Bachelorscriptie

MDS-codes en AMDS-codes afkomstig van algebraïsche krommen van geslacht nul en één

René Pannekoek

Voorwoord

Aber könnte man nicht sagen, dass die Regeln diesen Weg führen, auch wenn niemand ihn ginge? – Ludwig Wittgenstein

Deze scriptie houdt zich bezig met onderwerpen uit de coderingstheorie. Afgezien van de wiskundige complicaties die optreden als je er wat nader op ingaat, dient de coderingstheorie een verrassend praktisch doel, namelijk het zo goed mogelijk overbrengen van informatie. De beginselen van de coderingstheorie zijn dan ook goed toe te lichten door enkele vergelijkingen met onze spreektaal.

Gewone spreektaal bevat veel redundantie. Men zegt gewoonlijk niet: "geef mij de boter", maar "wil je mij de boter geven?" of zelfs "zou je mij misschien de boter willen geven?". Deze toevoegingen worden vaak uitgelegd als een manier om zinnen beleefder te laten klinken, maar wellicht wordt hier ook een informatietechnisch doel gediend.

Een gesprekspartner die bij het luisteren gehinderd wordt heeft meer kans om de tweede zin te verstaan, dan om de eerste zin te verstaan. De kans op het verstaan van de derde zin is nog groter. De redundantie in de tweede en derde zin maken de boodschap enigszins bestand tegen ruis op de lijn.

Hetzelfde fenomeen wordt gebruikt in digitaal verkeer, bijvoorbeeld in internetverkeer of communicatie tussen radiostations. Digitale gegevens worden voorzien van extra bits, die het mogelijk maken om de verzonden gegevens bij niet al te grove transmissiefouten toch correct te interpreteren. In de wiskunde is dit idee geformaliseerd in het begrip "code". Het "coderen" van informatie in deze zin betekent: het inbouwen van redundantie die de informatie bestendig maakt tegen kleine verstoringen. Het dient te worden opgemerkt dat coderen in deze zin niets te maken heeft met het ontoegankelijk maken van informatie voor derden; daarover gaat een andere tak van de wiskunde, cryptografie genaamd.

Het coderen van de gegevens gaat in blokken van een vaste lengte. De in zekere kringen zeer bekende "uitgebreide binaire Golay-code" neemt als invoer blokken van 12 bits en levert als uitvoer blokken van 24 bits: twee keer zoveel. De redundantie van de gegevens na codering is dus maar liefst 50%. In ruil hiervoor mogen er in een blok van 24 bits maar liefst drie verzendfouten worden gemaakt, zonder dat dit bij de decodering een probleem oplevert. Een licht gewijzigde strategie bestaat eruit dat de ontvanger per

blok kijkt of er iets is misgegaan, en, in het geval van een fout, verzoekt om een hernieuwde transmissie. In dat geval detecteert de Golay-code tot wel zeven fouten.

De Golay-code codeert dus steeds 12 bits in één keer. Er zijn $2^{12} = 4096$ van zulke blokken, en de Golay-code zet deze om in 4096 blokken van 24 bits. We kunnen deze 4096 reeksen van 24 bits zien als even zoveel "woorden" in een zekere taal, een soort digitaal vocabulaire, waarin alle woorden toevallig even lang zijn. Dit idee gebruiken we weer om een brug te slaan naar gewone spreektaal.

Soms verschillen twee woorden in het Nederlandse vocabulaire zo weinig van elkaar dat er misverstanden door kunnen ontstaan, zoals wanneer een caféhouder aan een van zijn serveersters vraagt: "heb je die plant daar zijn water al gegeven?", en de serveerster in plaats van "plant" "klant" verstaat. Dit misverstand wordt veroorzaakt doordat de twee woorden "klant" en "plant" onderling erg weinig verschillen. Een manier om dit coderingstheoretisch te formuleren is te zeggen dat de onderlinge *afstand* van de woorden "klant" en "plant" klein is (namelijk één letter).

De Golay-code heeft de wenselijke eigenschap dat de woorden in haar 4096 leden tellende vocabulaire geen van alle erg op elkaar lijken. De afstand tussen twee willekeurig gekozen woorden uit de Golay-code is dus niet al te klein. Om precies te zijn verschillen twee woorden uit de Golay-code altijd op minstens acht plaatsen van elkaar. Men zegt ook wel dat de afstand van de Golay-code, begrepen als de minimale afstand tussen twee van haar woorden, acht bedraagt.

Het doel van de coderingstheorie is het vinden van codes die een grote afstand combineren met een lage redundantie. Beide wensen kunnen niet tegelijkertijd worden bevredigd: codes met een grotere afstand hebben (bij gelijkblijvende lengte der blokken) veelal een grotere redundantie, en andersom bezitten codes met een lage redundantie vaak een kleinere afstand. Hierin valt een soort wet van behoud van energie te lezen, die in de coderingstheorie onder andere tot uitdrukking komt in de "Singleton-grens", die in deze scriptie min of meer centraal zal staan. Deze scriptie onderzoekt zogenaamde MDS-codes, die de eigenschap hebben dat geen van beide parameters verder kan worden geoptimaliseerd terwijl de andere gelijk blijft.

Algebraïsch-geometrische codes

In de jaren zeventig werd ontdekt dat de theorie van algebraïsche krommen gebruikt kan worden om goede codes mee te fabriceren. Met gladde algebraïsche krommen kunnen eindigdimensionale vectorruimten worden geassocieerd, de zogenaamde Riemann-Roch-ruimten, die kunnen worden "geprojecteerd" op de $\mathbb{F}_q^n$. Dit levert ons deelruimten van de $\mathbb{F}_q^n$, oftewel lineaire blokcodes. De stelling van Riemann-Roch vertelt ons vervolgens iets over de dimensie en de afstand van deze codes.

In deze scriptie richten we ons vooral op codes verkregen uit krommen van geslacht nul en één. De stelling van Riemann-Roch impliceert dat krommen van geslacht nul, bij geschikte keuze van de parameters, MDS-codes opleveren. Een vraag die onmiddellijk rijst is of we deze onuitputtelijke rijkdom aan MDS-codes kunnen classificeren: zijn de MDS-codes die we op deze manier krijgen lid van een familie of meerdere families die we op een andere manier al kenden, of kunnen we in principe alles nog verwachten van deze onderklasse van algebraïsch-geometrische codes? Ook onderzoeken we de voorwaarden waaronder een andere keuze van de betrokken parameters daadwerkelijk leidt tot een andere code, dat wil zeggen een code die niet equivalent of permutatie-equivalent is met de oorspronkelijke code.

Voor krommen van geslacht één is de zaak minder duidelijk: het Singleton-defect van een code is (wederom bij geschikte keuze van de parameters) hooguit gelijk aan één, maar het is niet uitgesloten dat we ook in deze contreien MDS-codes aantreffen. We stellen ons in deze scriptie niet tot doel om uit te zoeken wat voor het optreden van MDS-codes noodzakelijke en/of voldoende voorwaarden zijn. Wel gaan we na of er inderdaad MDS-codes te vinden zijn, en of deze MDS-codes al dan niet (permutatie-)equivalent zijn.

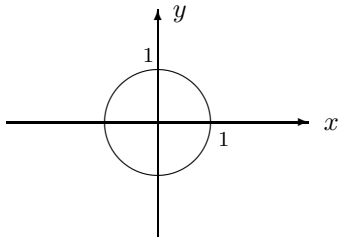
Voorkennis

Bij het doornemen van deze scriptie zal enige kennis van commutatieve algebra de lezer niet in de weg zitten. Echter, ook zonder deze kennis zijn de meeste bewijzen goed te volgen, mits de lezer bereid is enkele eenvoudige resultaten op gezag van de schrijver aan te nemen.

Inhoudsopgave

1 Algebraïsche krommen

In dit hoofdstuk behandelen we de benodigde voorkennis over *algebraïsche krommen*. Een voorbeeld van een algebraïsche kromme is de eenheidscirkel C in het platte vlak (de $\mathbb{R}^2$). Deze wordt gegeven door de polynoomvergelijking $x^2 + y^2 - 1 = 0$.



Eerst introduceren we in dit hoofdstuk het begrip *variëteit*. Daarna behandelen we de (vlakke) algebraïsche kromme als speciaal geval van een variëteit. Omdat vlakke krommen gegeven worden door nulpuntenverzameling van een enkel (irreducibel) polynoom f, blijft de notatie overzichtelijk. Na variëteiten en krommen in de affiene ruimte te hebben besproken, gaan we over op de projectieve ruimte. In de projectieve ruimte blijken krommen aan allerlei mooie eigenschappen te voldoen.
In hoofdstuk 2 bespreken we divisoren op krommen. Met divisoren associëren we bepaalde eindigdimensionale vectorruimtes over $\mathbb{F}_q$, en deze geven aanleiding tot foutcorrigerende codes. Met de stelling van Riemann-Roch kunnen we vervolgens de parameters van deze codes nader bepalen.
Met de hoofdletter K geven we steeds een algebraïsch afgesloten lichaam aan, een kleine letter k geeft een lichaam aan waaraan verder geen voorwaarden opgelegd zijn.

1.1 Affiene variëteiten

Zij K een algebraïsch afgesloten lichaam. We definiëren nu eerst *de affiene ruimte* $\mathbb{A}^n(K)$:

Definitie 1.1. *De affiene ruimte $\mathbb{A}^n(K)$, of eenvoudigweg $\mathbb{A}^n$, is de verzameling van alle n-tallen $(x_1, x_2, \ldots, x_n)$ met $x_i \in K$. Het lichaam K wordt ook wel het grondlichaam genoemd.*

We zien dus dat $\overline{\mathbb{Q}}$ en $\mathbb{C}^2$ verzamelingen zijn die geïdentificeerd kunnen worden met affiene ruimten. In deze eerste paragraaf gaan we kijken naar variëteiten die optreden als deelverzamelingen van affiene ruimten. We geven eerst een precieze definitie van het begrip variëteit:

Definitie 1.2. *Een affiene variëteit $V \subset \mathbb{A}^n(K)$ is een verzameling van de vorm*

$$\{(\xi_1, \xi_2, \ldots, \xi_n) \in \mathbb{A}^n(K) : f_i(\xi_1, \xi_2, \ldots, \xi_n) = 0 \text{ voor } 1 \leq i \leq m\}$$

waarin $m \in \mathbb{Z}_{\geq 1}$ en de $f_1, \ldots, f_m$ polynomen zijn in $K[x_1, x_2, \ldots, x_n]$. 0

We werken dus vooralsnog met de aanname dat het grondlichaam K algebraïsch afgesloten moet zijn. De cirkel C uit de inleiding ligt echter in de $\mathbb{R}^2$. Hoe moeten we C nu zien? We kunnen eerst C' definiëren als een variëteit over $\mathbb{C}^2$, gedefinieerd door het polynoom x^2+y^2-1. Dan is C de doorsnijding van C' met het reële vlak. In §1.3 zullen we nader kijken naar variëteiten over niet-algebraïsch afgesloten lichamen.

We zien dat we voor een variëteit in de $\mathbb{A}^n$ in het algemeen polynomen in n variabelen nodig hebben. Dit zet ons aan tot de volgende definitie:

Definitie 1.3. *De coördinatenring van de affiene ruimte $\mathbb{A}^n(K)$ is $K[x_1, x_2, \ldots, x_n]$, de polynoomring in n variabelen. We noteren de coördinatenring ook wel met $K[\mathbb{A}^n]$.*

We kunnen dus een variëteit $V \subset \mathbb{A}^n$ definiëren door een eindige deelverzameling $I \subset K[\mathbb{A}^n]$ te kiezen en V te kiezen als de nulpuntsverzameling van alle polynomen in I.

Definitie 1.4. *Zij $I \subset K[\mathbb{A}^n]$ een eindige deelverzameling. Met $V(I)$ noteren we de nulpuntenverzameling van I in $\mathbb{A}^n$, oftewel:*

$$V(I) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ voor alle } f \in I\}$$

Als I geschreven hebben als $I = \{f_1, \ldots, f_m\}$, noteren we $V(I)$ ook wel met $V(f_1, \ldots, f_m)$. We kunnen de definitie van $V(I)$ uitbreiden tot het geval waarin I een ideaal is in de $K[\mathbb{A}^n]$:

Stelling 1.5. *Zij $J \subset K[\mathbb{A}^n]$ een eindige verzameling en I het ideaal voortgebracht door de elementen van J. Zij nu $V(I)$ de verzameling*

$$V(I) := \{P \in \mathbb{A}^n : f(P) = 0 \text{ voor alle } f \in I\}$$

Dan zijn $V(I)$ en $V(J)$ dezelfde deelverzameling in de $\mathbb{A}^n$.

Bewijs. Er geldt zeker $V(I) \subset V(J)$, dus aan te tonen dat als alle elementen van J in $P \in \mathbb{A}^n$ verdwijnen, ook alle elementen van I in P verdwijnen. Neem $g \in I$, dan is g te schrijven als een eindige som $h_1 f_1 + h_2 f_2 + \ldots + h_m f_m$ met $h_i \in K[\mathbb{A}^n]$ en $f_i \in J$. Hieruit volgt dat $g(P) = 0$. Dit geldt voor willekeurige g, dus $P \in V(I)$. □

We kunnen ons afvragen of we onze definitie van V kunnen uitbreiden tot *alle* idealen $I \subset K[\mathbb{A}^n]$. Het antwoord luidt: ja. Noodzakelijke en voldoende voorwaarde hiervoor is dat I geschreven kan worden als $I = (f_1, \ldots, f_m)$. Een dergelijk ideaal heet *eindig voortgebracht*, om duidelijke redenen. Een ring R waarvan alle idealen eindig voortgebracht zijn heet *Noethers*. We vermelden de basisstelling van Hilbert:

Stelling 1.6 (Hilberts basisstelling). *Zij R een Noetherse ring en $n \geq 1$, dan is ook de polynoomring $R[x_1, x_2, \ldots, x_n]$ een Noetherse ring.*

Bewijs. [Kunz, blz. 11]. □

In ons geval geldt $R = K$. De idealen van een lichaam K zijn op één hand te tellen, namelijk (0) en K zelf, dus K is zeker Noethers. Dus ook $K[\mathbb{A}^n]$ is Noethers en al haar idealen corresponderen derhalve met variëteiten. Daarmee kunnen we $V(J)$ nu zelfs definiëren voor willekeurige deelverzamelingen $J \subset K[\mathbb{A}^n]$: we stellen gewoon $V(J) = V(I)$, waar I het ideaal is voortgebracht door J.

Definitie 1.7. *Zij $S \subset \mathbb{A}^n$ een deelverzameling. Definieer $I(S)$ als*

$$I(S) = \{f \in K[\mathbb{A}^n] \ : \ f(x) = 0 \text{ voor alle } x \in S\}.$$

Stelling 1.8. *Zij $S \subset \mathbb{A}^n$ een deelverzameling van een affiene ruimte. Dan is $I(S)$ een ideaal in de coördinatenring $K[\mathbb{A}^n]$.*

Bewijs. Stel $f, g \in I(S)$, dan geldt dat $f(x) = 0$ en $g(x) = 0$ voor alle $x \in S$, dus ook $(f+g)(x) = 0$ voor alle $x \in S$. Dus $f + g \in I(S)$. Zij $h \in K[\mathbb{A}^n]$ willekeurig, dan $h(x)f(x) = h(x) \cdot 0 = 0$ voor alle $x \in S$, dus $hf \in I(S)$. Tenslotte is $0 \in I(S)$ triviaal. Dus $I(S)$ is een ideaal. □

Merk op dat de operatoren $I(\cdot)$ en $V(\cdot)$ "inclusies omkeren". Dat wil zeggen dat als $I \subset J$ dan $V(I) \supset V(J)$. Evenzo geldt $V \subset W \Rightarrow I(V) \supset I(W)$.

We kunnen ons nu afvragen wat bij de cirkel C uit het voorbeeld, beschouwd als variëteit in de $\mathbb{A}^2(\mathbb{C})$, het geassocieerde ideaal $I(C)$ is. Het antwoord lijkt eenvoudig: "$I(C) = (x^2 + y^2 - 1)$". De laatste uitspraak vereist wel enige zorg: we moeten namelijk nagaan of het ideaal $(x^2 + y^2 - 1)$ alle functies bevat die verdwijnen op de eenheidscirkel. Dat dit geen vantevoren uitgemaakte zaak is kan worden ingezien door het ideaal $(x^2) \subset \mathbb{C}[x, y]$ te beschouwen. Dit ideaal definieert een verticale lijn door de oorsprong, noem deze lijn L. We zien echter dat $I(L)$ ook het element x moet bevatten, en dus ook (x), het hele ideaal voortgebracht door x. Het is eenvoudig in te zien, door beide inclusies te bewijzen, dat $I(L) = (x)$.

We zullen nu bewijzen dat $I(C) = (x^2 + y^2 - 1)$. Hiertoe moeten we bewijzen dat als $F(x, y)$ verdwijnt op C, dan $F(x, y) \equiv 0 \bmod x^2 + y^2 - 1$. Stel F is zodanig dat $F(x, y) = 0$ op de eenheidscirkel. We reduceren F eerst modulo ons ideaal. We gebruiken dat $y^2 \equiv 1 - x^2$, waarmee we $F(x, y)$ in de vorm $F(x, y) \equiv P(x) + Q(x)y \bmod x^2 + y^2 - 1$ kunnen brengen. We nemen eerst aan dat niet geldt dat $Q(x) \equiv 0$. Nu geldt dat (behoudens een eindig aantal nulpunten van $Q(x)$) bij elke waarde van x slechts één $y \in \mathbb{C}$ bestaat zodanig dat $F(x, y) = 0$. Neem aan dat $\tilde{x}$ zodanig is dat $Q(\tilde{x}) \neq 0$ en dat verder

$\tilde{x} \neq -1, 1$. Nu geldt dat de vergelijking $\tilde{x}^2 + y^2 = 1$ twee oplossingen heeft voor y, zeg $\tilde{y}$ en $-\tilde{y}$. Maar we concludeerden zojuist dat $F(\tilde{x}, \tilde{y})$ en $F(\tilde{x}, -\tilde{y})$ niet beide gelijk aan nul zijn. Onze aanname leidt dus tot een tegenspraak, dus $Q(x) \equiv 0$. Hieruit volgt ook dat $P(x) = 0$ en dus is de reductie van F modulo het ideaal $(x^2 + y^2 - 1)$ identiek aan 0, oftewel $F \in (x^2 + y^2 - 1)$.

Ons bewijs over $I(C)$ kunnen we compact noteren als

$$I(V(x^2 + y^2 - 1)) = (x^2 + y^2 - 1)$$

In het algemeen geldt zeker niet dat $I(V(I)) = I$, daar we al vonden dat $I(V(x^2)) = (x)$. Er is wel iets te zeggen over het verband tussen I en $I(V(I))$. Hierover bestaat een belangrijke stelling, die we nu zullen bespreken.

Als het grondlichaam algebraïsch afgesloten is (en dit nemen we in deze paragraaf steeds aan), is er een duidelijk verband tussen I en $I(V(I))$. Dit verband wordt geleverd door Hilberts *Nullstellensatz*. We hebben hiervoor het begrip *radicaal* nodig. Zij R een ring. Het radicaal van een ideaal $I \subset R$, genoteerd met $\mathrm{rad}(I)$ of ook wel $\sqrt{I}$, is gedefinieerd als

$$\mathrm{rad}(I) = \{x \in R : x^n \in I \text{ voor zekere } n\}.$$

Stelling 1.9 (Hilberts *Nullstellensatz*). $I(V(I)) = \mathrm{rad}(I)$.

Bewijs. Zie [Sha, App. §6, 281-282]. □

Merk op dat dit betekent dat $I(V(I)) = I$ dan en slechts dan als $I = \mathrm{rad}(I)$. We zeggen dan dat I een *radicaal ideaal* is. Priemidealen zijn altijd radicale idealen (dit tonen we nog aan in Gevolg 1.13b).

Uit de *Nullstellensatz* volgen enkele belangrijke eigenschappen van variëteiten over algebraïsch afgesloten lichamen, waarover later meer. Het bewijs is te lang om hier op te nemen. Wel kunnen we het volgende bewijzen:

Stelling 1.10. *Zij V een affiene variëteit. Dan geldt $V(I(V)) = V$.*

Bewijs. De inclusie $V \subset V(I(V))$ is triviaal. Stel omgekeerd dat V de nulpuntenverzameling is van $f_1, f_2, \ldots, f_k$, dan $f_1, f_2, \ldots, f_k \in I(V)$. In elk punt van $V(I(V))$ zijn $f_1, f_2, \ldots, f_k$ gelijk aan nul, dus is $V(I(V))$ bevat in de nulpuntenverzameling V. □

Een affiene variëteit V heet *irreducibel* als ze niet te schrijven is als $V = V_1 \cup V_2$ waarbij V_1, V_2 affiene variëteiten zijn waarvoor geldt dat $V_1 \subsetneq V$, $V_2 \subsetneq V$. We bewijzen nu dat irreducibele variëteiten in de $\mathbb{A}^n$ corresponderen met priemidealen in de coördinatenring $K[\mathbb{A}^n]$.

Stelling 1.11. *Een affiene variëteit $V \subset \mathbb{A}^n$ is irreducibel dan en slechts dan als $I(V)$ een priemideaal is.*

Bewijs. Neem eerst aan dat V irreducibel is, en neem $f_1, f_2 \in K[X_1, \ldots, X_n]$ zodanig dat $f_1 f_2 \in I(V)$. Beschouw nu de variëteiten $H_1 = V(f_1)$ en $H_2 = V(f_2)$. Omdat $f_1 f_2 = 0$ op V, is elk punt op V een punt van H_1 of een punt van H_2. Dus we hebben: $V = (V \cap H_1) \cup (V \cap H_2)$. Merk op dat de $V \cap H_i$ zelf variëteiten zijn, dus V is te schrijven als de vereniging van twee variëteiten. De irreducibiliteit van V geeft ons $V = V \cap H_1$ of $V = V \cap H_2$. Dit is equivalent met $V \subset H_1$ of $V \subset H_2$, hetgeen weer impliceert dat $f_1 \in I(V)$ of $f_2 \in I(V)$. Dus $I(V)$ is een priemideaal.

Omgekeerd, stel dat $V = V_1 \cup V_2$ met $V_i \subsetneq V$ $(i = 1, 2)$. Te bewijzen dat $I(V)$ geen priemideaal is. We hebben $I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$. We merken vervolgens op dat de inclusies $I(V) \subset I(V_i)$ $(i = 1, 2)$ strikt zijn. (Dit zien we omdat $V_i = V(I(V_i)) \neq V(I(V)) = V$.) Vervolgens kunnen we voor $i = 1, 2$ polynomen $f_i \in I(V_i) \backslash I(V)$ kiezen. Hieruit volgt dan dat $I(V)$ geen priemideaal is: $f_1 f_2 \in I(V)$ terwijl $f_i \notin I(V)$. □

Omdat een vraagstuk over variëteiten zich bijna altijd laat herleiden tot irreducibele variëteiten, beschouwen we in het vervolg alleen irreducibele variëteiten, tenzij anders aangegeven. Dit betekent dat we automatisch kunnen aannemen dat $I(V)$ een priemideaal is.

Tenslotte behandelen we enkele gevolgen van de *Nullstellensatz*. Dit met name omdat de situatie voor niet-algebraïsch afgesloten lichamen dan wat duidelijker uit de verf komt. Eerst een lemma.

Lemma 1.12. *Laat $\xi_i \in K$ voor $1 \leq i \leq n$. Het ideaal $I = (x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n) \subset K[\mathbb{A}^n]$ is een maximaal ideaal.*

Bewijs. Stel dat $I \subsetneq \mathfrak{m} \subsetneq K[x_1, x_2, \ldots, x_n]$ met $\mathfrak{m}$ een ideaal. Neem $f \in \mathfrak{m}$ willekeurig. We tonen aan dat ook $f \in I$. Dan kunnen we in de uitdrukking voor f alle x_i elimineren door de relaties $x_i \equiv \xi_i$ te gebruiken. We vinden zo dus een element $K \ni a \in \mathfrak{m}$, waarvoor tevens geldt dat $f - a \in I$. Door aanname geldt dat $\mathfrak{m} \neq K[\mathbb{A}^n]$, dus moet gelden dat $a = 0$. Dus $f - 0 \in I$ oftewel $f \in I$. □

Gevolg 1.13. *(a) Zij I een ideaal in de polynoomring $K[x_1, x_2, \ldots, x_n]$. Dan is $V(I)$ niet-leeg dan en slechts dan als $I \neq (1) = K[x_1, x_2, \ldots, x_n]$. (Dit heet ook wel de zwakke Nullstellensatz.)*
(b) Zij $\mathfrak{p}$ een priemideaal in de polynoomring $K[x_1, x_2, \ldots, x_n]$. Dan geldt $\mathfrak{p} = I(V(\mathfrak{p}))$.
(c) Zij $\mathfrak{m}$ een maximaal ideaal in de polynoomring $K[x_1, x_2, \ldots, x_n]$. Dan is $\mathfrak{m}$ van de vorm $(x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n)$ en $V(\mathfrak{m}) = (\xi_1, \xi_2, \ldots, \xi_n)$. Dat wil zeggen: de maximale idealen van $K[\mathbb{A}^n]$ corresponderen één-op-één met de punten van $\mathbb{A}^n$.

Bewijs. (a) Stel $V(I) = \varnothing$. We bewijzen dat $I = (1)$. We hebben $I(V(I)) = (1)$ omdat $V(I)$ leeg is. Dus $\mathrm{rad}(I) = (1)$. Volgens de definitie van het radicaal weten we nu dat 1^n en dus 1 voor zekere n in I moet zitten. Dus $1 \in I$ en $I = (1)$. De omkering is triviaal.
(b) Zij R willekeurig en $\mathfrak{p} \subset R$ een priemideaal, dan bewijzen we $\mathfrak{p} = \mathrm{rad}(\mathfrak{p})$. (Hieruit volgt meteen gevolg (b).) Stel namelijk dat $x^n \in \mathfrak{p}$ voor zekere $x \in R$ en $n \in \mathbb{N}$. Dan moet volgens de definitie van priemideaal $x^{n-1} \in \mathfrak{p}$ of $x \in \mathfrak{p}$. Als $x \in \mathfrak{p}$ zijn we klaar, dus neem aan dat $x^{n-1} \in \mathfrak{p}$. We zien dan dat $x^{n-2} \in \mathfrak{p}$ of $x \in \mathfrak{p}$, enzovoort. Dit proces eindigt, dus $x \in \mathfrak{p}$.
(c) Stel dat $\mathfrak{m} \subset K[\mathbb{A}^n]$ maximaal is en beschouw $V = V(\mathfrak{m})$. Er zijn twee mogelijkheden: V bestaat uit een enkel punt of V bestaat uit meer dan een punt. In het eerste geval, noem dit punt $P = (\xi_1, \xi_2, \ldots, \xi_n)$. De functies $x_i - \xi_i$ verdwijnen op P, dus het ideaal $\mathfrak{n} = (x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n)$ zit in $\mathfrak{m}$. Maar $\mathfrak{n}$ is reeds maximaal volgens het lemma, dus is $\mathfrak{m} = \mathfrak{n}$.
Stel dat V meerdere punten bevat, we leiden dan een tegenspraak af. Kies een $P = (\xi_1, \ldots, \xi_n) \in V$ en beschouw $I = I(P)$. Volgens de redenering van daarnet geldt $I = (x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n)$ voor $\xi_i \in K$. Omdat $I(\cdot)$ inclusies omkeert geldt $I(P) = I \supset \mathfrak{m} = I(V)$. De laatste gelijkheid volgt uit $\mathfrak{m} = \mathrm{rad}(\mathfrak{m})$, wegens (b), en de *Nullstellensatz*, die zegt dat $\mathfrak{m} = I(V(\mathfrak{m}))$. Dus geldt $I = \mathfrak{m}$ omdat $\mathfrak{m}$ maximaal is. Maar $V = V(I)$ kan alleen maar uit het punt $(\xi_1, \xi_2, \ldots, \xi_n)$ bestaan. Tegenspraak. □

We willen ons in het vervolg concentreren op *krommen* in het affiene vlak $\mathbb{A}^2(K)$. (Later bespreken we ook krommen in het projectieve vlak.)

Stelling 1.14. *De irreducibele variëteiten in de $\mathbb{A}^2(K)$ zijn (1) punten en (2) krommen $V(f)$ gegeven door een irreducibel polynoom $f \in K[x, y]$.*

Bewijs. Zie [Sha, blz. 24]. □

We kunnen niet-irreducibele variëteiten in de $\mathbb{A}^n$ altijd schrijven als een eindige vereniging van irreducibele variëteiten. Immers, een oneindige keten van inclusies $V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$ zou aanleiding geven tot een oneindige keten van inclusies $I(V_1) \subsetneq I(V_2) \subsetneq I(V_3) \subsetneq \cdots \subset K[x_1, x_2, \ldots, x_n]$ en dit is onmogelijk daar $K[x_1, x_2, \ldots, x_n]$ een Noetherse ring is. Dit motiveert ons om exclusief te kijken naar irreducibele krommen. We perken onze definitie van krommen daarom in tot het irreducibele geval:

Definitie 1.15. *Met een (algebraïsche) kromme over K bedoelen we een kromme $V(f)$ gegeven door een irreducibel polynoom $f \in K[x, y]$ en $f \neq 0$.*

1.2 Functies op affiene variëteiten

Zij $V = V(f) \subset \mathbb{A}^2$ een kromme over K met f irreducibel. Dan is $I(V) = (f)$ het bijbehorende ideaal. We definiëren de *coördinatenring van V* als

$$K[V] = K[x, y]/(f)$$

Stelling 1.16. *Neem V irreducibel. De ring $K[V]$ heeft dan geen nuldelers.*

Bewijs. f is irreducibel, dus (f) is een priemideaal, dus $K[x,y]/(f)$ is een domein (een commutatieve ring met eenheid en zonder nuldelers). □

Elementen van $K[V]$ kunnen worden beschouwd als onderling verschillende functies op de variëteit V. De uitdeling naar (f) zorgt ervoor dat als twee elementen van $K[x,y]$ op V overeenkomen, ze ook op hetzelfde element in $K[V]$ terecht komen onder de canonieke afbeelding $K[x,y] \to K[V]$. Dit maken we precies in de volgende definitie:

Definitie 1.17. *Zij g een element van $k[V]$ en $P = (\xi, \eta) \in V$ een punt op de kromme V. Dan definiëren we de functiewaarde van g in P, genoteerd met $g(P)$ of $g(\xi,\eta)$, als $\tilde{g}(P)$, waarbij $\tilde{g}$ een representant is van g in $k[\mathbb{A}^2]$.*

Het is niet lastig om na te gaan dat dit welgedefinieerd is. Bovendien bevat de ring $k[V]$ geen elementen $\neq 0$ die overal op V verdwijnen: stel $g \in k[V]$ is zodanig dat $g(P) = 0$ voor alle $P \in V$. Dan geldt voor elke representant $\tilde{g}$ van g dat $\tilde{g} \in I(V)$ per definitie. Wegens $I(V) = (f)$ krijgen we $g = 0 \in k[V]$ als enige mogelijkheid voor g.

Tenslotte definiëren we het *functielichaam van V*, genoteerd met $K(V)$, als het breukenlichaam van $K[V]$. Een alternatieve karakterisering in termen van f en de elementen van $k[\mathbb{A}^2]$ luidt:

$$K(V) = \left\{ \frac{g}{h} \;\middle|\; g,h \in K[x,y] \right\} / \sim_f \quad \text{met } \frac{g}{h} \sim_f \frac{g'}{h'} \text{ dan en slechts dan als } f \mid gh' - g'h$$

Het is duidelijk dat we moeten controleren dat deze definitie equivalent is met de definitie van $K(V)$ als breukenlichaam. Dit is een routinematige controle. Tot nog toe zijn deze uitdrukkingen g/h formele uitdrukkingen. We willen ze graag zien als welgedefinieerde functies op onze variëteit V.

Definitie 1.18. *Zij $w \in k(V)$. We noemen w een rationale functie op V. Zij $P = (\xi,\eta) \in V$. We noemen w regulier in P als er een representant $w = g/h$ bestaat, met $g,h \in k[V]$, zodanig dat $\tilde{h}(P) \neq 0$, waarbij $\tilde{h}$ weer een representant is in $k[\mathbb{A}^2]$ van h. In dat geval is de functiewaarde van w in P gedefinieerd als $\tilde{g}(P)/\tilde{h}(P)$. Hier zijn $\tilde{g}$ en $\tilde{h}$ wederom representanten van g en h.*

Wederom moeten we controleren dat dit welgedefinieerd is, daarvoor moeten we kijken wat er gebeurt onder de equivalentierelatie. Hier ontstaan geen problemen.

Propositie-definitie 1.19. *Gegeven een kromme V over een lichaam K. Bekijk een punt $P \in V$. De reguliere functies in P vormen een ring, die aangegeven wordt met $\mathcal{O}_P$, of als verwarring dreigt met $\mathcal{O}_{V,P}$.*

Bewijs. Zijn g/h en g'/h' twee representaties van reguliere functies in P, dan is hun som $j = (gh' + g'h)/hh'$. Uit $h(P) \neq 0$ en $h'(P) \neq 0$ volgt ook $h(P)h'(P) \neq 0$, dus j is regulier. Het is op dezelfde wijze duidelijk dat ook het product gg'/hh' regulier is. □

Stelling 1.20. *$\mathcal{O}_P$ is een lokale ring zonder nuldelers.*

Bewijs. Een *lokale ring* R is een ring met een uniek maximaal ideaal $\mathfrak{m}$, zodanig dat $\mathfrak{m} = R - R^*$. We beweren dat $\mathcal{O}_P$ een lokale ring is met maximaal ideaal $\mathfrak{m} := \{f \in \mathcal{O}_P : f(P) = 0\}$. Het is duidelijk dat $\mathfrak{m}$ inderdaad een ideaal is: als $f(P) = g(P) = 0$, dan ook $(f+g)(P)$ en $(hf)(P)$ voor willekeurige $h \in \mathcal{O}_P$. Tenslotte, als $h \notin \mathfrak{m}$, dan geldt dus $h = p/q$ met $p,q \in K[x,y]$ en $p(P), q(P) \neq 0$. Dit betekent dat $h^{-1} = q/p \in \mathcal{O}_P$, dus $h \in \mathcal{O}_P^*$.

De bewering over de nuldelers is triviaal, daar $\mathcal{O}_P \subset K(V)$ en $K(V)$ is een lichaam, dat dus geen nuldelers heeft. □

Het is ook meteen duidelijk waar de naam "lokale ring" vandaan komt. Verder merken we nog op dat een lokale ring R met maximaal ideaal $\mathfrak{m}$ ook wel genoteerd wordt met $(R, \mathfrak{m})$.

Neem V een kromme en noteer weer met $\pi : K[x,y] \to K[V]$ het canonieke homomorfisme. Neem $\mathfrak{m}$ een maximaal ideaal in $K[V]$, dan weten we uit de commutatieve algebra dat $\mathfrak{M} := \pi^{-1}(\mathfrak{m})$ een maximaal ideaal is in $K[x,y]$. Tevens geldt dat $0 \in \mathfrak{m}$. Laten we π^{-1} los op deze uitdrukking, dan krijgen we

$I(V) \subset \mathfrak{M}$. Omdat V inclusies omkeert, volgt hieruit dat het punt $V(\mathfrak{M})$ bevat is in V. We hebben dus weer een één-op-één-correspondentie tussen punten van V en maximale idealen in $K[V]$. (Vergelijk Gevolg 1.13(c).)

Stelling 1.21. *Zij $V \subset \mathbb{A}^n(K)$ een kromme in de $\mathbb{A}^2(K)$. Zij $\mathcal{O}_V$ de ring van functies die op alle punten van V regulier zijn. Dan geldt $\mathcal{O}_V = K[V]$.*

Bewijs. Het is duidelijk dat de functies in $K[V]$ regulier zijn op alle punten van V, dus $K[V] \subset \mathcal{O}_V$. Dat de omgekeerde inclusie ook geldt volgt uit een slimme toepassing van de *Nullstellensatz*, zie [2, blz 36]. Om deze reden wordt de coördinatenring $K[V]$ ook wel de *ring van reguliere functies op V* genoemd. □

1.2.1 De lokale ringen van een kromme

Bij het onderzoeken van krommen en hun functielichamen hebben we een belangrijk begrip uit de algebra nodig, namelijk de discrete valuatieringen.

Definitie 1.22. *Een lokale ring $(R, \mathfrak{m})$ heet een discrete valuatiering of* DVR *als er een t bestaat zodanig dat elke $f \in R$ met $f \neq 0$ geschreven kan worden als $f = ut^n$ voor zekere $u \in R^*$ en $n \in \mathbb{Z}_{\geq 0}$. De parameter t wordt ook wel lokale uniformisant genoemd.*

DVRen hebben allerlei mooie eigenschappen, waarvan we er nu enkele afleiden.

Stelling 1.23. *Zij $(R, \mathfrak{m})$ een* DVR *met t een lokale uniformisant. We hebben: $t \in R^* \Longrightarrow R$ is een lichaam.*

Bewijs. Zij $t \in R^*$, dan is elke uitdrukking ut^n een eenheid en is R dus een lichaam. □

Stelling 1.24. *Zij $(R, \mathfrak{m})$ een* DVR *die geen lichaam is. Dan geldt $\mathfrak{m} = (t)$ met t een lokale uniformisant.*

Bewijs. Omdat $t \notin R^*$ hebben we $t \in \mathfrak{m}$ en dus $(t) \subset \mathfrak{m}$. Zij nu $x \in \mathfrak{m}$, dan hebben we $x = ut^n$ met $u \in R^*$ en $n \in \mathbb{Z}_{\geq 0}$. Omdat x geen eenheid is moet gelden dat $n > 0$, dus $x \in (t)$. □

Stelling 1.25. *Zij C een kromme over K en neem $P = (\xi, \eta) \in C$. Noteer de affiene coördinatenring met $K[x, y]$. Neem voor $\mathfrak{m}$ het maximale ideaal in de lokale ring $\mathcal{O}_{C,P}$, dan is $\mathfrak{m} = (x - \xi, y - \eta)$.*

Bewijs. Duidelijk is dat $(x - \xi, y - \eta) \subset \mathfrak{m}$. Zij $f \in \mathfrak{m}$ willekeurig. Dan kunnen we de functie f reduceren modulo het ideaal $(x - \xi, y - \eta)$ door $x = \xi$, $y = \eta$ in te vullen. Dan vinden we dus een $a \in K$ zodanig dat $f \equiv a \bmod (x - \xi, y - \eta)$. Dan moet wel gelden dat $a = 0$ en $f \in (x - \xi, y - \eta)$. □

We hebben nu dus reeds een expliciete karakterisering van $\mathfrak{m}_P$ gevonden. We zullen aanstonds zien dat $(\mathcal{O}_P, \mathfrak{m}_P)$ in de regel een DVR is. (Wat "in de regel" precies is zullen we definiëren.) We kunnen ons dan afvragen of we de bijbehorende t kunnen uitdrukken in termen van x en y. Dit blijkt eenvoudig, zoals we in de nu volgende stellingen zullen zien.

Stelling 1.26. *Zij $(R, \mathfrak{m})$ een* DVR *zonder nuldelers met $\mathfrak{m} = (t)$. Neem $x \in R$. Dan is in de schrijfwijze $x = ut^r$ het getal $r \in \mathbb{Z}_{\geq 0}$ uniek bepaald.*

Bewijs. Neem aan dat $x = ut^r = vt^s$ met $u, v \in R^*$ en $r \geq s \geq 0$. Dan $t^s(ut^{r-s} - v) = 0$ waaruit volgt dat $ut^{r-s} = v$. Omdat t geen eenheid is moet gelden dat $r = s$. □

Merk op dat de restrictie "zonder nuldelers" ons niet in problemen zal brengen: de DVRen die wij tegenkomen zijn lokale ringen $\mathcal{O}_P$ die geen nuldelers bezitten volgens stelling 1.20.

Stelling 1.27. *Zij $(R, \mathfrak{m})$ een* DVR *zonder nuldelers. Als $\mathfrak{m} = (t_1, t_2, \ldots, t_m)$ waarbij $t_i \in R$, dan wordt $\mathfrak{m}$ voortgebracht door één van de t_i, dus $\mathfrak{m} = (t_p)$ voor een zekere $1 \leq p \leq m$.*

Bewijs. Volgens de definitie van een DVR is er een $t \in R$ zodanig dat $t_i = u_i t^{r_i}$ met $u_i \in R^*$. Voor alle r_i geldt $r_i > 0$, anders zou $(t_1, t_2, \ldots, t_m) = R$ zijn. Stel dat $r = \min_i r_i$, dan geldt $\mathfrak{m} = (t^r)$ en $r \geq 1$. Maar we hebben $t \in \mathfrak{m}$, dus we kunnen schrijven $t = xt^r$ voor $x \in R$. Hieruit volgt $t(1 - xt^{r-1}) = 0 \Longrightarrow xt^{r-1} = 1$. We weten dat t niet inverteerbaar is, dus $r - 1 = 0 \Longrightarrow r = 1$. Dus we hebben $r_p = 1$ voor zekere p. Hieruit volgt dat $\mathfrak{m} = (t) = (t_p)$. □

Opmerking 1.28. Zij $P = (\xi, \eta)$ een punt op een kromme. We zien dat als $(\mathcal{O}_P, \mathfrak{m}_P)$ een DVR is, het maximale ideaal $\mathfrak{m}_P$ voortgebracht wordt door ofwel $x - \xi$, ofwel $y - \eta$. Een andere manier om dit te zeggen is dat één van $x - \xi$ en $y - \eta$ kan worden gebruikt als lokale uniformisant. (Vaak zelfs beide.)

Definitie 1.29. *Zij $C \subset \mathbb{A}^2(K)$ een kromme en $P \in C$. We noemen C glad of niet-singulier in P dan en slechts dan als $\mathcal{O}_P$ een discrete valuatiering is. Als $\mathcal{O}_P$ geen discrete valuatiering is heet P een singulier punt.*

We zullen deze abstracte definitie vertalen naar een meer gangbare definitie in termen van de partiële afgeleiden van f, het bij C behorende polynoom. Hiervoor hebben we eerst nog een eenvoudig lemma nodig over polynomen in $K[x, y]$.

OPMERKING: We zouden een kromme graag singulier willen noemen als zij singuliere punten bevat en glad als ál haar punten glad zijn. Hier treedt echter het probleem op dat affiene krommen niet "compleet" zijn: we moeten voor singulariteitskwesties ook de zogenaamde "punten op oneindig" beschouwen.

Beschouw bijvoorbeeld de grafiek van de gewone "derdegraadsfunctie", in het xy-stelsel gegeven door de bekende (analytische) vergelijking $y = x^3$. Deze gedraagt zich overal keurig, en inderdaad zijn al haar (affiene) punten glad. Maar zij is singulier in een punt "op oneindig", dus is zij als kromme niet glad. Later zullen we dat precies maken.

Stelling 1.30. *Stel dat $f, g \in K[x, y]$ copriem zijn, dat wil zeggen: als er $h \in K[x, y]$ is zodanig dat $f, g \in (h)$, dan is $h \in K$. Dan bestaan er $\alpha, \beta \in K[x, y]$ zodanig dat $\alpha f + \beta g \in K[x]$.*

Bewijs. Definieer $\deg_y(h)$, waar $h \in K[x, y]$, als de hoogste graad van y die voorkomt in de uitdrukking voor h. Definieer T als de verzameling van alle polynomen van de vorm $sf + tg \neq 0$, waarin s en t ook polynomen zijn in $K[x, y]$. Kies nu een element $h \in T$ met $p = \deg_y(h)$ minimaal in T. Te bewijzen is dat $p = 0$. Neem aan dat $p \geq 1$, we leiden een tegenspraak af.

Zij $h = c_0(x) + c_1(x)y + \ldots + c_p(x)y^p$ en stel $c = c_p$. We kunnen nu de graad van het polynoom cf reduceren door steeds geschikte veelvouden van $y^i h$ af te trekken. Uiteindelijk vinden we een restpolynoom r_1 van graad $< \deg_y(h)$. Vanwege de minimaliteit van $\deg_y(h)$ geldt $r_1 = 0$. Dezelfde redenering gaat op voor cg. Dan zijn er dus $t_1, t_2 \in K[x, y]$ zodanig dat $cf + t_1 h = 0$ en $cg + t_2 h = 0$. Dus $cf, cg \in (h) \subsetneq K[x, y]$. De priemfactorisatie van h bevat zeker een irreducibel polynoom met y-graad > 0, noem dit polynoom $h_1 \mid h$. Dan geldt $h_1 \mid cf$, $h_1 \mid cg$. Maar $h_1 \nmid c$ en dus levert de irreducibiliteit van h_1 ons dat $h_1 \mid f$ en $h_1 \mid g$. Tegenspraak. □

Stelling 1.31. *Stel dat de kromme $C \subset \mathbb{A}^2(K)$ gegeven is als nulpuntenverzameling van een irreducibel polynoom $f \in K[x, y]$ en stel dat $f(P) = 0$. Dan is C singulier in P dan en slechts dan als $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$.*

Bewijs. We kunnen een translatie uitvoeren op de $\mathbb{A}^2$ zodat het te beschouwen punt P in de oorsprong $P = (0, 0)$ ligt. Dit verandert niets aan de waarden van $\frac{\partial f}{\partial x}(P)$ en $\frac{\partial f}{\partial y}(P)$.

We schrijven f uit als $f = f_1 + f_2 + \ldots + f_d$, waarbij $\deg(f_i) = i$. De f_i zijn hierbij uniek bepaald. (Merk ook op dat $f_0 = 0$ omdat $(0, 0) \in C$.) We zien dat het verdwijnen van de partiële afgeleiden in $(0, 0)$ equivalent is met $f_1 = 0$. Te bewijzen is dan "$f_1 \neq 0 \iff x$ is niet-singulier".

"$\Longleftarrow$" We mogen zonder verlies van algemeenheid aannemen dat y een lokale uniformisant is. Dan hebben we $x \sim_f vy^r$ voor zekere $v \in \mathcal{O}_P^*$. Zeg $v = v_1/v_2$ met v_i polynomen in $K[x, y]$ met $v_i(P) \neq 0$, dan betekent dit $v_2 x \sim_f v_1 y^r$ als identiteit in de ring $K[C]$. Als we x, y en de v_i opvatten als polynomen in de ring $K[x, y]$ betekent dit dat $v_2 x - v_1 y^r \in I(C) = (f)$.

Dus $f \mid v_2 x - v_1 y^r$. Merk op dat $v_2 x - v_1 y^r$ een lineaire term in x heeft, daar $v_2(P) \neq 0$. Als $f \in K[x, y]$ geen lineaire term zou hebben, heeft een willekeurig veelvoud fg dat ook niet. Dus $f_1 \neq 0$.

"$\Longrightarrow$" Neem aan dat $f_1 \neq 0$. We kijken weer naar de oorsprong P. Dan kunnen we f schrijven als $ax + by +$ hogere orde termen met a, b niet beide gelijk aan nul. Stel $a \neq 0$. Dan kunnen we f schrijven als $f = xp(x) - yq(x, y)$ met $p(0) \neq 0$. Dus $q/p \in \mathcal{O}_P$ en we kunnen x schrijven als $x \sim_f q/p \cdot y$.

We bewijzen nu dat $\mathcal{O}_P$ een DVR is met lokale uniformisant y. We moeten dus aantonen dat een willekeurig element $0 \neq a \in \mathcal{O}_P$ geschreven kan worden als $a \sim_f uy^n$ voor zekere $u \in \mathcal{O}_P^*$ en $n \in \mathbb{Z}_{\geq 0}$.

Gegeven $a \in \mathcal{O}_P$, kunnen we a schrijven als $g/h = h^{-1}g$ met g, h polynomen en $h \in \mathcal{O}_P^*$. Als $g(P) \neq 0$, is a een eenheid en zijn we klaar. Veronderstel dus dat a geen eenheid is, en dus dat $g(P) = 0$. Dan kunnen we in $g(x, y)$ de substitutie $x \sim_f q/p \cdot y$ gebruiken. Omdat $g(P) = 0$ heeft g geen constante termen, en dus geldt $g(x, y) \sim_f g_1 y$ voor zekere $g_1 \in \mathcal{O}_P$.

We kunnen op deze wijze steeds een factor y van g "afsplitsen". We moeten nu enkel nog aantonen dat dit proces uiteindelijk eindigt, dus dat we uiteindelijk krijgen dat $a = ug_k y^k$ voor zekere $k \in \mathbb{Z}_{>0}$, waarbij $u \in K(C)$ een element uit het functielichaam is zodanig dat $u(P) \neq 0$. Dit is equivalent met aantonen dat er een $k > 0$ is zodanig dat $g \notin (y^{k+1})$.

Dit bewijzen we als volgt. De polynomen f en g, beide opgevat als elementen van $K[x, y]$, zijn copriem. Dit volgt doordat f irreducibel is, dus als g niet copriem zou zijn met f zou moeten gelden dat $f \mid g$, hetgeen betekent dat $a = 0$, en dit geval hadden we reeds uitgesloten. Dus volgt uit het lemma, dat er $\alpha, \beta \in K[x, y]$ bestaan zodanig dat $\alpha f + \beta g \in K[y]$. Stel $y^m r(y) = \alpha f(x, y) + \beta g(x, y)$ voor zekere $m \in \mathbb{Z}_{\geq 0}$ en $r \in K[y]$ zodanig dat $r(0) \neq 0$. Merk op dat $r \in \mathcal{O}_P^*$. In $\mathcal{O}_P$ betekent dit dat $y^m \sim_f \beta r^{-1} g$, oftewel $y^m \in (g)$. Dit betekent dat (g) niet in (y^{m+1}) kan zitten: als $y^m \sim_f \gamma g$ en $g \sim_f \delta y^{m+1}$, dan $y^m \sim_f \gamma\delta y^{m+1} \Rightarrow y^m(\gamma\delta y - 1) \sim_f 0$. Het lichaam $K(C)$ heeft geen nuldelers, dus y moet een eenheid zijn. □

Zij $\mathcal{O}_P$ een DVR met maximaal ideaal $\mathfrak{m}_P = (t)$. Zij $a \in \mathcal{O}_P$ en schrijf $a = ut^n$. We schrijven $v_P(a) = n$ en we noemen n de *orde van a in P*. Volgens stelling 1.26 is n uniek bepaald, dus is v welgedefinieerd. Dus v_P is een afbeelding van $\mathcal{O}_P$ naar $\mathbb{Z}_{\geq 0}$. We kunnen v_P zelfs uitbreiden tot de hele $K(C)^*$ (merk op dat we 0 steeds uitsluiten), dus ook tot functies die niet-regulier zijn in P. Zij $g = h/j \in K(C)$ niet-regulier in P. Dan definiëren we $v_P(g) = v_P(h) - v_P(j)$. Dit is welgedefinieerd omdat als g_1/g_2 en g_3/g_4 dezelfde functie voorstellen in $K(C)$, ook $g_1 g_4$ en $g_2 g_3$ dezelfde functie voorstellen. Wegens de multiplicatieve eigenschap $v(fg) = v(f) + v(g)$ als $f, g \in \mathcal{O}_P$ geldt nu dat $v(g_1) + v(g_4) = v(g_2) + v(g_3)$, hetgeen aantoont dat v welgedefinieerd is op $K(C)^*$. De genoemde eigenschap leggen we nog even vast in een lemma:

Lemma 1.32. *Zijn $f, g \in k(C)^*$, dan geldt $v_P(fg) = v_P(f) + v_P(g)$ en $v_P(f^{-1}) = -v_P(f)$.*

Bewijs. Eerst tonen we de eigenschap aan voor $f, g \in \mathcal{O}_P$. Schrijf $f = ut^r$ en $g = vt^s$ en het resultaat volgt direct. Het resultaat voor $f, g \in k(C)^*$ volgt zoals boven beschreven. □

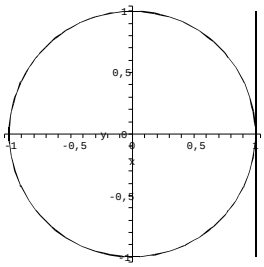
Voor niet-reguliere g is de grootheid $-v_P(g)$ dan intuïtief te begrijpen als *de orde van de pool* die g heeft in P. Dit leggen we vast in een definitie.

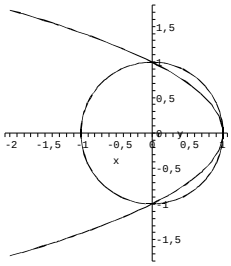
Definitie 1.33. *Zij P een regulier punt van een kromme C over K. Zij $a = g/h \in K(C)^*$ en $a \notin \mathcal{O}_P$. Dan zeggen we dat a een pool heeft in P en we noemen $-v_P(a)$ de orde van de pool van a in P.*

Voor niet-singuliere krommen C hebben we dus voor elk punt $P \in C$ een welgedefinieerde *valuatie*: $v_P : K(C)^* \longrightarrow \mathbb{Z}$. Deze v_P is erg belangrijk in het vervolg van deze scriptie.

1.2.2 Voorbeelden van lokale ringen en valuaties

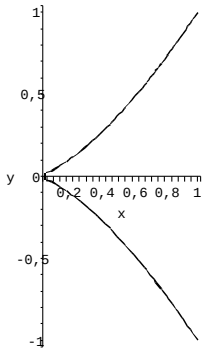
Zij C de kromme gedefinieerd door $f = x^2 + y^2 - 1$ over $\overline{\mathbb{Q}}$. Neem het punt $P = (1, 0)$ en beschouw $(\mathcal{O}_P, \mathfrak{m}_P)$. Wat is een voortbrenger voor $\mathfrak{m}_P$?
We merken op dat $\mathfrak{m}_P = (x - 1, y)$. Verder geldt $y^2 \sim_f (1 - x)(1 + x) \Longrightarrow x - 1 \sim_f -y^2/(x + 1)$ met $(x + 1) \in \mathcal{O}_P^*$, dus y is een lokale uniformisant in P en $\mathfrak{m}_P = (y)$. Dus $v_P(x - 1) = 2$.
Zij $Q = (\frac{3}{5}, \frac{4}{5}) \in C$. We hebben $\mathcal{O}_Q \supset \mathfrak{m}_Q = (5x - 3, 5y - 4)$. Stel $g = 5x - 3$, $h = 5y - 4$. Er geldt $(5x + 3)g = 25x^2 - 9 \sim_f 16 - 25y^2 = -(5y + 4)h$. Dus $g \sim_f -\frac{5y+4}{5x+3} h$, met $-\frac{5y+4}{5x+3} \in \mathcal{O}_Q^*$. Dus g en h zijn dus beide voortbrengers van $\mathfrak{m}_Q$.
Bekijken we de situatie over $\mathbb{C}$, dan betekent het feit dat $x - 1$ een nulpunt van orde ≥ 2 heeft in P dat de lijn $x = 1$ een *raaklijn* is aan de cirkel gedefinieerd door $x^2 + y^2 - 1$. (Zie onder.) Bekijk ook de functie $1 - x - y^2$. Aan de grafiek is te zien dat hij C raakt in P. Dit controleren we nu door $v_P(1 - x - y^2)$ te berekenen: $1 - x - y^2 \sim_f y^2/(x+1) - y^2 \sim_f -xy^2/(x+1)$. Nu is $-x/(x+1) \in \mathcal{O}_P^*$, dus $v_P(1 - x - y^2) = 2$.





OPMERKING. Uit dit voorbeeld blijkt dat we ook heel goed over raaklijnen kunnen spreken zonder afgeleiden uit te rekenen, of zonder ons druk te maken over het feit dat een kromme niet over $\mathbb{C}$ maar over $\overline{\mathbb{F}}_p$ gedefinieerd is: we kunnen gewoon naar de valuatie $v_P(\cdot)$ kijken.

Beschouw vervolgens de kromme gegeven door $f = y^2 - x^3$ en neem $R = (0,0)$. Het maximale ideaal in $\mathfrak{m}_R \subset \mathcal{O}_R$ wordt voortgebracht door (x,y), maar ditmaal is er geen voortbrenger t te vinden met $\mathfrak{m}_R = (t)$. Dit hangt samen met het feit dat voor de partiële afgeleiden geldt dat $\partial f/\partial x = \partial f/\partial y = 0$, en R dus een singulier punt is.



1.3 Variëteiten over niet-algebraïsch afgesloten lichamen

De klassieke algebraïsche meetkunde werd ontwikkeld voor variëteiten en krommen over algebraïsch afgesloten lichamen, zoals $\mathbb{C}$ of $\overline{\mathbb{Q}}$. In veel toepassingen zijn we niet geïnteresseerd in alle punten van een kromme, maar alleen die punten waarvan de coördinaten in een bepaald deellichaam liggen, bijvoorbeeld in een bepaald eindig lichaam. Dit laatste is in de coderingstheorie het geval.
Zij K algebraïsch afgesloten en $(f) \subset K[x,y]$ een priemideaal. We hebben gezien hoe (f) een deelverzameling $V = V(f) \subset \mathbb{A}^n(K)$ opleverde, een affiene kromme. Omgekeerd levert de variëteit V weer een ideaal $I(V)$ op waaruit we het polynoom f kunnen reconstrueren. We verliezen dus geen wezenlijke informatie door hetzij alleen f, hetzij alleen V te beschouwen.
Over niet-algebraïsch afgesloten lichamen is deze nette correspondentie er niet. Neem voor k een willekeurig niet-algebraïsch afgesloten lichaam. Met een priemideaal $(f) \subset k[x,y]$ correspondeert een unieke deelverzameling $V = V(f) \subset \mathbb{A}^2(k)$. Het omgekeerde is echter niet waar: het ideaal $I(V)$ levert ons in het algemeen niet iets op waaruit we ons oorspronkelijke polynoom f weer kunnen reconstrueren.
Dit laatste valt al in te zien met een heel triviaal voorbeeld. Het ideaal $J = (x^2+1) \subset \mathbb{R}[x,y]$ is een priemideaal (want x^2+1 is irreducibel over $\mathbb{R}$). $V(J)$ is de lege verzameling $\varnothing \subset \mathbb{R}$. Omgekeerd is $I(\varnothing) = \mathbb{R}[x,y]$: we zijn dus alle informatie kwijt die we in het begin hadden. Bijvoorbeeld definiëren de radicale idealen (x^2+1) en (x^2+y^2+5) dezelfde (lege) variëteit in de $\mathbb{A}^2(\mathbb{R})$.
In zekere zin hebben we over niet-algebraïsch afgesloten lichamen k dus "niet genoeg punten". Dit lossen we in de volgende paragraaf voor eindige lichamen op door ook punten over lichaamsuitbreidingen $k' \supset k$ mee te nemen. In deze paragraaf geven we enkele definities die geldig zijn voor willekeurige lichamen.

Definitie 1.34. *De affiene n-ruimte over k is net als voor algebraïsch afgesloten lichamen gedefinieerd als $\mathbb{A}^n(k) = k^n$.*

Definitie 1.35. *Een kromme $V(f) \subset \mathbb{A}^n(\overline{k})$ heet gedefinieerd over k als $f \in k[x, y]$.*

Als de variëteit V gedefinieerd is over k schrijven we voor V ook wel V/k. Merk op dat V/k nog steeds een verzameling in de $\mathbb{A}^n(\overline{k})$ voorstelt.

Definitie 1.36. *De verzameling van k-rationale punten van een kromme $V \subset \mathbb{A}^2(\overline{k})$, ook wel genoteerd met $V(k)$, wordt gegeven door*

$$V \cap \mathbb{A}^n(k)$$

Merk op dat de elementen van k binnen de algebraïsche uitbreiding $\overline{k}$ gekarakteriseerd worden door de eigenschap dat ze invariant blijven onder k-automorfismen van $\overline{k}$. Dit leidt tot een vaak gebruikte karakterisering van k-rationale punten, die in het geval van eindige lichamen ook nog eens een eenvoudige gedaante aanneemt:

Neem $\mathbb{F}_q$ een eindig lichaam. De verzameling $\mathbb{F}_q$-rationale punten van een variëteit $V \subset \mathbb{A}(\overline{\mathbb{F}}_q)$ wordt gegeven door de deelverzameling $W \subset V$ waarvan de coördinaten invariant zijn onder de Frobenius-afbeelding $\sigma : x \longmapsto x^q$.

Definitie 1.37. *Zij $f \in k[x, y]$ en $V := V(f)$ een kromme gedefinieerd over k. Het ideaal van V over k is gedefinieerd als*

$$I(V/k) = (f) \subset k[x, y]$$

Merk op dat $I(V/k)$ inderdaad een ideaal is van $k[x, y]$. Neem aan dat f irreducibel is in $\overline{k}[x, y]$. Ook al wordt in dat geval de variëteit V niet eenduidig bepaald door de k-rationale punten van V, ze is wel eenduidig bepaald door $I(V/k)$! Als V namelijk gedefinieerd is over k, dan geldt volgens de definitie dat

$$I(V) = I(V/k)\overline{k}[x, y]$$

Nu zijn we in staat de coördinatenring en het functielichaam voor V/K over k te definiëren.

Definitie 1.38. *De coördinatenring van de variëteit $V(f)$ gedefinieerd over k, genoteerd met $k[V]$, is gedefinieerd als*

$$k[V] = k[x, y]/(f)$$

Definitie 1.39. *Het functielichaam van V, genoteerd $k(V)$, over k is gedefinieerd als het breukenlichaam van $k[V]$.*

We kunnen $k(V)$ dus weer opvatten als breuken g/h met $g, h \in k[x, y]$ (of zo men wil geordende paren (g, h)) waarop op de volgende wijze equivalentieklassen zijn gedefinieerd:

$$g/h \sim_f g'/h' \text{ dan en slechts dan als } f \mid gh' - g'h$$

Deze laatste definitie is geheel analoog aan de definitie voor algebraïsch afgesloten lichamen in §1.2. Tenslotte zijn ook de lokale ringen van V te bekijken over k.

Definitie 1.40. *De lokale ring $\mathcal{O}_{V/k,\,x}$ is als volgt gedefinieerd:*

$$\mathcal{O}_{V/k,\,x} = \mathcal{O}_{V,\,x} \cap k(V)$$

Tenslotte nog een opmerking over irreducibiliteit. Het ideaal $(x^2 - 2y^2) \subset \mathbb{Q}[x, y]$ is een priemideaal in de ring $\mathbb{Q}[x, y]$, aangezien $x^2 - 2y^2$ irreducibel is in de ring $\mathbb{Q}[x, y]$. We kunnen hier echter niet de stelling uit §1.1 toepassen en concluderen dat $V(x^2 - 2y^2) \subset \mathbb{A}^2(\overline{\mathbb{Q}})$ irreducibel is. Dit is inderdaad niet het geval, want in $\overline{\mathbb{Q}}[x, y]$ hebben we $x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2})$, waaruit volgt dat $V(x^2 - 2y^2) = V(x + y\sqrt{2}) \cup V(x - y\sqrt{2})$.
Om te controleren of een kromme V gedefinieerd door een polynoom $f \in k[x, y]$ irreducibel is, moeten we dus nagaan of f irreducibel is over $\overline{k}[x, y]$. Alleen irreducibiliteit over $k[x, y]$ is dus niet voldoende!

1.3.1 Graad

We concentreren ons in deze deelparagraaf op eindige lichamen $k = \mathbb{F}_q$. We willen de punten van een variëteit $V/\mathbb{F}_q$ op de één of andere manier kunnen zien als punten over $\mathbb{F}_q$. De verzameling punten $x = (x_1, \ldots, x_n)$ waarvan de coördinaten x_i in $\mathbb{F}_q$ liggen is precies $V(\mathbb{F}_q)$, de verzameling $\mathbb{F}_q$-rationale punten. Het begrip *graad* geeft ons een manier om ook punten die niet in de $V(\mathbb{F}_q)$ zitten te zien als punten over $\mathbb{F}_q$.

Definitie 1.41. *We definiëren de Frobenius-afbeelding σ_q op de punten van $V \subset \mathbb{A}^n(\overline{\mathbb{F}}_q)$ componentsgewijs, dus:*

$$\sigma_q : (x_1, x_2, \ldots, x_n) \longmapsto (\sigma_q(x_1), \sigma_q(x_2), \ldots, \sigma_q(x_n)) = (x_1^q, x_2^q, \ldots, x_n^q)$$

Neem $y = (y_1, \ldots, y_n) \in V, y \notin V(\mathbb{F}_q)$. Dan hebben we $\sigma_q(y) \neq y$. Neem aan dat $m \in \mathbb{N}$ zodanig is dat $\sigma_q^m(y) = y$ en tevens $\sigma_q^i(y) \neq y$ voor $1 \leq i < m$. Zo'n m bestaat daar de y_i algebraïsch zijn over $\mathbb{F}_q$ en er dus getallen m_i bestaan zodanig dat $\sigma_q^{m_i}(y_i) = y_i$. Vervolgens valt eenvoudig af te leiden dat $m = \operatorname{lcm}(m_1, m_2, \ldots, m_n) \in \mathbb{N}$. Dan willen we $\mathbf{y} = \{y, \sigma_q(y), \sigma_q^2(y), \ldots, \sigma_q^{m-1}(y)\}$ opvatten als een punt over $\mathbb{F}_q$. In zekere zin laat σ_q het punt $\mathbf{y}$ nu invariant: de afbeelding σ_q toegepast op de elementen van de verzameling $\{y, \sigma_q(y), \sigma_q^2(y), \ldots, \sigma_q^{m-1}(y)\}$ levert dezelfde puntenverzameling op. Merk op dat we $\{y, \sigma_q(y), \sigma_q^2(y), \ldots, \sigma_q^{m-1}(y)\}$ ook kunnen schrijven als $\mathbf{y} = \bigcup_{i \geq 0} \sigma_q^i(y)$.

Definitie 1.42. *Zijn $\mathbf{y}$ en m als hierboven. Dan noemen we $\mathbf{y}$ een punt over $\mathbb{F}_q$ en m de graad van $\mathbf{y}$. We noteren dit met* $\deg(\mathbf{y}) = m$.

Een $\mathbb{F}_q$-rationaal punt x heeft dus graad 1, daar σ_q de coördinaten van x invariant laat. Als $y = (y_1, y_2, \ldots, y_m)$ zodanig is dat $y_i \notin \mathbb{F}_q$ voor zekere i, dan is de graad van y groter dan 1.

Voorbeeld 1.43. Beschouw de kromme $C/\mathbb{F}_5$ gegeven door $x^2 + y^2 - 1$. De $\mathbb{F}_5$-rationale punten zijn $(0, \pm 1)$, $(\pm 1, 0)$. Dit zijn dus de punten van graad 1. Dan hebben we over $\mathbb{F}_{25} \cong \mathbb{F}_5[\alpha]/(\alpha^2 - 2)$ bijvoorbeeld de punten $(\pm\alpha, \pm 2)$, $(\pm 2, \pm\alpha)$. Deze geven aanleiding tot punten van graad 2 over $\mathbb{F}_5$. Zo zijn $\{(2, \alpha), (2, -\alpha)\}$, $\{(\alpha, -2), (-\alpha, -2)\}$, enzovoort, punten op C van graad 2 over $\mathbb{F}_5$.

Neem weer een kromme $C/\mathbb{F}_q$ en een punt $y = (y_1, y_2, \ldots, y_n) \in C(\mathbb{F}_{q^m})$ met $m \geq 1$ en minimaal, wat betekent dat als $y \in C(\mathbb{F}_{q^r})$ dan $r \geq m$. We willen nu een verband leggen tussen m en de graad d van het punt $\mathbf{y} = \bigcup_{i \geq 0} \sigma_q^i(y)$. Uit $\sigma_q^d(y_i) = y_i$ voor alle i volgt dat $y_i \in C(\mathbb{F}_{q^d})$ voor alle i, dus $y \in C(\mathbb{F}_{q^d})$. Hieruit volgt $d \geq m$.

Verder volgt uit $y \in C(\mathbb{F}_{q^m})$ dat $y_i \in \mathbb{F}_{q^m}$ voor alle i. Dus $\sigma_q^m(y_i) = y_i$ voor alle i waaruit volgt dat $\sigma_q^m(y) = y$. Dus $m \geq d$. Combineren we dit met het voorgaande, dan verkrijgen we dus $d = m$. Hiermee is de volgende stelling bewezen:

Stelling 1.44. *Zij y een punt op een kromme $C/\mathbb{F}_q$. Laat $\mathbf{y} = \bigcup_{i \geq 0} \sigma_q^i(y)$. De volgende twee uitspraken zijn æquivalent.*
1. $y \in C(\mathbb{F}_{q^m})$ en $y \notin C(\mathbb{F}_{q^s})$ voor alle s waarvoor $1 \leq s < m$.
2. $\mathbf{y}$ heeft graad m.

Opmerking. Om de graad van punten van een kromme over een willekeurig lichaam k te definiëren hebben we de Galoisgroep $\mathrm{Gal}(K/k)$ nodig. Zij V/k een kromme en $P = (x_1, \ldots, x_n) \in V/k$ een punt en beschouw

$$\mathbf{P} := \mathrm{Gal}(K/k)(P) = \{\sigma(P) : \sigma \in \mathrm{Gal}(K/k)\}$$

de *baan* van P onder de werking van de Galoisgroep. Met behulp van Galoistheorie kan men inzien dat elke $\sigma(P)$ van de vorm $(\xi_1, \ldots, \xi_n)$ is, waarbij de ξ_i geconjugeerden zijn van de x_i onder de Galoisgroep $G(K/k)$. Dit levert, wederom met Galoistheorie, dat $\mathbf{P}$ een eindige verzameling is met cardinaliteit ten hoogste $\prod_{i=1}^n [k(x_i) : k]$. Nu is $\mathbf{P}$ een punt over k (omgekeerd is elk punt over k van bovenstaande vorm) en haar graad is $\#\mathbf{P}$.
Daar we deze definitie niet nodig hebben, zullen we er verder niet op ingaan.

1.4 De projectieve ruimte $\mathbb{P}^n$

Tot nu toe hebben we steeds gekeken naar variëteiten in de affiene ruimte. In de projectieve ruimte echter gedragen krommen zich nog beter. In deze paragraaf behandelen we de definitie van de projectieve ruimte en definiëren we projectieve krommen. Een definitie in woorden is eerst wel handig.

Neem een lichaam k vast. De n-dimensionale projectieve ruimte is de "geperforeerde ruimte" $\mathbb{A}^{n+1}(k) - \{0\}$ waarin twee punten $(x_0, x_1, \ldots, x_n)$ en $(y_0, y_1, \ldots, y_n)$ met elkaar geïdentificeerd worden als ze scalaire veelvouden van elkaar zijn. Nu preciezer geformuleerd:

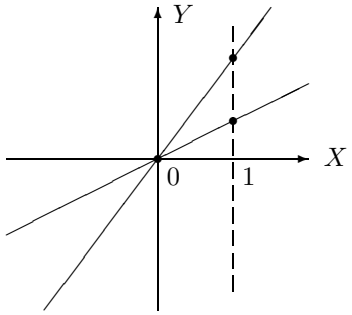
Definitie 1.45. *Zij k een lichaam. De projectieve n-ruimte over k is gedefinieerd als:*

$$\mathbb{P}^n(k) := (\mathbb{A}^{n+1} - \{0\})/\sim$$

met $(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)$ als er $\lambda \in k$ bestaat zodanig dat

$$(y_0, y_1, \ldots, y_n) = (\lambda x_0, \lambda x_1, \ldots, \lambda x_n).$$

Een alternatieve manier om over $\mathbb{P}^n(k)$ te denken is: "de verzameling lijnen door de oorsprong in $\mathbb{A}^{n+1}(k)$". Om $\mathbb{P}^n(k)$ te krijgen identificeer je namelijk precies alle punten die op hetzelfde lijnstuk in de $\mathbb{A}^{n+1}(k)$ liggen. We noteren de punten van $\mathbb{P}^n(k)$ met $(X_0 : X_1 : \cdots : X_n)$. Het zal duidelijk zijn dat deze schrijfwijze niet uniek is, zo is het punt $(1 : 0 : 0 : \cdots : 0)$ equivalent met $(\lambda : 0 : 0 : \cdots : 0)$ voor elke $\lambda \in k^*$. Om de situatie te verduidelijken kijken we naar $\mathbb{P}^1(\mathbb{R})$.



Boven is het affiene vlak over $\mathbb{R}$ afgebeeld. De lijnen door de oorsprong stellen elementen (punten) van $\mathbb{P}^1(\mathbb{R})$ voor. Door de doorsnijding met de lijn $X = 1$ te beschouwen zie je dat "bijna" alle punten van de $\mathbb{P}^1(\mathbb{R})$ corresponderen met punten in de $\mathbb{A}^1(\mathbb{R})$. De enige uitzondering is de lijn die samenvalt met de Y-as. Deze correspondeert met het punt $(0 : 1)$. (Dit is te zien door op te merken dat $(0 : 1) \sim (0 : \lambda)$ en de verzameling $\{(0, \lambda) \in \mathbb{A}^2 \mid \lambda \in k\}$ correspondeert met de Y-as.) Dit wordt ook wel het *punt op oneindig* genoemd, omdat de lijnen die er dichtbij liggen corresponderen met punten in de $\mathbb{A}^1$ die ver weg liggen van de oorsprong.

We kunnen in dit voorbeeld natuurlijk de "lijn van projectie" op allerlei manieren kiezen. Zo zou $y = 1$ ook voldoen. In dat geval zou het punt gerepresenteerd door $(1 : 0)$ op oneindig liggen. De punten vertegenwoordigd door $(\tau : 1)$ corresponderen dan met de affiene lijn $\mathbb{A}^1$.

We hebben dus, puur verzamelingstheoretisch gezien:

$$\mathbb{P}^1 \cong \mathbb{A}^1 \cup \{\text{punt op oneindig}\}$$

1.4.1 $\mathbb{A}^n$ zit in $\mathbb{P}^n$

In het algemeen geldt dat $\mathbb{P}^n$ kan worden opgevat als $\mathbb{A}^n$, aangevuld met punten op oneindig. In het geval van $\mathbb{P}^1$ is er één punt op oneindig. Het is belangrijk om de projectieve ruimte $\mathbb{P}^n$ op te vatten als een uitbreiding van de $\mathbb{A}^n$. Daartoe moeten we nu nog aangeven op welke manier $\mathbb{A}^n$ "in" de $\mathbb{P}^n$ zit.

Omdat we ons vooral interesseren voor $\mathbb{P}^2$ zullen we ons tot dat geval beperken. Daarnet in de bespreking van $\mathbb{P}^1$ zagen we dat we de punten van de vorm $(\tau : 1)$ kunnen identificeren met de $\mathbb{A}^1$. Ook bleek dat deze keuze min of meer willekeurig is: we zouden ook de punten van de vorm $(1 : \tau)$ kunnen nemen, maar deze keuze pakt in het geval van krommen het beste uit, vooral wat notatie betreft. We passen nu hetzelfde idee toe op de $\mathbb{P}^2$.

Definitie 1.46 (definitie van $\cdot^\sharp$ en $\cdot^\flat$). *Zij $P = (x, y) \in \mathbb{A}^2$ een affien punt, dan definiëren we het corresponderende projectieve punt $P^\sharp = (x : y : 1) \in \mathbb{P}^2$. Omgekeerd definiëren we voor een projectief punt $Q \in \mathbb{P}^2$ met Q van de vorm $(x : y : 1)$ het affiene punt $Q^\flat = (x, y) \in \mathbb{A}^2$.*

Het komt geregeld voor dat we zonder er uitvoerig bij stil te staan affiene punten in projectieve context plaatsen en andersom. In dat geval maken we dus (in gedachten) bovenstaande vertaalslag.

1.4.2 Homogene polynomen

Omdat punten in de projectieve ruimte geen unieke representatie bezitten, moeten we voorzichtig zijn met het definiëren van functies op projectieve ruimten en krommen. Om dit probleem op te lossen hebben we het begrip *homogeen polynoom* nodig. Merk op dat we projectieve coördinaten met hoofdletters noteren.

Definitie 1.47. *Zij $k[X_1, \ldots, X_\nu]$ een polynoomring. Neem $d \geq 0$. Een homogeen polynoom van graad d is een polynoom $F \in k[X_1, \ldots, X_\nu]$ waarvan alle termen graad d hebben.*

Lemma 1.48. *Het product van twee niet-homogene polynomen is niet-homogeen.*

Bewijs. Zij $f, g \in k[X_1, \ldots, X_\nu]$ beide niet-homogeen. We kunnen f en g schrijven als de som van homogene polynomen: $f = \sum_{i=m}^{M} f_i$ en $g = \sum_{i=n}^{N} g_i$ met de f_i en g_i homogeen van graad i, $m < M, n < N$ en f_m, f_M, g_n, g_N alle ongelijk aan nul. Dan is het product fg te schrijven als $\sum_{i=m+n}^{M+N} h_i$ met $\deg h_i = i$ en h_{m+n} en h_{M+N} ongelijk aan nul. □

Gevolg 1.49. *Zij $F_1 F_2 \cdots F_j$ de factorisatie van een homogeen polynoom $F \in k[X_1, \ldots, X_\nu]$ in irreducibele polynomen. Dan zijn de F_i alle homogeen.*

Omdat punten in de projectieve ruimte $\mathbb{P}^2$ met drie coördinaten worden genoteerd, lijkt het logisch om polynomen te beschouwen in drie variabelen, dus polynomen in de $k[X, Y, Z]$. In het projectieve vlak kunnen dan projectieve krommen worden gedefinieerd als de nulpuntenverzamelingen van homogene polynomen in $k[X, Y, Z]$. Verder zal blijken dat deze projectieve krommen opgevat kunnen worden als de *projectieve afsluiting* van hun affiene tegenhangers.

Eenvoudig gevolg 1.50. *Stel $F \in k[X, Y, Z]$ is homogeen van graad d. Dan hebben we voor alle $\lambda \in k$ dat $F(\lambda\xi_1, \lambda\xi_2, \lambda\xi_3) = \lambda^d F(\xi_1, \xi_2, \xi_3)$.*

Merk op dat een homogeen polynoom F van graad > 0 nog steeds geen welgedefinieerde functie is op de projectieve ruimte $\mathbb{P}^n$. Neem het punt $(x : y : z)$. We kunnen dit punt ook schrijven als $(\lambda x : \lambda y : \lambda z)$ met $\lambda \neq 1$. Dan is $F(x, y, z) \neq F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$. Wat is dus de zin van de homogene polynomen (in drie variabelen)? Welnu, hun nulpuntenverzamelingen zijn wél goed gedefinieerd in de $\mathbb{P}^2$.

Propositie-definitie 1.51. *Zij $F \in k[X, Y, Z]$ een homogeen polynoom van graad $d \in \mathbb{Z}_{\geq 0}$. Dan noemen we een projectief punt $P = (x : y : z) \in \mathbb{P}^2$ een nulpunt van F dan en slechts dan als $F(x, y, z) = 0$. In het bijzonder is de eigenschap dat P een nulpunt is niet afhankelijk van de gekozen representatie.*

Bewijs. Zij $F(x, y, z) = 0$. Een andere representant van P is van de vorm $(\lambda x : \lambda y : \lambda z)$ voor zekere λ. We moeten controleren dat dit ook een nulpunt is van F. Maar dit volgt eenvoudig: $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z) = \lambda^d \cdot 0 = 0$. □

Aangezien de nulpuntenverzameling van een homogeen polynoom dus welgedefinieerd blijkt te zijn, kunnen we overgaan tot de definitie van een projectieve kromme.

Definitie 1.52. *Een projectieve kromme V is de nulpuntenverzameling van F in $\mathbb{P}^2$, waarbij $F \in k[X, Y, Z]$ een irreducibel homogeen polynoom $\neq 0$ is.*

We schrijven voor V net als in het geval van een affiene kromme weer $V(F)$.

1.4.3 Het verband tussen affiene en projectieve variëteiten

Zoals gezegd kunnen we een projectieve variëteit zien als een projectieve afsluiting van een affiene variëteit. Met een voorbeeld lichten we nu toe hoe deze vertaalslag kan worden gemaakt.

Voorbeeld 1.53. Zij $V \subset \mathbb{P}^2(\overline{\mathbb{Q}})$ de projectieve variëteit gedefinieerd als nulpuntenverzameling van $X^2+Y^2-Z^2$. Wat zijn de $\mathbb{Q}$-rationale punten van deze kromme? We zijn dus op zoek naar "projectieve drietallen" $P=(x:y:z)$ zodanig dat $x^2+y^2=z^2$. Dus x, y en z zijn de zijden van een Pythagoras-driehoek! We mogen x, y en z naar believen herschalen met een factor λ, dus in het bijzonder mogen we aannemen dat $x,y,z \in \mathbb{Z}$ zonder dat we hierdoor punten uit het oog verliezen.

Gevraagd zijn dus eigenlijk Pythagoras-driehoeken met gehele zijden x,y en z. Maar hiervan kennen we er genoeg, bijvoorbeeld de 3-4-5-driehoek, de 5-12-13-driehoek en de 7-24-25-driehoek. Dit levert ons de punten $P_1=(3:4:5)$, $P_2=(5:12:13)$ en $P_3=(7:24:25)$. We zouden er ook voor kunnen kiezen om onze projectieve punten te "normaliseren" zodat steeds $z=1$ zou gelden: $P_1=(\frac{3}{5}:\frac{4}{5}:1)$, $P_2=(\frac{5}{13}:\frac{12}{13}:1)$ en $P_3=(\frac{7}{25}:\frac{24}{25}:1)$.

Misschien dat het op dit punt opvalt dat we het punt $(\frac{3}{5},\frac{4}{5})$ ook aantroffen op de "affiene cirkel" gegeven door het polynoom x^2+y^2-1. Na controle blijkt dat ook $(\frac{5}{13},\frac{5}{13})$ en $(\frac{7}{25},\frac{24}{25})$ op deze cirkel liggen. Is dit verklaarbaar? Welnu, stel dat $\xi^2+\eta^2=1$, dan is het drietal $(\xi:\eta:1)$ een nulpunt van $X^2+Y^2-Z^2$ en ligt het in V. Dus een punt op de affiene cirkel correspondeert met een uniek punt op V. Omgekeerd, stel dat $(x:y:z)\in V$, oftewel $x^2+y^2=z^2$. Normaliseren bleek de vorige keer een goed idee, dus neem aan dat $z\neq 0$. Dan krijgen we $(\frac{x}{z})^2+(\frac{y}{z})^2=1$ en het punt $(\frac{x}{z},\frac{y}{z})$ ligt dus op de affiene cirkel.

Dus omgekeerd corresponderen de projectieve punten waarvoor $z\neq 0$ uniek met punten op de affiene cirkel! Het probleem wordt gevormd door de punten met $z=0$: deze worden wederom de "punten op oneindig" genoemd. In het geval van V zijn er punten als $(1:\pm i:0)$ die op oneindig liggen. Merk op dat er geen $\mathbb{Q}$-rationale punten op oneindig liggen: stel $x,y\in\mathbb{Q}$ zodanig dat $(x:y:0)\in V$, dan $x^2+y^2=0$ en dat kan alleen als $x=0,y=0$, maar $(0:0:0)$ is geen punt in de projectieve ruimte.

Er is dus een expliciet verband tussen de polynomen f en F die de affiene respectievelijk projectieve versie van "dezelfde" kromme definiëren. Dit maken we formeel in de volgende definities.

Definitie 1.54. *Zij $f=\sum \alpha_{i_1,i_2}\ x^{i_1}y^{i_2}\in k[x,y]$ een polynoom van graad d. De homogenisering $f^\sharp$ is dan gedefinieerd als:*

$$f^\sharp = \sum \alpha_{i_1,i_2} X^{i_1}Y^{i_2}Z^{d-i_1-i_2} \in k[X,Y,Z]$$

Merk op dat $f^\sharp$ homogeen is van graad d.

We definiëren ook het omgekeerde procédé, *dehomogenisatie* genoemd:

Definitie 1.55. *Zij $F\in k[X,Y,Z]$ een irreducibel homogeen polynoom van graad d en $F\notin k[Z]$. De dehomogenisering $F^\flat$ is dan gedefinieerd als $F(x,y,1)$.*

Het is eenvoudig na te gaan dat de operaties homogenisatie en dehomogenisatie elkaars inverse zijn. Hiervoor is het wel belangrijk dat we bij de definitie van dehomogenisatie stipuleerden dat F irreducibel moest zijn en geen polynoom in Z alleen: een eventuele factor $g(Z)$ zou worden "weggegooid". Merk op dat dit alleen polynomen van de vorm αZ uitsluit, waar $\alpha\in k$. De nulpuntenverzamelingen van deze polynomen liggen "op oneindig" en hebben dus geen affiene punten.

Voorbeeld 1.56. *Zij $f=x^2+y^2-1$. De homogenisering is dan $f^\sharp = X^2\cdot Z^0+Y^2\cdot Z^0-1\cdot Z^2 = X^2+Y^2-Z^2$. Het gevolg van de homogenisering is dus dat ieder monoom in de uitdrukking van f wordt vermenigvuldigd met een macht van Z zodanig dat de totale graad op $d=2$ uitkomt.*
Zij $g=y^2-x^3-x-1$. Dan is de homogenisering $g^\sharp$ gegeven door $g^\sharp = Y^2\cdot Z^1-X^3\cdot Z^0-X\cdot Z^2-1\cdot Z^3 = Y^2Z-X^3-XZ^2-Z^3$.

Stelling 1.57. *Zij $f\in k[x,y]$ een irreducibel polynoom. Dan is $P\in\mathbb{A}^2$ een punt van $V(f)$ dan en slechts dan als $P^\sharp$ een punt is van $V(f^\sharp)\subset\mathbb{P}^2$.*

Bewijs. Zij $f \in k[x,y]$ en $P = (\xi, \eta)$ zodanig dat $f(P) = 0$. Dan wordt een representant van $P^\sharp$ gegeven door het projectieve drietal $(\xi : \eta : 1)$, en dan is $f^\sharp(P^\sharp) = f(P) = 0$. Omgekeerd, als $Q = (\xi : \eta : 1)$ een nulpunt is van $f^\sharp$, dan geldt per definitie dat $0 = f^\sharp(Q) = f(Q^\flat) = f(\xi, \eta)$. □

Stelling 1.58. *Zij $F \in k[X,Y,Z]$ een irreducibel homogeen polynoom en $F \notin k[Z]$. Dan is $P \in \mathbb{A}^2$ een punt van $V(F^\flat)$ dan en slechts dan als $P^\sharp$ een punt is van $V(F) \subset \mathbb{P}^2$*

Bewijs. Volledig analoog. □

We kunnen nu het intuïtief duidelijke begrip van projectieve afsluiting formaliseren in een definitie.

Definitie 1.59. *Zij $V \subset \mathbb{A}^n(k)$ een affiene kromme gegeven als nulpuntenverzameling van $f \in k[x,y]$. Dan is de projectieve afsluiting van V gedefinieerd als $V(f^\sharp)$. We zien onder meer dat $V(f)$ op een welgedefinieerde wijze "in" $V(f^\sharp)$ zit.*

Het omgekeerde proces, van een projectieve variëteit overgaan naar de bijbehorende affiene variëteit, is ook mogelijk:

Definitie 1.60. *Zij W een projectieve kromme gegeven als nulpuntenverzameling van een irreducibel homogeen polynoom $F \in k[X,Y,Z]$ met $F \notin k[Z]$. Definieer nu het polynoom*

$$f := F(x, y, 1) \in k[x, y]$$

Definieer vervolgens de affiene variëteit $V \subset \mathbb{A}^2$ als $V = V(f)$. V heet een affiene deelverzameling van W.

Het is op dit punt goed om stil te staan bij de keuze om f te definiëren als $F(x,y,1)$, in plaats van als $F(x,1,y)$. Als we $f' = F(x,1,y)$ nemen, dan definieert $V(f')$ immers ook een variëteit die "in" W zit. Een affien punt (ξ, η) correspondeert in dat geval met het projectieve punt $(\xi : 1 : \eta)$. Het interessante aan deze nieuwe correspondentie is dat we nu punten van de vorm $(\lambda : 1 : 0) \in \mathbb{P}^2$ kunnen zien als affiene punten, terwijl deze eerder "op oneindig" lagen en dus onbereikbaar waren. We onderzoeken de eigenschappen van een projectieve kromme meestal door ons te beperken tot een affiene deelverzameling. Hiervoor moeten we dus soms onze toevlucht nemen tot een andere keuze voor de inbedding $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$.

Voorbeeld 1.61. Zij $W \subset \mathbb{P}^2(\overline{\mathbb{Q}})$ de projectieve variëteit gegeven door $W = V(XY - Z^2)$. Dan kunnen we een affiene deelverzameling kiezen door bijvoorbeeld $X = 1$ te laten en $y = Y$, $x = Z$ te kiezen, hetgeen ons de variëteit $V(y - x^2) \subset \mathbb{A}^2$ oplevert: een parabool. Maar ook zouden we $Z = 1$ kunnen kiezen, hetgeen de affiene deelverzameling $V(xy - 1) \subset \mathbb{A}^2$ geeft, en dat is een hyperbool.
Dit is een voorbeeld van de algemene opmerking dat krommen zich "mooier" gedragen in de projectieve ruimte: we wisten al wel dat de hyperbool en de parabool eigenschappen gemeen hadden, maar in de projectieve ruimte blijken ze eigenlijk dezelfde kromme te zijn!

Definitie 1.62. *Neem $W = V(F)$ een projectieve kromme en $P \in W$. Stel V is een affiene deelverzameling van W die $P^\flat$ bevat. Dan noemen we W glad in P als V glad is in $P^\flat$.*

Stelling 1.63. *Een projectieve kromme $V(F) \in$ is glad in P dan en slechts dan als niet alle $\frac{\partial F}{\partial X}(P)$, $\frac{\partial F}{\partial Y}(P)$, $\frac{\partial F}{\partial Z}(P)$ gelijk zijn aan nul.*

Bewijs. Zij $f = F^\flat$. Te bewijzen is dat

$$\frac{\partial f}{\partial x}(P^\flat) = \frac{\partial f}{\partial y}(P^\flat) = 0 \iff \frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

De richting "$\Longleftarrow$" is triviaal, we bewijzen alleen de omgekeerde richting. Uit $\frac{\partial f}{\partial x}(P^\flat) = 0$ volgt $\frac{\partial F}{\partial X}(P) = 0$ en uit $\frac{\partial f}{\partial y}(P^\flat) = 0$ volgt $\frac{\partial F}{\partial Y}(P) = 0$. Dan is alleen nog $\frac{\partial F}{\partial Z}(P) = 0$ te bewijzen. Hiertoe nemen we zoals in het bewijs van stelling 1.31 aan dat $P = (0 : 0 : 1)$ zonder aan algemeenheid in te boeten. Dan heeft f geen constante term, wat impliceert dat F geen term heeft in Z alleen. Dan heeft F zeker geen lineaire term in Z, dus $\frac{\partial F}{\partial Z}(P) = 0$. □

Definitie 1.64. *Een projectieve kromme $C \subset \mathbb{P}^2(K)$ is glad als ze glad is in al haar punten.*

1.4.4 Functielichaam van een projectieve variëteit

In het begin van deze paragraaf kwamen we de vraag tegen, welke functies eigenlijk welgedefinieerd zijn in de projectieve ruimte of op een projectieve kromme. We bekijken eerst de projectieve ruimte $\mathbb{P}^2$. We zagen al dat de homogene polynomen van graad > 0 geen kandidaten waren. Beschouwen we echter het quotiënt F/G van twee homogene polynomen $F, G \in k[X, Y, Z]$ van gelijke graad d, dan zien we dat deze wel goed gedefinieerd is op de punten waar G geen nulpunt heeft:

$$\frac{F(\xi,\eta,\zeta)}{G(\xi,\eta,\zeta)} = \frac{\lambda^d F(\xi,\eta,\zeta)}{\lambda^d G(\xi,\eta,\zeta)} = \frac{F(\lambda\xi,\lambda\eta,\lambda\zeta)}{G(\lambda\xi,\lambda\eta,\lambda\zeta)}$$

Deze quotiënten van homogene polynomen kunnen beschouwd worden als "homogene rationale functies van graad nul". Dit geeft aanleiding tot de volgende definitie:

Definitie 1.65. *Een rationale functie f op de $\mathbb{P}^2$ is een tweetal (F, G) waar $F, G \in k[X, Y, Z]$ homogeen zijn van gelijke graad. Verder definiëren we de equivalentierelatie $\sim$: we hebben $(F, G) \sim (F', G')$ dan en slechts dan als $FG' - GF' = 0$. We schrijven ook wel $f = F/G$. Zij nu $x \in \mathbb{P}^2$ een projectief punt. Als geldt dat een rationale functie f een representatie F/G bezit zodanig dat $G(x) \neq 0$ (merk op dat deze voorwaarde onafhankelijk is van de representatie van het punt x als projectief drietal $(\xi : \eta : \zeta)$), dan heet f regulier in x.*

De verzameling rationale functies op het projectieve vlak $\mathbb{P}^2$ noteren we weer op de vertrouwde wijze als $k(\mathbb{P}^2)$. Het is eenvoudig te controleren dat $k(\mathbb{P}^2)$ een lichaam is. Als een rationale functie f regulier is in x, kunnen we spreken over de waarde van f in x. Dit leggen we vast in de volgende definitie.

Definitie 1.66. *Zij f een rationale functie die regulier is in $x = (\xi : \eta : \zeta)$ en F/G een representatie van f waarbij $F, G \in k[X, Y, Z]$ homogeen zijn van graad d met G zodanig dat $G(\xi, \eta, \zeta) \neq 0$. Dan definiëren we $f(x)$, de waarde van f in x, als $F(\xi, \eta, \zeta)/G(\xi, \eta, \zeta)$.*

Het is duidelijk dat $F(\xi, \eta, \zeta)/G(\xi, \eta, \zeta)$ onafhankelijk is van de keuze van de representatie van het projectieve punt x omdat F en G van dezelfde graad zijn.

De elementen van $k(\mathbb{A}^2)$ corresponderen één-op-één met die van $k(\mathbb{P}^2)$. We introduceren ook hier de afbeeldingen $\cdot^\sharp$ en $\cdot^\flat$, nu voor elementen van $k(\mathbb{A}^2)$ en $k(\mathbb{P}^2)$ respectievelijk.

Definitie 1.67. *Zij $f = g/h$ een element van $k(\mathbb{A}^2)$. Dan definiëren we $f^\sharp \in k(\mathbb{P}^2)$ als*

$$f^\sharp := g^\sharp / h^\sharp \cdot Z^{\deg h - \deg g}.$$

Omgekeerd, zij $j = F/G \in k(\mathbb{P}^2)$, dan definiëren we

$$j^\flat := F^\flat / G^\flat.$$

We moeten controleren dat verschillende representaties van $f \in k(\mathbb{A}^2)$ worden afgebeeld op equivalente tweetallen in $k(\mathbb{P}^2)$ en omgekeerd. Dit komt neer op veel schrijfwerk maar is verder triviaal. Zij W een projectieve variëteit met $W = V(F)$ waarin F irreducibel en homogeen en $F \notin k[Z]$. Zij verder $V = V(F^\flat)$ een affiene deelverzameling. We zijn nu in een positie om $k(W)$, het functielichaam van een projectieve variëteit W te definiëren:

Definitie 1.68. *We definiëren het functielichaam $k(W)$ van W als volgt:*

$$k(W) := \{f^\sharp : f \in k(V)\}$$

Opmerking 1.69. Merk op dat $v_P(f)$ via deze één-op-één-correspondentie nu ook gedefinieerd is voor elementen f van het projectieve functielichaam: $v_P(f) := v_{P^\flat}(f^\flat)$.

Een alternatieve karakterisering die uit de vorige definitie volgt is de volgende:

$$k(W) := \left\{ \frac{G}{H} : G, H \text{ homogeen van dezelfde graad} \right\} \text{ waarbij } \frac{G}{H} \sim \frac{G'}{H'} \text{ als } F \mid GH' - G'H$$

De equivalentie van deze twee definities wordt aangetoond in [Fulton, §4.1]. We besluiten deze paragraaf met een tweetal stellingen over projectieve krommen en hun functielichamen. Hiervoor hebben we de restrictie dat het grondlichaam K algebraïsch afgesloten is weer nodig.

Stelling 1.70. *Zij $W \in \mathbb{P}^2(K)$ een projectieve kromme. Stel $f \in K(W)$ een functie die overal op W regulier is. Dan geldt dat f constant is, oftewel er bestaat $\alpha \in K$ zodanig dat $f = \alpha$.*

Bewijs. [Sha, p. 59, Cor. 1.] □

Er zijn veel redenen om krommen in het projectieve vlak te bekijken in plaats van in het affiene vlak. De volgende stelling levert een bijzonder aantrekkelijke eigenschap van krommen in het projectieve vlak. In wat volgt zijn $C, D \subset \mathbb{P}^2(K)$ twee krommen gegeven door irreducibele homogene polynomen $F, G \in K[X, Y, Z]$. We hebben voorts de notie van het *snijgetal* nodig. Dit definiëren we eerst alleen voor de affiene oorsprong:

Definitie 1.71. *We definiëren $i(C, D; O)$, het snijgetal van C en D in de oorsprong, als $\dim_k k[[x, y]]/(f, g)$, waarbij $f = F^\flat, g = G^\flat$. Meer in woorden is dit de dimensie over k van de ring $k[[x, y]]$ van formele machtreeksen uitgedeeld naar het ideaal (f, g).*

De algemene definitie van het snijgetal $i(C, D; P)$ in een willekeurig projectief punt P volgt uit het feit dat het snijgetal niet verandert onder translaties of wanneer je een ander affien deel van de $\mathbb{P}^2$ bekijkt. Beter gezegd: het snijgetal is invariant onder projectieve transformaties. Zowel voor de welgedefinieerdheid van het snijgetal, als voor het bewijs van voorgaande beweringen, zij de lezer verwezen naar §3.3 van [Fulton].

Stelling 1.72 (Bézout). *Zij $\{P_i\}$ de verzameling snijpunten van C en D in $\mathbb{P}^2(K)$. Definieer*

$$n := \sum_i i(C, D; P_i)$$

Oftewel, n is het aantal snijpunten van C en D, snijgetallen meegerekend. Dan geldt $n = \deg f \deg g$.

Bewijs. [Shafarevich, blz. 172-3.] □

2 Divisoren, Riemann-Roch en codes

2.1 Divisoren

Met k wordt weer steeds een willekeurig lichaam aangeduid en met K zijn algebraïsche afsluiting. Zij verder C/k een gladde projectieve kromme.

Definitie 2.1. *Een divisor D over k op C is een eindige formele som*

$$D = n_1P_1 + n_2P_2 + \ldots + n_mP_m$$

waar de $P_1, P_2, \ldots, P_m \in C$ punten op de kromme zijn van willekeurige eindige graad over k, en de $n_i \in \mathbb{Z}$.

De divisoren op C over k vormen een abelse groep onder de opteloperatie die aangegeven wordt met $\operatorname{div} C/k$. We noteren verder $v_P(D) := n_P =$ de coëfficiënt van het punt P in D.

Zij $D = \sum_{P\in C} n_P P$ een divisor op C, dus $n_P \neq 0$ voor slechts eindig veel punten $P \in C$. We definiëren de *drager* van D, aangegeven met $\operatorname{supp}(D)$, als $\{P \mid n_P \neq 0\}$, de verzameling van punten die voorkomen in de uitdrukking voor D. De *graad* van D, ook wel $\deg D$, is gedefinieerd als $\sum_{P\in C} n_P$.

We definiëren een partiële ordening op de verzameling $\operatorname{div} C$: laat $D = \sum n_P P$ en $D' = \sum n'_P P$, we zeggen dat $D \succeq D'$ dan en slechts dan als $n_P \geq n'_P$ voor alle $P \in C$. Als bijvoorbeeld geldt dat $D \succeq 0$, dan hebben we $n_P \geq 0$ voor alle $P \in C$. In dat geval heet D een *effectieve divisor*.

Met een functie $f \in k(C)^*$ wordt op de volgende wijze een divisor geassocieerd, aangegeven met (f):

$$(f) := \sum_{P\in C} v_P(f) \cdot P$$

We moeten aantonen dat bovenstaande uitdrukking inderdaad een divisor voorstelt. Merk hiertoe op dat $f = g/h$ op de kromme C slechts een eindig aantal polen en nulpunten heeft. [Sha, p. 23-24, Ex. 3.] Dus $v_P(f) \neq 0$ voor slechts een eindig aantal punten. Merk verder op dat $(fg) = (f)+(g)$ en $(f/g) = (f)-(g)$, waarbij $f, g \in k(C)$, zoals volgt uit lemma 1.32. Een divisor van de vorm (f) met $f \in k(C)$ wordt ook wel hoofddivisor genoemd. Over hoofddivisoren hebben we de volgende stelling:

Stelling 2.2. *Zij $f \in k(C)$ een functie op C. Zij $D = (f)$. Dan geldt* $\deg D = 0$.

Bewijs. [Shafarevich, p. 154, Ex. 2.] □

Definitie 2.3. *Zij D, D' divisoren op C over k. Dan heten D en D' lineair equivalent (genoteerd met $D \sim D'$) als er een $f \in k(C)^*$ bestaat zodanig dat $D - D' = (f)$.*

Merk op dat bovenstaande daadwerkelijk een equivalentierelatie is: we hebben $D-D = (a)$ met $a \in k^* \Longrightarrow D \sim D$, dus $\sim$ is *reflexief*. $D - D' = (f) \Longrightarrow D' - D = (f^{-1})$ geeft ons de *symmetrie*. Tenslotte levert $D - D' = (f)$ en $D' - D'' = (g) \Longrightarrow D - D'' = (f) + (g) = (fg)$ de *transitiviteit*.

Neem D een divisor over k op C. We zijn nu in een positie om $L(D)$, de *Riemann-Roch-ruimte van D*, te definiëren.

Definitie 2.4. *Zij D een divisor op een gladde kromme $C/\mathbb{F}_q$. De Riemann-Roch-ruimte $L(D)$ is gedefinieerd als*

$$L(D) = \{f \in k(C) : (f) + D \succeq 0\} \cup \{0\}$$

Let op dat we alleen kijken naar functies in $k(C)$. Als f' zodanig is dat $(f') + D \succeq 0$, maar f' zit niet in $k(C)$ maar in $k'(C)$ met $k' \supset k$ een algebraïsche uitbreiding, dan zit f' dus niet in $L(D)$. Bij de bepaling van $L(D)$ speelt dus een rol over welk lichaam D een divisor is.

We leggen nu uit wat het betekent als een functie f in $L(D)$ zit. Schrijf weer $D = \sum n_P P$, dan is $f \in L(D) - \{0\}$ eenvoudigweg equivalent met $v_P(f) \geq -n_P$ voor alle $P \in C$. In $L(D)$ zitten dus functies met "hoogstens een n_P-voudige pool in P".

Stelling 2.5. *$L(D)$ is een vectorruimte over k.*

Bewijs. Neem eerst aan dat $f, g \in L(D)$ en $\alpha \in k$. Nu valt te bewijzen (i) dat $\alpha f \in L(D)$ en (ii) dat $f + g \in L(D)$. Welnu, als $v_P(f) = m$, dan geldt $v_P(\alpha f) = m$ omdat $\alpha \in \mathcal{O}_P^*$, dus (i) volgt onmiddellijk. Zij t een lokale uniformisant in $\mathcal{O}_P$. Dan zijn er $i, j \geq -n_P$ zodanig dat $f = ut^i$ en $g = vt^j$ voor zekere $u, v \in \mathcal{O}_P^*$. Neem zonder verlies van algemeenheid aan dat $i \geq j$, dan geldt $f + g = wt^j$ met $w = ut^{i-j} + v \in \mathcal{O}_P$. Dus $v_P(f + g) \geq j \geq -n_P \Longrightarrow f + g \in L(D)$. □

Stelling 2.6. *Zijn D, D' twee divisoren over k op C zodanig dat $D \sim D'$. Dan zijn $L(D)$ en $L(D')$ isomorf als k-vectorruimten.*

Bewijs. Neem aan dat $D - D' = (f)$ voor zekere $f \in \mathbb{F}_q(C)$. We kunnen een isomorfisme van vectorruimtes construeren tussen $L(D)$ en $L(D')$. We hebben $g \in L(D) \iff (g) \succeq -D \iff (fg) = (f) + (g) = D - D' + (g) \succeq D - D' - D = -D' \iff fg \in L(D')$. Definiëren we nu $\pi : L(D) \longrightarrow L(D')$ en $\xi : L(D') \longrightarrow L(D)$ door $\pi(g) = fg$ en $\xi(h) = h/f$, dan levert dit ons het gevraagde isomorfisme. □

Het volgende lemma zal later van pas komen als we ons met codes bezighouden.

Lemma 2.7. *Zij D een divisor over k op C waarvoor $L(D) \neq \{0\}$. Dan bestaat er een divisor $D' \succeq 0$ zodanig dat $D \sim D'$.*

Bewijs. Zij $f \in L(D), f \neq 0$. Neem $D' := (f) + D$. □

2.2 De stelling van Riemann-Roch

Zij D weer een divisor over k op een kromme C. We zagen dat $L(D)$ een k-vectorruimte is. Als zodanig heeft zij een dimensie $\dim_k L(D)$.

Definitie 2.8. *We definiëren $\ell(D) := \dim_k L(D)$.*

Lemma 2.9. *Als $\deg D < 0$, dan $\ell(D) = 0$.*

Bewijs. De afbeelding $\deg : \operatorname{div} C \longrightarrow \mathbb{Z}$ is een homomorfisme van additieve groepen. Voor iedere $f \in k(C)$ geldt $\deg(f) = 0$ en dus $\deg((f) + D) < 0$. Dit houdt in dat $(f) + D \not\succeq 0 \Longrightarrow f \notin L(D)$. □

Het probleem van de bepaling van $\ell(D)$ voor een gegeven D staat bekend als het *probleem van Riemann-Roch*. Er bestaat een gedeeltelijke oplossing voor dit probleem, namelijk de *stelling van Riemann-Roch*. Om deze te kunnen formuleren hebben we alleen nog het begrip *geslacht* nodig. Dit is een belangrijke invariant van algebraïsche krommen.

Definitie 2.10. *Zij $C \subset \mathbb{P}^2$ een gladde kromme gegeven door een irreducibel homogeen polynoom $f \in k[X, Y, Z]$ van graad d. Het geslacht van C, genoteerd met g of $g(C)$, is dan $g = \frac{1}{2}(d-1)(d-2)$.*

Stelling 2.11 (Riemann-Roch). *Zij $C/k \subset \mathbb{P}^2$ een gladde kromme met geslacht g en $D \in \operatorname{div} C$ een divisor over k. Dan is:*

$$\ell(D) \geq \deg D + 1 - g$$

Is bovendien $\deg D > 2g - 2$, dan geldt zelfs gelijkheid:

$$\ell(D) = \deg D + 1 - g$$

Bovenstaande is eigenlijk niet de "echte" stelling van Riemann-Roch maar een gevolg ervan. Voor onze doeleinden is ze echter net zo geschikt dan de echte Riemann-Roch-stelling, waarvoor we nog het begrip "canonieke divisorklasse" nodig zouden hebben. De canonieke divisorklasse laat zich lastig definiëren zonder tenminste een korte behandeling van het begrip Kähler-differentialen , en daarvoor is hier geen ruimte.

2.3 Codes

Zoals gezegd in de inleiding geven de vectorruimtes $L(D)$ aanleiding tot foutcorrigerende codes. Eerst nog even de nodige definities.

Definitie 2.12. *Zij $n \in \mathbb{Z}_{>0}$. Een foutcorrigerende code $\mathcal{C}$ over $\mathbb{F}_q$ is een lineaire deelruimte van $\mathbb{F}_q^n$. De parameters n en $k = \dim_{\mathbb{F}_q} \mathcal{C}$ heten respectievelijk de lengte en de dimensie van de code $\mathcal{C}$.*

Zij $\mathcal{C}$ bij de volgende definities een code over $\mathbb{F}_q$.

Definitie 2.13. *Een voortbrengermatrix van $\mathcal{C} \subset \mathbb{F}_q^n$ is een matrix van de vorm*

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix},$$

waarbij de $\mathbf{v}_i \in \mathbb{F}_q^n, 1 \leq i \leq k$ een basis vormen voor $\mathcal{C}$. We schrijven dan $\mathcal{C} = \operatorname{im} G$.

Definitie 2.14. *De duale code van $\mathcal{C}$, genoteerd met $\mathcal{C}^\perp$, is de lineaire deelruimte*

$$\mathcal{C}^\perp := \left\{ \mathbf{w} \in \mathbb{F}_q^n \;\middle|\; \mathbf{v}\mathbf{w}^\top = 0 \text{ voor alle } \mathbf{v} \in \mathcal{C} \right\}$$

Definitie 2.15. *Een pariteitsmatrix van $\mathcal{C} \subset \mathbb{F}_q^n$ is een matrix van de vorm*

$$\begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{n-k} \end{pmatrix},$$

waarbij $k = \dim_{\mathbb{F}_q} \mathcal{C}$ en de $\mathbf{w}_i \in \mathbb{F}_q^n, 1 \leq i \leq n-k$ een basis vormen voor $\mathcal{C}^\perp$. We schrijven dan:

$$\mathcal{C} = \ker \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{n-k} \end{pmatrix}^\top$$

Het is evident dat zowel een voortbrengermatrix als een pariteitsmatrix de bijbehorende code uniek bepaalt.

Stelling 2.16. *Zijn $G, G' \in \mathbb{F}_q^{k \times n}$ voortbrengermatrices van een code $\mathcal{C} \subset \mathbb{F}_q^n$, dan is er een $U \in \mathbb{F}_q^{k \times k}$ met $\det U \neq 0$ zodanig dat $G' = UG$.*

Bewijs. Zij $G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix}$ en $G' = \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_k \end{pmatrix}$. De $\mathbf{v}_i$ en $\mathbf{w}_i$ (met $1 \leq i \leq k$) zijn bases van $\mathcal{C}$, dus kunnen we schrijven $\mathbf{w}_i = \mathbf{u}_i G$ voor zekere $\mathbf{u}_i \in \mathbb{F}_q^k$. Hieruit volgt dan dat de keuze $U := \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_k \end{pmatrix}$ voldoet. Tenslotte zien we dat de lineaire onafhankelijkheid van de $\mathbf{w}_i$ impliceert dat ook de $\mathbf{u}_i$ lineair onafhankelijk zijn, dus $\det U \neq 0$. □

Definitie 2.17. *Een monomiale matrix is een vierkante matrix waarvan alle rijen en alle kolommen precies één element bevatten dat van nul verschilt.*

Een permutatiematrix is een vierkante matrix waarvan alle rijen en alle kolommen precies één element bevatten dat gelijk is aan één en voor de rest alleen nullen bevatten.

Definitie 2.18. *Twee codes $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}_q^n$ zijn equivalent (genoteerd als $\mathcal{C}_1 \sim \mathcal{C}_2$) als er matrices G_1, G_2 bestaan met $\mathcal{C}_1 = \operatorname{im} G_1$ en $\mathcal{C}_2 = \operatorname{im} G_2$ en er een monomiale matrix M bestaat zodanig dat $G_2 = G_1 M$.*

Het is eenvoudig na te gaan dat bovenstaande daadwerkelijk een equivalentierelatie definieert. Een sterkere equivalentierelatie is de permutatie-equivalentie:

Definitie 2.19. *Twee codes $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}_q^n$ zijn permutatie-equivalent als er matrices G_1, G_2 bestaan met $\mathcal{C}_1 = \operatorname{im} G_1$ en $\mathcal{C}_2 = \operatorname{im} G_2$ en er een permutatiematrix M bestaat zodanig dat $G_2 = G_1 M$.*

Combineren we stelling 2.16 met definities 2.18/2.19, dan volgt:

Gevolg 2.20. *Zijn $\mathcal{C}_1 = \operatorname{im} G_1$ en $\mathcal{C}_2 = \operatorname{im} G_2$ twee codes met $G_1, G_2 \in \mathbb{F}_q^{k\times n}$ matrices van volle rang, dus $\dim_{\mathbb{F}_q} \mathcal{C}_1 = \dim_{\mathbb{F}_q} \mathcal{C}_2 = k$. Dan zijn $\mathcal{C}_1$ en $\mathcal{C}_2$ equivalent (permutatie-equivalent) dan en slechts dan als er een niet-singuliere matrix $U \in \mathbb{F}_q^{k\times k}$ bestaat en een monomiale matrix (permutatiematrix) $M \in \mathbb{F}_q^{n\times n}$ zodanig dat $G_2 = UG_1M$.*

Om in de praktijk te controleren of twee voortbrengermatrices bij (permutatie-)equivalente codes horen zijn de volgende lemma's handig:

Lemma 2.21. *Zijn $G_1, G_2 \in \mathbb{F}_q^{k\times n}$ matrices van de vorm $\begin{pmatrix} I_k & A \end{pmatrix}$, waarbij I_k de k-bij-k-identiteitsmatrix is en $A \in \mathbb{F}_q^{k\times(n-k)}$ een willekeurige matrix. Kunnen we schrijven $G_2 = UG_1M$, waarbij $M \in \mathbb{F}_q^{n\times n}$ een monomiale (permutatie-) matrix is, dan geldt:*

$$U = \begin{pmatrix} G_{11} & G_{12} & \cdots & G_{1k} \\ G_{21} & G_{22} & \cdots & G_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ G_{k1} & G_{k2} & \cdots & G_{kk} \end{pmatrix}^{-1}$$

waarbij we $G := G_1M$ genomen hebben.

Bewijs. We kunnen als gegeven G_2 schrijven als $G_2 = \begin{pmatrix} I_k & A \end{pmatrix}$. Schrijf $G_1M = \begin{pmatrix} A_1 & A_2 \end{pmatrix}$ met $A_1 \in \mathbb{F}_q^{k\times k}$ en $A_2 \in \mathbb{F}_q^{k\times(n-k)}$. Dan hebben we $\begin{pmatrix} I_k & A \end{pmatrix} = G_2 = UG_1M = \begin{pmatrix} UA_1 & UA_2 \end{pmatrix}$ waaruit volgt dat $I_k = UA_1 \Longrightarrow U = A_1^{-1}$. □

Lemma 2.22. *Zijn $G_1, G_2 \in \mathbb{F}_q^{k\times n}$ matrices van volle rang, behorende bij equivalente codes (dus $G_2 = UG_1M$ met U en M zoals in gevolg 2.20). Dan is de Gauss-Jordan-normaalvorm van G_2 gelijk aan die van G_1M.*

Bewijs. Dit is lineaire algebra: de Gauss-Jordan-normaalvorm van twee matrices A, B met dezelfde dimensies is gelijk dan en slechts dan als er een vierkante matrix U bestaat met $\det U \neq 0$ en $A = UB$. □

Tot slot nog enkele definities:

Definitie 2.23. *Het gewicht van een codewoord $\mathbf{v} = (v_1, \ldots, v_n) \in \mathcal{C}$ is $\operatorname{wt}(\mathbf{v}) := \#\{i \mid v_i \neq 0 \text{ en } 1 \leq i \leq n\}$.*

Definitie 2.24. *Zijn $\mathbf{v}, \mathbf{w} \in \mathcal{C}$ codewoorden, dan is de afstand tussen $\mathbf{v}$ en $\mathbf{w}$ gelijk aan $d(\mathbf{v}, \mathbf{w}) := \operatorname{wt}(\mathbf{v} - \mathbf{w})$.*

Definitie 2.25. *We definiëren de afstand van een code $\mathcal{C}$ als $\operatorname{dist} \mathcal{C} := \min_{\mathbf{v}\in\mathcal{C}} \operatorname{wt}(\mathbf{v})$.*

Opmerking 2.26. *Een code $\mathcal{C}$ met lengte n, dimensie k en afstand d wordt ook wel een $[n, k]$-code of $[n, k, d]$-code genoemd.*

Definitie 2.27. *Een MDS-code is een $[n, k, n - k + 1]$-code.*

2.3.1 Reed-Solomon-codes

Een voorbeeld van een familie van codes wordt geleverd door de zogenaamde *Reed-Solomon-codes*.

Definitie 2.28. *De Reed-Solomon-code* $\mathrm{RS}_q(d,\alpha,m)$*, waarbij* $d \in \mathbb{Z}_{>0}, \alpha \in \mathbb{F}_q^*, m \in \mathbb{Z}_{>0}$ *is een* $[q-1,k,q-k]$*-code die wordt gegeven door de pariteitsmatrix:*

$$\mathrm{RS}_q(d,\alpha,m) := \ker \begin{pmatrix} 1 & \alpha^m & \alpha^{2m} & \cdots & \alpha^{(q-2)m} \\ 1 & \alpha^{m+1} & \alpha^{2(m+1)} & \cdots & \alpha^{(q-2)(m+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{m+d-2} & \alpha^{2(m+d-2)} & \cdots & \alpha^{(q-2)(m+d-2)} \end{pmatrix}^\top \subset \mathbb{F}_q^{q-1}$$

Om ons voor te bereiden op algebraïsche krommen bespreken we nu de *narrow-sense Reed-Solomon-codes*. Dit is een subklasse van de Reed-Solomon-codes met een elegante definitie. De gedaante waarin deze codes verschijnen zal bovendien maatgevend blijken te zijn voor de definitie van onze algebraïsch-geometrische codes.

Definitie 2.29. *Zij* $0 \leq k \leq q-1$*. We definiëren*

$$\mathcal{P}_k := \{\, f \in \mathbb{F}_q[x] \mid \text{de graad van } f \text{ is lager dan } k\} \cup \{0\}$$

Zij α *een voortbrenger van de multiplicatieve groep* $\mathbb{F}_q^*$*. De narrow sense Reed-Solomon-code* $\mathrm{RNS}_q(\alpha,k)$ *is als volgt gedefinieerd:*

$$\mathrm{RNS}_q(\alpha,k) := \left\{ \big(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})\big) \in \mathbb{F}_q^{q-1} \;\middle|\; f \in \mathcal{P}_k \right\} \subset \mathbb{F}_q^{q-1}$$

Opmerking 2.30. *Merk op dat een andere keuze voor een voortbrenger* α *leidt tot een permutatie-equivalente code. De rij* $\{\alpha^j\}_{j=0}^{j=q-2}$ *doorloopt namelijk alle elementen in de groep* $\mathbb{F}_q^*$*. We krijgen dus codes die op een permutatie van de kolommen na gelijk zijn, vandaar dat we ook* $\mathrm{RNS}_q(k)$ *schrijven.*

Zij $j < k$ en stel $\mathbf{f}_j = (1, \alpha^j, \alpha^{2j}, \ldots, \alpha^{(q-2)j}) \in \mathrm{RNS}_q(\alpha,k)$. We beweren dat een basis voor $\mathrm{RNS}_q(\alpha,k)$ wordt gegeven door $\{\mathbf{f}_0, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}\}$. Hiertoe moet nog worden aangetoond dat de $\mathbf{f}_j$'s lineair onafhankelijk zijn. Dit volgt uit het feit dat de matrix

$$\begin{pmatrix} \mathbf{f}_0 \\ \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{(q-2)} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{pmatrix}$$

volle rang heeft (de k-bij-k-submatrices zijn Vandermonde-matrices) en dus een voortbrengermatrix is voor $\mathrm{RNS}_q(\alpha,k)$.

2.4 Algebraïsch-geometrische codes

We richten ons nu op algebraïsche krommen. Omdat codes deelverzamelingen zijn van een $\mathbb{F}_q^n$ beschouwen we krommen over een eindig lichaam $\mathbb{F}_q$. Zij voor deze hele paragraaf C een gladde kromme over $\mathbb{F}_q$.

Definitie 2.31. *De algebraïsch-geometrische code* $\mathcal{C}(\mathcal{P},D)$ *is als volgt gedefinieerd:*

$$\mathcal{C}(\mathcal{P},D) := \big\{(f(P_1), f(P_2), \ldots, f(P_n)) \in \mathbb{F}_q^n : f \in L(D)\big\}$$

waarbij $D \in \operatorname{div} C$ *een divisor over* $\mathbb{F}_q$ *op* C *en* $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset C(\mathbb{F}_q)$ *een verzameling* $\mathbb{F}_q$*-rationale punten op* C *met* $\operatorname{supp}(D) \cap \mathcal{P} = \varnothing$*.*

Merk de analogie met de definitie van de *narrow-sense Reed-Solomon-codes* op. Merk ook op dat bovenstaande definitie niet uitsluit dat $\mathcal{C}(\mathcal{P},D)$ leeg is. Dit is bijvoorbeeld zeker het geval als $\deg D < 0$. Een licht gewijzigde definitie gebruikt een afbeelding α, gedefinieerd als volgt:

$$\begin{aligned} \alpha : L(D) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), f(P_2), \ldots, f(P_n)) \end{aligned}$$

Merk op dat $f \in L(D)$ betekent dat f regulier is in punten buiten $\mathrm{supp}(D)$. Bovenstaande evaluatieafbeelding is dus goed 1gedefinieerd. Dan geldt $\mathcal{C}(\mathcal{P}, D) := \mathrm{im}(\alpha) \subset \mathbb{F}_q$.

Zij $\{f_1, \ldots, f_k\}$ een basis voor $L(D)$. Dan spant $\{\alpha(f_1), \ldots, \alpha(f_k)\}$ de code $\mathcal{C}(\mathcal{P}, D)$ op. Het volgt dat we een basis voor $\mathcal{C}(\mathcal{P}, D)$ kunnen verkrijgen door een geschikte deelverzameling te kiezen van $\{\alpha(f_1), \ldots, \alpha(f_k)\}$. We zullen nu laten zien dat α onder soepele voorwaarden injectief is en de verzameling $\{\alpha(f_1), \ldots, \alpha(f_k)\}$ zelf een basis is van $\mathcal{C}(\mathcal{P}, D)$. Neem $\mathcal{P}$ en D als hiervoor.

Stelling 2.32. *Neem aan dat $2g - 2 < \deg D < n$, waarbij $g = g(C)$. De code $\mathcal{C}(\mathcal{P}, D)$ heeft parameters $[n, k, d]$ met $k = \ell(D) = \deg D + 1 - g$ en $d \geq n - \deg D = n - k + 1 - g$*

Bewijs. We hadden reeds $k = \dim_{\mathbb{F}_q} \mathcal{C} \leq \dim_{\mathbb{F}_q} L(D) = \deg D + 1 - g$ volgens Riemann-Roch. Neem een functie $f \in L(D)$ met $f \neq 0$ en stel dat $\mathbf{v} := \alpha(f)$ een vector is met r componenten gelijk aan nul. Dus $f(P_{i_j}) = 0$ voor $j = 1, 2, \ldots, r$. Dan geldt dat $f \in L(D - P_{i_1} - P_{i_2} - \ldots - P_{i_r})$ en de laatstgenoemde ruimte is dus niet-leeg. Dit impliceert dat $\deg(D - P_{i_1} - P_{i_2} - \ldots - P_{i_r}) \geq 0$ oftewel $r \leq \deg D < n$. Dit bewijst dat $\mathbf{v}$ niet de nulvector is. Dus de dimensie k is $\ell(D) = \deg D + 1 - g$.
Voor de afstand gebruiken we hetzelfde gegeven, namelijk dat het aantal nullen in een vector $\alpha(g)$ maximaal gelijk is aan $\deg D$, dus het aantal niet-nul componenten minstens gelijk aan $n - \deg D$. Combineren we dit met $k = \deg D + 1 - g$ dan krijgen we het tweede deel van de ongelijkheid voor d. □

Neem een puntenverzameling $\mathcal{P}$ en een divisor D met $2g(C) - 2 < \deg D < n$ zodanig dat $\mathrm{supp}(D) \cap \mathcal{P} = \varnothing$. We kunnen dan stelling 2.32 gebruiken om expliciet een voortbrengermatrix voor $\mathcal{C}(\mathcal{P}, D)$ te construeren. Als namelijk $\{f_1, f_2, \ldots, f_k\}$ een basis is voor $L(D)$, dan is $\{\alpha(f_1), \alpha(f_2), \ldots, \alpha(f_k)\}$ een basis voor $\mathcal{C}(\mathcal{P}, D)$. Dit leidt tot de volgende stelling.

Stelling 2.33. *Een voortbrengermatrix voor $\mathcal{C}(P, \mathcal{D})$ is:*

$$\begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix}$$

Opmerking 2.34. De code $\mathcal{C}(\mathcal{P}, D)$ is bepaald tot op (permutatie-)equivalentie. Er is namelijk een zekere vrijheid in de keuze van de voortbrengermatrix. Een andere indexering van de punten in $\mathcal{P}$ leidt tot een permutatie van de kolommen van bovenstaande voortbrengermatrix. Dit leidt tot een permutatie-equivalente code en dus tot een equivalente code. Het netste zou zijn om $\mathcal{C}(\mathcal{P}, D)$ op te vatten als een equivalentieklasse van codes. Als niettemin ergens in deze scriptie een uitspraak wordt gedaan over "de" code $\mathcal{C}(\mathcal{P}, D)$, betekent dit dat de uitspraak geldig is voor elke ordening van $\mathcal{P}$.

Ook de basis van $L(D)$ kan men op veel verschillende manieren kiezen, maar dit heeft geen invloed op de resulterende code. Merk hiertoe op dat twee verschillende basiskeuzen leiden tot voortbrengermatrices G, G' die gerelateerd zijn door $G = UG'$ met $U \in \mathbb{F}_q^{k \times k}$ een niet-singuliere matrix. Dus G en G' leveren dezelfde code op.

De uitdrukking $\mathcal{C}(\mathcal{P}, D)$ had in het voorgaande alleen betekenis als $\mathrm{supp}(D) \cap \mathcal{P} = \varnothing$. Echter, we kunnen haar ook een betekenis toekennen als niet aan deze voorwaarde voldaan is. De code $\mathcal{C}(\mathcal{P}, D)$ is dan echter slechts tot op equivalentie bepaald (alternatief kunnen we haar opvatten als een equivalentieklasse van codes). Hiertoe geven we een uitbreiding van definitie 2.31, die in het oude geval precies hetzelfde resultaat oplevert.

Definitie 2.35 (Uitgebreide definitie). *De algebraïsch-geometrische code $\mathcal{C}(\mathcal{P}, D)$ is als volgt gedefinieerd:*

$$\mathcal{C}(\mathcal{P}, D) := \left\{ ((t_1^{e_1} f)(P_1), (t_2^{e_2} f)(P_2), \ldots, (t_n^{e_n} f)(P_n)) \in \mathbb{F}_q^n : f \in L(D) \right\}$$

waarbij $D \in \mathrm{div}\, C$ een divisor over $\mathbb{F}_q$ op C is, de t_i lokale uniformisanten zijn in P_i en verder geldt dat $e_i = v_{P_i}(D)$, en $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset C(\mathbb{F}_q)$ een verzameling $\mathbb{F}_q$-rationale punten op C.

Merk op dat deze definitie inderdaad onderling verdraagbaar is met de oorspronkelijke definitie, aangezien $e_i = 0$ voor de punten P_i die niet bevat zijn in $\mathrm{supp}(D)$. Wel moeten we controleren dat $\mathcal{C}(\mathcal{P}, D)$ inderdaad een code is. Merk op dat de afbeelding $\alpha : L(D) \longrightarrow \mathbb{F}_q$ gedefinieerd door $\alpha(f) = (t_1^{e_1} f(P_1), t_2^{e_2} f(P_2), \ldots, t_n^{e_n} f(P_n))$ bij een vaste keuze van de t_i inderdaad een lineaire afbeelding is: het beeld $\mathcal{C}(\mathcal{P}, D) \subset \mathbb{F}_q^n$ is dus een lineaire ruimte. Een andere keuze van lokale uniformisanten t_i leidt tot een equivalente code.

Stelling 2.36. *Neem aan dat $2g(C) - 2 < \deg D < n$. De code $\mathcal{C}(\mathcal{P}, D)$ heeft parameters $[n, k, d]$ met $k = \ell(D) = \deg D + 1 - g$ en $d \geq n - \deg D = n - k + 1 - g$*

Bewijs. Het bewijs gaat hetzelfde als dat van stelling 2.32. □

Opmerking 2.37. We kunnen uit het voorgaande een belangrijke conclusie trekken, namelijk dat een kromme waarvan het aantal $\mathbb{F}_q$-rationale punten n bedraagt, ons codes over $\mathbb{F}_q$ kan leveren van maximaal lengte n.

2.4.1 MDS-codes en AMDS-codes

Een ander eenvoudig gevolg van stelling 2.32 heeft betrekking op MDS-codes. Codes afkomstig van krommen met een vergelijking van voldoend lage graad zijn MDS.

Gevolg 2.38. *Zij $C = V(F)$ een gladde projectieve kromme over $\mathbb{F}_q$ met $\deg F \leq 2$ en zij $\mathcal{P} \subset C(\mathbb{F}_q)$. Zij verder D een divisor over $\mathbb{F}_q$ op C met $0 \leq \deg D < \#\mathcal{P}$ en $\mathrm{supp}(D) \cap \mathcal{P} = \varnothing$. Dan is $\mathcal{C} := \mathcal{C}(\mathcal{P}, D)$ een MDS-code.*

Bewijs. Roep in herinnering dat een $[n, k, d]$-code een MDS-code is als $d = n - k + 1$. Zij nu $n = \#\mathcal{P}$ en $k = \deg D + 1$. Merk op dat uit $\deg F \leq 2$ volgt dat $g(C) = 0$. Volgens stelling 2.32 geldt nu dat $\mathcal{C}$ een $[n, k]$-code is. Volgens de Singleton-grens geldt dan dat $d \leq n - k + 1$ en bij gelijkheid is $\mathcal{C}$ een MDS-code. Weer volgens stelling 2.32 geldt dat $d \geq \#\mathcal{P} - \deg D = n - k + 1$. Dus $\mathcal{C}$ is een MDS-code. □

Over MDS-codes bestaat een belangrijk vermoeden, dat de toepasselijke naam "MDS-vermoeden" draagt:

Vermoeden 2.39 (MDS-vermoeden). *Zij $\mathcal{C}$ een $[n, k]$-MDS-code over $\mathbb{F}_q$, niet gelijk aan één van de volgende codes:*

1. $\mathbb{F}_q^n$;
2. $\mathrm{im}\,(1\ 1\ \cdots\ 1) \subset \mathbb{F}_q^n$, *de binaire repetitiecode;*
3. $\left\{ (\mathbf{v} \quad \sigma(\mathbf{v})) \;\middle|\; \mathbf{v} \in \mathbb{F}_2^{n-1} \right\}$, *hier stelt $\sigma(\mathbf{v})$ de pariteit van $\mathbf{v}$ voor, d.w.z. het aantal componenten van $\mathbf{v}$ dat van nul verschilt modulo 2;*

dan geldt $n \leq q + 2$. Als q oneven is geldt de sterkere grens $n \leq q + 1$.

Als we dit vermoeden accepteren hebben we dus een bovengrens aan de lengte van MDS-codes over een gegeven lichaam $\mathbb{F}_q$. Het is een bekend feit dat er voor elk eindig lichaam $\mathbb{F}_q$ een MDS-code bestaat die aan deze bovengrens voldoet. Dit valt als volgt in te zien. Verderop zullen we zien dat krommen van geslacht nul *isomorf* zijn aan de kromme $Z = 0$, hetgeen betekent dat voor een gladde kromme $C/\mathbb{F}_q$ met $g(C) = 0$ geldt dat $\#C(\mathbb{F}_q) = q + 1$. Opmerking 2.37 in combinatie met gevolg 2.38 vertelt ons dan dat we C kunnen gebruiken om een MDS-code over $\mathbb{F}_q$ van lengte $q + 1$ te construeren. We hebben daarvoor de uitgebreide definitie 2.35 nodig, daar we niet langer kunnen eisen dat $\mathcal{P} \cap \mathrm{supp}(D) = \varnothing$.

De Singleton-grens vertelt ons dat voor elke $[n, k, d]$-code geldt $d \leq n - k + 1$. Aan stelling 2.32 zien we dat gelijkheid optreedt voor gladde krommen met $g = 0$ en geschikte keuzes voor $\mathcal{P}$ en D. MDS-codes zijn in zekere zin optimaal. We voeren een begrip in om aan te geven "hoe ver" een code verwijderd is van optimaliteit in deze zin.

Definitie 2.40. *Het (Singleton-)defect δ van een code is $\delta := n - k + 1 - d$.*

Merk op dat een MDS-code defect $\delta = 0$ heeft.

Definitie 2.41. *Een AMDS-code is een code met defect $\delta = 1$.*

Blijkens stelling 2.32 kunnen we AMDS-codes (de afkorting betekent *Almost Maximum Distance Separated*) krijgen van krommen met geslacht één. We kunnen ons afvragen of de AMDS-codes de bovengrens die we voor de MDS-codes vonden kunnen overstijgen. Dit komt blijkens opmerking 2.37 neer op het vinden van krommen van geslacht één over $\mathbb{F}_q$ met meer dan $q+1$ punten. Deze krommen blijken in overvloed te bestaan:

Definitie 2.42. *Zij voor $q = p^r$ (p een priemgetal) het getal N_q gedefinieerd als:*

$$N_q := \begin{cases} q + \lfloor 2\sqrt{q} \rfloor \text{ voor } r \text{ oneven, } r \geq 3 \text{ en } \lfloor 2\sqrt{q} \rfloor \text{ deelbaar door } p \\ q + 1 + \lfloor 2\sqrt{q} \rfloor \text{ anders} \end{cases}$$

Stelling 2.43. *Zij $C/\mathbb{F}_q$ een gladde kromme van geslacht één. Dan geldt $\#C(\mathbb{F}_q) \leq N_q$. Bovendien bestaat er voor elk eindig lichaam $\mathbb{F}_q$ een gladde kromme $\widetilde{C}/\mathbb{F}_q$ met $\#\widetilde{C}(\mathbb{F}_q) = N_q$.*

Bewijs. Het bewijs maakt gebruik van zeer gevorderde ideeën uit de algebraïsche meetkunde. Een inleiding tot de ideeën uit het bewijs en een verdere verwijzing is te vinden in [vLvdG, §2.4]. □

2.5 Voorbeelden van codes

De eerste codes die we bekijken zijn afkomstig van de kromme $C/\mathbb{F}_5$ gegeven door $X^2 + Y^2 - Z^2$. De verzameling $\mathbb{F}_5$-rationale punten van deze krommen is $\{(0:1:\pm 1), (1:\pm 2:0), (1:0:\pm 1)\}$. Zij $P = (0:1:1)$.

We nemen onze divisor D gelijk aan P en stellen

$$\mathcal{P} = \{(0:1:-1), (1:2:0), (1:-2:0)\}.$$

Om met deze D en $\mathcal{P}$ een code te maken moeten we een basis vinden voor de Riemann-Roch-ruimte $L(D)$. Het vinden van zulke bases is een vraagstelling op zich, waar hier geen ruimte voor is. We stellen onszelf dus tevreden met het controleren van de bewering dat $\{1, Y/(X+Y-Z)\}$ een basis is voor $L(D)$.

Merk op dat $f \in L(D)$ zit dan en slechts dan als f overal op de kromme regulier is behalve mogelijkerwijs in P waar moet gelden dat $v_P(f) \geq -1$. We controleren eerst dat $f = Y/(X+Y-Z)$ daadwerkelijk in $L(D)$ zit. De noemer heeft volgens de stelling van Bézout twee nulpunten gemeen met de kromme, dit zijn dus precies $(1:0:1)$ en het punt P zelf. We willen de orde van f in deze punten onderzoeken en gaan daartoe over op affiene coördinaten. We schrijven dus $f = y/(x+y-1)$. Stelling 1.25 vertelt ons dat $\mathfrak{m}_P = (x, y-1)$.

Opmerking 2.44. In alles wat volgt zullen we de gelijkheid van twee elementen uit het functielichaam $k(C)$ van een kromme noteren met het "="-teken. Met andere woorden: we rekenen vanaf nu exclusief in $k(C)$, zonder terug te vallen op de "moederlichamen" $k(x,y)$ en $k_0(X,Y,Z)$ (het lichaam van homogene rationale functies van graad nul), waarvanuit $k(C)$ was gedefinieerd.

Merk op dat $x^2 = -(y-1)(y+1) \Longrightarrow (y-1) = -x^2/(y+1)$. Dus x is een lokale uniformisant in P. We schrijven nu f als

$$\frac{y}{x+y-1} = \frac{y}{x - x^2/(y+1)} = \frac{y}{x} \cdot \frac{y+1}{-x+y+1}$$

Hieraan zien we meteen dat $v_P(f) = -1$, omdat $v_P(x^{-1}) = -1$. Voorts laten we zien dat f in $(1:0:1)$ geen pool heeft, door f iets anders te schrijven:

$$\frac{y}{x+y-1} = \frac{y}{y - y^2/(x+1)} = \frac{x+1}{x-y+1}$$

en deze laatste uitdrukking heeft in $(1,0)$ (dat correspondeert met het projectieve punt $(1:0:1)$) de waarde $2/2 = 1$. Deze twee punten waren de enige "probleempunten" en zijn dus allebei in orde.

Nu moeten we alleen nog aantonen dat de elementen van onze basis lineair onafhankelijk zijn over $\mathbb{F}_5$. Neem hiertoe aan dat $a + by/(x + y - 1) = 0$. Dan geldt $(ax + (a + b)y - a)/(x + y - 1) = 0 \implies ax + (a + b)y - a = 0$. Dit geeft onmiddelijk dat $a = 0$ en dus ook $b = 0$.

Vervolgens kunnen we de basis evalueren in de punten van $\mathcal{P}$ en kunnen we stelling 2.33 gebruiken om een voortbrengermatrix voor $\mathcal{C}(\mathcal{P}, D)$ te vinden. Directe evaluatie in de punten van $\mathcal{P}$ levert geen problemen op: $f((0 : 1 : -1)) = 3$, $f((1 : 2 : 0)) = 4$ en $f((1 : -2 : 0)) = 2$. Dit levert de gedaante voor $\mathcal{C}(\mathcal{P}, D)$:

$$\mathcal{C}(\mathcal{P}, D) := \operatorname{im} \begin{pmatrix} 1 & 1 & 1 \\ 3 & 4 & 2 \end{pmatrix}$$

Volgens stelling 2.38 moet $\mathcal{C}(\mathcal{P}, D)$ een MDS-code zijn. Om dit te controleren gebruiken we de volgende stelling:

Stelling 2.45. *Zij $\mathcal{C}$ een code met $\mathcal{C} = \operatorname{im}(G)$, $G \in \mathbb{F}_q^{k \times n}$. $\mathcal{C}$ is een MDS-code dan en slechts dan als alle k-bij-k-minoren van G van nul verschillen.*

Bewijs. [Roman, thm. 5.3.4.] □

Het is snel na te gaan dat G voldoet aan bovenstaande voorwaarde, $\mathcal{C}(\mathcal{P}, D)$ is dus een MDS-code.

Voegen we nu de overige twee punten aan onze $\mathcal{P}$ toe, dan krijgen we

$$\mathcal{P}' := \{(0 : 1 : -1), (1 : 2 : 0), (1 : -2 : 0), (1 : 0 : -1), (1 : 0 : 1)\}$$

We vinden $f((1 : 0 : -1)) = 0$ en $f((1 : 0 : 1)) = 1$, hetgeen ons de volgende code levert:

$$\mathcal{C}(\mathcal{P}', D) := \operatorname{im} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 4 & 2 & 0 & 1 \end{pmatrix}$$

Ook deze code moet volgens stelling 2.38 een MDS-code zijn. Dit is wederom eenvoudig in te zien door de specifieke vorm van de matrix.

Voorbeeld 2.46. Tenslotte zullen we gaan zien dat Reed-Solomon-codes ook algebraïsch-geometrische codes zijn. Zij $\mathcal{X}/\mathbb{F}_q$ de gladde kromme gegeven door $Z = 0$. $\mathcal{X}$ is een gladde kromme van geslacht nul. De punten op deze kromme zijn van de vorm $(x : y : 0)$, waarbij $x, y \in \mathbb{F}_q$ en $xy \neq 0$. Noteer de elementen van $\mathbb{F}_q$ met $\alpha_0 := 0, \alpha_1 := 1, \alpha_2, \ldots, \alpha_{q-1}$. De $\mathbb{F}_q$-rationale punten van $\mathcal{X}$ zijn dan

$$\mathcal{X}(\mathbb{F}_q) = \{(1 : 0 : 0), (\alpha_0 : 1 : 0), (\alpha_1 : 1 : 0), \ldots, (\alpha_{q-1} : 1 : 0)\}$$

Stel $P_\infty := (1 : 0 : 0)$ en neem $D := (k - 1)P_\infty$ met $1 \leq k \leq q - 1$. Merk op dat $\deg D = k - 1$ en dus $\ell(D) = k$ volgens Riemann-Roch. Stel $P_i := (\alpha_i : 1 : 0)$. We nemen onze puntenverzameling $\mathcal{P}$ gelijk aan $\mathcal{P} := \{P_1, P_2, \ldots, P_{q-1}\}$. Na controle dat $\mathcal{P} \cap \operatorname{supp}(D) = \varnothing$ kunnen we de code $\mathcal{C}_{q,k} := \mathcal{C}(\mathcal{P}, D)$ vormen en aan de hand van stelling 2.32 concluderen dat $\mathcal{C}_{q,k}$ een $[q - 1, k, q - k]$-code is over $\mathbb{F}_q$.

We stellen nu dat een basis voor $L(D)$ is:

$$\left\{1, \frac{x}{y}, \frac{x^2}{y^2}, \ldots, \frac{x^{k-1}}{y^{k-1}}\right\}$$

We moeten nu wederom controleren (i) dat bovenstaande rationale functies in $(1 : 0 : 0)$ hooguit een $(k-1)$-voudige pool hebben en in alle andere punten van $\mathcal{X}$ regulier zijn; en (ii) dat ze lineair onafhankelijk zijn over $\mathbb{F}_q$.

(i) Merk op dat de rationale functie X^i/Y^i alleen polen heeft als $Y = 0$. Een snijpunt $(\xi : \eta : \zeta)$ voldoet dus aan $\eta = 0$, $\zeta = 0$, dus het enige snijpunt is in $P_\infty = (1 : 0 : 0)$. Vervolgens bepalen we de orde van de pool van X^i/Y^i in P_∞. We schakelen over op de affiene deelverzameling $X \neq 0$ met coördinaten $u = Y/X$ en $v = Z/X$. $\mathcal{X}$ heeft dan de vergelijking $v = 0$ en P_∞ is het punt $(0, 0)$. We weten dat u of v een lokale uniformisant is in P_∞ (zie opmerking 1.28). Maar $v = 0$, dus we kunnen nooit $f \in \mathcal{O}_{P_\infty}^*$ en $r \in \mathbb{Z}_{\geq 0}$ vinden zodanig dat $u = fv^r$. Derhalve is u een lokale uniformisant. Hieruit volgt dat $v_{P_\infty}(X^i/Y^i) = v_{P_\infty} u^{-i} = -i$. Dus inderdaad zitten bovenstaande functies in $L(D)$.

(ii) Neem aan dat

$$f = \sum_{j=0}^{k-1} a_j \frac{X^j}{Y^j} \;=\; 0 \;\text{ in } \mathbb{F}_q(\mathcal{X})$$

Geschreven als quotiënt van homogene polynomen hebben we $f = G/H$ met $G = \sum_{j=0}^{k-1} a_j X^j Y^{k-1-j}$ en $H = Y^{k-1}$. $G/H \sim 0$, dus $G \in (Z)$. Dit kan alleen als alle a_i gelijk zijn aan nul.

Met behulp van bovenstaande basis vinden we dus de elementen van $L(D)$ verschillend van nul precies de volgende functies zijn:

$$\sum_{j=0}^{k-1} c_j \frac{x^j}{y^j}$$

Onze code $\mathcal{C}(\mathcal{P}, D)$ wordt dan:

$$\mathcal{C}(\mathcal{P}, D) = \left\{ (f(P_1), f(P_2), \ldots, f(P_{q-1})) : f = \sum_{j=0}^{k-1} c_j \frac{x^j}{y^j},\ c_i \in \mathbb{F}_q \right\}$$

Zetten we de punten van $\mathcal{P}$ zoals boven in de vorm $(\alpha_i : 1 : 0)$, dan zien we dat $f(P_i) = \sum_{j=0}^{k-1} c_j \alpha_i^j$ een polynoom is in α_i alleen. Door alle $f \in L(D)$ te doorlopen, krijgen we alle polynomen van graad $\leq k-1$. We kunnen onze code dus ook beschrijven als:

$$\mathcal{C}(\mathcal{P}, D) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{q-1})) : f \in \mathcal{P}_k\}$$

waar $\mathcal{P}_k$ weer de verzameling van alle polynomen van graad $< k$ is. Dit is de *narrow sense Reed-Solomon-code* $\mathrm{RNS}_q(k)$ (zie opmerking 2.30).

2.6 Morfismen tussen krommen

In deze paragraaf bespreken we wat er met algebraïsch-geometrische codes gebeurt onder transformaties van de onderliggende krommen. Om het begrip "transformaties" in de vorige zin precies te maken hebben we eerst het concept van de rationale afbeelding nodig.

Definitie 2.47. *Zij $C/k \subset \mathbb{P}^2(K)$ een projectieve kromme. Een rationale afbeelding $\varphi : C \longrightarrow \mathbb{P}^m$ over k wordt gegeven door $m+1$ rationale functies $\{f_0, f_1, \ldots, f_m\}$ met $f_i \in k(C)$ en niet alle f_i gelijk aan de nulfunctie. We noteren φ ook wel met $\varphi = (f_0 : f_1 : \cdots : f_m)$. Twee rationale afbeeldingen $(f_0 : f_1 : \cdots : f_m)$ en $(g_0 : g_1 : \cdots : g_m)$, met $f_i, g_i \in k(C)$, definiëren dezelfde rationale afbeelding dan en slechts dan als er een $h \in k(C)^*$ bestaat zodanig dat $g_i = hf_i$ voor alle i.*

We kunnen elke rationale afbeelding ook uitdrukken met homogene polynomen. Hiertoe vermenigvuldigen we alle f_i, geschreven als quotiënten van homogene polynomen $f_i = G_i/H_i$, met het product van hun noemers. Een rationale functie wordt dan geschreven als een uitdrukking van de vorm $(F_0 : F_1 : \cdots : F_m)$ met $F_i \in k[X, Y, Z]$ homogene polynomen van gelijke graad. Merk hierbij op dat de F_i zelf *niet* in $k(C)$ zitten.

Definitie 2.48. *Zij $C \subset \mathbb{P}^2(K)$ een projectieve kromme en $P \in C$ een punt op de kromme. Een rationale afbeelding $\varphi : C \longrightarrow \mathbb{P}^m$ over k is regulier in P als φ kan worden geschreven als $\varphi = (f_0 : f_1 : \cdots : f_m)$ met $f_i \in \mathcal{O}_P$ voor alle i en $f_i(P) \neq 0$ voor tenminste één i. De afbeelding φ is regulier als ze in alle punten van C regulier is.*

Als we $\varphi = (F_0 : F_1 : \cdots : F_m)$ weer in termen van homogene polynomen hebben geschreven is regulariteit in P equivalent met de voorwaarde dat één van de F_i geen nulpunt heeft in P.

In punten waar een rationale afbeelding regulier is kunnen we spreken van de *waarde* van zo'n afbeelding. Zij $\varphi : C \longrightarrow \mathbb{P}^m$ een rationale afbeelding die regulier is in het punt P. Dan kunnen we dus φ schrijven als $\varphi = (f_0 : f_1 : \cdots : f_m)$ met $f_i \in \mathcal{O}_P$ en $f_i(P) \neq 0$ voor zekere i.

Definitie 2.49. *De waarde van φ in P is $\varphi(P) := (f_0(P) : f_1(P) : \cdots : f_m(P))$.*

We kunnen ook hier weer de schrijfwijze in homogene polynomen gebruiken. Als we φ schrijven als een $(m+1)$-tal homogene polynomen $\varphi = (F_0 : F_1 : \cdots : F_m)$, dan stelt $(F_0(P) : F_1(P) : \cdots : F_m(P))$ eenduidig een projectief punt voor.

Stelling 2.50. *Zij C een gladde projectieve kromme en $\varphi : C \longrightarrow \mathbb{P}^m(K)$ een rationale afbeelding. Dan is φ regulier.*

Bewijs. [vLvdG, §2.1]. □

Opmerking 2.51. De voorgaande stelling lijkt niet erg strenge voorwaarden op te leggen aan reguliere afbeeldingen. Men kan zich afvragen of er überhaupt voorbeelden van niet-reguliere afbeeldingen te geven zijn. Hiervoor hebben we volgens stelling 2.50 krommen C nodig die niet glad zijn, zoals de kromme gegeven door $Y^2 - X^3 = 0$ die we al zagen in paragraaf 1.2.2. De afbeelding $\varphi : C \longrightarrow \mathbb{P}^1$ gegeven door $(Y : X)$ is non-regulier in het punt $(0 : 0 : 1)$.

We zijn nu in staat om rationale afbeeldingen tussen krommen te definiëren.

Definitie 2.52. *Zijn C_1, $C_2 \subset \mathbb{P}^2(K)$ projectieve krommen, dan is een rationale afbeelding $\varphi : C_1 \longrightarrow C_2$ gedefinieerd als een rationale afbeelding $\varphi : C_1 \longrightarrow \mathbb{P}^2$ zodanig dat $\varphi(P) \in C_2$ voor alle $P \in C_1$ waar φ regulier is.*

Definitie 2.53. *Een morfisme $\varphi : C_1 \longrightarrow C_2$ over k is een rationale afbeelding over k die overal regulier is.*

Een belangrijke klasse van morfismen is die der isomorfismen.

Definitie 2.54. *Een isomorfisme $\varphi : C_1 \longrightarrow C_2$ (over k) is een morfisme (over k) waarvoor een morfisme $\psi : C_2 \longrightarrow C_1$ (over k) bestaat zodanig dat $\psi \circ \varphi = \mathrm{id}_{C_1}$ en $\varphi \circ \psi = \mathrm{id}_{C_2}$. Als C_1 en C_2 projectieve krommen zijn waartussen een isomorfisme φ (over k) bestaat, dan heten C_1 en C_2 isomorf (over k).*

Het is niet heel lastig om te bewijzen dat isomorfie een equivalentierelatie definieert op de verzameling van krommen over k.

Opmerking 2.55. Met id_C wordt het identiteitsmorfisme bedoeld waarvoor $\mathrm{id}_C(P) = P$ voor alle $P \in C$. Dit morfisme kan bijvoorbeeld worden gegeven als $\mathrm{id}_C = (X : Y : Z)$. In affiene coördinaten $x = X/Z, y = Y/Z$ is dit equivalent met $\mathrm{id}_C = (x : y : 1)$.

Definitie 2.56. *Zij $\varphi : C_1 \longrightarrow C_2$ een morfisme. Zij $D = \sum n_i P_i$ een divisor op C_1. Dan definiëren we $\varphi(D) := \sum n_i \, \varphi(P_i)$.*

Neem nu voor $C_1/\mathbb{F}_q$ en $C_2/\mathbb{F}_q$ twee gladde projectieve krommen waartussen een isomorfisme φ bestaat met inverse ψ. Beschouw $\mathcal{P} = \{P_1, \ldots, P_n\} \subset C_1$ en een divisor $D = \sum n_i P_i$ op C_1 over $\mathbb{F}_q$. Deze leveren ons op de vertrouwde wijze een code. Men kan zich nu afvragen wat er gebeurt als we in plaats hiervan naar C_2 kijken en $\mathcal{P}' := \{\varphi(P) : P \in \mathcal{P}\}$ en $D' := \varphi(D)$ nemen. (Merk op dat we niet eisen dat $\mathrm{supp}(D) \cap \mathcal{P}$ of $\mathrm{supp}(D') \cap \mathcal{P}'$ leeg zijn: met definitie 2.35 in het achterhoofd is dit ook geen enkel probleem.)

Stelling 2.57. *De codes zijn identiek: $\mathcal{C}(\mathcal{P}, D) = \mathcal{C}(\mathcal{P}', D')$.*

Alvorens we deze stelling bewijzen hebben we nog een extra lemma nodig. Het morfisme φ induceert een terugtrekking $\varphi^* : k(C_2) \longrightarrow k(C_1)$ met inverse $\psi^* : k(C_1) \longrightarrow k(C_2)$.

We zullen nu aangeven hoe deze terugtrekking er concreet uitziet. Schrijf $\varphi = (F_0 : F_1 : F_2)$ met F_i homogene polynomen van gelijke graad en zij $f = G/H \in k(C_2)$, dan is $\varphi^*(f) = G(F_0, F_1, F_2)/H(F_0, F_1, F_2)$. In [Shafarevich, §1.4.3] wordt aangetoond dat φ^* en ψ^* zelfs een lichaamsisomorfisme $k(C_1) \cong k(C_2)$ definiëren.

Lemma 2.58. *Zijn C_1/k, $C_2/k \subset \mathbb{P}^2(K)$ projectieve krommen, $P \in C_1$, $f \in k(C_2)$, en zij $\varphi : C_1 \longrightarrow C_2$ een isomorfisme. Dan geldt $v_P(\varphi^* f) = v_{\varphi(P)} f$.*

Bewijs. Zij $t \in k(C_2)$ een lokale uniformisant in $\varphi(P)$. We tonen aan dat $\varphi^* t$ een lokale uniformisant is in P. Hiertoe moeten we aantonen dat iedere $g \in k(C_1)$ te schrijven is als $g = u(\varphi^* t)^r$ met $r \in \mathbb{Z}$ en $u \in \mathcal{O}_P^*$. Omdat $t \in \mathcal{O}_{\varphi(P)}$ een lokale uniformisant is kunnen we $\psi^* g$ schrijven als $\psi^* g = v t^r$ met $r \in \mathbb{Z}$ en $v \in \mathcal{O}_{\varphi(P)}^*$. Passen we links en rechts in deze vergelijking terugtrekking toe en gebruiken we dat φ^* een lichaamsisomorfisme is, dan vinden we $g = \varphi^* v \, (\varphi^* t)^r$. Dit maakt het bewijs compleet, mits we aantonen dat $\varphi^* v$ regulier is in P en $(\varphi^* v)(P) \neq 0$. Dit volgt direct uit $v(\varphi(P)) \neq 0$. □

Nu we hebben aangetoond dat "de orde van een functie in een punt" behouden blijft onder isomorfismen, valt eenvoudig na te gaan dat φ^* en ψ^* de ruimten $L(D')$ en $L(D)$ bijectief op elkaar afbeelden. Zij $\{f_1, f_2, \ldots, f_k\}$ een basis voor $L(D')$. Via φ^* zien we dat $\{\varphi^* f_1, \varphi^* f_2, \ldots, \varphi^* f_k\}$ een basis is van $L(D)$. Om een voortbrengermatrix te construeren moeten we deze bases evalueren in respectievelijk $\mathcal{P}' = \{\varphi(P_1), \varphi(P_2), \ldots, \varphi(P_n)\}$ en $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.

Bewijs. Het bewijs is tenslotte voltooid met de constatering dat de twee resulterende voortbrengermatrices identiek zijn:

$$\begin{pmatrix} \varphi^* f_1(P_1) & \varphi^* f_1(P_2) & \cdots & \varphi^* f_1(P_n) \\ \varphi^* f_2(P_1) & \varphi^* f_2(P_2) & \cdots & \varphi^* f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi^* f_k(P_1) & \varphi^* f_k(P_2) & \cdots & \varphi^* f_k(P_n) \end{pmatrix} = \begin{pmatrix} f_1(\varphi(P_1)) & f_1(\varphi(P_2)) & \cdots & f_1(\varphi(P_n)) \\ f_2(\varphi(P_1)) & f_2(\varphi(P_2)) & \cdots & f_2(\varphi(P_n)) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(\varphi(P_1)) & f_k(\varphi(P_2)) & \cdots & f_k(\varphi(P_n)) \end{pmatrix}$$

□

Stelling 2.59. *Zij $C/\mathbb{F}_q$ een gladde kromme en D, D' lineair equivalente divisoren op C over $\mathbb{F}_q$. Zij $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ een verzameling punten op de kromme met $(\operatorname{supp}(D) \cup \operatorname{supp}(D')) \cap \mathcal{P} = \varnothing$. Dan zijn de codes $\mathcal{C}(\mathcal{P}, D)$ en $\mathcal{C}(\mathcal{P}, D')$ equivalent.*

Bewijs. Neem aan dat $D - D' = (f)$ met $f \in \mathbb{F}_q(C)$. We definiëren de isomorfe afbeeldingen $\pi(g) = fg$ en $\xi(h) = h/f$ zoals in stelling 2.6. Als dus $\{g_1, \ldots, g_k\}$ een basis is voor $L(D)$, dan is $\{fg_1, \ldots, fg_k\}$ een basis voor $L(D')$. We hebben dan de volgende voortbrengermatrices:

$$\mathcal{C}(\mathcal{P}, D) := \operatorname{im} \begin{pmatrix} g_1(P_1) & g_1(P_2) & g_1(P_3) & \cdots & g_1(P_n) \\ g_2(P_1) & g_2(P_2) & g_2(P_3) & \cdots & g_2(P_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_k(P_1) & g_k(P_2) & g_k(P_3) & \cdots & g_k(P_n) \end{pmatrix},$$

$$\mathcal{C}(\mathcal{P}, D') := \operatorname{im} \begin{pmatrix} f(P_1)g_1(P_1) & f(P_2)g_1(P_2) & f(P_3)g_1(P_3) & \cdots & f(P_n)g_1(P_n) \\ f(P_1)g_2(P_1) & f(P_2)g_2(P_2) & f(P_3)g_2(P_3) & \cdots & f(P_n)g_2(P_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f(P_1)g_k(P_1) & f(P_2)g_k(P_2) & f(P_3)g_k(P_3) & \cdots & f(P_n)g_k(P_n) \end{pmatrix}$$

Merk op dat f wegens $(f) = D - D'$ alleen nulpunten en polen kan hebben in $\operatorname{supp}(D) \cup \operatorname{supp}(D')$. Dit betekent dus dat $f(P_i)$ is gedefinieerd en dat geldt $f(P_i) \neq 0$ voor alle i. De tweede matrix kan uit de eerste worden gevormd na een herschaling van de i-de kolom met een factor $f(P_i)$. De twee codes zijn dus equivalent. □

We willen met de aldus verkregen middelen aantonen dat een "grote" klasse van codes verkregen uit krommen van geslacht nul equivalent zijn aan Reed-Solomon-codes. Hiervoor hebben we enkele lemma's nodig.

Lemma 2.60. *Zij $\mathcal{X}/\mathbb{F}_q$ de kromme gegeven door $Z = 0$ en D een divisor over $\mathbb{F}_q$ op $\mathcal{X}$ met $\deg D = 0$. Dan is D een hoofddivisor: er is een $f \in \mathbb{F}_q(\mathcal{X})$ zodanig dat $D = (f)$.*

Bewijs. [Shafarevich, §3.1.1, Example 2]. □

Lemma 2.61. *Zij $C/\mathbb{F}_q$ een gladde kromme van geslacht nul en $\mathcal{X}$ zoals hierboven. Dan zijn C en $\mathcal{X}$ isomorf over $\mathbb{F}_q$.*

Bewijs. [Shafarevich, §3.6.6, Corollary 3]. □

Zij nu $C/\mathbb{F}_q$ een kromme van geslacht nul. Door lemma's 2.60 en 2.61 te combineren concluderen we dat elke divisor van graad nul op C een hoofddivisor is.

Gevolg 2.62. Hieruit volgt ook dat twee divisoren D en D' op een gladde kromme C/k van geslacht nul, waarvoor $\deg D = \deg D'$, lineair equivalent zijn. Immers $\deg(D-D') = 0 \Longrightarrow \exists f \in K(C) : D - D' = (f)$.

Vervolgens hebben we nog een eigenschap nodig van de meetkunde van de kromme $\mathcal{X}/\mathbb{F}_q$ gegeven door $Z = 0$, zoals we die eerder tegenkwamen in voorbeeld 2.46.

Lemma 2.63. *Zij $\mathcal{X}$ als hierboven. Zijn $\{P_1, P_2\}, \{P_3, P_4\} \subset \mathcal{X}(\mathbb{F}_q)$ twee paren van onderling verschillende punten van $\mathcal{X}$. Er bestaat een isomorfisme $\varphi : \mathcal{X} \longrightarrow \mathcal{X}$ waarvoor $\varphi(P_1) = P_3$ en $\varphi(P_2) = P_4$.*

Bewijs. We zoeken een isomorfisme van de vorm $(X : Y : 0) \longmapsto (aX + bY : cX + dY : 0)$. We stellen $P_i = (\xi_i : \eta_i : 0)$. We drukken de eigenschap dat $\varphi(P_1) = P_3, \varphi(P_2) = P_4$ uit in lineaire vergelijkingen:

$$\begin{aligned} a\xi_1 + b\eta_1 &= \xi_3 s \\ c\xi_1 + d\eta_1 &= \eta_3 s \\ a\xi_2 + b\eta_2 &= \xi_4 t \\ c\xi_2 + d\eta_2 &= \eta_4 t \end{aligned}$$

waarbij s en t schaalfactoren zijn waarmee rekening gehouden wordt met verschillende representaties van hetzelfde projectieve punt. We schrijven bovenstaand stelsel als een matrixvermenigvuldiging:

$$\begin{pmatrix} \xi_1 & \eta_1 & 0 & 0 \\ 0 & 0 & \xi_1 & \eta_1 \\ \xi_2 & \eta_2 & 0 & 0 \\ 0 & 0 & \xi_2 & \eta_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} \xi_3 s \\ \eta_3 s \\ \xi_4 t \\ \eta_4 t \end{pmatrix}$$

De determinant van de matrix links is $-(\xi_1\eta_2 - \xi_2\eta_1)^2 = -\left[\det \begin{pmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{pmatrix}\right]^2$. Deze uitdrukking is $\neq 0$ omdat P_1 en P_2 verschillende projectieve punten zijn. Dat wil zeggen dat de matrix inverteerbaar is en er a, b, c, d te vinden zijn die aan de vergelijking voldoen.

Tenslotte moet nog worden aangetoond dat φ een isomorfisme is, dus dat er een morfisme ψ bestaat met $\psi = \varphi^{-1}$. We zoeken een ψ van de vorm $(X : Y : 0) \longmapsto (a'X + b'Y : c'X + d'Y : 0)$. We kunnen nu precies hetzelfde voortgaan als hierboven. Het enige verschil is dat we nu nodig hebben dat $P_3 \neq P_4$. □

Dit alles leidt tot de volgende stelling.

Stelling 2.64. *Zijn $C/\mathbb{F}_q$ een gladde kromme van geslacht nul, $\mathcal{P} \subset C(\mathbb{F}_q)$ een verzameling $\mathbb{F}_q$-rationale punten van C met $\#\mathcal{P} = q - 1$ en D een divisor over $\mathbb{F}_q$ op C zodanig dat* $\operatorname{supp}(D) \cap \mathcal{P} = \varnothing$ *en* $0 \leq \deg D < \#\mathcal{P}$. *Dan is $\mathcal{C}(\mathcal{P}, D)$ equivalent met een narrow-sense Reed-Solomon-code* $\mathrm{RNS}_q(k)$ *voor zekere k.*

Met andere woorden: algebraïsch-geometrische codes over $\mathbb{F}_q$ van lengte $q - 1$ en afkomstig van krommen van geslacht nul zijn equivalent met Reed-Solomon-codes.

Bewijs. We vormen een keten van drie equivalentierelaties tussen $\mathcal{C}(\mathcal{P}, D)$ en een onvervalste narrow-sense Reed-Solomon-code.

Volgens lemma 2.61 is C isomorf met $\mathcal{X}$, waarbij $\mathcal{X}$ de kromme is zoals in paragraaf 2.5. Zij $\varphi : C \longrightarrow \mathcal{X}$ een isomorfisme. Nu gebruiken we stelling 2.57 die zegt dat de code $\mathcal{C}(\mathcal{P}', D')$ van de kromme $\mathcal{X}$ identiek is aan de code $\mathcal{C}(\mathcal{P}, D)$, waarbij $\mathcal{P}' = \varphi(\mathcal{P}) \subset \mathcal{X}(\mathbb{F}_q)$ en $D' = \varphi(D)$.

We hebben $\#\mathcal{P}' = \#\mathcal{P} = q - 1$, dus er zijn twee $\mathbb{F}_q$-rationale punten op $\mathcal{X}$ niet bevat in $\mathcal{P}'$. Noem deze Q_1 en Q_2. Volgens lemma 2.63 is er een isomorfisme $\psi : \mathcal{X} \longrightarrow \mathcal{X}$ zodanig dat $\psi(Q_1) = (1 : 0 : 0)$ en $\psi(Q_2) = (0 : 1 : 0)$. Gebruiken we wederom stelling 2.57, dan vinden we dat $\mathcal{C}(\mathcal{P}', D')$ en $\mathcal{C}(\psi(\mathcal{P}'), \psi(D'))$ permutatie-equivalent zijn.

We kiezen nu de symbolen $P_1, P_2, \ldots, P_{q-1}, P_\infty$ zoals in voorbeeld 2.46. Zij vervolgens $k := \deg \psi(D')$ (= $\deg D$) en $D'' := kP_\infty$. De divisoren D'' en $\psi(D')$ hebben gelijke graad en zijn dus lineair equivalent volgens gevolg 2.62, dus uit 2.59 volgt dat $\mathcal{C}(\psi(\mathcal{P}'), \psi(D'))$ en $\mathcal{C}(\psi(\mathcal{P}'), D'')$ equivalente codes zijn (niet noodzakelijk permutatie-equivalent).

Merk nu op dat $\psi(\mathcal{P}') = \{P_1, P_2, \ldots, P_{q-1}\}$. Aan de hand van voorbeeld 2.46 zien we dat de code $\mathcal{C}(\psi(\mathcal{P}'), D'')$ een narrow-sense Reed-Solomon-code is. Uit onze keten van equivalenties volgt nu inderdaad dat $\mathcal{C}(\mathcal{P}, D)$ equivalent is met een narrow-sense Reed-Solomon-code:

$$\mathcal{C}(\mathcal{P}, D) = \mathcal{C}(\mathcal{P}', D') \sim \mathcal{C}(\psi(\mathcal{P}'), \psi(D')) \sim \mathcal{C}(\psi(\mathcal{P}'), D'')$$

□

Opmerking 2.65. In de literatuur (zie het boek van Huffman en Pless [5]) is bovendien sprake van *extended narrow-sense Reed-Solomon-codes* en de *generalized Reed-Solomon-codes*. Dit zijn respectievelijk $[q, k, q-k+1]$- en $[q+1, k, q-k+2]$-codes over $\mathbb{F}_q$. Van deze codes kan op exact dezelfde wijze worden aangetoond dat ze precies corresponderen met algebraïsch-geometrische codes van krommen van geslacht nul met lengte q resp. q+1. Het ietwat onoverzichtelijke scala aan verschillende typen Reed-Solomon-codes kan dus op een elegante manier worden geherformuleerd in termen van algebraïsch-geometrische codes afkomstig van krommen van geslacht nul, waarbij het resulterende type Reed-Solomon-code eenvoudigweg van de lengte van de code afhangt, oftewel van de cardinaliteit van $\mathcal{P}$.

2.7 De kromme $y^2 - x^3 - 3x$ over $\mathbb{F}_5$

We voeren nu nader onderzoek uit naar de kromme C gedefinieerd over $\mathbb{F}_5$ gegeven door $Y^2Z - X^3 - 3XZ^2 = 0$. Haar $\mathbb{F}_5$-rationale punten zijn:

$$(0:1:0), (0:0:1), (2:3:1), (2:2:1), (4:4:1), (4:1:1), (3:4:1), (3:1:1), (1:3:1), (1:2:1)$$

C is een gladde kromme met geslacht 1. Volgens stelling 2.43 heeft een kromme van geslacht 1 over $\mathbb{F}_5$ maximaal 10 punten: C heeft dus het maximale aantal punten.

Lemma 2.66. *Zij $\mathcal{C} := \mathcal{C}(\mathcal{P}, D)$, waarbij $\deg D > 0$, een algebraïsch-geometrische $[n, k, d]$-code afkomstig van C. Dan geldt $d \geq n - k$.*

Bewijs. Voor een divisor D op C met $\deg D > 0$ geldt met behulp van Riemann-Roch dat $k = \ell(D) = \deg D + 1 - g = \deg D$. Hieruit verkrijgen we met stelling 2.32 dat $d \geq n - k + 1 - g = n - k$. □

Een andere manier om dit te zeggen is dat voor het defect δ van een code afkomstig van C geldt dat $\delta \leq 1$. Men kan zich nu vanzelfsprekend afvragen of er codes afkomstig van C zijn te vinden met defect nul.

2.7.1 Codes met $n = 6$, $k = 3$

$[6, 3]_5$-codes afkomstig van C zijn, volgens lemma 2.66, $[6, 3, \geq 3]$-codes. De genoemde codes hebben dus ten hoogste defect één. We gaan nu op zoek naar codes met defect nul, dus $[6, 3, 4]$-codes afkomstig van C. We zijn ten eerste geïnteresseerd in de vraag of we deze überhaupt kunnen vinden. Ten tweede, wanneer we ze vinden, kunnen we ons afvragen welke van deze codes (permutatie-)equivalent zijn.

Eerst adresseren we de vraag hoeveel equivalentieklassen van $[6, 3, 4]$-codes er zijn over $\mathbb{F}_5$.

Stelling 2.67. *Zij $\mathcal{C}$ een $[n, k]$-MDS-code. Dan is $\mathcal{C}$ equivalent met een code* $\operatorname{im} G$ *met G van de vorm*

$$G = \left(\begin{array}{c|ccc} & 1 & \cdots & 1 \\ I_k & \vdots & & \\ & 1 & A & \end{array} \right)$$

waarbij $A \in \mathbb{F}_q^{(k-1)\times(n-k-1)}$ een matrix is.

Bewijs. Operaties die binnen een equivalentieklasse zijn toegestaan zijn het herschalen en permuteren van kolommen. We kunnen een voortbrengermatrix G' in Gauss-Jordan-normaalvorm brengen en dan door middel van kolommenpermutaties zorgen voor de vorm $\begin{pmatrix} I_k & A \end{pmatrix}$ met $A \in \mathbb{F}^{k\times(n-k)}$. Merk op dat voor alle elementen a_{ij} van A geldt dat $a_{ij} \neq 0$, omdat anders één van de rijen een gewicht zou hebben lager dan $n-k+1$. We kunnen dus de kolommen van A herschalen zodat ze van de vorm $\begin{pmatrix} 1 \\ \mathbf{a}_i \end{pmatrix}$ zijn. Vervolgens herschalen we de rijen 2 t/m k van de matrix zodanig dat de linkerkolom van A uit alleen enen bestaat. Hierna herschalen we de kolommen 1 t/m k van de hele matrix weer terug tot ook daar overal weer enen staan. □

Om na te gaan hoeveel equivalentieklassen van $[6,3]$-MDS-codes er bestaan over $\mathbb{F}_5$, lopen we eerst alle voortbrengermatrices van de vorm

$$G = \left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & & \\ & 1 & A & \end{array}\right)$$

langs, met $A \in \mathbb{F}_5^{2\times 2}$. Er zijn 4^4 keuzes voor A (merk namelijk wederom op dat $a_{ij} \neq 0$, waarbij de a_{ij} de elementen van A voorstellen), die we alle controleren met behulp van een Maple-procedure (zie A.3). We vinden zes 3×6-matrices die corresponderen met MDS-codes en die de vereiste, onderstaande gedaante hebben:

$$\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & a & b \\ & 1 & c & d \end{array}\right)$$

Deze zes matrices corresponderen volgens Maple met

$$(a,b,c,d) \in \{(2,3,3,4),(2,4,4,2),(3,2,4,3),(3,4,2,3),(4,2,2,4),(4,3,3,2)\}$$

Er zijn dus *ten hoogste* zes equivalentieklassen. Eerst stellen we met behulp van de procedure in A.4 vast dat het eerste, derde, vierde en vijfde viertal permutatie-equivalente codes en dus equivalente codes voortbrengen:

$$\operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 2 & 3 \\ & 1 & 3 & 4 \end{array}\right) \sim \operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 3 & 4 \\ & 1 & 2 & 3 \end{array}\right) \sim \operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 4 & 2 \\ & 1 & 2 & 4 \end{array}\right) \sim \operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 4 & 3 \\ & 1 & 3 & 2 \end{array}\right)$$

Ook het tweede en zesde viertal zijn permutatie-equivalent:

$$\operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 2 & 4 \\ & 1 & 4 & 2 \end{array}\right) \sim \operatorname{im}\left(\begin{array}{c|ccc} I_3 & 1 & 1 & 1 \\ & 1 & 3 & 2 \\ & 1 & 4 & 3 \end{array}\right)$$

Vervolgens laten we de procedure in A.5 los op het eerste en tweede viertal, en deze blijken equivalente codes op te leveren. Er is dus één enkele equivalentieklasse van $[6,3,4]$-codes over $\mathbb{F}_5$.

Nu is de vraag dus niet meer welke equivalentieklassen $[6,3]$-MDS-codes we kunnen vinden, maar óf we er één kunnen vinden: er is immers maar één klasse. We dienen nu eerst de genoemde codes in kaart te brengen. Om te zoeken met een computer dienen we slechts een eindig aantal codes te hoeven controleren.

Volgens 2.32 hebben we divisoren D nodig met $\deg D = 3$. De eerste vraag die dan rijst is: zijn er misschien eindig veel van zulke D? Helaas is dit niet het geval: $D := (n+3)P_1 - nP_2$ is een divisor van graad 3 voor elke keuze van $n \in \mathbb{Z}$ en P_1, P_2 $\mathbb{F}_5$-rationale punten.

We herinneren ons nu stelling 2.59. Als we ons geen zorgen maken over equivalente codes (en dat doen we niet), kunnen we kijken naar lineaire equivalentieklassen van divisoren. Bij vaste graad blijken er namelijk slechts eindig veel van deze equivalentieklassen te bestaan. Dit stellen we vast met een aantal lemma's. We bekijken de situatie voor een algemene kromme $C_1/\mathbb{F}_q$.

Elke divisor D waarvoor $L(D)$ niet leeg is, is volgens lemma 2.7 equivalent met een effectieve divisor. We hoeven dus voor codes $\mathcal{C}(\mathcal{P}, D)$ alleen te kijken naar effectieve divisoren D:

Lemma 2.68. *Zij $\mathcal{C}(\mathcal{P}, D)$ met D een divisor over $\mathbb{F}_q$ een code afkomstig van een gladde kromme $C_1/\mathbb{F}_q$, dan is er een effectieve divisor D' met $\deg D' = \deg D$ over $\mathbb{F}_q$ zodanig dat $\mathcal{C}(\mathcal{P}, D) \sim \mathcal{C}(\mathcal{P}, D')$.*

Bewijs. Zie lemma 2.7. □

Lemma 2.69. *Het aantal effectieve divisoren van een vaste graad k is eindig.*

Bewijs. Zij $D = \sum n_i P_i$ een effectieve divisor, dan is $\deg D = \sum n_i \deg P_i \geq \max \deg P_i$. Hieruit volgt $\deg P_i \leq \deg D = k$. We hebben dus een bovengrens voor de graad van de punten in $\mathrm{supp}(D)$. Er kan dus slechts nog een eindig aantal punten in $\mathrm{supp}(D)$ zitten, daar er slechts een eindig aantal projectieve drietallen $(x : y : z)$ is met x, y, z alle in een $\mathbb{F}_{q^i}$ met $i \leq k$. Zij P de verzameling punten op C_1 van hoogstens graad k over $\mathbb{F}_q$. Elk punt in P komt in D voor met een coëfficiënt n_P die voldoet aan $n_P \in [0, k]$. Dit geeft een maximaal aantal van $\#P^{k+1} < \infty$ combinaties. □

Opmerking 2.70. Het bewijs van lemma 2.69 suggereert ook meteen een plan van aanpak voor een algoritme dat bij alle effectieve divisoren D langsloopt: gegeven een lijst van punten in $P = \{P_1, P_2, \ldots, P_N\}$, lopen we alle mogelijke combinaties $(n_{P_1}, n_{P_2}, \ldots, n_{P_N})$ langs. In de praktijk valt het aantal effectieve divisoren van lage graad erg mee.

We zijn nu in staat om een algemene stelling te formuleren aan de hand waarvan we een volledige zoektocht naar $[6, 3]$-codes kunnen ondernemen:

Stelling 2.71. *Zij $C_1/\mathbb{F}_q$ een gladde kromme van geslacht g. Zij $\mathcal{C} := \mathcal{C}(\mathcal{P}, D)$ een $[n, k]$-code over $\mathbb{F}_q$ afkomstig van C_1 waarin $\mathcal{P}$ en D voldoen aan de voorwaarden in stelling 2.32. Dan zijn er punten $P_1, P_2, \ldots, P_n \in C_1(\mathbb{F}_q)$ en een effectieve D' divisor van graad $k - 1 + g$ zodanig dat*

$$\mathcal{C} \sim \mathcal{C}(\{P_1, P_2, \ldots, P_n\}, D')$$

Merk op dat we voor een volledige zoektocht dus alle mogelijke verzamelingen $\mathcal{P} \subset C_1(\mathbb{F}_q)$ moeten onderzoeken en voor elke keuze van $\mathcal{P}$ vervolgens alle effectieve divisoren. Als we een $[6, 3, 4]$-code aantreffen kunnen we stoppen: we hebben dan in één klap alle equivalentieklassen te pakken. Aanvankelijk hebben we alleen gezocht naar codes $\mathcal{C}(\mathcal{P}, D)$ waarbij D en $\mathcal{P}$ voldoen aan de aanvullende voorwaarden $\mathrm{supp}(D) \subset C(\mathbb{F}_5)$ en $\mathrm{supp}(D) \cap \mathcal{P} = \varnothing$. Hiermee vonden we 39 $[6, 3]$-MDS-codes, waarvan we door middel van A.4 vaststelden dat ze allemaal permutatie-equivalent waren.

Opmerking 2.72. Het feit dat alle gevonden codes tot dezelfde permutatie-equivalentieklasse behoren, betekent wellicht, met in het achterhoofd stelling 2.57, dat veel van de verschillende keuzes van $\mathcal{P}$ en D in elkaar overgevoerd worden door automorfismen van onze kromme C.

Opmerking 2.73. Door een beperking van het computerpakket Magma kunnen er geen codes $\mathcal{C}(\mathcal{P}, D)$ worden geëvalueerd waarbij $\mathrm{supp}(D) \cap \mathcal{P} \neq \varnothing$. Dit was gelukkig in dit geval geen echt probleem, daar we ook buiten deze speciale klasse van codes om al MDS-codes aantroffen.

2.7.2 Codes met $n = 6$, $k = 2$

$[6, 2]_5$-codes afkomstig van C zijn, volgens stelling 2.32, $[6, 2, \geq 4]$-codes. We gaan nu op zoek naar $[6, 2, 5]$-codes, die dus MDS-codes zijn, afkomstig van C. We zijn weer geïnteresseerd in de vraag hoeveel equivalentieklassen van $[6, 2, 5]$-codes er zijn, en hoeveel daarvan voorkomen als algebraïsch-geometrische code afkomstig van C.

Eerst onderzoeken we weer het eerste deel van de vraag. Hier komt stelling 2.67 van pas. Een $[6, 2]$-MDS-code is equivalent met een code $\mathrm{im}\, G$ waarbij

$$G := \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & a & b & c \end{array}\right)$$

Wat zijn mogelijke waarden voor a, b en c? We kunnen wederom een Maple-procedure gebruiken zoals beschreven in A.3, maar er is een elegantere manier. Schrijf $G = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \end{pmatrix}$. We perken eerst het aantal mogelijkheden in. Omdat $\mathbf{g}_1$ en $\mathbf{g}_2$ codewoorden van een [6,2]-MDS-code zijn en dus gewicht ≥ 5 hebben

geldt $a, b, c \neq 0$. Voorts geldt ook dat $a, b, c \neq 1$ omdat anders het verschil $\mathbf{g}_1 - \mathbf{g}_2$ gewicht ≤ 4 zou hebben. Tenslotte: stel dat a, b, c niet paarsgewijs verschillend zijn, stel dan zonder verlies van algemeenheid dat $a = b$. Dan heeft het codewoord $a\mathbf{g}_1 - \mathbf{g}_2$ gewicht ≤ 4. De conclusie is dat (a, b, c) een permutatie is van $(2, 3, 4)$ (merk op dat dit inderdaad een MDS-code oplevert volgens 2.45) en dat G gevormd kan worden uit de matrix

$$G' := \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 & 4 \end{array}\right)$$

door een permutatie van de kolommen. Dus de code $\operatorname{im} G$ is equivalent met $\operatorname{im} G'$ en er bestaat dus één enkele equivalentieklasse van $[6, 2]_5$-MDS-codes.

We hebben in A.8 en A.9 alle codes $\mathcal{C}(\mathcal{P}, D)$ afgezocht waarbij $\mathcal{P} \subset C(\mathbb{F}_5)$ en D een divisor over $\mathbb{F}_5$ op C waarvoor $\operatorname{supp}(D) \cap \mathcal{P} = \varnothing$. Het resultaat was negatief: er werd geen enkele $[6, 2, 5]$-code gevonden.

Ook hier geldt weer wat we in opmerking 2.73 al zeiden: door een beperking in Magma hebben we niet alle mogelijkheden kunnen naspeuren. Hierdoor is helaas niet met zekerheid te zeggen dat er geen $[6, 2]$-MDS-code kan worden gemaakt van C.

A Gebruikte Magma- en Maple-procedures in 2.7

A.1 Bepalen van $C(\mathbb{F}_5)$

Onderstaande Magma-code werd gebruikt voor het bepalen van de $\mathbb{F}_5$-rationale punten van C.

```
F<w> := GF(5);
A2<x,y> := AffineSpace(F, 2);
f := y^2-x^3-3*x;
X := Curve(A2, f);
places := Places(X, 1);
#places;
places;
```

De uitdraai van deze code staat op pagina 36.

A.2 Implementatie van stelling 2.45

Om te controleren of een code $\mathcal{C}$ met voortbrengermatrix $M \in \mathbb{F}^{k\times n}$ een MDS-code is gebruiken we de Maple-procedure `num_zero_minors`, die de hulpprocedure `iszeromodp` aanroept. Zij $p := \text{kar}\,\mathbb{F}$, dan is $\mathcal{C}$ een MDS-code dan en slechts dan als het commando `num_zero_minors(M,n,k,p);` de output "0" oplevert.

```
with(linalg);

num_zero_minors := proc( M, n, k, p ) local i,j,count,subsets,ksubsets;
  subsets := combinat[choose](n,k);    # initialiseer alle k-tallen kolommen
                                       # deze corresponderen 1-1 met de k-bij-k minoren
  count := 0;                          # stel het aantal nul-minoren aanvankelijk op 0
  for i from 1 to binomial(n,k) do
    if det(submatrix(M,1..k,subsets[i])) = 0 mod p then
      count := count + 1; fi;          # heeft de minor determinant nul?
    od;
  count
end proc:
```

A.3 Zoeken naar equivalentieklassen van $[6,3]_5$-MDS-codes

De volgende Maple-procedure gebruikten we om alle equivalentieklassen van $[6,3]_5$-MDS-codes op te sporen.

```
for a from 2 to 4 do for b from 2 to 4 do for c from 2 to 4 do for d from 0 to 4 do

  # definieer de voortbrengermatrix G:
  G:=matrix(3,6,[1,0,0,1,1,1,0,1,0,1,a,b,0,0,1,1,c,d]);

  # onderzoek of G een MDS-code oplevert:
  if num_zero_minors(G,6,3,5) = 0 then
    print([a,b,c,d]);
  fi;

od; od; od; od;
```

De uitdraai van deze code staat op pagina 37.

A.4 Nagaan van permutatie-equivalentie

De volgende Maple-procedure gaat na of twee codes permutatie-equivalent zijn. Gebruikt worden hier gevolg 2.20 en lemma 2.22. Gegeven hun voortbrengermatrices $G, H \in \mathbb{F}^{k\times n}$ en $p := \text{kar } \mathbb{F}$ luidt het commando `qEquivalent(G,H,n,p);`. Er is geen output wanneer de codes niet permutatie-equivalent zijn, wanneer ze dat wel zijn wordt dit afgedrukt inclusief het aantal benodigde iteraties.

```
with(LinearAlgebra);
with(LinearAlgebra:-Modular):

qEquivalent := proc(G,H,n,p) local lijst,perm,unitM,i,M,N;

  # eerst brengen we H in Gauss-Jordannormaalvorm:
  N:=ReducedRowEchelonForm(H);
  # voor de zekerheid reduceren we het resultaat modulo p:
  N:=Mod(p,N,integer[]);

  # we maken een lijst met alle mogelijke permutaties van {1,2,...,n}
  # die we gebruiken om alle mogelijke permutatiematrices mee te maken:
  lijst := combinat[permute](n);
  unitM := IdentityMatrix(n);

  for i from 1 to n! do

    # maak permutatiematrix:
    perm:=SubMatrix(unitM,1..n,lijst[i]);

    # breng het product G * perm in GJ-normaalvorm, en reduceer modulo p:
    M:=Mod(p,ReducedRowEchelonForm(MatrixMatrixMultiply(G,perm)),integer[]);

    # nu kunnen we controleren of G en H dezelfde GJ-normaalvorm hebben:
    if Equal(M,N) then print("De codes zijn permutatie-equivalent. Gevonden \\
    na ",i," iteraties."); break; fi;
  od;
end proc:
```

A.5 Het nagaan van equivalentie

De volgende serie Maple-commando's gaat na of twee codes, gegeven door voortbrengermatrices M_1 en M_2, equivalent zijn. Gebruikt worden lemma 2.21 en wederom gevolg 2.20. Ze gebruikt de hulpprocedure `NormMat`.

```
with(linalg);
lijst := combinat[permute](n);
n=6;

for i from 1 to n! do

  # initialiseer de permutatiematrix:
  perm:=submatrix(unitM,1..n,lijst[i]);

  # initialiseer de schaalfactoren voor de monomiale transformaties:
  for a from 1 to 4 do for b from 1 to 4 do for c from 1 to 4 do

    # permuteer de kolommen van M_1:
    G:=evalm(M1&*perm);
```

```
    # we herschalen de kolommen 1 t/m 3 van het product:
    G:=NormMat(mulcol(G,1,a)); G:=NormMat(mulcol(G,2,b)); G:=NormMat(mulcol(G,3,c));

    # ... en gebruiken nu lemma 2.21:
    U:=Inverse(transpose(matrix([col(G, 1), col(G, 2), col(G, 3)]))) mod p;

    # we berekenen het product U * M_1 * perm. als de matrices U en perm
    # leiden tot equivalentie, verschillen mogelijkerwijs alleen kolommen 4 t/m 6
    # nog een schaalfactor van de kolommen van M_2:
    GG:=NormMat(U&*G);

    # we onderzoeken daartoe de rang van de 3x2-matrices die wordt gevormd door
    # overeenkomstige kolommen van M_1 en M_2 naast elkaar te zetten:
    for j from 4 to 6 do R[j]:=rank(matrix([col(GG,j),col(M2,j)])) od;
    RR:=mul(R[j],j=k+1..n);

    # indien alle rangen gelijk zijn aan 1, hebben we succes:
    if RR = 1 then print(GG,i,[a,b,c]) else fi

  od: od: od:
  if irem(i,10) = 0 then print(i) else fi
od:
```

A.6 De hulpprocedure NormMat

Dit is een eenvoudige Maple-procedure die een matrix reduceert modulo p:

```
NormMat:=proc(A) global p;
  local M;
  M:=evalm(A);
  M:=map(modp,simplify(evalm(M)),p);
  RETURN(evalm(M));
end proc:
```

A.7 Het vinden van $[6,3]_5$-MDS-codes afkomstig van C

Dit is een implementatie in Magma van het algoritme dat wordt gesuggereerd in stelling 2.71. We doorzoeken hier codes $\mathcal{C}(\mathcal{P}, D)$ afkomstig van de kromme C, met $\mathcal{P} \subset C(\mathbb{F}_q)$ waarvoor $\#\mathcal{P} = 6$, en D een divisor over $\mathbb{F}_q$ op C met $\deg D = 3$ en $D \succeq 0$.

```
# initialiseer grondlichaam k = F_5:
F<w> := GF(5);
# initialiseer de affiene ruimte A^2(k):
A2<x,y> := AffineSpace(F, 2);
# definieer de vergelijking van de kromme:
f := y^2-x^3-3*x;
# maak de kromme aan:
X := Curve(A2, f);

# teller die bijhoudt bij welke P (deelverzameling van de punten) we zijn:
counter:=0;

# een manier om alle 4-deelverzamelingen van onze tien punten langs te lopen:
for i in [1..7] do
```

```
for j in [i+1..8] do
for k in [j+1..9] do
for l in [k+1..10] do

    # we onderzoeken een nieuwe P, dus teller omhoog:
    counter:=counter+1;

    # initialiseer de verzameling F_5-rationale punten op C:
    places := Places(X, 1);

    # definieer onze vier punten P_1, P_2, P_3 en P_4 (die dus NIET in P zitten)
    P1:=places[i]; P2:=places[j]; P3:=places[k]; P4:=places[l];

    # sluit P_1 t/m P_4 uit van P:
    Exclude(~places,P1);
    Exclude(~places,P2);
    Exclude(~places,P3);
    Exclude(~places,P4);

    # we lopen hier alle mogelijke effectieve divisoren van
    # graad 3 langs die met P_1 t/m P_4 kunnen worden gemaakt:

    for c1 in [0..3] do
       for c2 in [0..3-c1] do
           for c3 in [0..3-c1-c2] do
           c4 := 3-c1-c2-c3;

           # definieer divisor:
           D := c1*Divisor(P1)+c2*Divisor(P2)+c3*Divisor(P3)+c4*Divisor(P4);

           # maak AG-code:
           AGC := AlgebraicGeometricCode(places,D);

           # onderzoek het gewicht van de code: is ze MDS?
           if MinimumWeight(AGC) eq 4 then
               AGC;
               places;
               counter;
               break c1;
           end if;
           end for;
       end for;
    end for;

end for;
end for;
end for;
end for;
```

A.8 $[6,2]_5$-MDS-codes $\mathcal{C}(\mathcal{P},D)$ met $\mathbf{supp}(D) \subset C(\mathbb{F}_5)$

Dit is een implementatie in MAGMA van het algoritme dat wordt gesuggereerd in stelling 2.71. We doorzoeken hier codes $\mathcal{C}(\mathcal{P},D)$ afkomstig van de kromme C, met $\mathcal{P} \subset C(\mathbb{F}_q)$ waarvoor $\#\mathcal{P} = 6$, en D een divisor over $\mathbb{F}_q$ op C met $\deg D = 2$ en $D \succeq 0$.

```
F<w> := GF(5);
A2<x,y> := AffineSpace(F, 2);
f := y^2-x^3-3*x;
X := Curve(A2, f);

counter:=0;

# loop alle mogelijke 4-deelverzamelingen van F_5-rationale punten langs:
for i in [1..7]    do
for j in [i+1..8] do
for k in [j+1..9] do
for l in [k+1..10] do

    counter:=counter+1;

    places := Places(X, 1);

    # sluit vier punten uit van P:
    P1:=places[i]; P2:=places[j]; P3:=places[k]; P4:=places[l];
    Exclude(~places,P1);
    Exclude(~places,P2);
    Exclude(~places,P3);
    Exclude(~places,P4);

    # loop alle divisoren van graad 2 bij langs:
    for c1 in [0..2] do
       for c2 in [0..2-c1] do
           for c3 in [0..2-c1-c2] do
           c4 := 2-c1-c2-c3;
           D := c1*Divisor(P1)+c2*Divisor(P2)+c3*Divisor(P3)+c4*Divisor(P4);
           AGC := AlgebraicGeometricCode(places,D);

           # is de resulterende code MDS?
           if MinimumWeight(AGC) eq 5 then
               AGC;
               places;
               counter;
               break c1;
           end if;
           end for;
       end for;
    end for;

end for;
end for;
end for;
end for;
```

A.9 $[6,2]_5$-MDS-codes $\mathcal{C}(\mathcal{P},D)$ met $\mathbf{supp}(D) \subset C(\mathbb{F}_{25})$

Dit is een implementatie in MAGMA van het algoritme dat wordt gesuggereerd in stelling 2.71. We doorzoeken hier codes $\mathcal{C}(\mathcal{P},D)$ afkomstig van de kromme C, met $\mathcal{P} \subset C(\mathbb{F}_q)$ waarvoor $\#\mathcal{P} = 6$, en D een divisor over $\mathbb{F}_{25}$ op C met $\deg D = 2$ en $D \succeq 0$. Merk op dat dit impliceert dat $D = 1 \cdot Q$ met $Q \in C(\mathbb{F}_{25})$.

```
F<w> := GF(5);
A2<x,y> := AffineSpace(F, 2);
f := y^2-x^3-3*x;
X := Curve(A2, f);

counter:=0;

# initialiseer de punten van graad 2:
plz := Places(X, 2);

# loop alle mogelijke 4-deelverzamelingen van F_5-rationale punten langs:
for i in [1..7]    do
for j in [i+1..8] do
for k in [j+1..9] do
for l in [k+1..10] do

    counter:=counter+1;

    places := Places(X, 1);

    # sluit de vier punten uit van P:
    P1:=places[i]; P2:=places[j]; P3:=places[k]; P4:=places[l];
    Exclude(~places,P1);
    Exclude(~places,P2);
    Exclude(~places,P3);
    Exclude(~places,P4);

    # loop alle divisoren van graad 2 bij langs, oftewel: loop
    # alle punten van graad 2 bij langs:
    for c5 in [1..5] do

         P1 := plz[c5];
         D := Divisor(P1);
         AGC := AlgebraicGeometricCode(places,D);

         # is de resulterende code MDS?
         if MinimumWeight(AGC) eq 5 then
           AGC;
           places;
           counter;
         end if;

    end for;

end for;
end for;
end for;
end for;
```

Literatuurverwijzing

1. Fulton, W., *Algebraic Curves*, Addison-Wesley, 1989.
2. Huffman, W.C., Pless, V., *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.
3. Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.
4. Van Lint, J.H., Van der Geer, G., *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser, 1988.
5. Roman, S., *Coding and Information Theory*, Springer-Verlag, 1992.
6. Shafarevich, I., *Basic Algebraic Geometry*, Springer-Verlag, 1994.
7. Tsfasman, M.A. en Vladut, S.G., *Algebraic-geometric codes*, Kluwer Academic Publishers, 1991.
8. Zariski, O., Samuel, P., *Commutative Algebra II*, Springer-Verlag, 1976.