3 matrix en $v = \begin{pmatrix} X \\ Y \\ U \end{pmatrix}$.*

De vergelijking $\langle Av, v \rangle = 0$ beschrijft in $\mathbb{P}^2$:

(i) een irreducibele kwadriek als $\det(A) \neq 0$*;*

(ii) twee snijdende lijnen als rang$(A) = 2$*;*

(iii) een (dubbele) lijn als rang$(A) = 1$*.* □

In geval (iii) is de vergelijking van het vlak $\text{Ker}(A)$ natuurlijk ook precies de vergelijking van de gegeven (dubbele) lijn in $\mathbb{P}^2$.
In geval (ii) kan je in het vlak $\text{Beeld}(A)$ precies twee lijnen vinden zodat $\langle Av, v \rangle = 0$ voor alle v op die lijnen: dit komt omdat we hier in feite de hele situatie mogen beperken tot het beeld van A, en dat heeft dimensie 2 en dus krijgen we een homogene kwadratische vergelijking in 2 variabelen. Elk van de twee gevonden lijnen spant samen met $\text{Ker}(A)$ een vlak op. De beide in K^3 zo verkregen vlakken corresponderen precies met de gevraagde lijnen in $\mathbb{P}^2$.

2.4 Het verband tussen de krommen in $\mathbb{A}^2$ en de krommen in $\mathbb{P}^2$.

2.4.1 We zien de $\mathbb{A}^2$ steeds als deelverzameling van $\mathbb{P}^2$ door de afbeelding

$$\begin{array}{rcl}(x,y) & \mapsto & (1:x:y) \text{ met inverse} \\ (u:x:y) & \mapsto & \left(\frac{x}{u},\frac{y}{u}\right) \quad (u\neq 0).\end{array}$$

Zij $Z=Z(f)$ een kromme van graad n in $\mathbb{A}^2$, $f=\sum c_{ij}X^iY^j$. Een punt $(u:x:y)\in\mathbb{A}^2\subset\mathbb{P}^2$, dus met $u\neq 0$, behoort tot de kromme precies dan als

$$\sum c_{ij}\left(\frac{x}{u}\right)^i\left(\frac{y}{u}\right)^j=0.$$

De noemers werken we weg door met u^n te vermenigvuldigen. We krijgen de vergelijking

$$\sum c_{ij}u^{n-i-j}x^iy^j=0.$$

Dit is een homogene vergelijking van graad n. Het bijbehorende polynoom geven we aan met f^*:

$$f^*(U,X,Y)=U^nf\left(\frac{X}{U},\frac{Y}{U}\right)=\sum c_{ij}U^{n-i-j}X^iY^j.$$

Deze f^* ontstaat dus uit f door elke term met die macht van U te vermenigvuldigen die de graad op n brengt.
Er geldt dus, dat $Z(f^*)$ een n-de graadskromme in $\mathbb{P}^2$ is, met de eigenschap

$$Z(f^*)\cap\mathbb{A}^2=Z(f)$$

of, in wat uitvoeriger notatie waarin duidelijker uitkomt dat het om krommen in $\mathbb{P}^2$ resp. $\mathbb{A}^2$ gaat,

$$Z_{\mathbb{P}^2}(f^*)\cap\mathbb{A}^2=Z_{\mathbb{A}^2}(f).$$

Inderdaad: $f^*(1,X,Y)=f(X,Y)$.
De punten van $Z_{\mathbb{P}^2}(f^*)\setminus Z_{\mathbb{A}^2}(f)$ zijn precies de oplossingen $(0:\lambda:\mu)$ van $f^*(0,x,y)=0$. Ze heten de punten op oneindig van $Z_{\mathbb{A}^2}(f)$ omdat ze op de oneigenlijke rechte $u=0$ in $\mathbb{P}^2$ liggen.

Bewering: Het aantal punten op ∞ is $\leq n$.

Bewijs. We schrijven f in homogene componenten: $f=\sum_0^n f_i$. Dan is

$$f^*(U,X,Y)=\sum_i U^{n-i}f_i(X,Y).$$

Voor de punten op oneindig levert dit de vergelijking

$$f^*(0,x,y)=f_n(x,y)=0.$$

De ontbinding van $f^*(0,X,Y)=f_n(X,Y)$ in lineaire factoren $\ell_1,\ldots,\ell_n$ levert voor elke lineaire factor een punt. Hiervan kunnen sommige samenvallen. Dus het aantal punten op ∞ is $\leq n$. □

Voorbeelden 2.4.2 1. We kiezen voor $Z_{\mathbb{A}^2}(f)$ een 2de-graadskromme en werken het lijstje van standaardkwadrieken in 1.3.2 af.

(i) $f = X^2$, $f^* = X^2$, met één punt, $(0:0:1)$ op oneindig

(ii) $f = XY$, $f^* = XY$, twee punten, $(0:1:0)$ en $(0:0:1)$ op oneindig

(iii) $f = X(X-1)$, $f^* = X(X-U)$, één punt, $(0:0:1)$ op oneindig

(iv) $f = X^2 + Y$, $f^* = X^2 + UY$, één punt, $(0:0:1)$ op oneindig

(v) $f = XY - 1$, $f^* = XY - U^2$, twee punten op oneindig, $(0:1:0)$ en $(0:0:1)$.

We merken nog op dat de gevallen (ii) en (iii) projectief gezien gelijkwaardig zijn, want in beide gevallen gaat het om twee snijdende rechten. In geval (ii) is het snijpunt een eigenlijk punt, in geval (iii) een oneigenlijk punt. Bij het doorsnijden met $\mathbb{A}^2$ verdwijnt dit oneigenlijke snijpunt en houden we twee evenwijdige rechten in $\mathbb{A}^2$ over. Evenzo hebben we in geval (iv) en (v) irreducibele kwadrieken, die projectief gelijkwaardig zijn. In geval (iv) raakt deze aan de oneigenlijke rechte (er zijn "twee samenvallende" snijpunten), in geval (iv) snijdt hij de oneigenlijke rechte in twee verschillende punten.
De kwadrieken (iv) en (v) zijn wel door een projectieve, maar niet door een affiene transformatie in elkaar over te voeren. Affiene transformaties zijn op te vatten als speciale projectieve transformaties, namelijk die welke de oneigenlijke rechte invariant laten (niet puntsgewijs, maar in z'n geheel).

2. Voor de kubische kromme $f = X^3 + Y^3 - XY$ is $f^* = X^3 + Y^3 - UXY$ en er zijn drie punten op oneindig, namelijk $(0:\omega^i:-1)$ (voor $i = 0, 1, 2$), waarbij ω een wortel $\neq 1$ van de vergelijking $x^3 = 1$ is. Althans als $kar(k) \neq 3$. In geval dat $kar(k) = 3$, is er maar één punt op oneindig, namelijk $(0:1:-1)$ omdat in zo'n lichaam geldt $x^3 + y^3 = (x+y)^3$.

2.4.3 *(Dé)homogeniseren.* Boven hebben we uitgaande van een al of niet homogeen polynoom $f(X,Y)$ het homogene polynoom $f^*(U,X,Y) = U^n f\left(\frac{X}{U}, \frac{Y}{U}\right)$ gevormd. Dit zou men het *homogeniseren* van f kunnen noemen. Als je in $f^*(U,X,Y)$ voor U de waarde 1 substitueert krijg je f terug. Dit is dan *déhomogeniseren.* De notatie hiervoor is

$$f_*(X,Y) = f(1,X,Y) \text{ voor een homogeen polynoom } f = f(U,X,Y).$$

Blijkbaar geldt

$$(f^*)_* = f \text{ voor elke } f = f(X,Y) \in k[X,Y].$$

Omgekeerd:

$$(f_*)^* = f \text{ als } f \text{ homogeen in } U,X,Y \text{ is en niet deelbaar door } U.$$

Als de homogene f wél deelbaar is door U, dan $f = U^d g(U,X,Y)$ met $d \geq 1$ en g niet deelbaar door U; in dit geval is $(f_*)^* = g$. Meetkundig is dit ook wel duidelijk: $Z_{\mathbb{P}^2}(f)$ bevat de oneigenlijke rechte $Z_{\mathbb{P}^2}(U)$ als irreducibele component. Bij het doorsnijden met $\mathbb{A}^2$ raakt men die kwijt.

2.4.4 Toepassing: het oplossen van $x^4 + ax^3 + bx^2 + cx + d = 0$.
Een formule voor de wortels van een kwadratische vergelijking kennen we allemaal. Het volgende geval, de derdegraads vergelijking, is door een substitutie $X := x + \alpha$ te herleiden tot

$$x^3 + ax + b = 0.$$

Dit kan als volgt worden opgelost. Merk op dat

$$(\lambda+\mu)^3 - 3\lambda\mu(\lambda+\mu) - (\lambda^3 + \mu^3) = 0.$$

Hieraan zie je dat de nulpunten van $x^3 + ax + b$ te schrijven zijn als $x = \lambda + \mu$, waarbij

$$\begin{cases} \lambda\mu = & -a/3 \\ \lambda^3 + \mu^3 = & -b. \end{cases}$$

Er volgt dat λ^3 en μ^3 de wortels zijn van $Y^2 + bY - a^3/27 = 0$, en daarmee is een formule voor λ, μ en dus voor $x = \lambda + \mu$ gevonden.
We gaan als kleine toepassing van de tot nu toe behandelde theorie de vierdegraads vergelijking tot bovenstaand geval herleiden. Herschrijf daartoe de vergelijking

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

als een stelsel

$$\begin{cases} F := & x^2 - y & = 0 \\ G := & y^2 + axy + by + cx + d & = 0. \end{cases}$$

Dit vatten we op als het vinden van de snijpunten van twee kwadrieken. Dit gaan we oplossen met behulp van een eenvoudige observatie: de gezochte snijpunten veranderen niet, wanneer we bij de tweede vergelijking t maal de eerste optellen, voor willekeurige $t \in K$. Anders gezegd: we mogen de kwadriek gegeven door $G = 0$ vervangen door die met $G + tF = 0$.
Het idee is nu, deze $t \in K$ zo te kiezen dat de nieuwe kwadriek een dubbele lijn of een vereniging van twee lijnen is. Deze lijnen zijn dan eenvoudig op te schrijven (zie § 2.3.3), en de snijpunten van $F = 0$ met zo'n lijn zijn vervolgens gemakkelijk te berekenen. Daarmee is het probleem dan opgelost.
Een geschikte $t \in K$ vind je als volgt. Na homogeniseren wordt de nieuwe kwadriek in $\mathbb{P}^2$ gegeven door

$$tX^2 = Y^2 + dU^2 + aXY + cXU + (b - t)YU = 0.$$

Een t als gevraagd is dan vanwege Stelling 2.3.4 een oplossing van

$$\det \begin{pmatrix} 2t & a & c \\ a & 2 & b - t \\ c & b - t & 2d \end{pmatrix} = 0.$$

Dit is "slechts" een derdegraads vergelijking, en die konden we al ...

2.4.5 Tot slot van deze inleiding over krommen in $\mathbb{P}^2$ willen we nog een beroemde stelling, de stelling van Bézout, vermelden. Ter toelichting eerst het volgende.
Voor een snijpunt van een rechte met een kromme in $\mathbb{P}^2$ kan men een multipliciteit definiëren precies zoals in $\mathbb{A}^2$ (zie 1.4.2): met een projectieve transformatie maak je er eerst een 'gewoon' punt van en je gaat verder te werk zoals in 1.4.2. Daarbij moet natuurlijk aangetoond worden dat de zo gedefinieerde multipliciteit invariant is onder projectieve transformaties. Dit is wat bewerkelijk (maar niet moeilijk) en we laten het daarom achterwege. Daarna is het niet moeilijk te zien dat elke rechte, die niet in z'n geheel tot de kromme behoort, precies n snijpunten, geteld met multipliciteit, met een kromme van graad n heeft.
Voor de snijpunten van willekeurige krommen in $\mathbb{A}^2$ en $\mathbb{P}^2$ kan men ook een multipliciteit definiëren. Dit is lastiger. Voor krommen in $\mathbb{P}^2$ geldt nu:

Stelling van Bézout. Twee krommen $Z(f)$ en $Z(g)$ in $\mathbb{P}^2$ van graad m respectievelijk n hebben precies mn snijpunten als deze geteld worden met multipliciteit en onder de voorwaarde dat f en g geen gemeenschappelijke component hebben (onderling ondeelbaar zijn).

Voor een tamelijk lang, maar volkomen elementair bewijs van deze stelling verwijzen we naar Appendix A, § 4 van het boekje Joseph H. Silverman en John Tate, *Rational Points on Elliptic Curves.* (Springer-Verlag, Undergraduate Texts in Mathematics, 1992.)
In $\mathbb{A}^2$ geldt de stelling niet. Bij elke kromme $Z_{\mathbb{A}^2}(f)$ kan men wel een kromme $Z_{\mathbb{A}^2}(g)$ vinden met $Z_{\mathbb{A}^2}(g) \cap Z_{\mathbb{A}^2}(f) = \emptyset$. Bijvoorbeeld $g = f + 1$. De missende snijpunten vindt men in de $\mathbb{P}^2$ op de oneigenlijke rechte. (In ons voorbeeld: als graad $(f) = n$ dan is $g^* = f^* + X_0^n$ en $Z_{\mathbb{P}^2}(f^*) \cap Z_{\mathbb{P}^2}(g^*) = Z_{\mathbb{P}^2}(f^*) \cap Z_{\mathbb{P}^2}(X_0^n)$ bestaat precies uit n^2 punten, geteld met multipliciteit, als we afspreken dat een m-voudig snijpunt P van $Z_{\mathbb{P}^2}(f^*)$ en $Z_{\mathbb{P}^2}(X_0)$ als een (mn)-voudig snijpunt van $Z_{\mathbb{P}^2}(f^*)$ en $Z_{\mathbb{P}^2}(X_0^n)$ telt).

3 Affiene en projectieve verzamelingen in dimensie n.

3.1 Algebraïsche verzamelingen in $\mathbb{A}^n$.

3.1.1 De affiene n-dimensionale ruimte $\mathbb{A}^n$ bestaat uit de punten $(a_1, \ldots, a_n) \in k^n$. *Reguliere functies* op $\mathbb{A}^n$ zijn polynomen $f \in k[X_1, \ldots, X_n]$ die opgevat worden als functies $\mathbb{A}^n \to k$ door middel van de formule $f(P) = f(a_1, \ldots, a_n)$ als $P = (a_1, \ldots, a_n)$.
Een *algebraïsche verzameling* in $\mathbb{A}^n$ is per definitie een verzameling $Z = Z(T)$ waarbij $T \subset k[X_1, \ldots, X_n]$ een verzameling polynomen is en $Z(T)$ de verzameling van de gemeenschappelijke nulpunten van alle $f \in T$:

$$Z(T) = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ voor iedere } f \in T\}.$$

Voorbeelden 3.1.2

1. Elk punt P vormt een algebraïsche verzameling, want als $P = (a_1, \ldots, a_n)$, dan $\{P\} = Z(\{X_1 - a_1, \ldots, X_n - a_n\})$

2. $(n = 3.)$ Neem $T = \{X^2 + Y^2 - 1, X^2 + Y^2 + Z^2 - 2\}$. Dan bestaat $Z(T)$ uit twee "cirkels" in de vlakken $z = \pm 1$: $Z(T) = Z(I)$ waarbij I het volgende ideaal in $k[X, Y, Z]$ is: $I = (X^2 + Y^2 - 1, X^2 + Y^2 + Z^2 - 2) = (X^2 + Y^2 - 1, Z^2 - 1)$ en $Z(I) = Z(X^2 + Y^2 - 1, Z - 1) \cup Z(X^2 + Y^2 - 1, Z + 1)$.

3. $(n = 3)$. De verzameling $Z(\{X^2 - Y^2, X + Z\}) = \{(a, a, -a) \mid a \in k\} \cup \{(a, -a, -a) \mid a \in k\}$ bestaat uit twee snijdende rechten.

4. Als T uit één niet-constant polynoom f bestaat dan heet $Z(f)$ een *hyper-oppervlak* ($n = 2$: kromme, $n = 3$: *oppervlak*), een d-de graads (hyper-)oppervlak als graad $(f) = d$. Een *kwadriek* in $\mathbb{A}^3$ is weer een 2-de graads oppervlak. Een *kubisch oppervlak* in $\mathbb{A}^3$ wordt door een derdegraads polynoom, b.v. $X^3 + Y^3 + Z^3 + 1$ gegeven.

3.1.3 Elke algebraïsche verzameling kan ook door eindig veel vergelijkingen worden gegeven, m.a.w. elke algebraïsche verzameling $\neq \emptyset$, $\mathbb{A}^n$ is doorsnede van eindig veel hyper-oppervlakken. Dit volgt uit Hilberts basis-stelling (zie onder) in combinatie met:

$Z(T) = Z(J)$, waarbij J het door T voortgebrachte ideaal is.

Bewijs. Het door T voortgebrachte ideaal J bestaat uit de polynomen van de vorm $g_1 f_1 + \cdots + g_k f_k$ met $g_1, \ldots, g_k \in k[X_1, \ldots, X_n]$, $f_1, \ldots, f_k \in T$ $(k = 0, 1, 2, \cdots)$. Hieruit volgt gemakkelijk: $P \in Z(T) \Leftrightarrow P \in Z(J)$.

Stelling 3.1.4 Hilbert's basisstelling. *Elk ideaal J in $k[X_1, \ldots, X_n]$ wordt door eindig veel polynomen voortgebracht, d.w.z. $J = (f_1, \ldots, f_r)$ voor zekere $f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$.*

Gevolg. Elke algebraïsche verzameling $Z(T)$ is met geschikte polynomen $f_1, \cdots, f_r$ te schrijven als $Z(T) = Z(\{f_1, \ldots, f_r\})$.

Definitie 3.1.5 Een ring heet een *Noetherse ring* als alle idealen in de ring door eindig veel elementen worden voortgebracht.
Hilbert's basisstelling zegt dus dat $k[X_1, \ldots, X_n]$ een Noetherse ring is. Voor $n = 1$ weten we dit: $k[X]$ is zelfs een hoofdideaalring, d.w.z. elk ideaal wordt door één element voortgebracht [Algebra 3.4.1]. Men moet dus nog bewijzen: R Noethers $\Rightarrow R[X]$ Noethers. Hiervoor verwijzen we naar een standaardtekst over commutatieve algebra, b.v. H. Matsumura, *Commutative Algebra*, of Chapter II § 3 Theorem 3.3 van M. Reid, *Undergraduate Algebraic Geometry*, Cambridge Univ. Press, 1994 (5de gecorrigeerde herdruk).

3.2 De Zariski-topologie op $\mathbb{A}^n$.

Met behulp van Hilbert's basisstelling kan men algebraïsche verzamelingen schrijven als vereniging van eindig veel "irreducibelen" en wel – onder zekere voorwaarden – weer uniek. Daar de situatie voor $n \geq 3$ veel gecompliceerder is dan bij $n = 2$ (je hebt punten, "krommen", "oppervlakken", $\cdots$, hyperoppervlakken) beschouwt men eerst de collectie van alle algebraïsche verzamelingen in $\mathbb{A}^n$.

Stelling 3.2.1 *De vereniging van twee (dus ook van eindig veel) algebraïsche verzamelingen en de doorsnede van willekeurig veel algebraïsche verzamelingen is weer een algebraïsche verzameling. Verder zijn $\emptyset$ en $\mathbb{A}^n$ algebraïsche verzamelingen.*

Bewijs. $Z(T_1) \cup Z(T_2) = Z(T_1T_2)$ waarbij T_1T_2 bestaat uit alle producten f_1f_2 met $f_1 \in T_1, f_2 \in T_2$. Inderdaad: als $P \in Z(T_1)$ of $P \in Z(T_2)$, dan $f_1(P)f_2(P) = 0$ voor alle $f_1f_2 \in T_1T_2$; als $P \notin Z(T_1) \cup Z(T_2)$ dan is er een $f_1 \in T_1$ met $f_1(P) \neq 0$ en een $f_2 \in T_2$ met $f_2(P) \neq 0$, dus $P \notin Z(T_1T_2)$, want $(f_1f_2)(P) \neq 0$. Verder is $\bigcap_{i \in I} Z(T_i) = Z(\bigcup_{i \in I} T_i)$ voor elke collectie $\{Z(T_i) \mid i \in I\}$ van algebraïsche verzamelingen. Tenslotte: $Z(1) = \emptyset$, $Z(0) = \mathbb{A}^n$.

De lezer zal bij de voorgaande stelling ongetwijfeld gedacht hebben aan de gesloten verzamelingen in $\mathbb{R}^n$ bekend uit de analyse of in een algemene metrische of zelfs topologische ruimte. Ter herinnering:

Definitie 3.2.2 Zij X een verzameling. Een topologie op X is een collectie $\mathcal{T}$ van deelverzamelingen van X welke aan de volgende voorwaarden voldoet:

(i) $\emptyset, X \in \mathcal{T}$

(ii) $Y_1, Y_2 \in \mathcal{T} \Rightarrow Y_1 \cap Y_2 \in \mathcal{T}$

(iii) $Y_i \in \mathcal{T}$ voor alle $i \in I \Rightarrow \bigcup_{i \in I} Y_i \in \mathcal{T}$ (met I een willekeurige index-verzameling).

De deelverzamelingen Y van X met $Y \in \mathcal{T}$ heten open verzamelingen. Een deelverzameling Z van X heet gesloten als $X - Z$ open is. De collectie $\mathcal{T}'$ van alle gesloten verzamelingen voldoet aan

(i') $X, \emptyset \in \mathcal{T}'$

(ii') $Z_1, Z_2 \in \mathcal{T}' \Rightarrow Z_1 \cup Z_2 \in \mathcal{T}'$

(iii') $Z_i \in \mathcal{T}'$ voor alle $i \in I \Rightarrow \bigcap_{i \in I} Z_i \in \mathcal{T}'$.

Er geldt verder: als $\mathcal{T}'$ een collectie deelverzamelingen van X is, die voldoet aan (i'), (ii'), (iii') en we definiëren $\mathcal{T}$ door: $\mathcal{T} = \{X - Z \mid Z \in \mathcal{T}'\}$, dan is $\mathcal{T}$ een topologie op X en $\mathcal{T}'$ de collectie van alle gesloten deelverzamelingen in deze topologie. Zo'n paar $(X, \mathcal{T})$ of $(X, \mathcal{T}')$ noemt men een *topologische ruimte*.

Dank zij de genoemde eigenschappen van de collectie van de algebraïsche verzamelingen kan men in de algebraïsche meetkunde dankbaar gebruik maken van allerlei topologische begrippen en resultaten!

Definitie 3.2.3 De algebraïsche verzamelingen in $\mathbb{A}^n$ vormen de gesloten verzamelingen van een topologie op X: deze topologie heet de *Zariski-topologie* op $\mathbb{A}^n$.

3.2.4 Een algebraïsche verzameling in $\mathbb{A}^n$ noemt men daarom ook wel *algebraïsch gesloten* of *Zariski-gesloten* of kortweg *gesloten*. In het geval dat $k = \mathbb{C}$ moet men natuurlijk goed onderscheiden tussen de "gewone", in de analyse gebruikte, topologie en de Zariski-topologie. De laatste is veel zwakker dan de "gewone" topologie op $\mathbb{C}^n$: elke Zariski-gesloten verzameling in $\mathbb{C}^n$ is ook "gewoon gesloten", maar niet omgekeerd; zie het volgende voorbeeld 1.

Voorbeelden 3.2.5

1. De gesloten deelverzamelingen van $\mathbb{A}^1$ zijn: $\emptyset, \mathbb{A}^1$, de eindige deelverzamelingen van $\mathbb{A}^1$. In het geval dat $k = \mathbb{C}$ vormen de Zariski-gesloten deelverzamelingen van $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$ dus een zéér kleine deelcollectie van de "gewoon gesloten" verzamelingen van $\mathbb{C} = \mathbb{R}^2$.

2. De functie $f(z) = e^{2\pi iz}$ is een prachtige functie ten opzichte van de gewone topologie op $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$ (holomorf, dus zeker continu en differentieerbaar). Maar voor de Zariski-topologie is de functie f zelfs niet continu: ga maar na dat bijvoorbeeld het volledig origineel van de Zariski-open verzameling $\mathbb{C} \setminus \{1\}$ niet Zariski-open is.

3. De gesloten deelverzamelingen van $\mathbb{A}^2$ zijn:
$\mathbb{A}^2, \emptyset$, eindige deelverzamelingen en de verzamelingen van de vorm $\{\text{eindig}\} \cup$ kromme.

Het "zwakke" karakter van de Zariski-topologie valt ook op als men naar de topologische afsluiting van verzamelingen kijkt. Ter herinnering:

Definitie 3.2.6 De *afsluiting* $\overline{Y}$ van een deelverzameling Y van een topologische ruimte $(X, \mathcal{T})$ is de kleinste gesloten verzameling in X welke Y bevat; $\overline{Y}$ is de doorsnede van alle gesloten verzamelingen welke Y bevatten en is ook te karakteriseren door de volgende twee voorwaarden:

1. $Y \subset \overline{Y}$ en $\overline{Y}$ is gesloten

2. $Y \subset Z \subset X$ met Z gesloten $\Rightarrow \overline{Y} \subset Z$.

Een $Y \subset X$ heet *dicht in* X als $\overline{Y} = X$.

Voorbeeld 3.2.7 Elke oneindige deelverzameling van $\mathbb{A}^1$ ligt dicht in $\mathbb{A}^1$. Dit geldt dus ook voor $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$ met de Zariski-topologie. Zo is voor $Y = \{\frac{1}{n} \mid n = 1, 2, \cdots\} \subset \mathbb{C}$ in de 'gewone' topologie $\overline{Y} = \{0\} \cup Y$, in de Zariski-topologie $\overline{Y} = \mathbb{C}$. Dit is geheel in overeenstemming met: een polynoom met oneindig veel nulpunten (één variabele) is identiek nul. Zo'n polynoom is namelijk een continue functie $\mathbb{A}^1(k) \to k$ (hier met k en $\mathbb{A}^1(k)$ beide voorzien van de Zariski-topologie) en een continue functie, die op een dichte deelverzameling nul is, is overal nul.

3.3 $\mathbb{P}^n$ en de Zariski-topologie op $\mathbb{P}^n$.

Een voorbeeld van het gebruik van de Zariski-topologie is het bepalen van de projectieve afsluiting in $\mathbb{P}^2$ van een kromme $Z \subset \mathbb{A}^2$. Dit blijkt namelijk de topologische afsluiting $\overline{Z}$ van de kromme gezien als verzameling in de $\mathbb{P}^2$ te zijn (zie 3.3.6). De Zariski-topologie op $\mathbb{P}^2$, algemeen $\mathbb{P}^n$, wordt als volgt ingevoerd:

Definitie 3.3.1 De *projectieve* n-dimensionale ruimte $\mathbb{P}^n$ (of beter $\mathbb{P}^n(k)$) bestaat uit de equivalentieklassen $(a_0 : a_1 : \ldots : a_n)$ van de $(n+1)$-tallen $(a_0, a_1, \ldots, a_n) \in k^{n+1} - \{(0, 0, \ldots, 0)\}$. De daarbij gebruikte equivalentie-relatie is: $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ als er een $0 \neq \lambda \in k$ is zodat $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$. En $(a_0, \ldots, a_n)$ heten *homogene coördinaten* van $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$.

De punten van $\mathbb{P}^n$ kan men zoals bij de $\mathbb{P}^2$ identificeren met de rechten door $(0, \ldots, 0)$ in k^{n+1}.
Een polynoom $f \in k[X_0, \ldots, X_n]$ kan niet gebruikt worden om een functie $\mathbb{P}^n \to k$ te definiëren omdat de homogene coördinaten van een punt $P \in \mathbb{P}^n$ niet uniek zijn. Voor een *homogeen* polynoom f geldt evenwel, als graad $(f) = d$, dat $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$. Men kan dus wel over de *nulpunten van een homogeen polynoom* spreken.

Definitie 3.3.2 Voor een collectie T van *homogene* polynomen $\in k[X_0, \ldots, X_n]$ definieert men:

$$Z(T) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ voor iedere } f \in T\}$$

Er geldt weer $Z(T) = Z(J)$, waarbij J het door T voortgebrachte ideaal is, als de volgende afspraak gemaakt wordt: een ideaal heet homogeen als het voortgebracht wordt door homogene polynomen en per definitie geldt voor een *homogeen ideaal* J :

$$Z(J) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ voor elke } \textit{homogene } f \in J\}$$

Een verzameling $Z(T)$ of $Z(J)$ heet een *algebraïsche verzameling* in $\mathbb{P}^n$. Net zoals bij $\mathbb{A}^n$ gaat men na dat deze algebraïsche verzamelingen de gesloten verzamelingen van een topologie op $\mathbb{P}^n$ vormen. Dit is de *Zariski-topologie op* $\mathbb{P}^n$.

3.3.3 De standaard-inbedding $\mathbb{A}^n \to \mathbb{P}^n$, met $(a_1, \ldots, a_n) \mapsto (1 : a_1 : \cdots : a_n)$ identificeert $\mathbb{A}^n$ met de open deelverzameling $U_0 = \{(a_0 : \cdots : a_n) \mid a_0 \neq 0\}$ van $\mathbb{P}^n$. U_0 ligt dicht in $\mathbb{P}^n$. Om dit te zien en om te zien dat de projectieve afsluiting van een kromme hetzelfde is als de topologische afsluiting beschrijven we eerst in het algemeen de afsluiting van een verzameling Y (in $\mathbb{A}^n$ of $\mathbb{P}^n$) met behulp van het ideaal van Y:

Definitie 3.3.4 Voor een deelverzameling Y van $X = \mathbb{A}^n$ respectievelijk $X = \mathbb{P}^n$ verstaat men onder het *ideaal van* Y het ideaal van alle polynomen die nul zijn op Y respectievelijk het ideaal voortgebracht door alle homogene polynomen die nul zijn op Y. De notatie hiervoor is $I(Y)$.

Stelling 3.3.5 *Voor $X = \mathbb{A}^n$ of $X = \mathbb{P}^n$, voorzien van de Zariski-topologie, en $Y, Y_1, Y_2 \subset X$ geldt*

(i) $Y_1 \subset Y_2 \Rightarrow I(Y_1) \supset I(Y_2), Y \subset Z(I(Y))$

(ii) Y *is gesloten* $\Leftrightarrow Y = Z(I(Y))$

(iii) $\overline{Y} = Z(I(Y))$.

Bewijs. (i) is een direct gevolg van de definitie van $I(Y)$. B.v.: elke (homogene) $f \in I(Y)$ is nul in elk punt van Y, dus $Y \subset Z(I(Y))$.
(ii) "$\Leftarrow$" is triviaal. "$\Rightarrow$": As Y gesloten is, dan is Y van de vorm $Z(T)$. Elke $f \in T$ is nul op Y, dus $T \subset I(Y)$. Dit geeft $Z(I(Y)) \subset Z(T) = Y$. De omgekeerde inclusie staat in (i).
(iii) volgt uit: $Y \subset Z$ met Z gesloten $\Rightarrow$ (wegens i)) $I(Y) \supset I(Z) \Rightarrow Z(I(Y)) \subset Z(I(Z)) = Z$; de laatste gelijkheid is in ii) bewezen. (We gebruikten bovendien tweemaal de triviale implicatie $T_1 \subset T_2 \Rightarrow Z(T_1) \supset Z(T_2)$).

Voorbeeld 3.3.6

1. $n = 2$. Zij $Z = Z_{\mathbb{A}^2}(f) \subset \mathbb{A}^2 \subset \mathbb{P}^2$ een kromme in $\mathbb{A}^2$, opgevat als deelverzameling van $\mathbb{P}^2$. Dan is $\overline{Z} = Z_{\mathbb{P}^2}(f^*)$. Bewijs: Omdat $Z(f^*)$ gesloten is (in $\mathbb{P}^2$) en $Z(f)$ bevat, geldt zeker $\overline{Z} \subset Z(f^*)$. Voor de omgekeerde inclusie gebruiken we Stelling 3.3.5 (ii) en Hilberts Nullstellensatz voor $n = 2$, die zegt dat $Z_{\mathbb{A}^2}(f) = Z_{\mathbb{A}^2}(\hat{f})$, waarbij $\hat{f} = f_1 \cdots f_t$ en $f = f_1^{n_1} \cdots f_t^{n_t}$ de ontbinding van f in irreducibele factoren is (vergelijk Stelling 1.2.8). We laten het aan de lezer over hieruit af te leiden dat $I(\overline{Z}) \subset ((\hat{f})^*) =$ het homogene ideaal voortgebracht door $(\hat{f})^*$ in $k[X_0, X_1, X_2]$. Dit geeft met stelling 3.3.5 (ii) dat $\overline{Z} = Z(I(\overline{Z})) \supset Z(\hat{f}^*) = Z(f^*)$, waarbij de laatste "=" weer aan de lezer overgelaten wordt.

2. $\mathbb{A}^n$ ligt dicht in $\mathbb{P}^n$. Bewijs: beschouw het ideaal van $\mathbb{A}^n \subset \mathbb{P}^n$. Dit wordt voortgebracht door de homogene polynomen f met de eigenschap dat $f(1, a_1, \ldots, a_n) = 0$ voor elke $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Dit kan alleen voor $f = 0$, en daaruit volgt de bewering.

3.4 De Noethereigenschap van $\mathbb{A}^n$ en $\mathbb{P}^n$.

Het doel van de volgende twee topologische definities zal duidelijk zijn als men voor "gesloten verzameling" leest "algebraïsche verzameling": je wilt zo'n verzameling schrijven als vereniging van kleinere die niet verder te splitsen zijn – irreducibele. De tweede definitie zondert de ruimten af waarin, voor elke gesloten verzameling, dit splitsingsproces na eindig veel stappen klaar is. Beide definities hebben niet zo veel zin voor de "gewone" topologieën.

Definitie 3.4.1 1. Een gesloten deelverzameling Y van een topologische ruimte X heet *irreducibel* als Y niet geschreven kan worden als $Y = Y_1 \cup Y_2$ met Y_1, Y_2 gesloten en beide echt kleiner dan Y. Evenwel is, per definitie, de lege verzameling *niet* irreducibel.

2. Een topologische ruimte heet een *Noetherruimte* als voor iedere dalende rij gesloten verzamelingen $Y_1 \supset Y_2 \supset \cdots \supset Y_n \supset \cdots$ geldt: er is een getal r met $Y_r = Y_{r+1} = \cdots$; men zegt ook: als elke dalende rij van gesloten verzamelingen *stationair* wordt.

Opmerking: Men kan 'irreducibel' ook definieren voor willekeurige deelverzamelingen Y van een topologische ruimte X. Dan heet Y irreducibel als $\overline{Y}$ irreducibel is. Dit is gelijkwaardig met: Y is niet te schrijven als $Y = Y_1 \cup Y_2$ met $Y_1, Y_2 \neq Y$ en Y_1 en Y_2 *gesloten in* Y. Een verzameling $Z \subset Y$ heet gesloten in Y als $Z = Y \cap W$ voor een $W \subset X$, die gesloten is in X.

Voorbeelden 3.4.2 1. In $\mathbb{A}^2$ zijn de enige gesloten irreducibele deelverzamelingen de hele $\mathbb{A}^2$, de irreducibele krommen, en de verzamelingen bestaande uit een punt. In $\mathbb{P}^1$ zijn alleen $\mathbb{P}^1$ zelf en de losse punten gesloten irreducibele verzamelingen. In het bijzonder is dus $\mathbb{P}^1$ een Noetherruimte. Iedere oneindige deelverzameling van $\mathbb{P}^1$ is irreducibel (zo'n deelverzameling is niet gesloten tenzij het de hele $\mathbb{P}^1$ is).

2. Uit de expliciete beschrijving van de Zariski-topologie op $\mathbb{A}^2$ volgt de Noethereigenschap van die ruimte vrij snel. Laat $Y_1 \supset Y_2 \supset \cdots$ een dalende rij gesloten deelverzamelingen van $\mathbb{A}^2$ zijn. Als één van de verzamelingen Y_i eindig is, dan is de rij natuurlijk stationair. Als geen enkele Y_i eindig is, dan moet men wat nauwkeuriger te werk gaan. We kunnen veronderstellen dat $Y_i \neq \mathbb{A}^2$ vanaf zekere index. Die Y_i schrijven we als een vereniging $E \cup Z_1 \cup \cdots \cup Z_t$ (alles moet eigenlijk een index i hebben) waarbij $Z_1, \ldots, Z_t$ irreducibele krommen zijn en E een eindige verzameling is die niets met $Z_1 \cup \cdots \cup Z_t$ gemeen heeft. Als voor $j > i$ geldt dat Y_j echt kleiner is dan Y_i, dan is er van Y_i een kromme afgegaan (en eventueel bij E wat punten van deze kromme erbij gekomen) of er zijn wat punten van E afgevallen. Daaruit besluit men dat de rij stationair wordt.

Stelling 3.4.3 *$\mathbb{A}^n$ en $\mathbb{P}^n$ zijn Noetherruimtes.*

Bewijs. Als $Y_1 \supset Y_2 \supset \cdots$ een dalende rij gesloten verzamelingen in $X = \mathbb{A}^n$ respectievelijk $X = \mathbb{P}^n$ is, dan is $I(Y_1) \subset I(Y_2) \subset \cdots$ een stijgende rij idealen in $k[X_1, \ldots, X_n]$ respectievelijk $k[X_0, \ldots, X_n]$. Het volgend lemma – een direct gevolg van Hilbert's basisstelling – zegt dat zo'n rij stationair wordt: er is een r met $I(Y_r) = I(Y_{r+1}) = \cdots$. Maar dit geeft $Z(I(Y_r)) = Z(I(Y_{r+1})) = \cdots$, dus $Y_r = Y_{r+1} = \cdots$, want de Y_i zijn gesloten (stelling 3.3.5 (ii)). □

Lemma 3.4.4 *In een Noetherse ring R, dus in het bijzonder in ringen zoals $k[X_1, \ldots, X_n]$ en $k[X_0, X_1, \ldots, X_n]$, wordt elke stijgende rij idealen stationair; dat wil zeggen: bij elke rij $J_1 \subset J_2 \subset \cdots$ van idealen is er een r met $J_r = J_{r+1} = \cdots$*

Bewijs. Volgens aanname wordt elk ideaal van R door eindig veel elementen voortgebracht. Voor een stijgende rij idealen $J_1 \subset J_2 \subset \cdots$ is de vereniging J van alle J_i ook een ideaal. Er zijn eindig veel elementen $f_1, \ldots, f_t$ die J voortbrengen. Voor zekere r behoren $f_1, \ldots, f_t$ tot J_r. Dan is $J = J_r$ en $J_r = J_{r+1} = \cdots$. □

Dat elke niet lege algebraïsche verzameling te schrijven is als vereniging van eindig veel irreducibelen en wel uniek (onder een nogal vanzelfsprekende voorwaarde), is nu een direct gevolg van:

Stelling 3.4.5 *In een Noetherruimte X kan iedere niet lege gesloten verzameling Y geschreven worden als eindige vereniging $Y = Y_1 \cup \cdots \cup Y_r$ van irreducibele gesloten deelruimten. Als we eisen dat $Y_i \not\subset Y_j$ voor $i \neq j$ dan zijn de $Y_1, \cdots, Y_r$ uniek bepaald. Men noemt ze de* irreducibele componenten van Y.

Bewijs. We onderstellen dat het eerste gedeelte van de stelling onjuist is. Zij $\mathcal{S}$ de collectie van de niet lege, gesloten deelverzamelingen Y van X die niet een eindige vereniging van irreducibele gesloten deelverzamelingen zijn en zij $Y \in \mathcal{S}$. Dan is Y niet irreducibel en niet leeg. Dus Y heeft een ontbinding $Y = Y_1 \cup Z_1$ met $Y_1 \in \mathcal{S}$ of $Z_1 \in \mathcal{S}$. Neem aan dat $Y_1 \in \mathcal{S}$. Die ontbinden we in $Y_2 \cup Z_2$. Zoals daarnet kunnen we weer aannemen dat $Y_2 \in \mathcal{S}$, enzovoort. Hiermee vinden we een oneindige echt dalende rij van gesloten deelverzamelingen. Dit is in tegenspraak met het feit dat X een Noetherruimte is.
Bij twee ontbindingen van Y in irreducibele gesloten deelverzamelingen $Y = Y_1 \cup \cdots \cup Y_s = Y_1' \cup \cdots \cup Y_t'$ gaan we als volgt te werk: $Y_1' = \bigcup_{i=1}^{s} Y_1' \cap Y_i \Rightarrow Y_1' \subset Y_i$ voor zekere i omdat Y_1' irreducibel is. Na omnummeren mogen we aannemen $Y_1' \subset Y_1$. Ook $Y_1 \subset Y_j'$ voor zekere j. Die j moet 1 zijn omdat $Y_1' \subset Y_1 \subset Y_j'$. Dus $Y_1 = Y_1'$. Op analoge wijze ziet men dat er bij iedere i een unieke j is met $Y_i' = Y_j$ en omgekeerd. Dus zijn de twee ontbindingen op volgorde na gelijk. □

3.5 Hilbert's Nullstellensatz: het verband tussen idealen en algebraïsche verzamelingen.

Hilbert's Nullstellensatz geeft voor een ideaal J in $k[X_1, \ldots, X_n]$ een nauwkeurige beschrijving van het ideaal van de bijbehorende algebraïsche verzameling $Z(J) \subset \mathbb{A}^n$. De consequenties hiervan voor homogene idealen en verzamelingen in $\mathbb{P}^n$ worden in 3.6 behandeld.

3.5.1 Voor elk ideaal J in $R := k[X_1, \ldots, X_n]$ geldt $J \subset I(Z(J))$, want elke $f \in J$ is nul op $Z(J)$ en behoort dus tot het ideaal van $Z(J)$. Dit ideaal, $I(Z(J))$, kan groter dan J zijn. Bijvoorbeeld, als $f \notin J$ maar $f^2 \in J$, dan is $(f(P))^2 = 0$ en dus ook $f(P) = 0$ voor elke $P \in Z(J)$, zodat $f \in I(Z(J))$ (anders gezegd: R/J kan nilpotenten hebben, maar $R/I(Z(J))$ niet. Dit zagen we al bij een kromme $Z(f)$ in $\mathbb{A}^2 : I(Z(f)) = (\hat{f})$, waarbij $\hat{f} = f_1 \cdots f_t$ als $f = f_1^{n_1} \cdots f_t^{n_t}$ de ontbinding van f in niet-equivalente irreducibele factoren is. Dus als een polynoom g nul is op $Z(f)$, dan is g deelbaar door $\hat{f}$ maar niet noodzakelijk door f. Wél is er een $m \geq 1$ met $g^m \in (f)$. Dit generaliseert tot (3) hieronder.

3.5.2 Hilbert's Nullstellensatz. Zij $R = k[X_1, \ldots, X_n]$. Dan:

(1) Voor elk ideaal J in R met $J \neq R$ is $Z(J)$ niet leeg.

(2) Elk maximaal ideaal m in R is van de vorm $m = (X_1 - \lambda_1, \ldots, X_n - \lambda_n)$ voor zekere $\lambda_1, \ldots, \lambda_n \in k$.

(3) Zij J een ideaal in R en veronderstel $f \in R$ en f is nul op $Z(J)$. Dan is er een $n \geq 1$ zodat $f^n \in J$.

Commentaar.

1. Bij (2) valt op te merken dat voor elke $P = (\lambda_1, \ldots, \lambda_n) \in \mathbb{A}^n$ het ideaal $m := (X_1 - \lambda_1, \ldots, X_n - \lambda_n)$ een maximaal ideaal van R is, want het is de kern van het evaluatie-homomorfisme $R \to k$ met $f \mapsto f(P)$. (2) zegt dat elk maximaal ideaal zo verkregen wordt.

2. De uitspraak (1) wordt ook wel de zwakke vorm van Hilbert's Nullstellensatz genoemd. Dez volgt gemakkelijk uit (2). Immers, is J een ideaal $\neq R$, kies dan een maximaal ideaal $m \supset J$. Schrijf $m = (X_1 - \lambda_1, \ldots, X_n - \lambda_n)$, dan is $(\lambda_1, \ldots, \lambda_n) \in Z(m) \subset Z(J)$.

3. Ook (3) $\Rightarrow$ (1) is niet zo moeilijk. Stel namelijk dat $Z(J)$ leeg is. Neem $f = 1 \in R$. Omdat $Z(J) = \emptyset$, voldoet deze f aan de voorwaarde in (3), en dus $1 = 1^n \in J$ voor zekere $n \geq 1$. Dit impliceert $J = R$.

4. *Bewijs van (1) $\Rightarrow$ (3).*
We gebruiken de afkorting $k[X] = k[X_1, \ldots, X_n]$, $f(X) = f(X_1, \ldots, X_n)$. Stel $J \subset k[X]$ wordt voortgebracht door $f_1, \ldots, f_r$ en stel $g \in k[X]$ en g is nul op $Z(J)$. Men ziet nu gemakkelijk dat het ideaal J^* in $k[X, Y]$ (Y een onbepaalde), dat voortgebracht wordt door $f_1, \ldots, f_r$ en $Yg - 1$, geen nulpunt in $\mathbb{A}^{n+1}$ heeft. Dus $J^* = k[X, Y]$ volgens (1) en er is een relatie
$$J_1(X, Y)f_1(X) + \cdots + J_r(X, Y)f_r(X) + b(X, Y)(Yg(X) - 1) = 1$$
We mogen wel aannemen $g \neq 0$. Daar Y een onbepaalde is mogen we hiervoor het element $\frac{1}{g} \in k(X)$ (het breukenlichaam van $k[X]$) substitueren en na wegwerken van de noemers vinden we een relatie
$$\tilde{a}_1 f_1 + \cdots + \tilde{a}_r f_r = g^N \text{ in } k[X]; \text{ dus } g^N \in J.$$

5. We tonen ook nog aan dat (2) volgt uit (1). Neem daarvoor een maximaal ideaal m. Kies $(\lambda_1, \ldots, \lambda_n) \in Z(m)$; dit kan vanwege (1). Schrijf $m' := (X_1 - \lambda_1, \ldots, X_n - \lambda_n)$, dan geldt dus dat $Z(m') \subset Z(m)$. Hieruit volgt $m \subset I(Z(m)) \subset I(Z(m')) = m'$, en dus $m = m'$ omdat m maximaal is.

6. Bovenstaande opmerkingen tezamen impliceren, dat de drie beweringen in de stelling equivalent zijn. Hilbert's Nullstellensatz wordt meestal bewezen door (2) aan te tonen. Voor een bewijs hiervan verwijzen we naar een standaard tekst over commutatieve algebra, b.v. H. Matsumura, Commutative Algebra; zie ook Chapter II, §3 van M. Reid, *Undergraduate Algebraic Geometry*.

7. Het is duidelijk dat de stelling alleen voor algebraïsch gesloten lichamen geldt.

Definitie 3.5.3 Onder het *radicaal van een ideaal* J in een ring R verstaat men

$$\sqrt{J} := \{f \in R \mid \text{ er is een } m \geq 1 \text{ zódat } f^m \in J\}.$$

Een ideaal J met $\sqrt{J} = J$ heet een *radicaal-ideaal*.

Gevolg 3.5.4

(i) Voor elk ideaal J in $R = k[X_1, \ldots, X_n]$ geldt $I(Z(J)) = \sqrt{J}$.

(ii) Voor elke deelverzameling Y van $\mathbb{A}^n$ is $I(Y)$ een radicaal-ideaal.

Bewijs: (i) is Hilbert's Nullstellensatz (3), en (ii) is duidelijk. □

Voorbeeld 3.5.5

1. $R = k[X_1, \ldots, X_n]$ is een ontbindingsring. Dus als $f \in R$ een irreducibel polynoom is, dan is $J = (f)$ een priemideaal. De factorring R/J heeft dan geen nuldelers, dus ook geen nilpotenten. Een priemideaal is dus een radicaal-ideaal en $\sqrt{(f)} = (f)$ als f irreducibel is.

2. $\sqrt{(X_1^3, X_2^3, \ldots, X_n^3)} = (X_1, \ldots, X_n)$. Bewijs: dit blijkt uit Gevolg 3.5.4 (i), door te kiezen $J = (X_1^3, X_2^3, \ldots, X_n^3)$ en dus $Z(J) = \{0, \ldots, 0)\}$ en daarom $I(Z(J)) = (X_1, \ldots, X_n)$.

We geven nog een samenvatting en een definitie.

Stelling 3.5.6 *(Het verband tussen de algebraïsche verzamelingen in $\mathbb{A}^n$ en de idealen van $R = k[X_1, \ldots, X_n]$).*

(1) Voor elke algebraïsche verzameling Y van $\mathbb{A}^n$ zijn er eindig veel polynomen $f_1, \ldots, f_m$ met $Y = Z(\{f_1, \ldots, f_m\})$

(2) R is een Noetherse ring, $\mathbb{A}^n$ is een Noetherse ruimte.

(3) $J_1 \subset J_2 \subset R \Rightarrow Z(J_1) \supset Z(J_2), Y_1 \subset Y_2 \subset \mathbb{A}^n \Rightarrow I(Y_1) \supset I(Y_2)$.

(4) $Z(J)$ is een gesloten verzameling, $I(Y)$ is een radicaal-ideaal.

(5) $I(Z(J)) = \sqrt{J}$, $Z(I(Y)) = \overline{Y}$.

(6) Z en I leveren een $1-1$-korrespondentie, die de inclusie omkeert, tussen de radicale idealen van R en de algebraïsche deelverzamelingen van $\mathbb{A}^n$. Onder deze korrespondentie geldt: J is priemideaal $\Leftrightarrow$ $Z(J)$ is irreducibel.

Bewijs. (1) en (2): Hilbert's basisstelling; (3) en (4): triviaal; (5) links: Hilberts Nullstellensatz; rechts: stelling 3.3.5.
De eerste bewering uit (6) volgt uit (5). De tweede bewering gaat als volgt. Stel $Z(J)$ is irreducibel en stel $fg \in J$ voor zekere $f, g \in R$. Dan $Z(J) \subset Z(fg) = Z(f) \cup Z(g)$. Dus $Z(J) = (Z(f) \cap Z(J)) \cup (Z(g) \cap Z(J))$. Omdat $Z(J)$ irreducibel is volgt hieruit $Z(J) \subset Z(f)$ of $Z(J) \subset Z(g)$, dus $f \in \sqrt{J} = J$ of $g \in \sqrt{J} = J$. Omgekeerd, stel $Z(J)$ is niet irreducibel. Als $Z(J) = \emptyset$, dan $J = \sqrt{J} = I(Z(J)) = R$, dus J niet priem. Als $Z(J) \neq \emptyset$ dan zijn er gesloten verzamelingen $Y_1, Y_2 \neq Z(J)$ met $Z(J) = Y_1 \cup Y_2$. Hieruit leidt men gemakkelijk af $J = I(Z(J)) = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$ en $J \neq I(Y_1)$ en $J \neq I(Y_2)$. Dan is er een $f_1 \in I(Y_1) - J$ en een $f_2 \in I(Y_2) - J$. Het product $f_1 f_2$ is nul op $Y_1 \cup Y_2 = Z(J)$ en behoort dus tot J. Dus J is niet priem. □

Definitie 3.5.7 Een *affiene variëteit* is een gesloten irreducibele deelverzameling van een $\mathbb{A}^n$.

Daar ieder priemideaal een radicaal-ideaal is, bestaat er bij vaste n een $1-1$-korrespondentie tussen de affiene variëteiten in de $\mathbb{A}^n$ en de priemidealen in $k[X_1, \ldots, X_n]$.

3.6 Het verband tussen de algebraïsche verzamelingen in $\mathbb{P}^n$ en de homogene idealen in $k[X_0, \ldots, X_n]$.

Zoals we zagen, bestaat een gesloten deel van $\mathbb{P}^n$ precies uit de punten waar alle *homogene* polynomen uit een zeker ideaal nul zijn. En het ideaal $I(Y)$ van een $Y \subset \mathbb{P}^n$ bestaat niet alleen uit de homogene polynomen die nul zijn op Y (die collectie is meestal niet eens een ideaal), maar $I(Y)$ bevat ook alle lineaire combinaties van zulke polynomen. Dit leidt ertoe dat projectieve versies van de in § 3.5 genoemde eigenschappen er net even anders uitzien.

Lemma 3.6.1 *Zij $J \subset k[X_1, \ldots, X_n]$ een homogeen ideaal. Schrijf $f \in J$ als $f = f_0 + f_1 + \ldots + f_t$ waarin elke f_i homogeen is van graad i.*
Dan zijn ook alle $f_i \in J$.

Bewijs. Omdat J homogeen is, is $f \in J$ te schrijven als $f = \sum g_j b_j$ voor zekere homogene $b_j \in J$. Door ook alle g_j uit te schrijven als som van hun homogene delen, is dan te zien dat de f_i als combinatie van de b_j's te schrijven zijn. Dit levert $f_i \in J$. □

Een direct gevolg van bovenstaand lemma en Hilbert's basisstelling is een "homogene basisstelling" :

Gevolg 3.6.2 *Elk homogeen ideaal in $k[X_1, \ldots, X_n]$ is te schrijven als $(f_1, \ldots, f_t)$ voor een zekere collectie homogene $f_i \in J$.* □

Een tweede nuttige hulpstelling over homogene idealen is

Lemma 3.6.3 *Is $J \subset k[X_1, \ldots, X_n]$ een homogeen ideaal, dan evenzo $\sqrt{J}$.*

Bewijs. We weten al dat inderdaad $\sqrt{J}$ een ideaal is, dus het volstaat te bewijzen dat de homogene delen van een $f \in \sqrt{J}$ ook in $\sqrt{J}$ zitten. Neem dus $f = f_0 + \ldots + f_t$, met $f^N \in J$ en de f_i homogeen van graad i. Dan is $(f_0 + \ldots + f_t)^N \in J$, dus omdat J een homogeen ideaal is, volgt uit Lemma 3.6.1 dat alle homogene stukken hiervan ook in J zitten. Het stuk van de hoogste graad hierin is f_t^N, dus volgt dat $f_t \in \sqrt{J}$. Maar dan is ook $f - f_t = f_0 + \ldots + f_{t-1} \in \sqrt{J}$. Bovenstaand argument herhaald toepassen levert nu dat alle $f_i \in \sqrt{J}$. □
Het verband tussen algebraïsche verzamelingen in $\mathbb{P}^n$ en homogene idealen in $R = k[X_0, \ldots, X_n]$ ziet er als volgt uit.

Stelling 3.6.4 *1. Voor een homogeen ideaal $J \in R$ geldt*

$$Z(J) \subset \mathbb{P}^n \text{ is leeg } \Leftrightarrow \text{Er is een } N \text{ zodat } (X_0, \ldots, X_n)^N \subset J.$$

2. Een algebraïsche $Y \subset \mathbb{P}^n$ is te schrijven als $Z(\{f_1, \ldots, f_r\})$ voor homogene $f_i \in R$.

3. $\mathbb{P}^n$ is Noethers.

4. Voor een homogeen ideaal $J \subset R$ met $\sqrt{J} \neq (X_0, \ldots, X_n)$ geldt $I(Z(J)) = \sqrt{J}$.
Voor elke $Y \subset \mathbb{P}^n$ geldt $Z(I(Y)) = \overline{Y}$.

5. Door Z en I wordt een bijectie gegeven, die de inclusie omkeert, tussen de homogene radicale idealen $\neq (X_0, \ldots, X_n)$ van R en de algebraïsche deelverzamelingen van $\mathbb{P}^n$.
Hierbij corresponderen priemidealen precies met irreducibele algebraïsche deelverzamelingen.

Bewijs. (1) Voor $J = R$ is de uitspraak triviaal. Is $J \neq R$, schrijf dan $J = (f_1, \ldots, f_r)$ voor homogene $f_i \in R$. Beschouw $V = Z(J) = Z(\{f_1, \ldots, f_r\}) \in \mathbb{A}^{n+1}$. Uit de Nullstellensatz volgt dat $V \neq \emptyset$. En omdat alle f_i homogeen zijn, geldt dat als $(\alpha_0, \ldots, \alpha_n) \in \mathbb{A}^{n+1}$ in V zit, dan ófwel $(\alpha_0, \ldots, \alpha_n) = (0, \ldots, 0)$, ófwel het projectieve punt $(\alpha_0 : \ldots : \alpha_n)$ zit in $Z(J) \subset \mathbb{P}^n$. De conclusie is, dat indien $Z(J) \subset \mathbb{P}^n$ leeg is, dan geldt $V = \{(0, \ldots, 0)\}$. En dan ook $(X_0, \ldots, X_n) = I(V) = \sqrt{J}$. Dit bewijst $\Rightarrow$, en $\Leftarrow$ is triviaal.
(2) is precies Gevolg 3.6.2, en (3) is Stelling 3.4.3.
(4) Voor de formule $I(Z(J)) = \sqrt{J}$ merken we op, dat beide homogene idealen zijn (de linker per definitie, en de rechter vanwege Lemma 3.6.3). Het volstaat dus, te bewijzen dat deze idealen dezelfde homogene polynomen bevatten.
Laat dus $f \in I(Z(J))$ homogeen zijn. Dit wil precies zeggen, dat f homogeen is en $f(P) = 0$ voor elke $P \in Z(J) \subset \mathbb{P}^n$. (Merk op dat voor de implicatie terug het gegeven $\sqrt{J} \neq (X_0, \ldots, X_n)$ wordt gebruikt.) Omdat f homogeen is, is de gegeven eigenschap equivalent met $f(Q) = 0$ voor elke $Q \in Z(J) \in \mathbb{A}^{n+1}$. Vanwege de Nullstellensatz is dit hetzelfde als $f \in \sqrt{J}$.
De overige beweringen in (4) en (5) worden op exact dezelfde manier als in het bewijs van Stelling 3.5.6 aangetoond. □
Zo komen we, in de laatste regels van deze inleiding over algebraïsche meetkunde, nog net toe aan de definitie van de belangrijkste in dit vak bestudeerde objecten:

Definitie 3.6.5 Een *projectieve variëteit* is een gesloten irreducibele deelverzameling van een $\mathbb{P}^n$.

Anders gezegd, een projectieve variëteit is de nulpuntsverzameling in $\mathbb{P}^n$ van een homogeen priemideaal in $k[X_0, \ldots, X_n]$.

4 Opgaven

1. Toon aan dat het ideaal van de cirkel $C : x^2 + y^2 = 4, z = 2$ (in $\mathbb{R}^3$) gelijk is aan $I = (X^2 + Y^2 - 4, Z - 2)$.

2. Toon aan dat het ideaal M van de kromme $C_3 = \{(t, t^2, t^3) \mid t \in \mathbb{R}\} \subset \mathbb{R}^3$ gelijk, is aan $M = (Y - X^2, Z - X^3)$ en dat $\mathbb{R}[X, Y, Z]/M \cong \mathbb{R}[T]$.

3. Zij k een algebraïsch gesloten lichaam, $f \in k[X]$ en $Z(f)$ de nulpuntsverzameling van f. Toon aan: als $g \in k[X]$ nul is in elk punt van $Z(f)$, dan is er een $m \geq 1$ zó dat $g^m \in (f)$ en omgekeerd. Geldt dit ook als k niet algebraïsch gesloten is?

4. Neem $F := x^4 + y^4 - 1$ en $G := x^3y + y^3 + x$, beide in $k[x, y]$. Laat zien: G is irreducibel, en mits $\mathrm{kar}(k) \neq 2$, ook F is irreducibel. Bepaal vervolgens een $f \neq 0$ in $k[x]$ die in het ideaal voortgebracht door F en G zit.

   (De vlakke kromme $Z(F)$ heet de *Fermat kromme met exponent* 4, en $Z(G)$ heet de *Klein kromme.*)

5. Voor $t \in \mathbb{C}$ nemen we $C_t := Z(tx(x - 1) + (1 - t)(x + 1)y)$. Bepaal voor elke $t \in \mathbb{C}$ de standaardvorm op affiene transformaties na van deze kwadriek.

6. Breng iedere 2-de graads polynoom $f \in \mathbb{R}[X, Y]$ op een "standaardvorm" door reële affiene transformaties te gebruiken (methode van 1.3.2). Ter controle: er zijn negen mogelijkheden.

7. Ga na, dat $C := Z(x^2y^2(x^2 - y^2) + x^8 + y^8)$ irreducibel is. Bepaal de snijpuntsmultipliciteit in $(0, 0)$ van C met een willekeurige lijn door $(0, 0)$.

   Probeer ook een plaatje te maken van de reële punten van C.

8. Zij $Z = Z(f)$ een n-de graadskromme en $L = Z(\ell)$ een lijn.

   (i) Wanneer is $\mathcal{L} \cap Z$ een oneindige verzameling?

   (ii) Geef een voorbeeld met $L \cap Z = \emptyset$.

9. Een *morfisme* $\varphi : \mathbb{A}^2 \to \mathbb{A}^2$ is een afbeelding die de vorm $\varphi(a_1, a_2) = (P(a_1, a_2), Q(a_1, a_2))$ heeft, waarbij $P, Q \in k[X, Y]$. Het morfisme φ heet een *automorfisme* als φ bijectief is en φ^{-1} ook een morfisme is.

   (i) Laat zien: iedere affiene transformatie is een automorfisme van $\mathbb{A}^2$.

   (ii) Toon aan: $\varphi : \mathbb{A}^2 \to \mathbb{A}^2, (a_1, a_2) \mapsto (a_1, a_1^2 + a_2)$ is een automorfisme.

10. (i) Geef een lijn $L \subset \mathbb{A}^2$ die door φ uit Opgave 9(ii) op de parabool $Z(X^2 - Y)$ wordt afgebeeld.

    (ii) Is er ook een automorfisme φ van $\mathbb{A}^2$ en een lijn $L \subset \mathbb{A}^2$ met $\varphi(L) =$ de hyperbool $Z(XY - 1)$? Aanwijzing: als φ en L bestaan, dan heeft de hyperbool een nogal speciale parametrisering.

11. Bewijs, dat een automorfisme van $\mathbb{A}^2(\mathbb{C})$ (zie Opgave 9) de eigenschap heeft, dat $\det J \in \mathbb{C}^*$. Hier is J de jacobi matrix $\begin{pmatrix} \frac{\partial P}{\partial X} & \frac{\partial P}{\partial Y} \\ \frac{\partial Q}{\partial X} & \frac{\partial Q}{\partial Y} \end{pmatrix}$

    Het *Jacobi probleem* is de vraag, of ook de omkering geldt: als $\det J \in \mathbb{C}^*$, dan volgt uit de inverse functie stelling van de analyse, dat het gegeven automorfisme φ overal locaal een

inverse heeft. Maar die inverse functie stelling geeft geen uitsluitsel op de vraag, of die inverse dan ook weer door polynomen gegeven wordt, met andere woorden, of φ een automorfisme is. Totnutoe is het Jacobi probleem onopgelost.

12. Ga na, dat het begrip "singulier punt" behouden blijft onder affiene transformaties.

13. Bepaal de singuliere punten van

    (i) de lemniscaat $(x^2+y^2)^2 = a^2(x^2-y^2)$ met $a \neq 0$.

    (ii) $y^2 = x^2(x-1)$.

    (iii) $y^2 = x^3$.

14. Neem $f \neq g$, beide irreducibel, geen scalair veelvoud van elkaar, en $P \in Z(f) \cap Z(g)$. Laat zien dat $P \in Z(fg)$ een singulier punt is.

15. Bewijs: voor $f \in k[x,y]$ van graad 2, met $\mathrm{kar}(k) \neq 2$, geldt $Z(f)$ bevat een lijn dan en slechts dan als er een punt $P \in Z(f)$ bestaat met de eigenschap $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$.

16. Toon aan dat in $kar \neq 2$ de lemniscaat uit Opgave 13(i) irreducibel is en bewijs dat ze een parametrisering toelaat (hint: snij de lemniscaat met de familie kwadrieken $x^2+y^2 = t(x-y)$).

17. Zij Z de derde-graads kromme $y^2 = x^3+1$ $(kar(k) \neq 2,3)$.

    (i) Vind de lijnen die de kromme in precies één punt snijden.

    (ii) Bepaal van de punten uit (i) die punten P waarvoor de raaklijn in P aan de kromme een drie-voudig snijpunt met Z heeft. Deze speciale punten heten *buigpunten* van de kromme.

    (iii) Bepaal, in termen van partiële afgeleiden van f in P, de conditie waaronder P een buigpunt van $Z(f)$ is (voor $Z = Z(f)$ een kromme van graad n en $\mathrm{kar}(k) \neq 2$). Controleer, dat voor het geval $k = \mathbb{R}$ de gevonden conditie voor een kromme van de vorm $Y - g(X) = f(X,Y)$ overeénkomt met de in de analyse gehanteerde definitie.

18. Toon aan dat de "Fermat-kromme" $x^3+y^3 = 1$ in kar $\neq 3$ niet geparametriseerd kan worden (imiteer de bewijzen van 1.6.5 en lemma 1.6.6; gebruik $a^3-b^3 = (a-b)(a-\omega b)(a-\omega^2 b)$, waarbij $1 \neq \omega \in k$, $\omega^3 = 1$ (dus $1+\omega+\omega^2 = 0$)).

19. Bereken dat de ring van reguliere functies op de kromme $Z(Y^2-X^3)$ isomorf is met de deelring van $k[t]$ bestaande uit de polynomen $\sum_{i<\infty} a_i T^i$ met $a_1 = 0$.

20. De automorfismengroep van $\mathbb{P}^1(k)$ is $PG\ell(2,k)/\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid 0 \neq \lambda \in k\}$.

    (i) Laat zien dat deze groep, na identificatie van $\mathbb{P}^1$ met $k \cup \{\infty\}$, juist de groep van de gebroken lineaire afbeeldingen $z \mapsto \frac{az+b}{cz+d}$ (met $ad-bc \neq 0$) van $k \cup \{\infty\}$ is.

    (ii) Laat zien dat de afbeeldingen σ uit (i) met $\sigma(\infty) = \infty$ de affiene transformaties van $k = \mathbb{A}'(k)$ opleveren.

21. (i) Laat $\{P_1,P_2,P_3\}$ en $\{Q_1,Q_2,Q_3\}$ twee drietallen in $\mathbb{P}^1$ zijn. Toon aan dat er precies één automorfisme σ van $\mathbb{P}^1$ is met $\sigma(P_i) = Q_i (i = 1,2,3)$.

    (ii) Hoe luidt het analogon van (i) voor het projectieve vlak $\mathbb{P}^2$?

22. We identificeren $\mathbb{A}^2$ met de deelverzameling $U_0 = \{(a_0 : a_1 : a_2) \mid a_0 \neq 0\}$ van $\mathbb{P}^2$ via de standaardinbedding. Verklaar waarom affiene transformaties op te vatten zijn als dié automorfismen σ van $\mathbb{P}^2$ waarvoor $\sigma(L) = L$; hierbij is $L = \mathbb{P}^2 \backslash \mathbb{A}^2$ de rechte op oneindig.

23. Bereken de punten op oneindig van de volgende krommen:

    (i) de lemniscaat (§1, opg. 8)

    (ii) de elliptische kromme $y^2 = x(x-1)(x-\lambda)$

    (iii) de hyperelliptische kromme $y^2 = (x-\lambda_1)\dots(x-\lambda_n)$ $(n \geq 3)$.

24. Probeer met de in dit hoofdstuk beschreven methode de volgende vergelijkingen op te lossen:

    (i) $x^4 + 2x^3 - 2x - 2 = 0$;

    (ii) $x^4 + 2x^3 + 2x + 2 = 0$.

25. (i) Geef een formule voor de inbedding van $\mathbb{A}^n$ in $\mathbb{P}^n$.

    (ii) Zij Z het cubische oppervlak $x_1^3 + x_2^3 + x_3^3 + 1 = 0$ in $\mathbb{A}^3$. Toon aan dat Z irreducibel is. Hoe maakt men van Z een projectieve variëteit in de $\mathbb{P}^3$? Wat zijn de punten op oneindig?

26. Zij $Y \subset \mathbb{A}^2$ de algebraïsche verzameling bestaande uit een irreducibele kromme $Z(f)$ en een punt P niet op $Z(f)$ Wat is $I(Y)$?

27. (i) Bepaal voortbrengers van het ideaal $I(Y)$ van de verzameling $Y = \{(1,0),(0,1)\}$ in $\mathbb{A}^2$

    (ii) Toon aan $\mathcal{O}(Y) \cong k \times k$.

    (iii) Dezelfde vraag als in (i) voor de homogene idealen van $Y_1 = \{(1:1:0),(1:0:1)\}$ en $Y_2 = \{(1:0:0),(0:1:0),(0:0:1)\}$ in $\mathbb{P}^2$.

28. Een deelverzameling Y van een topologische ruimte X heet *compact* als er bij iedere open overdekking $(U_i)_{i\in I}$ van Y (d.w.z. elke U_i is open in X en $Y \subset \cup_{i\in I} U_i$) er eindig veel elementen $i_1, \cdots, i_n \in I$ zijn met $Y \subset U_{i_1} \cup \cdots \cup U_{i_n}$.

    (i) Toon aan dat elke (algebraïsche) deelverzameling van $\mathbb{A}^n(k)$ of $\mathbb{P}^n(k)$ compact is.

    (ii) Bewijs dat elke Zariski-gesloten deelverzameling van $\mathbb{A}^n(\mathbb{C})$ ook gewoon gesloten is.

    (iii) De gewone topologie op $\mathbb{P}^n(\mathbb{C})$, $\mathcal{T}_g$, wordt als volgt gedefinieerd:

    $$U \in \mathcal{T}_g \Leftrightarrow \{(a_0, \cdots, a_n) \in \mathbb{C}^{n+1} \mid (a_0 : \cdots : a_n) \in U\} \text{ is gewoon open in } \mathbb{C}^{n+1}.$$

    Bewijs dat $\mathbb{P}^n(\mathbb{C})$ compact is voor de gewone topologie $\mathcal{T}_g$. Stellingen die U bij het bewijs van (iii) kunt gebruiken zijn:

    (1) Een gesloten en begrensde deelverzameling van $\mathbb{R}^m$ is compact

    (2) Het beeld van een compacte verzameling onder een continue afbeelding is compact.

29. Zij a een homogeen ideaal in $k[X_0, \cdots, X_n]$. We beschouwen $Z_{\mathbb{P}^n}(\mathrm{a})$ in $\mathbb{P}^n$ en $Z_{\mathbb{A}^{n+1}}(\mathrm{a})$ in $\mathbb{A}^{n+1}$. Toon aan:

    (i) $Z_{\mathbb{P}^n}(\mathrm{a}) = \{(p_0 : p_1 : \cdots : p_n) \mid 0 \neq (p_0, \cdots, p_n) \in Z_{\mathbb{A}^{n+1}}(\mathrm{a})\}$

    (ii) $Z_{\mathbb{A}^{n+1}}(\mathrm{a}) = \{(0, \cdots, 0)\} \Leftrightarrow \sqrt{\mathrm{a}} = (X_0, \cdots, X_n)$

(iii) $Z_{\mathbb{P}^n}(\mathrm{a}) \neq \emptyset \Leftrightarrow \sqrt{\mathrm{a}} \underset{\neq}{\subset} (X_0, \cdots, X_n)$.

30. We vatten $\mathbb{A}^n$ op als deelverzameling van $\mathbb{P}^n$ onder de standaardinbedding. Voor een ideaal a in $k[X_1, \cdots, X_n]$ definieren we $\mathrm{a}^* \subset k[X_0, \cdots, X_n]$ als het ideaal voortgebracht door $\{f^* \mid f \in \mathrm{a}\}$, waarbij

$$f^* = X_0^d f\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right) \text{ als } f \in k[X_1, \cdots, X_n], \text{ graad } (f) = d.$$

Toon aan

(1) $\mathbb{A}^n$ ligt dicht in $\mathbb{P}^n$.

(2) $\overline{Z_{\mathbb{A}^n}(\mathrm{a})} = Z_{\mathbb{P}^n}(\mathrm{a}^*)$.

Chapter 2

Dynkin diagrammen en Wortelsystemen

0 Inleiding

In dit hoofdstuk houden we ons bezig met een mengeling van combinatoriek (grafen en functies daarop), lineaire algebra (met name zekere al of niet positief definiete bilineaire vormen) en groepen (voortgebracht door spiegelingen in een collectie hyperoppervlakken in een inproductruimte).
Er blijken sterke verbanden tussen deze onderwerpen te bestaan. Een centrale rol hierbij wordt gespeeld door bepaalde grafen, die *Dynkin diagrammen* worden genoemd. De groepen en grafen die we hier tegenkomen, worden in heel uiteenlopende delen van de wetenschap gebruikt. Bijvoorbeeld in de scheikunde (crystallografie), in elementaire deeltjes fysica, en in wiskundige onderwerpen zoals Lie groepen en Lie algebra's, singulariteiten theorie enzovoorts.
Bij het schrijven van dit hoofdstuk is niet gepoogd, alles zo algemeen mogelijk te houden. Het uitgangspunt is geweest, op een zo simpel mogelijke manier een indruk te geven hoe Dynkin diagrammen op een heel natuurlijke manier naar voren komen uit bepaalde elementaire vragen over groepen, spiegelingen en grafen. Daarbij zijn twee gemakkelijk te lezen teksten gebruikt:

- De eerste 5 pagina's van het overzichtsartikel
  Idun Reiten, *Dynkin Diagrams and the Representation Theory of Algebras*, verschenen in Notices of the AMS, Volume 44, Number 5, May 1997.

- M. van der Put, *Wortelsystemen*, 6 pagina's in het dictaat "Meetkundige Problemen" van F. Takens, Uitgave maart 1988.

Er bestaan ook veel uitgebreidere teksten over de genoemde onderwerpen; voor wie er veel meer over wil weten noemen we

- J.E. Humphreys, *Reflection groups and Coxeter groups.* Cambridge Studies in Advanced Math., **29**, Cambridge Univ. Press, 1990.

- (Hoofdstuk 5 in) J-P. Serre, *Algèbres de Lie semi-simples complexes.* W.A. Benjamin, Inc., New York, 1966.

- N. Bourbaki, *Groupes et Algèbres de Lie Chap. 4, 5 et 6*, Masson, Paris etc., 1981.

- (Hoofdstuk 4 in) J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups.* Springer-Verlag, Grundlehren series vol. 290, 1993 (second edition).

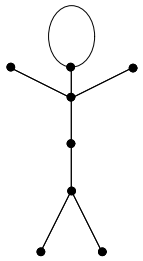
- (Hoofdstuk 1 in) W. Ebeling, *Lattices and Codes.* Vieweg, Braunschweig, 1994.

1 Grafen en bilineaire vormen

1.1 De graaf

Definitie 1.1.1 Onder een *graaf* Σ zullen we hier verstaan een niet-lege eindige verzameling $\{1, \ldots, n\}$ (de *punten* van Σ), waarbij we verder bepaalde paren $\{i, j\}$ van punten een of meerdere keren "verbinden" (de *kanten* van Σ).
De graaf heet *samenhangend* als vanuit een willekeurig punt van de graaf via de kanten ieder ander punt te bereiken is.

Een graaf Σ is weer te geven door een plaatje waarin de punten van Σ gewoon als punten worden getekend, en de kanten als verbindingslijntjes tussen die punten:



Een graaf Σ met n punten wordt volledig beschreven door de bijbehorende *incidentiematrix* $A = (a_{ij})$. Dit is per definitie de $n \times n$ matrix waarvoor a_{ij} gelijk is aan het aantal kanten tussen i en j. Zo'n matrix is symmetrisch, want de kanten in onze grafen hebben geen richting. Verder staan er alleen niet-negatieve gehele getallen in zo'n incidentiematrix. Matrixvermenigvuldigen werkt precies zo, dat A^m op de i, j-plek het aantal manieren om over m kanten van i naar j te komen heeft staan. Dus samenhangend zijn van de graaf kan ook geformuleerd worden door te zeggen dat er een $m \geq 1$ bestaat zodat $I + A + A^2 + \ldots + A^m$ een matrix is waarin het getal 0 niet voorkomt. De identiteitsmatrix I staat in deze som omdat anders de uitspraak onjuist zou zijn voor een graaf bestaande uit precies één punt en geen kanten.
Merk ook op dat a_{ii} in de incidentiematrix het aantal kanten van i naar zichzelf voorstelt. Zulke kanten worden wel de *lusjes* van de graaf genoemd.

Conventie: we zullen ons vanaf nu alleen bezighouden met samenhangende grafen, die bovendien geen lusjes hebben.

Deze afspraak betekent voor de incidentiematrix A, dat $a_{ii} = 0$ voor elke i, en bovendien is er een $m \geq 1$ zodat in de matrix $I + A + A^2 + \ldots + A^m$ het getal 0 niet voorkomt.

Definitie 1.1.2 De *Cartan matrix* van een graaf is per definitie de matrix $C = 2I - A$, waarin I de identiteitsmatrix is, en A de incidentiematrix van de graaf.

Omdat we hebben afgesproken dat onze grafen geen lusjes hebben, heeft de Cartan matrix $C = (c_{ij})$ dus als coefficienten $c_{ii} = 2$ voor elke i, en voor $i \neq j$ is $-c_{ij}$ het aantal kanten tussen i en j.

1.1.3 We zullen in dit hoofdstuk onder meer een volledig antwoord geven op de volgende

Vraag 1.1.4 Voor welke grafen Σ (samenhangend, zonder lusjes) is het mogelijk om aan elk punt i een positief geheel getal f_i toe te kennen zodat voor elke i geldt

$$2f_i \geq \sum f_j,$$

waarbij de som wordt genomen over alle kanten tussen i en z'n "buren" j. We eisen daarbij bovendien dat er een i is waarvoor de gevraagde ongelijkheid ook echt een ongelijkheid is, dus $2f_i \neq \sum f_j$.

De laatste eis van geen gelijkheid lijkt nogal vreemd. Maar we zullen zien dat juist door die eis het antwoord heel mooi wordt.

Voorbeeld 1.1.5 We nemen de graaf Σ bestaande uit 2 punten $\{1,2\}$, met $n \geq 1$ kanten daartussen. De Cartan matrix van deze graaf is dus $C = \begin{pmatrix} 2 & -n \\ -n & 2 \end{pmatrix}$. Een paar positieve gehele getallen (f_1, f_2) als bedoeld in Vraag 1.1.4 moet dan voldoen aan $2f_1 \geq nf_2$ en $2f_2 \geq nf_1$. Uit de ongelijkheden volgt $4f_1 \geq 2nf_2 \geq n^2 f_1$, en omdat niet beide ongelijkheden gelijkheden mogen zijn levert dit $4 > n^2$ en dus $n = 1$. Dus zo'n paar kan alleen bestaan als er slechts één kant is tussen 1 en 2, en in dat geval werkt het paar $(1,1)$.

1.1.6 De gestelde vraag formuleren we nu in termen van de Cartan matrix $C = (c_{ij})$.

Schrijf f voor de kolomvector met coördinaten $f_1, \cdots, f_n$. Wat we willen is, dat $2f_i \geq \sum f_j$. De bijdrage van $j \neq i$ in deze som is gelijk aan f_j maal het aantal kanten tussen i en j. Met andere woorden, die bijdrage is precies $-c_{ij}f_j$. Ook geldt $c_{ii} = 2$, en dus is de eis te schrijven als

$$c_{ii}f_i \geq \sum_{j \neq i} -c_{ij}f_j,$$

oftewel als

$$\sum_{j=1}^{n} c_{ij}f_j \geq 0.$$

Hier staat precies, dat de $i$de coördinaat van het product $C \cdot f$ niet negatief mag zijn. En de eis dat we niet voor elke i gelijkheid wilden, zegt dat ook $C \cdot f \neq 0$ moet zijn. Hiermee hebben we aangetoond:

Propositie 1.1.7 *Zij Σ een graaf (samenhangend, zonder lusjes) met Cartanmatrix C.*
Dan is Vraag 1.1.4 voor Σ equivalent met het bestaan van een vector $f \in \mathbb{R}^n$ met positieve gehele coördinaten, zodat $C \cdot f \neq 0$ en alle coördinaten van $C \cdot f$ zijn ≥ 0. □

1.2 De bilineaire vorm

Het standaard inproduct op $\mathbb{R}^n$ noteren we als $\langle \cdot, \cdot \rangle$. Zoals bekend uit de lineaire algebra is dit een *bilineaire* vorm; dat wil zeggen $\langle v, w \rangle$ is lineair in elk van z'n argumenten v en w. De vorm is ook *symmetrisch*, oftewel $\langle v, w \rangle = \langle w, v \rangle$. Tenslotte is de vorm *positief definiet*, dat wil zeggen dat $\langle v, v \rangle > 0$ als $v \neq 0$. De standaardbasis voor $\mathbb{R}^n$ noteren we als $e_1, \ldots, e_n$. Deze is *orthonormaal* voor het standaardinproduct, dat wil zeggen $\langle e_i, e_j \rangle = \delta_{ij}$ (de Kronecker delta).
Bij een symmetrische $n \times n$ matrix $B = (b_{ij})$ kunnen we ook een symmetrische bilineaire vorm maken, namelijk $\langle Bv, w \rangle$. Deze is weer symmetrisch omdat B het is (merk op dat geldt $b_{ij} = \langle Be_j, e_i \rangle$). Deze vorm is in het algemeen zeker niet positief definiet (bijvoorbeeld zou B de nulmatrix kunnen zijn!). Geven we de vector v weer door coördinaten $x_1, \ldots, x_n$, dan wordt $\langle Bv, v \rangle$ een homogene vorm van graad 2 in de x_i's. De coefficient van x_i^2 daarin is b_{ii}, en die van $x_i x_j$ (voor $i \neq j$) is $b_{ij} + b_{ji} = 2b_{ij}$. Uit de lineaire algebra weten we, dat deze vorm positief definiet is, precies dan als alle eigenwaarden van B positief zijn. Dit zullen we niet gebruiken. Wel merken we op, dat een noodzakelijke (niet voldoende) voorwaarde voor positief definiet zijn is, dat $b_{ii} = \langle Be_i, e_i \rangle > 0$ voor elke i.

Definitie 1.2.1 De symmetrische, bilineaire vorm bij een graaf Σ met Cartanmatrix C is $\langle Cv, w \rangle$. Verder schrijven we $q_\Sigma(v) = \frac{1}{2}\langle Cv, v \rangle$ en we noemen dit de kwadratische vorm bij Σ.

Zijn $x_1, \ldots, x_n$ de coördinaten van v, dan is dus q_Σ de homogene kwadratische uitdrukking in de x_i's met 1 als coefficient van elke x_i^2, terwijl de coefficient van $x_i x_j$ voor $i \neq j$ gelijk is aan de tegengestelde van het aantal kanten tussen i en j.

Vraag 1.2.2 Voor welke grafen Σ (samenhangend, zonder lusjes) is q_Σ positief definiet?

Voorbeeld 1.2.3 Neem $n \geq 2$ en zij Σ de graaf met punten $\{1, 2, \ldots, n\}$ en precies één kant tussen elk van $\{1, 2\}, \ldots, \{1, n\}$. (Dus een waaier van $n-1$ kanten vanuit het centrum 1.) De vorm q_Σ hierbij is

$$x_1^2 + \ldots + x_n^2 - x_1x_2 - x_1x_3 - \ldots - x_1x_n.$$

We substitueren $x_1 = a$ en $x_2 = \ldots = x_n = b$, dan staat er

$$a^2 - (n-1)ab + (n-1)b^2.$$

Dit is alleen maar positief voor elke $(a, b) \neq (0, 0)$ indien de discriminant $(n-1)^2 - 4(n-1) = (n-1)(n-5)$ negatief is, oftewel als $n = 2, 3$ of 4.
En in elk van deze drie overblijvende gevallen blijkt ook inderdaad de vorm q_Σ positief definiet te zijn. Immers, schrijf

$$q_\Sigma(x_1, \ldots, x_n) = \frac{5-n}{4}x_1^2 + (\frac{1}{2}x_1 - x_2)^2 + \ldots + (\frac{1}{2}x_1 - x_n)^2.$$

Hiermee kan je natuurlijk ook direct zien voor welke n de vorm positief definiet is, zonder de truuk met de a en de b.

Er blijkt een mooi verband te bestaan tussen Vraag 1.1.4 en Vraag 1.2.2:

Propositie 1.2.4 *Zij Σ met Cartanmatrix $C = (c_{ij})$ en vorm q_Σ gegeven. Een positief antwoord op Vraag 1.1.4 voor Σ impliceert een positief antwoord op Vraag 1.2.2. Preciezer gezegd:*
Als er een f bestaat met positieve gehele coördinaten waarvoor geen enkele coördinaat van $C \cdot f$ negatief is en $C \cdot f \neq 0$, dan volgt dat q_Σ positief definiet is.

Bewijs. Neem f zoals gegeven in de Propositie. Bij elke paar punten i, j van Σ maken we een vorm

$$q_{i,j} := \frac{-c_{ij}}{f_i f_j}(f_i x_j - f_j x_i)^2.$$

Bezie dan $\sum q_{i,j}$, waar de som genomen wordt over alle paren punten i, j met $i < j$ van Σ. Coefficienten vergelijken levert, dat

$$2q_\Sigma = \sum_{i<j} q_{i,j} + \sum_{i=1}^{n} \frac{(Cf)_i}{f_i}x_i^2,$$

waarbij $(Cf)_i$ de $i$de coördinaat van $C \cdot f$ voorstelt. Dit geeft een schrijfwijze van q_Σ als som van kwadraten met positieve coefficienten. Dus in ieder geval geldt $q_\Sigma(v) \geq 0$ voor elke $v \in \mathbb{R}^n$.
Stel nu dat $q_\Sigma(x_1, \ldots, x_n) = 0$. Dan is ieder van de kwadraten in de schrijfwijze hierboven nul. Dus ook $x_i = 0$ voor elke i met $(Cf)_i \neq 0$ (merk op dat er zulke i zijn). Uitgaande van een i met $x_i = 0$, neem een kant tussen i en een j. Dan is ook $q_{i,j}(x_1, \ldots, x_n) = 0$, en dat levert uitgeschreven, dat $x_j = 0$. De samenhang van Σ impliceert vervolgens dat alle $x_i = 0$. Hiermee is aangetoond dat q_Σ positief definiet is. □

1.2.5 In feite blijkt het verband tussen beide vragen zelfs nog mooier: ze zijn equivalent. Dat zullen we veel verderop in dit hoofdstuk (Gevolg 1.5.6) bewijzen.

1.3 De Weyl groep en de wortels

Laat de graaf Σ met Cartanmatrix $C = (c_{ij})$ gegeven zijn. Bij elk punt i van Σ wordt een lineaire afbeelding

$$\sigma_i \ : \ \mathbb{R}^n \longrightarrow \mathbb{R}^n, \quad x \mapsto x - \langle Cx, e_i\rangle e_i$$

gemaakt. Merk op dat $\sigma_i(e_j) = e_j - c_{ij}e_i$, dus in het bijzonder $\sigma_i(e_i) = -e_i$. De afbeeldingen σ_i hebben orde 2, dat wil zeggen $\sigma_i^2 = id$ en $\sigma_i \neq id$. Dit kan je zien als de "reden" waarom in de Cartanmatrix per definitie het getal 2 op de diagonaal wordt gezet: alleen dan heeft elke σ_i orde 2. Elke σ_i is dus een element van de groep $\mathrm{GL}(n, \mathbb{R})$ van inverteerbare lineaire afbeeldingen van $\mathbb{R}^n$ naar zichzelf.
In het geval dat $\langle Cv, w\rangle$ een inproduct op $\mathbb{R}^n$ definieert (met andere woorden, als deze vorm positief definiet is), dan is σ_i de loodrechte spiegeling ten opzichte van dit inproduct in het hypervlak loodrecht op e_i.

Definitie 1.3.1 De *Weyl groep* W_Σ van een graaf Σ is per definitie de ondergroep van $\mathrm{GL}(n, \mathbb{R})$ voortgebracht door alle σ_i.
De *wortels* van Σ zijn de vectoren in de verzameling

$$R_\Sigma := \{\sigma(e_i) \mid 1 \leq i \leq n, \ \sigma \in W_\Sigma\}.$$

Een aantal eigenschappen van de Weyl groep en de bijbehorende wortels staan opgesomd in de volgende

Propositie 1.3.2 *Laat Σ een graaf zijn met Cartanmatrix C, Weyl groep W en verzameling wortels R.*

1. *Er geldt dat $0 \notin R$ en R bevat een basis voor $\mathbb{R}^n$.*
2. *Elke $\sigma \in W$ behoudt de vorm $\langle Cv, w\rangle$, dat wil zeggen $\langle C\sigma(v), \sigma(w)\rangle = \langle Cv, w\rangle$.*
3. *Voor elke $r \in R$ geldt $\langle Cr, r\rangle = 2$.*
4. *Ten opzichte van de standaardbasis wordt elke $\sigma \in W$ gegeven door een matrix met gehele coefficienten.*
5. *Er geldt $R \subset \mathbb{Z}^n$.*
6. *Voor elke $r \in R$ is $\sigma_r \ : \ x \mapsto x - \langle Cx, r\rangle r$ een element van W.*
7. *Voor $r_1, r_2 \in R$ is $\sigma_{r_1}(r_2) - r_2$ een geheel veelvoud van r_1.*

Bewijs. (1) Omdat de $\sigma \in W$ inverteerbaar zijn, is $\sigma(e_i) \neq 0$, dus $0 \notin R$. Verder bevat R per definitie de standaardbasis van $\mathbb{R}^n$.
(2) Het is voldoende, dit aan te tonen voor de voortbrengers $\sigma_i \in W$. Daarvoor geldt

$$\begin{aligned}\langle C\sigma_i(v), \sigma_i(w)\rangle &= \langle Cv - \langle Cv, e_i\rangle Ce_i, w - \langle Cw, e_i\rangle e_i\rangle \\ &= \langle Cv, w\rangle - \langle Cv, e_i\rangle\langle Cw, e_i\rangle - \langle Cv, e_i\rangle\langle Ce_i, w\rangle + \\ &\quad + \langle Cv, e_i\rangle\langle Cw, e_i\rangle\langle Ce_i, e_i\rangle \\ &= \langle Cv, w\rangle,\end{aligned}$$

waarbij gebruikt is dat $\langle Ce_i, e_i\rangle = 2$ en ook dat C symmetrisch is.
(3) Laat $r = \sigma(e_i) \in R$. Vanwege (2) is dan

$$\langle Cr, r\rangle = \langle C\sigma(e_i), \sigma(e_i)\rangle = \langle Ce_i, e_i\rangle = 2.$$

(4) Omdat $\sigma_i(e_j) = e_j - c_{ij}e_i$, worden de σ_i's ten opzichte van de standaardbasis gegeven door matrices met gehele coefficienten. Elke $\sigma \in W$ is te schrijven als een product $\sigma = \sigma_{i_1} \cdot \ldots \cdot \sigma_{i_t}$ (negatieve machten komen niet voor omdat elke σ_i z'n eigen inverse is). Dus ook de matrix van een $\sigma \in W$ heeft gehele coefficienten.
(5) volgt direct uit (4) en uit het feit dat de e_i in $\mathbb{Z}^n$ zitten.
(6) Laat $r \in R$, en schrijf $r = \sigma(e_i)$ met $\sigma \in W$. Dan geldt $\sigma \cdot \sigma_i = \sigma_r \cdot \sigma$, zoals met behulp van (2) direct uit de definities valt na te rekenen. Met andere woorden, $\sigma_r = \sigma \cdot \sigma_i \cdot \sigma^{-1}$, en dat is een element van de groep W.
(7) Laat $r_1, r_2 \in R$, dan is per definitie $\sigma_{r_1}(r_2) - r_2 = \langle Cr_2, r_1\rangle r_1$. Vanwege (5) en het feit dat de coefficienten van C geheel zijn volgt dat $\langle Cr_2, r_1\rangle \in \mathbb{Z}$. □

1.4 Het verband

In deze paragraaf geven we het verband tussen enerzijds de Weyl groep en de wortels van een graaf, en anderzijds positief definiet zijn van de kwadratische vorm. We beginnen met

Lemma 1.4.1 *Laat Σ een graaf zijn met Cartanmatrix C en Weyl groep W.*
Als de vorm $\langle Cv, w\rangle$ positief definiet is, dan is de actie van W op $\mathbb{R}^n$ irreducibel (dat wil zeggen, er bestaat geen lineaire deelruimte $V \neq (0), \neq \mathbb{R}^n$ die door elk element van W weer binnen zichzelf wordt afgebeeld).

Bewijs. Stel dat $V \neq (0)$ een deelruimte is die door W naar zichzelf wordt afgebeeld. Kies dan $v \in V$ met $v \neq 0$. Omdat de vorm bij Σ positief definiet is, bestaat er een standaard basisvector e_i met $\langle Ce_i, v\rangle \neq 0$. Zowel v als $\sigma_i(v)$ zijn elementen van V, en dus ook hun verschil $v - \sigma_i(v) = \langle Ce_i, v\rangle e_i \in V$. Hieruit volgt dat $e_i \in V$. Neem nu een j zodat er in Σ een kant loopt tussen i en j. Dan is per definitie $\langle Ce_i, e_j\rangle \neq 0$, en $e_i - \sigma_j(e_i) = \langle Ce_i, e_j\rangle e_j$ zit in V, dus ook $e_j \in V$. Uit de samenhang van Σ volgt dan dat alle standaard basisvectoren in V zitten, en dus $V = \mathbb{R}^n$.□

Het volgende lemma lijkt sterk op het bovenstaande maar is wat lastiger te bewijzen.

Lemma 1.4.2 *Laat Σ een graaf zijn met Cartanmatrix C en Weyl groep W.*
Als de groep W eindig is, dan is de actie van W op $\mathbb{R}^n$ irreducibel.

Bewijs. Stel dat de lineaire deelruimte $V_1 \subset \mathbb{R}^n$ door elk element van W op zichzelf wordt afgebeeld. We zullen eerst laten zien, dat er een deelruimte $V_2 \subset \mathbb{R}^n$ bestaat met dezelfde eigenschap, en zodat $V_1 \oplus V_2 = \mathbb{R}^n$ (dat wil zeggen, elke vector in $\mathbb{R}^n$ is te schrijven als som $v_1 + v_2$ met $v_i \in V_i$, en $V_1 \cap V_2 = (0)$). Dit is een bekend argument uit de representatietheorie van eindige groepen: kies een lineaire afbeelding $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ met $\varphi^2 = \varphi$ en $\varphi(\mathbb{R}^n) = V_1$ (een projectie op V_1, dus). Definieer vervolgens

$$P := \frac{1}{\#W} \sum_{\sigma \in W} \sigma\varphi\sigma^{-1}.$$

Dan is ook P een projectie op V_1, immers elke vector uit $\mathbb{R}^n$ wordt door P naar V_1 afgebeeld, en bovendien is $P(v) = v$ voor $v \in V_1$. De reden dat we naar P kijken in plaats van naar de oorspronkelijke φ, is dat P als extra eigenschap heeft dat $\sigma P = P\sigma$ voor $\sigma \in W$.
Neem nu $V_2 := \mathrm{Ker}(P) = \mathrm{Beeld}(id - P)$. Het is evident dat deze de gezochte eigenschappen heeft. Schrijf $e_1 = v_1 + v_2$, met $v_i \in V_i$. Omdat

$$2 = \langle Ce_1, e_1\rangle = \langle Ce_1, v_1\rangle + \langle Ce_1, v_2\rangle,$$

is $\langle Ce_1, v_i\rangle \neq 0$ voor een i. We nemen aan dat dit geldt voor $i = 1$ (verwissel anders de rollen van V_1 en V_2). We kunnen nu verder redeneren op precies dezelfde wijze als in het bewijs van Lemma 1.4.1: er geldt

$$0 \neq \langle Cv_1, e_1\rangle e_1 = v_1 - \sigma_1(v_1) \in V_1,$$

en dus $e_1 \in V_1$. Alle e_j waarvoor er een kant is tussen 1 en j zitten dan ook in V_1, enzovoorts. De samenhang van Σ impliceert zo, dat $V_1 = \mathbb{R}^n$. □

Stelling 1.4.3 *Voor een graaf Σ met Cartanmatrix C, Weyl groep W en verzameling wortels R zijn de volgende drie uitspraken equivalent.*

1. *De vorm $\langle Cv, w\rangle$ is positief definiet.*
2. *De verzameling wortels R is eindig.*
3. *De Weyl groep W is eindig.*

Bewijs. De implicatie (1) $\Rightarrow$ (2) volgt uit Propositie 1.3.2. Immers, deze zegt onder meer dat de wortels vectoren zijn met gehele coördinaten en lengte $\sqrt{2}$ ten opzichte van het door $\langle Cv, w\rangle$ gegeven inproduct. Van zulke vectoren kunnen er maar eindig veel bestaan.
(2) $\Rightarrow$ (3): elk element van W werkt als een permutatie op de verzameling wortels R. En omdat R een basis van $\mathbb{R}^n$ bevat, legt deze permutatie zo'n element van W helemaal vast. Is dus R eindig, dan zijn er maar eindig veel permutaties van R en dus is ook W dan eindig.
Tenslotte bewijzen we (3) $\Rightarrow$ (1). Definieer daartoe voor $v, w \in \mathbb{R}^n$ de vorm

$$[v, w] := \sum_{\sigma\in W} \langle \sigma(v), \sigma(w)\rangle.$$

Omdat $\langle\cdot,\cdot\rangle$ een inproduct is, is $[\cdot,\cdot]$ het ook. En bovendien is het zo gemaakt, dat de $\sigma \in W$ orthogonaal zijn ten opzichte van $[\cdot,\cdot]$; dat wil zeggen $[\sigma(v), \sigma(w)] = [v, w]$ voor alle $v, w \in \mathbb{R}^n$ en alle $\sigma \in W$.
Er bestaat dan een matrix A zodat $\langle Cv, w\rangle = [Av, w]$ voor alle $v, w \in \mathbb{R}^n$. Immers, kies een orthonormale basis $\{f_1, \ldots, f_n\}$ ten opzichte van $[\cdot,\cdot]$, neem $a_{i,j} = \langle Cf_j, f_i\rangle$ en A zo dat $Af_i = \sum_j a_{i,j} f_j$ voor alle i. Dan geldt

$$\begin{aligned}[A\sigma(v), \sigma(w)] &= \langle C\sigma(v), \sigma(w)\rangle \\ &= \langle Cv, w\rangle = [Av, w] \\ &= [\sigma Av, \sigma w],\end{aligned}$$

dus $A\sigma = \sigma A$ voor elke $\sigma \in W$.
Merk nu op, dat uit (3) en Lemma 1.4.2 volgt dat de actie van W op $\mathbb{R}^n$ irreducibel is. Het onderstaande Lemma 1.4.5 impliceert dan dat geldt $A = \lambda I$ voor een $\lambda \in \mathbb{R}$. En dus $\langle Cv, v\rangle = \lambda[v, v]$. Dit impliceert (1), want door bijvoorbeeld $v = e_1$ in te vullen zie je dat $\lambda > 0$, en verder is $[v, v] > 0$ voor elke $v \neq 0$. □

Lemma 1.4.4 *Als A en S twee $n \times n$ matrices met coefficienten in een lichaam K zijn, waarvoor geldt dat $AS = SA$ en rang$(I - S) = 1$, dan heeft A een eigenwaarde $\lambda \in K$.*

Bewijs. Omdat rang$(I - S) = 1$, is er een vector $v \neq 0$ in K^n die het beeld van $I - S$ voortbrengt. Schrijf $v = (I - S)x = x - Sx$ voor zekere x, dan volgt $Av = Ax - ASx = Ax - SAx = (I - S)Ax$. Met andere woorden, Av zit in het beeld van $I - S$, en is dus te schrijven als λv voor zekere $\lambda \in K$.
□

Lemma 1.4.5 *Stel dat een groep $G \subset GL(n, \mathbb{R})$ de volgende twee eigenschappen heeft:*

1. *G werkt irreducibel op $\mathbb{R}^n$ (oftewel, zoals al eerder gezegd, de enige lineaire deelruimten die door elk element van G binnen zichzelf worden afgebeeld zijn 0 en $\mathbb{R}^n$).*

2. *Er is een $\sigma \in G$ met de eigenschap $rang(I - \sigma) = 1$.*

Als dan voor elke $\sigma \in G$ geldt dat $A\sigma = \sigma A$ voor zekere matrix A, dan is $A = \lambda I$ voor een $\lambda \in \mathbb{R}$.

Bewijs. Uit de tweede eigenschap en Lemma 1.4.4 volgt dat A een eigenwaarde $\lambda \in \mathbb{R}$ heeft. Zij V_λ de bijbehorende eigenruimte. Uit het gegeven dat A met elke $\sigma \in G$ commuteert volgt dat elke $\sigma \in G$ deze eigenruimte weer binnen zichzelf afbeeldt. Omdat $V_\lambda \neq 0$ levert de eerste eigenschap van de groep G nu dat $V_\lambda = \mathbb{R}^n$, oftewel dat $A = \lambda I$. □

We zullen tenslotte nog enkele eigenschappen afleiden van de verzameling wortels en de werking van de Weyl groep daarop, voor het geval dat de equivalente uitspraken van Stelling 1.4.3 gelden. Merk op, dat voor de bewijzen die we hieronder geven, in feite uit deze paragraaf alleen Lemma 1.4.1 wordt gebruikt.

Lemma 1.4.6 *Als de vorm q_Σ positief definiet is, dan geldt voor een tweetal wortels $r, s \in R$ dat $\langle Cr, s\rangle \in \{0, \pm 1, \pm 2\}$. En $\langle Cr, s\rangle = \pm 2$ precies dan, als $r = \pm s$.*

Bewijs. Propositie 1.3.2 (3) zegt dat $\langle Cr, r\rangle = \langle Cs, s\rangle = 2$. De ongelijkheid van Cauchy-Schwarz, toegepast op het inproduct $\langle Cv, w\rangle$ en op de vectoren r, s levert dan, dat $\langle Cr, s\rangle^2 \leq \langle Cr, r\rangle \cdot \langle Cs, s\rangle = 4$. De ongelijkheid hierin is een gelijkheid precies dan als $r = \pm s$. Omdat ook $\langle Cr, s\rangle \in \mathbb{Z}$ vanwege Propositie 1.3.2 (7), volgt het lemma. □

Propositie 1.4.7 *Als de vorm q_Σ positief definiet is, dan is de actie van de Weyl groep W op de verzameling wortels R transitief. (Dat wil zeggen, bij elk tweetal $r, s \in R$ bestaat een $\sigma \in W$ met $\sigma(r) = s$.)*

Bewijs. Laat twee wortels r, s gegeven zijn. Beschouw de verzameling S bestaande uit alle wortels van de vorm $\sigma(r)$, waarbij σ de Weyl groep doorloopt. Het opspansel in $\mathbb{R}^n$ van deze verzameling is een lineaire deelruimte die door W weer binnen zichzelf wordt afgebeeld. Vanwege Lemma 1.4.1 is dat dus de hele $\mathbb{R}^n$. Dit impliceert, dat er een $\sigma \in W$ is met $\langle C\sigma(r), s\rangle \neq 0$ (want anders zou s loodrecht staan op elke vector in onze verzameling S ten aanzien van het door $\langle Cv, w\rangle$ gegeven inproduct, en dan zou gelden $s = 0$). Neem zo'n σ en schrijf $t = \sigma(r) \in S$.
We moeten bewijzen dat $s \in S$. Merk daartoe allereerst op, dat als $v \in S$ dan ook $-v \in S$. Immers, een element $v \in S$ is een wortel; vanwege Propositie 1.3.2 (6) is dan de spiegeling $\sigma_v \in W$ en derhalve $-v = \sigma_v(v) \in S$. Hieruit volgt, dat we door eventueel s door $-s$ te vervangen mogen aannemen dat $\langle Ct, s\rangle > 0$. Lemma 1.4.6 zegt dan, dat uit dit inproduct 1 of 2 komt.
Is $\langle Ct, s\rangle = 2$, dan volgt bovendien uit Lemma 1.4.6 dat $s = t \in S$, en we zijn klaar. Het resterende geval is dat $\langle Ct, s\rangle = 1$. Maar in dat geval geeft een eenvoudige berekening dat $-s = \sigma_t\sigma_s(t) \in S$, en opnieuw volgt $s \in S$. □

1.5 Classificatie

We komen nu terug op Vraag 1.2.2: voor welke grafen Σ is de vorm q_Σ positief definiet? Het blijkt, dat zulke grafen allemaal te classificeren zijn. Om dit te doen, leiden we een aantal eigenschappen af van grafen Σ waarvoor q_Σ positief definiet is.

Lemma 1.5.1 *Als q_Σ positief definiet is, dan bevat Σ geen punten $i \neq j$ waartussen meerdere kanten liggen.*

Bewijs. Stel dat er $m \geq 1$ kanten liggen tussen i en j. Bekijk de vector $v = (x_1, \ldots, x_n)$ met $x_i = m$ en $x_j = 2$ en $x_k = 0$ als $k \notin \{i, j\}$. Dan is $q_\Sigma(v) = m^2 + 4 - m \cdot 2 \cdot m = 4 - m^2$. Omdat dit positief moet zijn, is $m = 1$. (alternatief bewijs: gebruik Lemma 1.4.6.) □

Lemma 1.5.2 *Als q_Σ positief definiet is, dan bevat Σ geen cykels (dat wil zeggen, een rij punten $1, \ldots, m$ met een kant tussen i en $i+1$, voor elke $i < m$, en een kant tussen 1 en m).*

Bewijs. Neem anders de vector $v = (x_1, \ldots, x_n)$ met $x_i = a_i$ voor $i \leq m$ en $x_i = 0$ voor $i > m$. Dan is $q_\Sigma(v) = a_1^2 + \ldots + a_m^2 - a_1a_2 - a_2a_3 - \ldots - a_ma_1$. Dit levert 0 op als we alle $a_i = 1$ kiezen. □

Lemma 1.5.3 *Als q_Σ positief definiet is, dan bevat Σ geen punt waar meer dan drie kanten bij elkaar komen.*

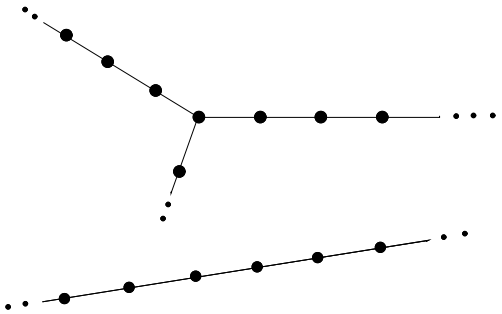
Bewijs. Dit is precies de uitspraak van Voorbeeld 1.2.3. □

Lemma 1.5.4 *Als q_Σ positief definiet is, dan bevat Σ hooguit één punt waar drie kanten bij elkaar komen.*

Bewijs. Als er meerdere zulke punten van Σ zouden zijn, dan bevat Σ een deelgraaf met $4 + r$ punten als volgt:

Neem dan de vector v met als coördinaten 1 corresponderend met de vier eindpunten van deze deelgraaf, 2 met de overige r punten van de deelgraaf, en 0 verder. Dan is $q_\Sigma(v) = 1^2 + 1^2 + 1^2 + 1^2 + r \cdot 2^2 - 4 \cdot 2 - (r-1) \cdot 4 = 0$, in tegenspraak met het positief definiet zijn. □

De vier lemma's tonen aan, dat er nog maar twee mogelijke "vormen" voor een graaf met positief definiete bijbehorende vorm mogelijk zijn: het is ofwel een rij punten met tussen elke twee opeenvolgenden precies één kant, ofwel het zijn drie van zulke rijen met een gemeenschappelijk eindpunt.



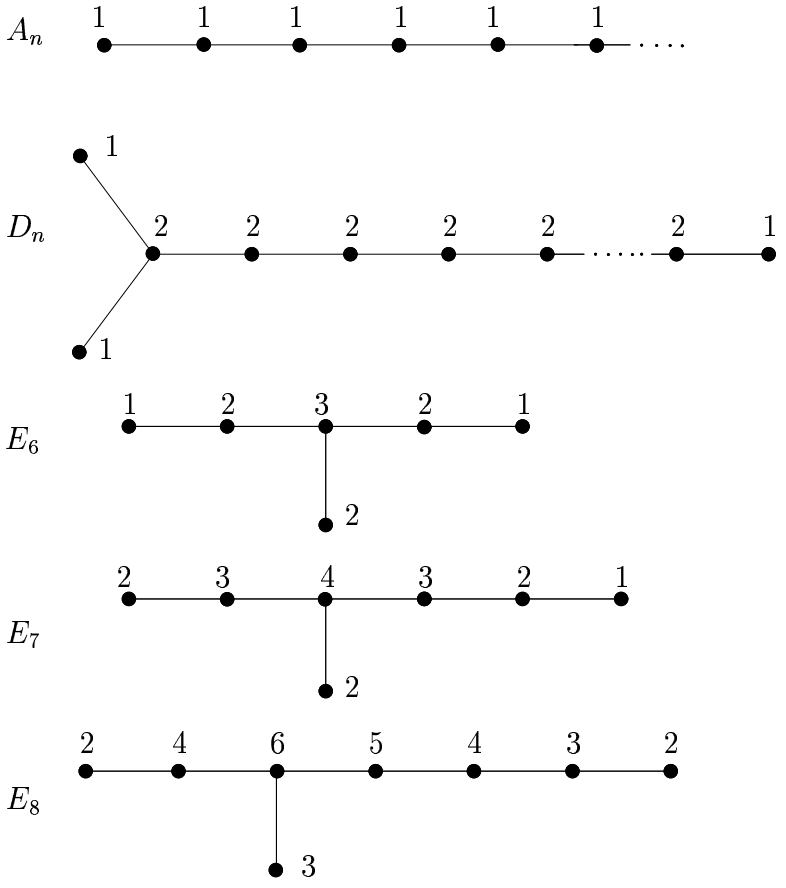
De tweede mogelijkheid gaan we nu verder analyseren. Noem het aantal punten in de drie takken respectievelijk $p+1, q+1$ en $r+1$, waarbij we mogen aannemen dat $p \leq q \leq r$. De graaf bestaat dus uit $n = p + q + r + 1$ punten. Schrijf $\mathbb{R}^n = \mathbb{R} \oplus P \oplus Q \oplus R$, waarbij $\mathbb{R}$ correspondeert met het gemeenschappelijk eindpunt en P, Q, R met de rest van de drie takken. Dus $\dim P = p$, enzovoorts. Omdat er behalve voor het gemeenschappelijke eindpunt geen kanten zijn tussen punten van verschillende takken, geldt $P \perp Q$ en $P \perp R$ en $Q \perp R$ voor het inproduct $\langle Cv, w\rangle =: [v, w]$. Neem in P de vector $v_P = \frac{1}{p+1}(p, \ldots, 2, 1)$ (uitgeschreven op de basis corresponderend met punten van onze graaf; de volgorde is zo dat de grootste coördinaat bij de basisvector hoort die direct naast het gemeenschappelijke eindpunt 'ligt'). Geheel analoog hebben we $v_Q \in Q$ en $v_R \in R$. We bepalen

nu $[v,v] = \langle Cv, v\rangle$ voor de vector $v = 1 \oplus v_P \oplus v_Q \oplus v_R$. Hiervoor is het handig, v te schrijven als som van de 4 gegeven componenten. Er geldt $[v_P, v_Q] = [v_P, v_R] = [v_Q, v_R] = 0$. Verder $[1,1] = 2$ en $[1, v_P] = -p/(p+1)$. En tenslotte $[v_P, v_P] = \frac{2}{(p+1)^2}\left(\sum_{i=1}^{p} i^2 - \sum_{i=1}^{p} i(i-1)\right) = p/(p+1)$. Zo volgt dat $[v,v] = 2 + p/(p+1) + q/(q+1) + r/(r+1) - 2p/(p+1) - 2q/(q+1) - 2r/(r+1) = 1/(p+1) + 1/(q+1) + 1/(r+1) - 1$.
Deze uitdrukking is positief omdat we aannemen dat onze vorm positief definiet is. Met andere woorden, we hebben hier de voorwaarde

$$1/(p+1) + 1/(q+1) + 1/(r+1) > 1$$

afgeleid. Van deze ongelijkheid zijn gemakkelijk alle mogelijke oplossingen te vinden. Immers, we hebben $1 \le p \le q \le r$, dus $1/2 \ge 1/(p+1) \ge 1/(q+1) \ge 1/(r+1)$. Hieruit volgt dat $p = 1$, want anders waren alle drie breuken $\le 1/3$ en dus hun som ≤ 1. Je kan nu verder eenvoudig alle mogelijkheden aflopen. Als ook $q = 1$, dan mag $r \ge 1$ willekeurig zijn. Is $q = 2$, dan volgt $1/2 + 1/3 + 1/(r+1) > 1$ en dus $r = 2$ of $r = 3$ of $r = 4$. En voor $q \ge 3$ zijn er geen oplossingen. Hiermee komen we tot het volgende resultaat.

Stelling 1.5.5 *De samenhangende grafen Σ met de eigenschap dat de door hun Cartanmatrix gegeven bilineaire vorm positief definiet is, zijn de grafen A_n met $n \ge 1$ punten en D_n met $n \ge 4$ punten en E_6 en E_7 en E_8, gegeven als volgt:*



Bewijs. We hebben al gezien dat de enige mogelijkheden voor een samenhangende graaf met positieve bilineaire vorm, de in de stelling gegeven grafen zijn. Wat dus overblijft, is inzien dat inderdaad al deze grafen aanleiding geven tot een positief definiete bilineaire vorm. Dit volgt direct uit Propositie 1.2.4, als voor de daar genoemde vector f degene wordt genomen met coördinaten zoals in bovenstaande grafen staat aangegeven. □

Merk op, dat bovenstaand bewijs meteen ook de omkering van Propositie 1.2.4 bewijst:

Gevolg 1.5.6 *Zij Σ een samenhangende graaf met Cartanmatrix C en kwadratische vorm q_Σ. Dan is q_Σ positief definiet precies dan, als er een vector f bestaat met positieve gehele coördinaten waarvoor geldt dat geen enkele coördinaat van Cf negatief is en bovendien dat $Cf \neq 0$. Deze equivalente uitspraken gelden alleen voor de door de diagrammen A_n, D_n en E_6, E_7, E_8 gegeven grafen.* □

Definitie 1.5.7 De grafen genoemd in Stelling 1.5.5 worden *Dynkin diagrammen* (ook wel, Coxeter diagrammen) van type A_n, D_n respectievelijk E_6 of E_7 of E_8 genoemd.

1.6 De voorbeelden

We gaan nu voor elk van de Dynkin diagrammen het aantal wortels bepalen, en iets over de bijbehorende Weyl groep zeggen. Hiertoe gaan we als volgt te werk.
Stel dat we in een zekere $\mathbb{R}^m$, voorzien van het standaard inproduct, vectoren $r_1, \ldots, r_n$ vinden zodat $\langle r_i, r_j \rangle$ precies de Cartan matrix is van een Dynkin diagram. Dan zijn deze vectoren lineair onafhankelijk, want de Cartan matrix van een Dynkin diagram is inverteerbaar. Zij $V \subset \mathbb{R}^m$ de lineaire deelruimte opgespannen door de r_i's. De lineaire afbeeldingen φ_i, gegeven door $\varphi_i(v) = v - \langle v, r_i \rangle r_i$, beelden dan V op V af, en ten opzichte van de gegeven basis voor V leveren ze precies dezelfde matrices als de voortbrengers van de Weyl groep behorende bij het gegeven Dynkin diagram. Met andere woorden, we kunnen de verzameling wortels identificeren met de beelden van de r_i's onder producten van de φ_j's, en de Weyl groep met de groep voortgebracht door de φ_j's.

Voorbeeld 1.6.1 A_n.
Kies in $\mathbb{R}^{n+1}$ met standaard orthonormale basis $e_1, \ldots, e_{n+1}$ de vectoren

$$r_1 = e_2 - e_1, \quad r_2 = e_3 - e_2, \quad \ldots\ldots, \quad r_n = e_{n+1} - e_n.$$

Dan geldt $\langle r_i, r_i \rangle = 2$ en $\langle r_i, r_j \rangle$ is 0 als $|i-j| \geq 2$ en $= -1$ als $|i-j| = 1$. Dus deze vectoren leveren precies het Dynkin diagram A_n. De bijbehorende "spiegelingen" φ_i, gezien als lineaire afbeelding op de hele $\mathbb{R}^{n+1}$, voldoen aan $\varphi_i(e_j) = e_j$ als $j \neq i, i+1$ en $\varphi_i(e_i) = e_{i+1}$ en $\varphi_i(e_{i+1}) = e_i$. Dus φ_i verwisselt e_i en e_{i+1} en houdt alle overige standaard basisvectoren vast. Elke permutatie van de $n+1$ basisvectoren is als product van zulke buurverwisselingen te schrijven, en de conclusie is dat de Weyl groep in dit geval isomorf is met de permutatie groep S_{n+1}. Het beeld van een wortel r_j onder zo'n permutatie is van de vorm $e_k - e_\ell$, met $k \neq \ell$, en elk van deze vectoren komt als beeld voor.
Er zijn dus in totaal $n(n+1)$ wortels, en de Weyl groep bestaat uit $(n+1)!$ elementen.

Voorbeeld 1.6.2 D_n voor $n \geq 4$.
Door een van de "pootjes" van het diagram D_n weg te laten ontstaat het diagram A_{n-1}. We beginnen dus met de vectoren

$$r_1 = e_2 - e_1, \quad r_2 = e_3 - e_2, \quad \ldots\ldots, \quad r_{n-1} = e_n - e_{n-1}$$

in $\mathbb{R}^n$. Hieraan moet dan nog een vector r_n worden toegevoegd die voldoet aan $\langle r_n, r_i \rangle = 2$ voor $i = n$ en $= -1$ voor $i = 2$ en $= 0$ voor alle overige i. Het is eenvoudig na te gaan dat

$$r_n = e_1 + e_2$$

een vector is die aan deze eisen voldoet.
De werking van φ_1 tot en met φ_{n-1} op de vectoren $e_1, \ldots, e_n$ kennen we al uit het voorbeeld van de A_n: deze brengen een groep isomorf met de permutatie groep S_n voort. Verder is $\varphi_n(e_i) = e_i$ voor $i \geq 3$ en $\varphi_n(e_1) = -e_2$ en $\varphi_n(e_2) = -e_1$. Er volgt dat $\varphi_1\varphi_n$ de eerste twee basisvectoren van teken verwisselt en de overige vasthoudt. Door dit te combineren met andere permutaties, zijn ieder tweetal basisvectoren van teken te verwisselen. Producten van zulke tekenwisselingen leveren alle afbeeldingen die een even aantal basisvectoren van teken verwisselen en de overige vasthouden. Zo vind je, dat de Weyl groep bestaat uit producten van permutaties en zulke tekenwisselingen; er geldt dus

$$\#W_{D_n} = 2^{n-1}n! \quad \text{voor } n \geq 4.$$

De wortels zijn dan alle vectoren $\pm e_k \pm e_\ell$ met $k \neq \ell$. Hiervan zijn er in totaal $2n(n-1)$.

Voorbeeld 1.6.3 E_8.
Door een pootje van het Dynkin diagram van E_8 wat in te korten, ontstaat het diagram van D_7. We beginnen daarom met de vectoren

$$r_2 = e_2 - e_1, \quad r_3 = e_3 - e_2, \quad \ldots\ldots, \quad r_7 = e_7 - e_6 \quad \text{en} \quad r_8 = e_1 + e_2$$

in $\mathbb{R}^8$. Hieraan voegen we dan nog een $r_1 \in \mathbb{R}^8$ toe die moet voldoen aan $\langle r_1, r_i \rangle = 2$ voor $i = 1$ en $= -1$ voor $i = 2$ en $= 0$ voor de overige i. Een van de beide vectoren die hieraan voldoen is

$$r_1 = \frac{1}{2}(1, -1, -1, -1, -1, -1, -1, -1, 1)\,.$$

Door net als in de voorbeelden van A_n en D_n de werking van de voortbrengers van de Weyl groep op de standaard basisvectoren uit te rekenen, volgt vrij snel dat de verzameling wortels in dit geval bestaat uit alle $\frac{1}{2}(\pm 1, \pm 1, \pm 1, \pm 1, \pm 1, \pm 1, \pm 1, \pm 1)$ waarin een even aantal mintekens voorkomen, plus alle vectoren $\pm e_k \pm e_\ell$ met $k \neq \ell$. In totaal zijn er dus $2^7 + 2 \cdot 8 \cdot 7 = 240$ wortels.
Het is wat lastig om ook de orde van de Weyl groep te bepalen. We zullen gebruik maken van het volgende resultaat.

Stelling 1.6.4 *Gegeven een Dynkin diagram dat bestaat uit n punten, met Cartan matrix C. Stel dat $s_i \in \mathbb{R}^n$ een vector $\neq 0$ is met $\langle Cs_i, e_j \rangle = 0$ voor $i \neq j$.*
Dan geldt Stab$(s_i) = \langle \sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n \rangle$ (de ondergroep van W voortgebracht door de σ_j met $i \neq j$).
Hierin is Stab(s) de stabilisator *van s; dit is de ondergroep $\{\sigma \in W \mid \sigma(s) = s\}$ van W.*

Deze stelling schijnt voor het eerst bewezen te zijn door de Duitse wiskundige E. Witt in 1941. Merk op dat $\sigma_j(s_i) = s_i - \langle Cr_j, s_i \rangle r_j$, en dat is gelijk aan s_i zodra $j \neq i$. Dit bewijst dat de ondergroep voortgebracht door zulke σ_j inderdaad in Stab(s_i) zit. De omgekeerde inclusie is niet zo snel te zien. We laten het bewijs achterwege; zie ervoor onder andere het boek L.C. Benson en C.T. Grove, *Finite Reflection Groups*. Springer-Verlag, GTM 99, second edition, 1985, pagina 77. Voor elk gegeven Dynkin diagram en een geschikt gekozen i is de stelling overigens redelijk eenvoudig te bewijzen.

In het geval van de E_8 kiezen we $s_7 = e_7 + e_8$. Die staat niet alleen loodrecht op $r_1, \ldots, r_6, r_8$ maar het is bovendien een wortel. Uit Propositie 1.4.7 volgt, dat de beelden van s_7 onder W precies alle wortels zijn, en dat zijn er 240. Er volgt dan dat $\#W = 240 \cdot \#\text{Stab}(s_7)$. De stelling van Witt zegt in dit geval, dat deze stabilisator de groep is voortgebracht door de spiegelingen behorend bij de wortels $r_1, \ldots, r_6, r_8$. Deze wortels horen bij het diagram E_7, dus kennelijk is Stab$(s_7) \cong W_{E_7}$.
We zullen hieronder zien, dat deze $2^{10} \cdot 3^4 \cdot 5 \cdot 7$ elementen heeft, en dan volgt

$$\#W_{E_8} = 240 \cdot 2^{10} \cdot 3^4 \cdot 5 \cdot 7 = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7.$$

Voorbeeld 1.6.5 E_7.
In het voorbeeld van E_8 hebben we de basiswortels bij E_7 al gevonden, en in feite ging dat door alles te beperken tot de deelruimte $(\mathbb{R}\cdot(e_7+e_8))^\perp \subset \mathbb{R}^8$.
De bijbehorende wortels zijn dan alle $\pm e_k \pm e_\ell$ met $k \neq \ell$ en $k,\ell \leq 6$, verder $\pm e_7 \mp e_8$ en tenslotte alle $\frac{1}{2}(\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\mp 1)$ (de laatste coördinaat moet tegengesteld zijn aan die ervoor) met een even aantal mintekens. In totaal levert dit $60+2+64=126$ wortels.
De orde van de Weyl groep is met eenzelfde idee als bij E_8 te vinden: neem de wortel $s_1 = e_7 - e_8$, deze staat loodrecht op $r_2,\ldots,r_6,r_8$. Laatstgenoemde wortels leveren een systeem D_6, en uit de stelling van Witt volgt dat de stabilisator van s_1 in W_{E_7} een groep is met $2^5\cdot 6! = 2^9\cdot 3\cdot 5$ elementen. Voor de Weyl groep zelf geldt dan

$$\#W_{E_7} = 126\cdot 2^9\cdot 3\cdot 5 = 2^{10}\cdot 3^3\cdot 5\cdot 7.$$

Voorbeeld 1.6.6 E_6.
Ook voor het resterende geval van de E_6 kan je beginnen met de voor E_8 gegeven vectoren. De deelverzameling $r_1,r_2,\ldots,r_5,r_8$ daarvan levert de Cartan matrix van E_6, en ze spannen de deelruimte $(\mathbb{R}\cdot(e_6+e_8)+\mathbb{R}(e_7+e_8))^\perp \subset \mathbb{R}^8$ op. We vinden dan de wortels $\pm e_k \pm e_\ell$ met $k\neq\ell$ en $k,\ell\leq 5$, en alle $\frac{1}{2}(\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\pm 1,\mp 1)$ met een even aantal mintekens, en zesde en zevende coördinaat beide tegengesteld aan de laatste coördinaat. In totaal zijn dat $40+32=72$ wortels.
Definieer $s_8 = \frac{1}{2}(1,1,1,1,1,-1,-1,1)$. Dit is een wortel, en bovendien eentje die loodrecht staat op elk van $r_1,\ldots,r_5$. Omdat deze bij een A_5 horen, heeft de ondergroep $\mathrm{Stab}(s_8)$ van W_{E_6} dus 6! elementen. Zo volgt

$$\#W_{E_6} = 72\cdot 6! = 2^7\cdot 3^3\cdot 5.$$

2 Wortelsystemen

2.1 Definitie en eigenschappen

De wortels bij een diagram A_n, D_n, E_6, E_7 of E_8 corresponderen volgens § 1.6 met een eindige collectie R van vectoren in een inproductruimte. De spiegelingen σ_r bij deze wortels permuteren de verzameling R, en daarom brengen ze een eindige groep voort. We gaan nu meer van dit soort eindige groepen maken door uit te gaan van eindige deelverzamelingen van $\mathbb{R}^n$ met analoge eigenschappen als de reeds behandelde wortels.
We werken steeds in $\mathbb{R}^n$ voorzien van het standaard inproduct. Voor $r\in\mathbb{R}^n$ met $r\neq 0$ wordt de loodrechte spiegeling σ_r in het hyperoppervlak $\{v\in\mathbb{R}^n \mid \langle v,r\rangle = 0\}$ gegeven door $\sigma_r(x) = x - 2\frac{\langle x,r\rangle}{\langle r,r\rangle}r$. Merk op dat σ_r en $\sigma_{\lambda r}$ voor $\lambda\neq 0$ dezelfde spiegelingen zijn.

Definitie 2.1.1 1. Een (gereduceerd en irreducibel) *wortelsysteem* in $\mathbb{R}^n$ is een eindige verzameling $r\subset\mathbb{R}^n$ (de elementen ervan noemen we *wortels*) die voldoet aan

(WS1) $0\notin R$ en R bevat een basis voor $\mathbb{R}^n$.

(WS2) Voor alle $r\in R$ is $\sigma_r(R)\subset R$.

(WS3) Voor $r,s\in R$ is $\sigma_r(s)-s$ een geheel veelvoud van r.

(WSred) Als $r\in R$ en $\lambda r\in R$, dan $\lambda = \pm 1$.

(WSirr) Er bestaat geen ontbinding $R = R_1\cup R_2$ met $R_1\neq\emptyset\neq R_2$ en $\langle r_1,r_2\rangle = 0$ voor alle $r_1\in R_1$ en $r_2\in R_2$.

2. De *Weyl groep* bij een wortelsysteem R is de (eindige) groep $W = W_R := \langle \sigma_r \mid r \in R \rangle$ voortgebracht door alle spiegelingen σ_r.

Opmerkingen 2.1.2 (a) Dat de zo gedefinieerde Weyl groep eindig is, volgt uit het feit dat een $\sigma \in W$ een permutatie op R levert; omdat R een basis van $\mathbb{R}^n$ bevat legt zo'n permutatie de lineaire afbeelding σ vast.

(b) Als R een wortelsysteem is, dan is voor vaste $\lambda \neq 0$ de verzameling $\lambda R := \{\lambda r \mid r \in R\}$ en zelfs $R \cup \lambda R$ dat ook. Maar deze systemen leveren dezelfde Weyl groep als R. Vandaar dat we ons vrijwel altijd beperken tot gereduceerde wortelsystemen, en zelfs zo'n systeem vaak zo schalen dat een kortste vector $r \in R$ de lengte 1 heeft.

(c) Een ontbinding $R = R_1 \cup R_2$ als genoemd in (WSirr) levert een opsplitsing $\mathbb{R}^n = V_1 \oplus V_2$ in twee onderling loodrechte lineaire deelruimten. De Weyl groep beeldt deze ruimten V_i binnen zichzelf af, en is het product van de Weyl groepen behorend bij $R_i \subset V_i$. Het levert dus geen serieuze beperking om alleen irreducibele wortelsystemen te behandelen.

(d) De wortels bij A_n, D_n, E_6, E_7 en E_8 leveren voorbeelden van gereduceerde, irreducibele wortelsystemen.

Conventie: een wortelsysteem zullen we in de rest van deze tekst gereduceerd en irreducibel veronderstellen.

Propositie 2.1.3 *De actie op $\mathbb{R}^n$ van de Weyl groep bij een wortelsysteem is irreducibel.*

Bewijs. (Vergelijk dit met het bewijs van Propositie 1.4.1.) Stel $V \neq (0)$ is een lineaire deelruimte die door W binnen zichzelf wordt afgebeeld. Kies $v \neq 0$ in V, en kies een $r \in R$ met $\langle v, r \rangle \neq 0$ (dit kan vanwege (WS1)). Door naar $\sigma_r(v) - v$ te kijken zie je dat $r \in V$. Met hetzelfde argument volgt voor elk rijtje wortels $r_0 = r, r_1, \ldots, r_i = s$ met $\langle r_j, r_{j+1} \rangle \neq 0$ voor alle j, dat ook $s \in V$. De verzameling van alle zo verkregen wortels s noemen we R_1, de collectie resterende wortels R_2. Er geldt $\langle r_1, r_2 \rangle = 0$ voor alle $r_1 \in R_1$ en $r_2 \in R_2$, dus vanwege (WSirr) is $R_2 = \emptyset$. Er volgt dat $V = \mathbb{R}^n$. □

2.1.4 De hoek φ met $0 \leq \varphi \leq \pi$ tussen twee wortels r, s wordt bepaald door de formule $\cos\varphi = \frac{\langle r,s \rangle}{||r|| \cdot ||s||}$. Merk op dat $\sigma_r(s) - s = 2\frac{\langle r,s \rangle}{\langle r,r \rangle} r \in \mathbb{Z} \cdot r$ vanwege (WS3), dus is

$$n(s,r) := 2\frac{\langle r, s \rangle}{\langle r, r \rangle} \in \mathbb{Z}.$$

Evenzo is dan $4\cos^2\varphi = n(s,r) \cdot n(r,s) \in \mathbb{Z}$. Op het nog eventueel omwisselen van r en s na levert dit de volgende tabel van mogelijkheden.

$4\cos^2\varphi$	$n(s,r)$	$n(r,s)$	φ	lengtes	orde$(\sigma_r\sigma_s)$
4	2	2	0	$r = s$	1
4	-2	-2	π	$r = -s$	1
3	3	1	$\pi/6$	$\|\|s\|\| = \sqrt{3} \cdot \|\|r\|\|$	6
3	-3	-1	$5\pi/6$	$\|\|s\|\| = \sqrt{3} \cdot \|\|r\|\|$	6
2	2	1	$\pi/4$	$\|\|s\|\| = \sqrt{2} \cdot \|\|r\|\|$	4
2	-2	-1	$3\pi/4$	$\|\|s\|\| = \sqrt{2} \cdot \|\|r\|\|$	4
1	1	1	$\pi/3$	$\|\|s\|\| = \|\|r\|\|$	3
1	-1	-1	$2\pi/3$	$\|\|s\|\| = \|\|r\|\|$	3
0	0	0	$\pi/2$	(?)	2

Voor het bepalen van de orde van $\sigma_r\sigma_s$ in deze tabel merken we op, dat de afbeelding de identiteit is op de ruimte $\{r,s\}^\perp$, en op het opspansel van r en s is de afbeelding zonder veel moeite uit te rekenen.
Merk op dat bij A_n, D_n, E_6, E_7 en E_8 alle wortels dezelfde lengte hebben, dus daar zijn de mogelijkheden nog beperkter dan ze in principe volgens deze tabel kunnen zijn.

2.2 Diagrammen

Om tot een classificatie van alle mogelijke wortelsystemen te komen, gaan we proberen hetzelfde te doen als voor de al behandelde gevallen. Daar begonnen we met n wortels die een basis vormen, en daar maakten we een graaf bij. Om ook in het algemenere geval zo'n deelverzameling te krijgen wordt het begrip "simpele wortel" ingevoerd.

Definitie 2.2.1 Kies bij een wortelsysteem R een $t \in \mathbb{R}^n$ met $\langle t, r\rangle \neq 0$ voor alle $r \in R$. Dit levert een ontbinding $R = R_t^+ \cup R_t^-$ in *positieve wortels*

$$R_t^+ := \{r \in R \mid \langle r, t\rangle > 0\}$$

en *negatieve wortels* $R_t^- := R \setminus R_t^+ = \{-r \mid r \in R_t^+\}$.
Een $r \in R_t^+$ heet *ontbindbaar* als $r = r_1 + r_2$ met $r_1, r_2 \in R_t^+$, en $r \in R_t^+$ heet *simpel* als r niet ontbindbaar is. De verzameling simpele wortels noteren we als S_t.

Lemma 2.2.2 *Voor twee simpele wortels $r \neq s$ geldt $\langle r, s\rangle \leq 0$.*

Bewijs. Als zou gelden $\langle r, s\rangle > 0$, dan zouden $n(r,s)$ en $n(s,r)$ beide in $\{1,2,3\}$ zitten. Deze getallen kunnen niet allebei 2 zijn want dan zou $r = s$. Dus na eventueel omwisselen van r en s mogen we aannemen $n(r,s) = 1$. Dit betekent dat $\sigma_s(r) = r - s$. Afhankelijk van of $r - s \in R_t^+$ of $s - r \in R_t^+$ is dan $r = (r-s) + s$ of $s = (s-r) + r$ niet simpel. □

Lemma 2.2.3 *De simpele wortels vormen een basis voor $\mathbb{R}^n$.*

Bewijs. (WS1) zegt dat de wortels $\mathbb{R}^n$ opspannen. De positieve wortels doen dat dan ook. Uit de definitie van ontbindbare positieve wortels volgt dat deze een lineaire combinatie van simpele wortels zijn. Dus de simpele wortels spannen $\mathbb{R}^n$ op.
Stel dat er een lineaire relatie is tussen simpele wortels. Deze is te schrijven als $\sum a_i r_i = \sum b_j s_j$, met de r_i, s_j simpele wortels, $r_i \neq s_j$ voor alle i,j en $a_i \geq 0, b_j \geq 0$. Gebruik makend van Lemma 2.2.2 volgt dat $v := \sum a_i r_i = \sum b_j s_j$ voldoet aan $\langle v, v\rangle \leq 0$, en dus $v = 0$. Dit impliceert $0 = \langle v, t\rangle = \sum a_i \langle r_i, t\rangle = \sum b_j \langle s_j, t\rangle$, en daaruit concluderen we dat alle $a_i = b_j = 0$. □

Propositie 2.2.4 *De Weyl groep bij een wortelsysteem wordt al door de spiegelingen σ_r behorend bij simpele wortels r voortgebracht.*

Bewijs. Zij W^+ de groep voortgebracht door alle σ_r voor r simpel. Merk op dat als $s = \sigma(r)$ voor $\sigma \in W^+$ en r simpel, dan volgt $\sigma_s = \sigma\sigma_r\sigma^{-1} \in W^+$ (vergelijk het bewijs van Propositie 1.3.2(6); in ons geval gebruik je dat spiegelingen orthogonale afbeeldingen zijn). Het volstaat dus, te laten zien dat elke wortel beeld van een simpele wortel is onder een afbeelding uit W^+. Equivalent hiermee: is r een wortel, dan bestaat er een $\sigma \in W^+$ met $\sigma(r) \in S_t$. Dit is als volgt te zien.
Voor een wortel s noteren we het hyperoppervlak loodrecht op s als V_s. Omdat R gereduceerd is, geldt $V_s = V_{s'}$ precies dan als $s = \pm s'$.
Er zijn maar eindig veel wortels en dus ook maar eindig veel zulke hyperoppervlakken, dus bestaat $\tilde{t} \in V_r$ met $\tilde{t} \notin V_s$ voor alle wortels $s \neq \pm r$. Dit houdt in dat $\langle \tilde{t}, \pm r\rangle = 0$ en $\langle \tilde{t}, s\rangle \neq 0$ voor

alle wortels $s \neq \pm r$. Door t' voldoende dicht bij $\tilde{t}$ in de juiste richting te kiezen vind je dat $|\langle t', s\rangle| > \langle t', r\rangle > 0$ (dus in het bijzonder nog steeds $\langle t', s\rangle \neq 0$) voor alle $s \neq \pm r$.
Deze t' kan nu gebruikt worden om positieve wortels $R^+_{t'}$ en simpele wortels $S_{t'}$ te definieren. Er geldt dat $r \in S_{t'}$, want $r = s_1 + s_2$ met de $s_i \in R^+_{t'}$ zou impliceren dat $\langle r, t'\rangle = \sum_i \langle s_i, t'\rangle = \sum_i |\langle s_i, t'\rangle|$, in tegenspraak met de keuze van t'.
Kies $\sigma \in W^+$ zo dat $\langle \sigma(t'), s\rangle \geq 0$ voor alle $s \in S_t$; dit kan vanwege Opgave 20. Omdat $\langle \sigma(t'), s\rangle = \langle t', \sigma^{-1}(s)\rangle \neq 0$ voor alle wortels s, levert $\sigma(t')$ precies dezelfde collectie positieve wortels als de oorspronkelijke t. Derhalve is ook $S_t = S_{\sigma(t')} = \sigma(S_{t'})$ en dus $\sigma(r) \in S_t$. □

Voor $r \neq s$ simpele wortels geldt $n(r, s) \in \{-3, -2, -1, 0\}$. De hoek tussen twee zulke wortels is af te lezen uit het product $n(r, s)n(s, r)$; deze is $\pi/2, 2\pi/3, 3\pi/4$ of $5\pi/6$. We gaan deze informatie weergeven door een graaf.

Definitie 2.2.5 Gegeven een wortelsysteem R met verzameling simpele wortels S_t. Door eventueel alles met een factor λ te vermenigvuldigen mogen we aannemen dat de lengte van de kortste vector in S_t gelijk aan 1 is.
Het *Dynkin diagram* bij R bestaat uit een graaf plus aanvullende informatie, als volgt. Voor elke $r \in S_t$ nemen we een punt, en bij dat punt schrijven we het getal $\langle r, r\rangle$.
Voor elk paar $r \neq s$ in S_t met $\langle r, s\rangle \neq 0$ nemen we een kant tussen de bijbehorende punten, en bij die kant schrijven we het getal $m(r, s) := n(r, s)n(s, r) \in \{1, 2, 3\}$.
Verder wordt algemeen de conventie gebruikt, dat het getal 1 bij een punt of kant niet wordt genoteerd.

Propositie 2.2.6 *Het Dynkin diagram bij een wortelsysteem is als graaf samenhangend.*

Bewijs. Indien niet, dan zouden alle simpele wortels behorend bij een samenhangscomponent loodrecht staan op die bij een andere component. Dit zou impliceren dat de Weyl groep niet irreducibel werkt op $\mathbb{R}^n$, want het opspansel van de vectoren bij zo'n samenhangscomponent wordt op zichzelf afgebeeld. □

Opmerking 2.2.7 Uit het Dynkin diagram is het inproduct $\langle \cdot, \cdot \rangle$ weer af te lezen. Immers, dit wordt volledig bepaald door de inproducten $\langle r_i, r_j\rangle$ waar de r_i de gegeven basis van simpele wortels doorlopen. Als $i = j$ heeft dit de waarde gelijk aan het getal bij punt i van de graaf. Als $i \neq j$ dan is $\langle r_i, r_j\rangle^2 = \frac{1}{2}m(r_i, r_j) \cdot \langle r_i, r_i\rangle \cdot \langle r_j, r_j\rangle$ (het product van de getallen bij de punten i en j en bij de kant $\{i, j\}$). Dit bepaalt $\langle r_i, r_j\rangle$ omdat we ook weten dat het ≤ 0 is.
Voor een vector $v = \sum a_r r$ (som over de simpele wortels r) is dus $\langle v, v\rangle$ gelijk aan de som met als termen $a_r^2 \cdot \langle r, r\rangle$ plus voor elk paar $\{r, s\}$ met $r \neq s$ een term $-a_r a_s \sqrt{\langle r, r\rangle\langle s, s\rangle m(r, s)}$.

2.3 Classificatie en voorbeelden

Om alle (gereduceerde en irreducibele) wortelsystemen in $\mathbb{R}^n$ te vinden zullen we eerst alle grafen bepalen met getallen op de punten en kanten, waarvoor de bilineaire vorm die dit definieert op $\mathbb{R}^n$ inderdaad positief definiet is.
Als eerste stap vervangen we elke $r \in S_t$ door $r/||r||$. Op deze manier raken we de getallen bij de punten van de graaf kwijt: als $v = \sum b_r r/||r||$, dan is

$$\langle v, v\rangle = \sum_r b_r^2 - \sum_{\{r,s\}} b_r b_s \sqrt{m(r, s)}.$$

Alle grafen bepalen met getallen $m(r, s) \in \{0, 1, 2, 3\}$ waarvoor dit positief definiet is, gaat op vrijwel dezelfde manier als we dat al eerder voor het geval met alle $m(r, s) \in \{0, 1\}$ hebben gedaan.

Dezelfde argumenten als in § 1.5 tonen aan dat er geen cykels mogen voorkomen, en dat er geen punten zijn waar ≥ 4 kanten samenkomen. We mogen en zullen verder aannemen dat er een kant is met $m(r,s) \geq 2$, want de resterende gevallen zijn al behandeld.

Lemma 2.3.1 *In een Dynkin diagram komen niet zowel een punt op minstens drie kanten als een kant met een getal ≥ 2 voor.*

Bewijs. Neem de vector met coefficient a in het punt op minstens drie kanten, coefficient b direct ernaast op één tak, idem coefficient c op een andere tak, allemaal a's op de derde tak tot aan een kant met $m = m(r,s) \geq 2$, en een d net voorbij die kant. De kwadratische vorm heeft hierbij een waarde $\leq a^2+b^2+c^2+d^2-ab-ac-\sqrt{m}ad = (b-a/2)^2+(c-a/2)^2+(d-\sqrt{m}a/2)^2+(2-m)a^2/4$, en dat wordt ≤ 0 voor zekere vectoren $\neq 0$. □

Dit beperkt de mogelijkheden al tot een rij punten $1, 2, \ldots, n$ met steeds één kant tussen i en $i+1$. Ga zelf na:

Lemma 2.3.2 *In een Dynkin diagram met punten $1, \ldots, n$ en kanten tussen alle i en $i+1$:*

(a) komt een getal ≥ 2 hoogstens een keer bij een kant voor.

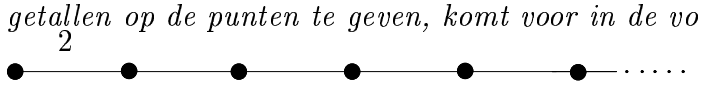
(b) komt een getal 3 bij een kant niet voor als $n \geq 3$.

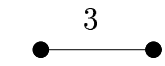
(c) komt een getal ≥ 4 niet voor bij een kant (dat wisten we al, maar je kan het ook inzien door naar positief definiet zijn te vragen).

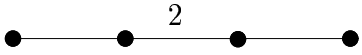
(d) komt een getal 2 bij een kant $\neq \{1,2\}$ en $\neq \{n-1, n\}$ niet voor als $n \geq 5$.

(Voor (d): schrijf, gerekend vanaf de kant met een getal 2, in één richting de coördinaten $a, 2b, b$ en in de andere richting $2c, c$ en verder nullen. De zo verkregen uitdrukking is niet positief definiet.) Uit dit lemma volgt direct:

Propositie 2.3.3 *Elk Dynkin diagram met tenminste één kant voorzien van een getal ≥ 2, zonder getallen op de punten te geven, komt voor in de volgende lijst:*







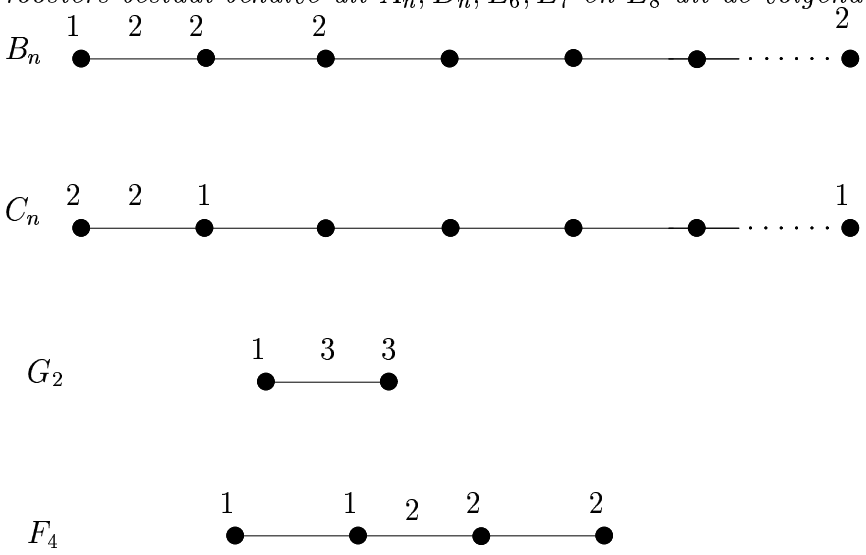
□

We hoeven nu alleen nog te kijken of het mogelijk is, getallen op de punten te zetten zo dat deze grafen ook werkelijk grafen bij een wortelsysteem zijn.

Lemma 2.3.4 *Als $r \neq \pm s$ wortels zijn met $m(r,s) = m$ en $||r|| \geq ||s||$, dan is $\langle r, r\rangle = m\langle s, s\rangle$. In een (gereduceerd en irreducibel) wortelsysteem komen hoogstens twee verschillende lengten van wortels voor.*

Bewijs. De eerste bewering is af te lezen uit de tabel in § 2.1.4. Voor de tweede, merk op dat de uitspraak juist is voor simpele wortels, en de overige zijn daar beelden van onder de Weyl groep; deze transformaties veranderen de lengte niet. □

Stelling 2.3.5 *De complete lijst van Dynkin diagrammen bij gereduceerde en irreducibele wortelroosters bestaat behalve uit A_n, D_n, E_6, E_7 en E_8 uit de volgende grafen:*



Bewijs. Dat dit alle mogelijke grafen zijn hebben we al beredeneerd. Door ergens bij een punt een getal 1 te zetten, volgt met Lemma 2.3.4 bovenstaande lijst. We moeten dan tenslotte nog aantonen dat er bij deze grafen ook echt wortelsystemen horen. Dat doen we in de volgende lijst voorbeelden. □

Voorbeeld 2.3.6 B_n en C_n.
Voor B_n kiezen we in $\mathbb{R}^n$ de vectoren

$$r_1 = e_1,\ r_2 = e_1 - e_2,\ r_3 = e_2 - e_3, \ldots, r_n = e_{n-1} - e_n.$$

Deze hebben de juiste inproducten en vormen een basis voor $\mathbb{R}^n$. De spiegelingen $\sigma_i := \sigma_{r_i}$ worden als volgt beschreven. Er geldt $\sigma_1(e_j) = e_j$ voor $j \geq 2$ en $\sigma_1(e_1) = -e_1$. Voor $i \geq 2$ is σ_i de buurverwisseling van e_i en e_{i-1}.
Zo is in te zien dat het wortelsysteem bestaat uit alle vectoren $\pm e_i$ en $\pm e_k \pm e_\ell$ (met $k \neq \ell$). Dat zijn er in totaal $2n^2$.
De Weyl groep bestaat uit alle combinaties van tekenwisselingen en permutaties op de standaard basisvectoren. Deze heeft dus $2^n \cdot n!$ elementen.

Door in dit voorbeeld r_1 met $\sqrt{2}$ te vermenigvuldigen en de overige r_i door $\sqrt{2}$ te delen, ontstaat C_n. Deze verandering heeft geen invloed op de Weyl groep, en evenmin op het aantal wortels.

Voorbeeld 2.3.7 G_2.
Neen $r_1 = (1, 0)$ en $r_2 = (-3/2, \sqrt{3}/2)$ in $\mathbb{R}^2$.
De Weyl groep wordt voortgebracht door σ_{r_1} en door $\sigma_{r_1}\sigma_{r_2}$; deze laatste afbeelding is een spiegeling over 60 graden.

Zo vinden we voor de Weyl groep de diedergroep D_6 (symmetriegroep van de regelmatige zeshoek) met 12 elementen, en we vinden ook 12 wortels (precies de elementen met norm ≤ 3 in $\mathbb{Z}[(-1+\sqrt{-3})/2] \subset \mathbb{C} \cong \mathbb{R}^2$).

Voorbeeld 2.3.8 F_4.

De vectoren

$$r_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4),\ r_2 = e_4,\ r_3 = e_3 - e_4 \quad \text{en } r_4 = e_2 - e_3$$

in $\mathbb{R}^4$ hebben de goede lengten en waarden $n(r_i, r_j)$.
Met wat gepuzzel volgt dat R bestaat uit alle $\pm e_i$ en alle $\pm e_k \pm e_\ell$ (voor $k \neq \ell$) en alle $\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4$. In totaal zijn dit $8 + 24 + 16 = 48$ wortels, de helft met lengte 1 en de andere helft met lengte 2.
De orde van de Weyl groep laat zich bijvoorbeeld met de bij E_8 genoemde stelling van Witt bepalen. Neem namelijk de wortel e_1. De baan hiervan onder W bestaat uit alle 24 wortels van lengte 1. En de stabilisator is $\langle \sigma_{r_2}, \sigma_{r_3}, \sigma_{r_4} \rangle$, precies de Weil groep van B_3. Dit impliceert

$$\#W_{F_4} = 24 \cdot \#W_{B_3} = 2^7 \cdot 3^2 = 1152.$$

2.3.9 We bewijzen tenslotte een resultaat over het *wortelrooster* bij een Dynkin diagram.

Definitie 2.3.10 Het *wortelrooster* Λ_R bij een wortelsysteem $R \subset \mathbb{R}^n$ bestaat per definitie uit alle lineaire combinaties met gehele coefficienten van de elementen van R.

Dit wortelrooster is inderdaad een *rooster*; dat wil zeggen het is een groep ten opzichte van de optelling van vectoren, het bevat een basis voor $\mathbb{R}^n$ en elke begrensde verzameling in $\mathbb{R}^n$ bevat slecht eindig veel elementen van het wortelrooster.

Propositie 2.3.11 *Zij R een wortelsysteem van type A_n, D_n, E_6, E_7 of E_8. We schalen dit zo, dat alle wortels inproduct 2 met zichzelf hebben. Het bijbehorende wortelrooster noteren we als Λ. Dan geldt dat $R = \{v \in \Lambda \mid \langle v, v \rangle = 2\}$.*

Bewijs. Schrijf $\tilde{R} = \{v \in \Lambda \mid \langle v, v \rangle = 2\}$. Er geldt $R \subset \tilde{R}$, vanwege Propositie 1.3.2. We hoeven dus alleen nog de andere inclusie te bewijzen. Dit gaat als volgt. Merk op, dat $\tilde{R}$ een wortelsysteem is. Dit wortelsysteem is bovendien gereduceerd, want alle elementen hebben dezelfde lengte. Bovendien is $\tilde{R}$ irreducibel. Immers, als $\tilde{R} = R_1 \cup R_2$ met $R_1 \perp R_2$, dan zou dit ook een opdeling van $R \subset \tilde{R}$ opleveren. Dan moet wel $R \subset R_1$ of $R \subset R_2$, omdat R een irreducibel wortelsysteem is. Maar $R^\perp = (0)$, dus er zou volgen dat ofwel R_1 ofwel R_2 de lege verzameling is. Neem nu een verzameling simpele wortels in $\tilde{R}$ en maak het bijbehorende Dynkin diagram. Dit is ook weer een diagram van type A_n, D_n, E_6, E_7 of E_8, want alle wortels hebben dezelfde lengte. Bovendien bevat het een zelfde soort wortelsysteem. Hieruit volgt de gevraagde gelijkheid. □

Voorbeeld 2.3.12 De vectoren met lengte $\sqrt{2}$ in het wortelrooster bij A_n corresponderen met de rijtjes gehele getallen $(a_1, \ldots, a_n)$ die voldoen aan

$$a_1^2 + \ldots + a_n^2 - a_1a_2 - a_2a_3 - \ldots - a_{n-1}a_n = 1.$$

Uit Propositie 2.3.11 volgt dat het aantal oplossingen precies het aantal wortels bij A_n is, en dat is $n(n+1)$. Ook zonder deze propositie is dit aantal wel te vinden, bijvoorbeeld door de vergelijking te herschrijven als

$$a_1^2 + (a_1 - a_2)^2 + (a_2 - a_3)^2 + \ldots + (a_{n-1} - a_n)^2 + a_n^2 = 2.$$

Controleer zelf dat deze inderdaad precies $n(n+1)$ gehele oplossingen heeft.

3 Opgaven

1. Zij K_n de volle graaf, dat wil zeggen de graaf bestaande uit n punten en precies één kant tussen ieder tweetal $i \neq j$ daarvan. Beantwoordt Vraag 1.1.4 voor K_n.

2. Stel dat de graaf Σ (zonder lusjes) een eindige vereniging is van disjuncte samenhangende grafen Σ_i. Ga na dat Vraag 1.1.4 geldt voor Σ precies dan als het geldt voor een van de Σ_i, terwijl voor alle andere de zwakkere vorm geldt waarbij niet ergens ook ongelijkheid wordt geeist. Hoe zit dat met Vraag 1.2.2?

3. Laat zien dat, hoewel er oneindig veel samenhangende grafen met n punten zijn, er toch slechts eindig veel kunnen zijn waarvoor Vraag 1.2.2 geldt.

   Een sterkere vorm hiervan: toon aan dat een graaf met n punten waarvoor Vraag 1.2.2 geldt, hoogstens $n-1$ kanten heeft.

4. Bewijs dat als Vraag 1.2.2 geldt voor Σ, dan ook voor elke deelgraaf (= een graaf die je uit Σ krijgt door een aantal punten en alle kanten daarheen weg te halen).

5. Bij de samenhangende graaf Σ die twee punten $i \neq j$ bevat met precies één kant ertussen, maken we $\overline{\Sigma}$ door de kant tussen i en j te verwijderen en vervolgens i en j te identificeren.

   Ga na dat als Vraag 1.2.2 voor Σ geldt, dan ook voor $\overline{\Sigma}$. (Met dit gegeven kan je alternatieve bewijzen maken voor een aantal lemma's uit §1.4)

   Geef een voorbeeld waaruit blijkt dat de omkering niet geldt.

6. Bepaal direct uit de definities de Weyl groep en de verzameling wortels van A_2, dat is de graaf met twee punten en een kant ertussen.

7. Laat zien dat uitgaande van een graaf, als r en λr beide wortels zijn dan volgt $\lambda = \pm 1$, en ook $\sigma_r = \sigma_{-r}$.

8. Gegeven een graaf Σ met q_Σ positief definiet. Wanneer geldt dat $\sigma_r \sigma_s = \sigma_s \sigma_r$ voor wortels r, s?

   Bepaal ook de orde van $\sigma_r \sigma_s$.

9. Neem een graaf bestaande uit 2 punten met $n \geq 1$ kanten ertussen. Ga na of de actie van de Weyl groep irreducibel is. Wat kan je zeggen over de Weyl groep als ondergroep van $\mathrm{SL}(2, \mathbb{Z})$?

10. (a) Laat zien dat als de Cartan matrix C van een samenhangende graaf inverteerbaar is, dan werkt de Weyl groep irreducibel. (Imiteer bijvoorbeeld het bewijs van Lemma 1.4.1)

    (b) Omgekeerd, is $v \neq 0$ een vector met $Cv = 0$, dan geldt $\sigma(v) = v$ voor elke σ in de Weyl groep, dus als de graaf uit minstens twee punten bestaat is in dit geval de actie van de Weyl niet irreducibel.

11. Toon aan dat als de Cartan matrix bij een graaf inverteerbaar is, dan bestaat het centrum van de Weyl groep uit hoogstens twee elementen. (Het centrum van een groep G bestaat uit alle $h \in G$ met $hg = gh$ voor elke $g \in G$).

    Probeer het centrum te bepalen voor een aantal van de gevallen A_n, D_n, E_6, E_7, E_8.

12. Bepaal alle grafen bestaande uit 3 punten waarvoor geldt dat de bijbehorende Weyl groep *niet* irreducibel werkt op $\mathbb{R}^3$.

13. Bewijs de stelling van Witt (1.6.4) voor het speciale geval van A_n. Hoe groot is de stabilisator in zo'n geval, en hoeveel beelden heeft de genomen vector s_i onder de actie van W?

14. Onderzoek in welke gevallen men voor de vector s_i in Stelling 1.6.4 een *wortel* kan nemen.

    Wat kan je in zo'n geval zeggen over de groep $\langle \sigma_1, \ldots, \sigma_{i-1}, \sigma_{s_i}, \sigma_{i+1}, \ldots, \sigma_n \rangle$?

    Ga na dat als r_i wordt vervangen door de wortel s_i, dan blijft in ieder geval onafhankelijkheid van de n gegeven vectoren over. Wat gebeurt er met het Dynkin diagram?

15. Ga na dat in het voorbeeld over E_8 inderdaad alle $\pm e_k \pm e_\ell$ wortels zijn.

16. Beschrijf een element van orde 7 en ook een van orde 8 in de Weyl groep van E_8.

17. Maak een schets van elk van de gereduceerde, irreducibele wortelsystemen in $\mathbb{R}^2$. (Dat zijn A_2, B_2 en G_2.)

18. Bewijs de bewering over de ordes van $\sigma_r \sigma_t$ in de tabel van § 2.1.4.

19. Ga na dat elk element van een wortelsysteem te schrijven is als een combinatie $\sum a_s s$ van simpele wortels, waarbij ofwel alle $a_s \geq 0$ zijn, ofwel alle $a_s \leq 0$.

20. Maak bij een wortelsysteem met simpele wortels S_t de "kamer" $C := \{x \in \mathbb{R}^n \mid \langle x, r \rangle \geq 0 \text{ voor alle } r \in S_t\}$. Ga na dat elke $v \in \mathbb{R}^n$ door een product van spiegelingen bij de simpele wortels binnen C is af te beelden. (Idee: er geldt $t \in C$; neem de vector $w = \sigma(v)$ met σ een product van de genoemde spiegelingen, waarvoor de afstand tot t minimaal is, en ga na dat $w \in C$.)

21. Bewijs dat de groep voortgebracht door de spiegelingen bij de simpele wortels irreducibel werkt op $\mathbb{R}^n$.

22. Geef een bewijs van Lemma 2.3.2.

23. Gebruik eenzelfde argument als in het bewijs van Propositie 2.2.4 om te bewijzen dat als S_t en $S_{t'}$ de simpele wortels zijn uitgaande van een vector t respectievelijk t', dan is er een element van de Weyl groep dat S_t op $S_{t'}$ afbeeldt. Laat zien dat hieruit volgt dat het Dynkin diagram bij een wortelsysteem niet van de keuze van de vector t afhangt.

24. Het voorbeeld van F_4 heeft te maken met het volgende. Begin met de quaternionen $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ met $ij = -ji = k$ en $jk = -kj = i$ en $ki = -ik = j$ en $i^2 = j^2 = k^2 = -1$. Bij een $x \in \mathbb{H}$ hebben we z'n geconjugeerde $\overline{x}$ die de coefficient van i, j en k van teken wisselt. Verder hebben we het spoor $S(x) = x + \overline{x}$ en de norm $N(x) = x\overline{x}$, beide rationale getallen.

    Ga na dat de quaternionen x waarvoor geldt dat $N(x) \in \mathbb{Z}$ en bovendien $S(x), S(ix), S(jx), S(kx) \in \mathbb{Z}$ een ring vormen.

    Bepaal de eenheden en elementen van norm 2 in deze ring. Zie je een verband met F_4?

25. Hoeveel oplossingen heeft de vergelijking $q_\Sigma(v) = 1$ met Σ het Dynkin diagram D_n en v in het bijbehorende wortelrooster? Probeer deze vergelijking ook zonder de hier behandelde theorie op te lossen.

Tentamen Algebra & Meetkunde, 20 februari 1998, 14.00–17.00.

1. Neem $V := Z(x^2 + 2xy - 2y^2 + 2x + 2y + 1) \subset \mathbb{A}^2$, gezien over een algebraïsch afgesloten lichaam K.

   (a) Bepaal alle singuliere punten van V (onderscheid de gevallen $\mathrm{kar}(K) = 3$ en $\mathrm{kar}(K) \neq 3$).

   (b) Wat voor type kwadriek is V?

2. Gegeven een irreducibel polynoom $F \in K[x, y]$, met K algebraïsch afgesloten. Neem $V := Z(F) \subset \mathbb{A}^2$.

   (a) Toon aan dat als $\mathrm{graad}(F) = 1$, dan bevat V geen singuliere punten.

   (b) Toon aan dat als $\mathrm{graad}(F) = 2$ of 3, dan bevat V hooguit 1 singulier punt (hint: als er meerdere singuliere punten zijn, neem dan een lijn door twee ervan, en onderzoek het aantal snijpunten gerekend met multipliciteit van zo'n lijn met V).

   (c) Geef een voorbeeld van een irreducibele F van graad 4, waarvoor $Z(F)$ twee singuliere punten heeft.

3. Neem $I = (yw^2 - x^3, y^2, zx) \subset K[x, y, z, w]$.

   (a) Beschrijf $Z(I) \subset \mathbb{P}^3$.

   (b) Bepaal het radicaal van I.

4. (a) Neem een graaf bestaande uit 2 punten en geen kanten. Bepaal de Weyl groep bij deze graaf en ook het aantal wortels.

   (b) Neem vervolgens een graaf met $n+m$ punten, die bestaat uit de vereniging (niet samenhangend) van de Dynkin diagrammen bij A_n en bij A_m. Hoeveel wortels horen er bij deze graaf?

5. Zij C de $n \times n$ Cartan matrix behorend bij een Dynkin diagram van type A_n, D_n, E_6, E_7 of E_8. Stel dat in $\mathbb{R}^n$ vectoren $r_1, \ldots, r_n$ gegeven zijn zodat de matrix $(\langle r_i, r_j \rangle)_{i,j}$ gelijk is aan C.

   De spiegelingen σ_i met $\sigma_i(v) = v - \langle v, r_i \rangle r_i$ geven dan aanleiding tot een verzameling wortels $R \subset \mathbb{R}^n$.

   Definieer

   $$\tilde{R} := \left\{ v \in \mathbb{R}^n \mid v = \sum_{r \in R} a_r r \text{ met alle } a_r \in \mathbb{Z} \text{ en } \langle v, v \rangle = 2 \right\}.$$

   (a) Laat zien dat $\tilde{R}$ een wortelsysteem is.

   (b) Laat zien dat $\tilde{R}$ gereduceerd is.

   (c) Laat zien dat $\tilde{R}$ irreducibel is.

   (d) Laat zien dat $\tilde{R} = R$ (idee: $\tilde{R}$ hoort, als gereduceerd en irreducibel wortelsysteem, bij een Dynkin diagram. Ga na dat dit alleen maar het diagram kan zijn waarbij R gemaakt is).