**Lennart Ackermans**

# Oplosbaarheid van kegelsneden

**Bachelorscriptie**

**Scriptiebegeleider: dr. Marco Streng**

**16 maart 2016**


**Mathematisch Instituut, Universiteit Leiden**

# Inhoudsopgave



# 1 Inleiding

Zij $K$ een lichaam. Een kegelsnede over $K$ is de nulpuntenverzameling in $\mathbb{P}^2(K)$ van een kwadratische vorm $f \in K[X, Y, Z]$ ongelijk aan 0. We kijken in deze scriptie naar de diagonaalvorm in drie variabelen $f = aX^2 + bY^2 + cZ^2$ met $a, b, c \in K$, en beschouwen de lichamen $K = \mathbb{Q}$, $K = F(t)$ voor een lichaam $F$ en het lichaam van $p$-adische getallen $K = \mathbb{Q}_p$.

Centraal in de scriptie staan lokaal-globaalprincipes, stellingen die de oplosbaarheid van een kwadratische vorm reduceren tot de oplosbaarheid van die vorm modulo (machten van) priemidealen. We zijn geïnteresseerd in nulpunten van $f$ in $\mathbb{P}^2(K)$. We willen bepalen of er een niet-triviale (ongelijk aan $\mathbf{0}$) oplossing bestaat, en zo ja, die oplossingen vinden.

In hoofdstuk 2 introduceren we de $p$-adische getallen, om het lokaal-globaalprincipe voor kegelsneden over $\mathbb{Q}$ te kunnen behandelen. In hoofdstuk 3 behandelen we het lokaal-globaalprincipe voor kegelsneden over rationale functielichamen en presenteren we een algoritme om dit soort kegelsneden op te lossen. Het algoritme is door de auteur van deze scriptie geïmplementeerd in SageMath (zie hoofdstuk 4), en kent al implementaties in Maple en Magma van Van Hoeij en Cremona [1].

# 2 Kegelsneden over $p$-adische getallen

## 2.1 Inleiding

In 1897 bedacht Kurt Hensel de $p$-adische getallen, met als doel de technieken van machtreeksen naar de getaltheorie te brengen. Een $p$-adisch geheel getal, voor een zeker priemgetal $p$, definieerde hij als een formele som

$$\sum_{i=0}^{\infty} a_i p^i,$$

met $a_i \in \mathbb{Z}$ zodat $0 \leq a_i < p$. Het bleek dat de verzameling van deze "getallen" een ring vormde.

Het nut van Hensels getallen werd pas echt duidelijk toen Helmut Hasse in 1923 het door Minkowski bedachte lokaal-globaalprincipe in $p$-adische getallen formuleerde, waardoor de theorie aanzienlijk overzichtelijker werd. Zie Schwermer [3] voor een historisch overzicht.

In dit hoofdstuk bewijzen we een aantal belangrijke stellingen over $p$-adische getallen, en sluiten af met twee formuleringen van het lokaal-globaalprincipe voor kegelsneden over $\mathbb{Q}$.

## 2.2 $p$-adische getallen

**Definitie 2.1.** Zij $I$ een partieel geordende verzameling en $(A_i)_{i\in I}$ een familie ringen. Laat $f_{i,j} : A_j \to A_i$ homomorfismen zijn voor alle $i \leq j \in I$ zodat

$$f_{i,i} = \mathrm{id}_{A_i}, \tag{1}$$
$$f_{i,k} = f_{i,j} \circ f_{j,k} \qquad \text{voor alle } i \leq j \leq k. \tag{2}$$

Dan is de **inverse limiet** van het **inverse systeem** $((A_i)_{i\in I}, (f_{i,j})_{i\leq j\in I})$ de verzameling

$$\varprojlim_{i\in I} A_i = \{\vec{a} \in \prod_{i\in I} A_i : a_i = f_{i,j}(a_j) \text{ voor alle } i \leq j \in I\}.$$

Ter verduidelijking van de definitie kunnen we een invers systeem met $I = \mathbb{Z}_{\geq 0}$ als volgt noteren:

$$A_0 \xleftarrow{f_{0,1}} A_1 \xleftarrow{f_{1,2}} A_2 \longleftarrow \dots$$

De inverse limiet is met coëfficiëntsgewijze optelling en vermenigvuldiging een deelring van de productring $\prod_{i\in I} A_i$: omdat $f_{i,j}$ homomorfismen zijn, is de inverse limiet gesloten onder optelling en vermenigvuldiging, en zitten de eenheidselementen voor de optelling en vermenigvuldiging in de inverse limiet. Als $x \in \varprojlim_{i\in I} A_i$, dan geldt $-x \in \varprojlim_{i\in I} A_i$.

**Definitie 2.2.** De ring van $p$-adische getallen is

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{Z}_{\geq 0}} (\mathbb{Z}/p^n\mathbb{Z}),$$

waarbij $f_{i,j}$ (als in definitie 2.1) het natuurlijke homomorfisme van $\mathbb{Z}/p^j\mathbb{Z}$ naar $\mathbb{Z}/p^i\mathbb{Z}$ is.

**Propositie 2.3.** *Een element $x \in \mathbb{Z}_p$ is deelbaar door $p^n$ als en slechts als $x_n = 0$.*

*Bewijs.* Als $x$ deelbaar is door $p^n$, dan geldt vanzelfsprekend $x_n = 0 \in \mathbb{Z}/p^n\mathbb{Z}$. Voor de andere implicatie, stel $x_n = 0$. Dan geldt $x_i = 0$ voor alle $i \leq n$. Stel nu dat $x_i$ niet deelbaar is door $p^n$ voor een zekere $i > n$. Dan is $x_n \equiv x_i \pmod{p^n}$ niet 0; tegenspraak, dus $x_i$ is deelbaar door $p^n$ voor alle $i \geq 0$. Zij nu $\alpha_i \in \mathbb{Z}$ voor alle $i \geq 0$ zodat $p^n\alpha_i \equiv x_{i+n} \pmod{p^{i+n}}$, en zij $x'_i := (\alpha_i \bmod p^i) \in \mathbb{Z}/p^i\mathbb{Z}$. Dan geldt $p^n x'_i = x_i \in \mathbb{Z}/p^i\mathbb{Z}$. Dus $x' := (x'_i)_{i\in\mathbb{Z}_{\geq 0}}$ is de gezochte deler als $x' \in \mathbb{Z}_p$. Voor $0 \leq j \leq i$ geldt $p^n\alpha_j \equiv x_{j+n} \equiv x_{i+n} \equiv p^n\alpha_i \pmod{p^{j+n}}$, dus $x'_i \equiv \alpha_i \equiv \alpha_j \equiv x'_j \pmod{p^j}$. Er volgt dat $x' \in \mathbb{Z}_p$, dus $x$ is deelbaar door $p^n$. □

We verkrijgen een isomorfisme $\mathbb{Z}_p/p^n\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ gedefiniëerd door $x + p^n\mathbb{Z}_p \mapsto x_n$. We schrijven daarom $x_n = (x \bmod p^n)$ voor de $n$'de coördinaat van $x \in \mathbb{Z}_p$.

Er is een inclusie $\mathbb{Z} \subset \mathbb{Z}_p$ door $z \in \mathbb{Z}$ te identificeren met $x_n = (z \mod p^n)$. Bijvoorbeeld: $-2 \in \mathbb{Z}$ is $(-2, -2, \ldots) = (0, 1, 7, 25, \ldots) \in \mathbb{Z}_3$.

**Propositie 2.4.** *Er geldt:*

*(a) Een element $x \in \mathbb{Z}_p$ is een eenheid als en slechts als $x$ niet deelbaar door $p$ is.*

*(b) Elke $x \in \mathbb{Z}_p$ met $x \neq 0$ kan uniek geschreven worden als $x = p^n u$, met $u \in \mathbb{Z}_p^*$ en $n \in \mathbb{Z}_{\geq 0}$.*

*Bewijs.* Zij $x \in \mathbb{Z}_p$ niet deelbaar door $p$. Dan is $x_n$ niet deel baar door $p$, dus geldt $\gcd(x_n, p^n) = 1$, dus $x_n$ heeft een inverse $x_n^{-1} \in \mathbb{Z}/p^n\mathbb{Z}$. Omdat inversen uniek zijn geldt $x_{n-1}^{-1} \equiv x_n^{-1} \bmod p^{n-1}$. Wegens de coëfficiëntsgewijze operaties op $\mathbb{Z}_p$ volgt dat $(x_0^{-1}, x_1^{-1}, \ldots) \in \mathbb{Z}_p$ de inverse van $x$ is.

Voor de andere implicatie: als $p$ een deler van $x$ is, dan geldt $x_1 = 0 \in \mathbb{Z}/p\mathbb{Z}$, en dus is $x_1$ niet inverteerbaar. Er volgt dat $x$ niet inverteerbaar is.

Voor (b), zij $n \in \mathbb{Z}_{\geq 0}$ zodat $x_n = 0$ en $x_{n+1} \neq 0$. Dan is $x$ deelbaar door $p^n$ en niet door hogere machten van $p$, dus zij $u \in \mathbb{Z}_p$ zodat $x = p^n u$. Dan is $u$ niet deelbaar door $p$, en wegens (a) is $u$ een eenheid. Schrijven we $x = p^m v$ met $m < n$ en $v \in \mathbb{Z}_p$, dan is $v$ deelbaar door $p$, dus wegens (a) geen eenheid. Als voor $v \in \mathbb{Z}_p^*$ geldt dat $p^n u = p^n v$, dan geldt voor alle $i \geq 0$ dat $p^n u \equiv p^n v \pmod{p^{i+n}}$, dus $u \equiv v \pmod{p^i}$. Er volgt dat de schrijfwijze $x = p^n u$ met $u \in \mathbb{Z}_p^*$ en $n \in \mathbb{Z}_{\geq 0}$ uniek is. □

Zij $x, y \in \mathbb{Z}_p \setminus \{0\}$. Dan geldt voor zekere $u, v \in \mathbb{Z}_p^*$, $m, n \in \mathbb{Z}$ dat $xy = p^{n+m}uv$, en vervolgens dat $p^{n+m}uv \not\equiv 0 \pmod{p^{n+m+1}}$, want $uv$ is niet deelbaar door $p$. Er volgt $xy \neq 0$, dus $\mathbb{Z}_p$ is een domein.

**Definitie 2.5.** Schrijf $x \in \mathbb{Z}_p \setminus \{0\}$ als $x = p^n u$ voor een zekere $u \in \mathbb{Z}_p^*$ en $n \in \mathbb{Z}_{\geq 0}$. Dan heet het getal $n$ de $p$-adische valuatie van $x$, genoteerd als $v_p(x)$. We spreken af dat $v_p(0) = \infty$.

Er geldt $v_p(xy) = v_p(x) + v_p(y)$ en $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

**Definitie 2.6.** De $p$-adische absolute waarde is gedefinieerd als $|x|_p = p^{-v_p(x)}$, en de $p$-adische afstand als $d_p(x, y) = |x - y|_p$. We spreken af dat $|0|_p = 0$.

Voor het gemak noteren we $|\cdot|$ zonder index $p$ als uit de context duidelijk is in welke $p$-adische ring we zitten. Voor $x, y, z \in \mathbb{Z}_p$ geldt $|x - x| = 0$, $|x - y| = |y - x|$, $|x - z| = |(x - y) + (y - z)| \leq \max\{|x - y|, |y - z|\} \leq |x - y| + |y - z|$ en $|x| = 0$ impliceert $x = 0$. Dus $\mathbb{Z}_p$ is een metrische ruimte.

**Definitie 2.7.** Het lichaam $\mathbb{Q}_p$ van $p$-adische getallen is het quotiëntenlichaam van $\mathbb{Z}_p$.

Een element $x \in \mathbb{Q}_p^*$ is te schrijven als $x = p^n u$ met $u \in \mathbb{Z}_p^*$ en $n \in \mathbb{Z}$. De $p$-adische valuatie op $\mathbb{Q}_p$ is op dezelfde manier gedefinieerd als op $\mathbb{Z}_p$: $v_p(x) := n$.

De $p$-adische absolute waarde is natuurlijk ook gedefinieerd op $\mathbb{Z} \subset \mathbb{Z}_p$ en $\mathbb{Q} \subset \mathbb{Q}_p$. In het algemeen definiëren we een absolute waarde op $\mathbb{Q}$ als een multiplicatieve functie $|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ waarvoor de de afstandsfunctie $d(x, y) = |x - y|$ een metriek op $\mathbb{Q}$ is. Alexander Ostrowski bewees in 1916 dat alle absolute waardes op $\mathbb{Q}$ equivalent zijn aan een $p$-adische absolute waarde, de Euclidische absolute waarde of de triviale absolute waarde (gedefinieerd door $|x| = 0$ als $x = 0$ en $|x| = 1$ als $x \neq 0$). Hierbij betekent equivalent dat de verzamelingen Cauchy-rijtjes voor beide metrieken dezelfde zijn. Zie Koblitz [2, p. 3] voor een bewijs.

Een gebruikelijke constructie van de $p$-adische getallen wordt verkregen door $\mathbb{Z}_p$ en $\mathbb{Q}_p$ te definiëren als de topologische vervollediging van $(\mathbb{Z}, |\cdot|_p)$ respectievelijk $(\mathbb{Q}, |\cdot|_p)$. Wegens de stelling van Ostrowski zijn $\mathbb{R}$ en de $p$-adische lichamen $\mathbb{Q}_p$ alle mogelijke vervolledigingen van $\mathbb{Q}$. De constructie van de $p$-adische getallen als vervollediging laten we niet zien, maar we laten wel zien dat $\mathbb{Z}_p$ volgens onze definitie inderdaad een volledige metrische ruimte is.

**Propositie 2.8.** *De ring $\mathbb{Z}_p$ met de metriek van de p-adische absolute waarde is een volledige metrische ruimte.*

*Bewijs.* We bewijzen dat iedere Cauchyrij in $\mathbb{Z}_p$ een limiet heeft. Zij $(x_n)_{n\in\mathbb{Z}_{\geq 0}}$ een Cauchyrij in $\mathbb{Z}_p$. Let op: een $p$-adisch element $x_n$ in het rijtje is óók een rijtje, met termen in quotiëntringen van $\mathbb{Z}$. De Cauchy-eigenschap impliceert dat er voor alle $k \in \mathbb{N}$ een $N_k \in \mathbb{N}$ is zodat voor alle $n > N_k$ geldt dat $v_p(x_n - x_{N_k}) \geq k$, ofwel dat $(x_n \bmod p^i) = (x_{N_k} \bmod p^i)$ voor alle $i \leq k$. We definiëren de limiet $y \in \mathbb{Z}_p$ door

$$y_k = (x_{N_k} \bmod p^k) \quad \text{voor } k \geq 0.$$

Dat wil zeggen, de $k$'de term van de limiet $y$ is gelijk aan de $k$'de term van de $N_k$'de term uit de Cauchyrij. Wegens het voorafgaande geldt voor alle $i, k \in \mathbb{N}$ met $i < k$ dat $y_i = (x_{N_i} \bmod p^i) = (x_{N_k} \bmod p^i) = (y_k \bmod p^i)$, dus $y$ zit in $\mathbb{Z}_p$. Voor $k \in \mathbb{N}$ willekeurig groot en $n \geq N_k$ geldt $v_p(y - x_n) \geq k$, dus $y$ is de limiet. □

We kunnen $p$-adische getallen opschrijven als Cauchyreeksen. Neem bijvoorbeeld $y = 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \ldots \in \mathbb{Z}_3$. Er geldt $2 \cdot 3 + \ldots + 2 \cdot 3^n \equiv -3 \pmod{3^{n+1}}$, dus de limiet is $y = -2$.

## 2.3 Lemma van Hensel

Het Lemma van Hensel is een belangrijke stelling in de theorie van $p$-adische getallen, die ons in staat stelt nulpunten te vinden van $p$-adische polynomen. In deze paragraaf bewijzen we het Lemma van Hensel en passen we het toe op een klasse van kegelsneden.

**Propositie 2.9** (Taylor voor $p$-adische polynomen)**.** *Laat $f \in \mathbb{Z}_p[X]$, $x, y, z \in \mathbb{Z}_p$ en $n \in \mathbb{Z}_{\geq 0}$ zijn zodat $y = x + p^n z$. Dan is er een $a \in \mathbb{Z}_p$ zodat*

$$f(y) = f(x) + p^n z f'(x) + p^{2n} a.$$

*Bewijs.* De term van graad $i \in \mathbb{Z}_{\geq 0}$ van $f$ met coëfficiënt $a_i \in \mathbb{Z}_p$, geëvalueerd in $y$, is gelijk aan

$$[f]_i(y) = a_i(x + p^n z)^i = a_i x^i + i a_i x^{i-1} p^n z + \ldots + a_i p^{in} z^i \tag{3}$$

$$= [f]_i(x) + p^n [f]'_{i-1}(x) z + \ldots + a_i p^{in} z^i. \tag{4}$$

Vanaf de derde term van vergelijking (4) bevat elke term een factor $p^{2n}$, dus de gezochte $a$ bestaat. □

De volgende bewijzen zijn gebaseerd op Serre [4].

**Lemma 2.10.** *Laat $f \in \mathbb{Z}_p[X]$ en $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}_{\geq 0}$ zijn zodat $f(x) \equiv 0 \pmod{p^n}$ en $k = v_p(f'(x))$, en stel $0 \leq 2k < n$. Dan is er een $y \in \mathbb{Z}_p$ zodat*

$$f(y) \equiv 0 \pmod{p^{2n-2k}}, \quad v_p(f'(y)) = k \quad \text{en} \quad y \equiv x \pmod{p^{n-k}}.$$

*Bewijs.* We schrijven $y = x + p^{n-k} z$ en zoeken $z \in \mathbb{Z}_p$ zodat de andere congruentie en gelijkheid gelden. Propositie 2.9 (Taylor) geeft voor een zekere $a \in \mathbb{Z}_p$,

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} a. \tag{5}$$

Wegens de aanname $f(x) \equiv 0 \pmod{p^n}$ geldt $f(x) = p^n b$ met $b \in \mathbb{Z}_p$, en wegens de definitie $k = v_p(f'(x))$ geldt $f'(x) = p^k c$ met $c \in \mathbb{Z}_p^*$. We kunnen vergelijking (5) nu herschrijven naar

$$f(y) = p^n(b + zc) + p^{2n-2k} a.$$

Als we $z$ zo kiezen dat

$$b + zc \equiv 0 \pmod{p^{n-2k}},$$

dan geldt $f(y) \equiv 0 \pmod{p^{2n-2k}}$. Taylor toepassen op $f'(y)$ geeft

$$f'(y) = f'(x) + p^{n-k} z f''(x) + p^{2n-2k} a' \equiv f'(x) \equiv p^k c \pmod{p^{n-k}}.$$

Er geldt $n - k > k$, dus we hebben $v_p(f'(y)) = k$. □

Het bewijs van lemma 2.10 geeft een methode om gegeven een oplossing in $\mathbb{Z}/p\mathbb{Z}$ een oplossing in de $p$-adische getallen te vinden. Dit noemen we Henselverheffing (Engels: *Hensel lifting*). De methode is analoog aan de methode van Newton voor het vinden van nulpunten in de reële getallen: de berekening van $z$ komt neer op $z = -\frac{f(x)}{f'(x)}$. Een iteratie komt steeds dichter bij een nulpunt te liggen volgens de $p$-adische metriek. De volgende stelling van Hensel geeft aan wanneer het proces convergeert.

**Stelling 2.11** (Lemma van Hensel)**.** *Zij $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x \in (\mathbb{Z}_p)^m$, $n$, $k$, $j \in \mathbb{Z}$ zodat $1 \leq j \leq m$ en $k = v_p(\frac{\partial f}{\partial X_j}(x))$. Stel dat*

$$0 \leq 2k < n \quad \textit{en} \quad f(x) \equiv 0 \pmod{p^n}.$$

*Dan is er een $y \in (\mathbb{Z}_p)^m$ met $f(y) = 0$ en $y \equiv x \pmod{p^{n-k}}$.*

*Bewijs.* We bewijzen de stelling door een Cauchyrij te maken waarbij opeenvolgende elementen worden verkregen door lemma 2.10 toe te passen. Stel eerst $m = 1$. Door lemma 2.10 toe te passen op $x_0 := x \in \mathbb{Z}_p$ krijgen we $x_1 \in \mathbb{Z}_p$ zodat opnieuw aan de voorwaarden voldaan wordt:

$$x_1 \equiv x_0 \pmod{p^{n-k}}, \quad f(x_1) \equiv 0 \pmod{p^{n+1}} \quad \text{en} \quad v_p(f'(x_1)) = k.$$

In het algemeen geldt dat als $x_n \in \mathbb{Z}_p$ voldoet aan de voorwaarden, dat $x_{n+1}$ verkregen met lemma 2.10 voldoet aan de voorwaarden. We construeren op deze manier een rijtje $(x_q)_{q \in \mathbb{Z}_{\geq 0}}$ met

$$x_{q+1} \equiv x_q \pmod{p^{n+q-k}}, \quad f(x_q) \equiv 0 \pmod{p^{n+q}}.$$

Dit is een Cauchy-rijtje, want voor $q, r \in \mathbb{Z}$ met $q < r$ geldt $|x_q - x_r| \leq p^{k-n-q}$. Voor de limiet $y$ geldt $f(y) \equiv 0 \bmod p^n$ voor alle $n \in \mathbb{N}$, dus $f(y) = 0$, en $y \equiv x \pmod{p^{n-k}}$.

Voor $m > 1$, noteer $x = (x_i) \in (\mathbb{Z}_p)^m$ en zij $f^* \in \mathbb{Z}_p[X_j]$ het polynoom verkregen door $X_i$ voor alle $i \neq j$ te vervangen door $x_i$. Nu kan het geval $m = 1$ worden toegepast op $f^*$ en $x_j$. (Dit geeft dat er een $y_j \equiv x_j \pmod{p^{n-k}}$ is zodat $f^*(y_j) = 0$.) Nemen we $y_i = x_i$ voor $i \neq j$, dan volgt dat $y = (y_j)$ de gewenste oplossing is. □

Het Lemma van Hensel maakt het mogelijk om het bestaan van nulpunten van $p$-adische polynomen te bepalen zonder die te berekenen. Dit is onder andere nuttig omdat er – zoals we in het volgende hoofdstuk zullen zien – een relatie bestaat tussen het bestaan van $p$-adische oplossingen en het bestaan van oplossingen in $\mathbb{Z}$ en $\mathbb{Q}$. Het volgende gevolg maakt het Lemma van Hensel makkelijk toepasbaar op het onderwerp van deze scriptie.

**Gevolg 2.12.** *Zij $f = aX^2 + bY^2 + cZ^2 \in \mathbb{Z}[X, Y, Z]$ en $p \in \mathbb{Z}$ een oneven priem zodat $p \nmid abc$. Dan heeft $f$ een niet-triviaal nulpunt in $\mathbb{Z}_p^3$.*

*Bewijs.* We bewijzen eerst dat $f$ een niet-triviaal nulpunt heeft in $(\mathbb{Z}/p\mathbb{Z})^3$ en gebruiken vervolgens het Lemma van Hensel. Zij $S_1 = \{a + by^2 \in \mathbb{Z}/p\mathbb{Z} : 0 \leq y \leq \frac{p-1}{2}\}$. Laat $y_1, y_2 \in \mathbb{Z}/p\mathbb{Z}$, zodat $y_1$ en $y_2$ niet beide 0 zijn en $0 \leq y_1, y_2 \leq \frac{p-1}{2}$ geldt. Stel $a + by_1^2 = a + by_2^2$. Dan geldt $y_1^2 = y_2^2$, want $b \not\equiv 0 \pmod{p}$ wegens $p \nmid abc$. Dus $(y_1 + y_2)(y_1 - y_2) = y_1^2 - y_2^2 = 0$. Er geldt $y_1 + y_2 \neq 0$, want $0 < y_1 + y_2 \leq p - 1$, dus $y_1 = y_2$. Het aantal elementen van $S_1$ is dus $\frac{p+1}{2}$, en met hetzelfde bewijs geldt dat $\#S_2 = \#\{-cy^2 \in \mathbb{Z}/p\mathbb{Z} : 0 \leq y \leq \frac{p-1}{2}\} = \frac{p+1}{2}$. Dus $\#S_1 + \#S_2 = p + 1 > \#\mathbb{Z}/p\mathbb{Z}$. Dus $S_1$ en $S_2$ hebben een gemeenschappelijk element $a + by^2 = -cz^2$ met $x, y \in \mathbb{Z}/p\mathbb{Z}$. Er volgt dat $(1, y, z)$ een nulpunt is van $f$ in $(\mathbb{Z}/p\mathbb{Z})^3$.

Er geldt $\frac{\partial f}{\partial X}(1, y, z) \equiv 2a \not\equiv 0 \pmod{p}$, want $p \nmid 2a$. Stelling 2.11 geeft dat $f$ een nulpunt $(x, y, z) \in \mathbb{Z}_p^3$ heeft met $x \equiv 1 \bmod p$, dus $f$ heeft een niet-triviaal nulpunt. □

In het geval dat $p$ een deler is van een van de coëfficiënten, zeg $p \mid a$, geldt $f \equiv by^2 + cz^2 \pmod{p}$. Neem aan dat $p$ geen deler is van $bc$. In een geschikte uitbreiding van $\mathbb{Z}/p\mathbb{Z}$ factoriseert $f$ dan als $f = b(y + \sqrt{-\frac{c}{b}}z)(y - \sqrt{-\frac{c}{b}}z)$. In het bewijs van propositie 2.15 zullen we zien dat er in dit geval alleen een niet-triviale oplossing in $\mathbb{Z}_p^3$ bestaat als $-\frac{c}{b}$ een kwadraat is in $\mathbb{Z}/p\mathbb{Z}$.

## 2.4 Lokaal-globaalprincipe

We beschouwen in dit hoofdstuk de kwadratische vorm $f = aX^2 + bY^2 + cZ^2 \in \mathbb{Z}[X, Y, Z]$, waarbij $a$, $b$ en $c$ paarsgewijs copriem en kwadraatvrij (niet deelbaar door een kwadraat) zijn, en in het bijzonder de kegelsnede over $\mathbb{Q}$

$$f = aX^2 + bY^2 + cZ^2 = 0. \tag{6}$$

Merk op dat voor een willekeurige kwadratische vorm $g \in \mathbb{Z}[X, Y, Z]$ de oplosbaarheid van de vergelijking $g = 0$ equivalent is met de oplosbaarheid van een vergelijking die aan onze eisen voldoet, door te schalen en te substitueren. Ook kegelsneden in $\mathbb{Q}[X, Y, Z]$ kunnen op deze manier worden teruggebracht naar kegelsneden in $\mathbb{Z}[X, Y, Z]$.

Als $(x, y, z) \in \mathbb{Q}_p^3 \setminus \mathbb{Z}_p^3$ een oplossing van vergelijking (6) is en $n = -\min\{v_p(x), v_p(y), v_p(z)\}$, dan is $(p^n x, p^n y, p^n z) \in \mathbb{Z}_p^3$ ook een oplossing, dus we kunnen het probleem van het vinden van een oplossing van $f$ in $\mathbb{Q}_p^3$ reduceren tot het vinden van een oplossing in $\mathbb{Z}_p^3$.

We bekijken nu een belangrijk resultaat van Helmut Hasse uit 1923, bekend als de stelling van Hasse-Minkowski of het lokaal-globaalprincipe. De stelling zegt dat het bestaan van een niet-triviale oplossing van $f$ in een getallenlichaam $K$ equivalent is met het bestaan van lokale oplossingen – het bestaan van een niet-triviale oplossing in de vervolledigingen van $K$ voor elke absolute waarde op $K$. Wegens de stelling van Ostrowski betekent dit in het geval van $K = \mathbb{Q}$ dat $f$ een niet-triviale oplossing in $\mathbb{R}^3$ en alle $p$-adische lichamen $\mathbb{Q}_p^3$ heeft.

De stelling van Hasse komt overeen met een resultaat van Minkowski uit 1890 dat vrij technisch is. Met behulp van de door Hensel bedachte $p$-adische getallen kwam Hasse met een makkelijk hanteerbare variant. In 1785 is een equivalente vorm van deze stelling al bewezen door Legendre. Zie Schwermer [3] voor een historisch overzicht.

**Stelling 2.13** (Hasse-Minkowski)**.** *Vergelijking* (6) *heeft een niet-triviale oplossing in* $\mathbb{Q}^3$ *als en slechts als vergelijking* (6) *een niet-triviale oplossing heeft in* $\mathbb{R}^3$ *en* $\mathbb{Q}_p^3$ *voor alle priemen* $p \in \mathbb{Z}_{>0}$.

**Stelling 2.14** (Legendre)**.** *Vergelijking* (6) *heeft een niet-triviale oplossing in* $\mathbb{Q}^3$ *als en slechts als vergelijking* (6) *een niet-triviale oplossing heeft in* $\mathbb{R}^3$ *en de volgende congruenties oplosbaar zijn:*

$$x^2 \equiv -bc \pmod{|a|}, \quad x^2 \equiv -ca \pmod{|b|}, \quad x^2 \equiv -ab \pmod{|c|}.$$

We bewijzen de stellingen niet, maar laten wel een gedeeltelijk bewijs zien van de equivalentie.

**Propositie 2.15.** *De volgende uitspraken zijn equivalent:*

1. *Vergelijking* (6) *heeft een niet-triviaal nulpunt in* $\mathbb{Z}_p^3$ *voor alle* ***oneven*** *priemen* $p \in \mathbb{Z}_{>0}$.
2. *De volgende congruenties zijn oplosbaar:*

$$X^2 \equiv -bc \pmod{|a|}, \quad X^2 \equiv -ca \pmod{|b|}, \quad X^2 \equiv -ab \pmod{|c|}.$$

*Bewijs.* We beginnen met de implicatie $1 \Rightarrow 2$. Kies voor alle oneven priemen $p \mid a$ een niet-triviaal nulpunt $0 \neq (x_p, y_p, z_p) \in \mathbb{Z}_p^3$. We bewijzen dat $-bc$ een kwadraat is in $\mathbb{Z}/p\mathbb{Z}$. Stel zonder verlies van algemeenheid $k = v_p(z_p) \leq v_p(y_p)$. We maken als volgt een nieuwe oplossing $(x_p', y_p', z_p')$ met $p \nmid z_p'$. Omdat $f(x_p, y_p, z_p) \equiv ax_p^2 \equiv 0 \pmod{p^{2k}}$ geldt $p^{2k} \mid ax_p^2$. Er geldt dat $a$ kwadraatvrij is, dus $p^k$ is een deler van $x_p$. Nu geldt dat $(\frac{x_p}{p^k}, \frac{y_p}{p^k}, \frac{z_p}{p^k})$ een nulpunt van $f$ is in $\mathbb{Z}_p^3$; stel zonder verlies van algemeenheid dat $k = 0$.

Er geldt $f(x_p, y_p, z_p) \equiv by_p^2 + cz_p^2 \equiv 0 \pmod{p}$ en $z_p^2 \not\equiv 0 \pmod{p}$. We kunnen dus door $z_p^2$ delen en krijgen $-bc \equiv \frac{b^2 y_p^2}{z_p^2} \equiv \left(\frac{by}{z_p}\right)^2 \pmod{p}$. Dus $-bc$ is een kwadraat in $\mathbb{Z}/p\mathbb{Z}$. In $\mathbb{Z}/2\mathbb{Z}$ is alles een kwadraat. Er volgt dat $-bc$ een kwadraat is in $\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$, waarbij $p_1, \ldots, p_n$ de priemdelers van $a$ zijn. De Chinese reststelling geeft dat $-bc$ een kwadraat is in $\mathbb{Z}/a\mathbb{Z}$. De andere twee congruenties volgen uit de symmetrie van $f$.

Voor $2 \Rightarrow 1$ hoeven we alleen de gevallen $p \mid abc$ te bekijken, want voor $p \nmid abc$ heeft $f$ wegens gevolg 2.12 altijd een nulpunt. Stel zonder verlies van algemeenheid $p \mid a$. Zij $x \in \mathbb{Z}$ zodat $x^2 \equiv -bc \pmod{p}$. Dan geldt $f(0, c, x) \equiv 0 \pmod{p}$ en $\frac{\partial f}{\partial Y}(0, c, x) \equiv 2bc \not\equiv 0 \pmod{p}$. Stelling 2.11 (Hensel) geeft dat $f$ een nulpunt in $\mathbb{Z}_p$ heeft. □

De implicatie naar rechts van stelling 2.13 is triviaal, omdat $\mathbb{Q}$ in $\mathbb{Q}_p$ en $\mathbb{R}$ bevat is. Propositie 2.15 bewijst dus ook de implicatie naar rechts van stelling 2.14. Zie Serre [4] voor de andere implicatie.

# 3 Kegelsneden over functielichamen

## 3.1 Inleiding

Voor $F$ een lichaam met karakteristiek ongelijk aan 2, een functielichaam $K = F(t)$ en coëfficiënten $a, b, c \in K^*$, beschouwen we de kegelsnede over $F(t)$

$$aX^2 + bY^2 + cZ^2 = 0. \tag{1}$$

We willen weten wanneer deze vergelijking een niet-triviale oplossing heeft, en een oplossing vinden als die bestaat.

We behandelen een variant van het lokaal-globaalprincipe voor kegelsneden over functielichamen. De hoofdstelling (stelling 3.2) lijkt op stelling 2.14, en het bewijs (dat we nu wel laten zien) gaat op een vergelijkbare manier. In plaats van de eis dat de kegelsnede een oplossing over $\mathbb{R}$ heeft eisen we nu dat een andere kegelsnede, waarvan de coëfficiënten gelijk zijn aan de kopcoëfficiënten van de oorspronkelijke kegelsnede, een oplossing heeft. In plaats van oplossingen over $p$-adische uitbreidingen te bekijken, bekijken we nu oplossingen over "gewone" eindige lichaamsuitbreidingen van $F$. Het is met behulp van de theorie van valuaties (zoals de $p$-adische valuatie in het vorige hoofdstuk) mogelijk om inzicht te verkrijgen in de overeenkomsten tussen de situatie in dit hoofdstuk en die in het vorige hoofdstuk, maar we gaan hier niet verder op in.

In de volgende paragraaf introduceren we het oplosbaarheidscertificaat en bewijzen we dat dit altijd bestaat als vergelijking (1) een niet-triviale oplossing heeft. In paragraaf 3.3 bewijzen we de omgekeerde implicatie, door een algoritme van Van Hoeij en Cremona [1] te presenteren dat op basis van een oplosbaarheidscertificaat een oplossing geeft.

We laten nu zien dat elke kegelsnede als in vergelijking (1) is om te zetten naar een kegelsnede die aan de volgende kenmerken voldoet, op zo'n manier dat (a) de nieuwe vergelijking een niet-triviaal nulpunt heeft als en alleen als de oude dat heeft, en (b) we met een nulpunt van de nieuwe vergelijking gemakkelijk een nulpunt van de oude vergelijking kunnen vinden.

1. $a, b, c \in F[t]$.
2. $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$.
3. $a$, $b$, en $c$ zijn kwadraatvrij: niet deelbaar door een kwadraat $d^2$ met $d \in F[t]$ en $\deg(d) > 0$.

In de stellingen en het algoritme in dit hoofdstuk gaan we uit van coëfficiënten die aan deze eisen voldoen. Het omzetten van een kegelsnede gaat als volgt. Voor eis 1: door te vermenigvuldigen met de noemers zorgen we dat $a, b, c \in F[t]$; de nulpunten van (1) blijven dan onveranderd.

Voor eis 2, deel $a, b$ en $c$ door $\gcd(a, b, c)$. Zij $g = \gcd(a, b)$. Als $\deg(g) > 0$, vervang $a, b, c$ dan met $a/g, b/g, cg$. Als $(x, y, z) \in K^3$ nu een oplossing is van de nieuwe vergelijking, dan is $(x, y, gz)$ een oplossing van de oude vergelijking. Doe de analoge bewerking voor $\gcd(b, c)$ en $\gcd(c, a)$. Herhaal dit totdat eis 2 geldt. Dit kan in een eindig aantal stappen, want in elke stap wordt de graad van $abc$ kleiner.

Voor eis 3: als $a$, $b$ of $c$ deelbaar is door een kwadraat $d^2$, dan vervangen we $a$ door $a/d^2$. Als $(x, y, z) \in K^3$ een oplossing is van de nieuwe vergelijking, dan is $(x/d^2, y, z)$ een oplossing van de oude vergelijking. Omdat aan eis 2 al voldaan is geldt nadat $a$, $b$ en $c$ kwadraatvrij zijn dat ook $abc$ kwadraatvrij is.

De bewijzen en algoritmes in dit hoofdstuk zijn gebaseerd op Van Hoeij en Cremona [1].

## 3.2 Het oplosbaarheidscertificaat

We schrijven $\mathcal{S}_a$ voor de verzameling monische irreducibele elementen $p \in F[t]$ die $a$ delen. Schrijf verder

$$L_p = F[t]/(p).$$

Laat $f_a, f_b, f_c \in F[t][u]$ de polynomen

$$f_a = bu^2 + c, \quad f_b = cu^2 + a, \quad f_c = au^2 + b$$

zijn. Voor $f \in F[t][u]$ schrijven we $(f \bmod p) \in L_p[u]$ voor het polynoom met coëfficiënten (van $f$) modulo $p$.

Verder noteren we $d_a, d_b, d_c$ voor de graden van $a, b, c$ en $l_a, l_b, l_c$ voor de kopcoëfficiënten van $a, b, c$.

We presenteren eerst een vereenvoudigde versie van het algoritme van Van Hoeij en Cremona [1], met het volgende gevalsonderscheid:

$$\text{geval} := \begin{cases} 0, & \text{als } d_a \equiv d_b \equiv d_c \pmod 2 \\ 1, & \text{anders.} \end{cases}$$

Het gevalsonderscheid is niet noodzakelijk maar maakt het makkelijker om een oplossing te vinden als geval $= 1$. Aan het eind van paragraaf 3.3 wijzigen we dit gevalsonderscheid zodat meer situaties onder het algoritmisch makkelijke geval vallen, waarmee we het algoritme van Van Hoeij en Cremona [1] krijgen.

**Definitie 3.1.** Een oplosbaarheidscertificaat van vergelijking (1) is een lijst met:

- Voor alle $p \in \mathcal{S}_a$ een nulpunt van $(f_a \bmod p)$ in $L_p$.
- Voor alle $p \in \mathcal{S}_b$ een nulpunt van $(f_b \bmod p)$ in $L_p$.
- Voor alle $p \in \mathcal{S}_c$ een nulpunt van $(f_c \bmod p)$ in $L_p$.
- Als geval $= 0$: een niet-triviale oplossing in $F^3$ of oplosbaarheidscertificaat van de vergelijking

$$l_a x^2 + l_b y^2 + l_c z^2 = 0. \tag{2}$$

**Stelling 3.2.** *Vergelijking* (1) *heeft een niet-triviale oplossing als en alleen als er een oplosbaarheidscertificaat bestaat.*

Als geval $= 0$ moeten we een oplossing vinden van vergelijking (2), een kegelsnede over $F$ in plaats van $F[t]$. In het geval dat $F$ weer een functielichaam is kunnen we ons algoritme opnieuw uitvoeren, en is het algoritme dus recursief. Zoniet, dan zijn we aangewezen op andere algoritmes om een oplossing te vinden. Voor $F = \mathbb{Q}$ bestaan er algoritmes die gebaseerd zijn op stelling 2.14. Als $F = \mathbb{F}_q$ kunnen we een oplossing vinden door een eindig aantal mogelijkheden te proberen (maar er bestaat een algoritme dat sneller is).

We bewijzen de implicatie naar rechts van stelling 3.2. Zie de volgende paragraaf voor de rest van het bewijs.

**Lemma 3.3.** *Als vergelijking* (1) *een niet-triviale oplossing* $(x, y, z) \in K^3$ *heeft, dan heeft vergelijking* (2) *een niet-triviale oplossing in* $F^3$.

*Bewijs.* Zij $(x, y, z)$ zo'n oplossing en $d$ het maximum van de graden van $ax^2, by^2$ en $cz^2$. Deze polynomen hebben ofwel alle dezelfde graad $d$, of twee hebben graad $d$ en de derde een strikt kleinere graad. In het eerste geval vormen de kopcoëfficiënten van $x, y, z$ een oplossing van vergelijking (2). In het tweede geval, stel zonder verlies van algemeenheid dat $\deg(ax^2) < d$. Dan is $(0, l_y, l_z)$ een oplossing van vergelijking (2), waarbij $l_y$ en $l_z$ de kopcoëfficiënten van $y$ en $z$ zijn. □

**Lemma 3.4.** *Stel dat vergelijking* (1) *een niet-triviale oplossing* $(x, y, z) \in K^3$ *heeft. Dan bestaat er een oplosbaarheidscertificaat.*

*Bewijs.* Door de oplossing te schalen kunnen we aannemen dat $x, y, z \in F[t]$ en $\gcd(x, y, z) = 1$ geldt. Zij $p \in \mathcal{S}_a$. Er geldt nu $0 = ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \pmod{p}$. Noteer $\bar{y} = (y \bmod p) \in L_p$. Omdat $b$ en $c$ niet deelbaar zijn door $p$, zijn $\bar{y}$ en $\bar{z}$ beide 0 of beide ongelijk aan 0. Als ze allebei 0 zijn, dan geldt $p^2 \mid by^2 + cz^2 = -ax^2$. Omdat $a$ kwadraatvrij is geldt dan $p \mid x$, maar dat is in tegenspraak met $\gcd(x, y, z) = 1$. Dus $\bar{y}$ en $\bar{z}$ zijn ongelijk aan 0, en $\bar{y}/\bar{z}$ is een oplossing van $f_a \bmod p$. Op dezelfde manier vinden we nulpunten van $f_b$ en $f_c$ modulo de priemdelers van $b$ respectievelijk $c$. Als geval $= 0$, dan is de vierde benodigdheid bewezen door lemma 3.3. Er volgt dat er een oplosbaarheidscertificaat bestaat. □

## 3.3 Nulpunt vinden

We bewijzen stelling 3.2 door een algoritme te presenteren dat gegeven een oplosbaarheidscertificaat een oplossing van vergelijking (1) geeft. Dit bewijst tevens dat we van een willekeurige kegelsnede over $F(t)$ de oplosbaarheid kunnen bepalen en de oplossing kunnen vinden, als we het volgende kunnen:

- factoriseren in $F[t]$;
- van elementen in $L_p$ bepalen of het kwadraten zijn en zo ja, een wortel trekken;
- van kegelsneden over $F$ bepalen of ze een oplossing hebbben en zo ja, een oplossing vinden.

**Algoritme VindPunt**
**Invoer:** $a, b, c \in K^*$ die voldoen aan de eisen 1, 2 en 3 uit de inleiding, en een oplosbaarheidscertificaat.
**Uitvoer:** Een niet-triviale oplossing $(x, y, z) \in K$ van vergelijking (1).

1. Laat $d_a, d_b, d_c$ de graden van $a, b, c$ zijn.
2. Laat $\mathcal{S}_a, \mathcal{S}_b, \mathcal{S}_c$ de verzamelingen met dezelfde naam uit het oplosbaarheidscertificaat zijn.
3. Als $d_a \equiv d_b \equiv d_c \pmod 2$, laat geval $= 0$, en anders geval $= 1$.
4. Als geval $= 0$, laat $l_a, l_b, l_c \in F$ de kopcoëfficiënten van $a, b, c$ zijn, en laat $(l_x, l_y, l_z)$ de oplossing van vergelijking (2) zijn, afkomstig uit het oplosbaarheidscertificaat.
5. Laat $A = \left\lceil \frac{d_b + d_c}{2} \right\rceil - \text{geval}$, $B = \left\lceil \frac{d_c + d_a}{2} \right\rceil - \text{geval}$, $C = \left\lceil \frac{d_a + d_b}{2} \right\rceil - \text{geval}$.
6. Zij $V = \{(x, y, z) \in F[t]^3 : \deg(x) \le A, \deg(y) \le B, \deg(z) \le C\}$. Dit is een vectorruimte over $F$ van dimensie $A + B + C + 3$. Voor $p \in S_a \cup S_b \cup S_c =: \mathcal{S}$, zij $\alpha$ een nulpunt van $f_a \bmod p$, $f_b \bmod p$ respectievelijk $f_c \bmod p$. Zij $\phi_p : V \longrightarrow L_p$ gegeven door

$$(x, y, z) \longmapsto \begin{cases} y - \alpha z \bmod p, & \text{als } p \in \mathcal{S}_a, \\ z - \alpha x \bmod p, & \text{als } p \in \mathcal{S}_b, \\ x - \alpha y \bmod p, & \text{als } p \in \mathcal{S}_c. \end{cases}$$

   Zij verder, voor geval 0, $L_\infty = F^3$ en definieer $\phi_\infty : V \oplus F \to F^3$ door

$$\phi_\infty(x, y, z, w) = (x_A - l_x w, y_B - l_y w, z_C - l_z w),$$

   waarbij $x_A$, $y_B$ en $z_C$ de $A$'de, $B$'de respectievelijk $C$'de coëfficiënt van $x$, $y$ en $z$ zijn. Laat

$$\begin{cases} \phi : V \longrightarrow \left( \bigoplus_{p \in \mathcal{S}} L_p \right), \quad (x, y, z) \longmapsto (\phi_p(x, y, z))_{p \in \mathcal{S}}, & \text{als geval} = 1, \\ \phi : V \oplus F \longrightarrow \left( \bigoplus_{p \in \mathcal{S} \cup \{\infty\}} L_p \right), \quad (x, y, z, w) \longmapsto (\phi_p(x, y, z, w))_{p \in \mathcal{S} \cup \{\infty\}}, & \text{als geval} = 0. \end{cases}$$

Dit zijn lineaire afbeeldingen, want $L_p$ is een vectorruimte van dimensie $\deg(p)$ en de quotiëntafbeelding $F[t] \to L_p$ is lineair.

7. Bereken de kern van $\phi$ en kies een niet-triviaal element.

*Bewijs van de correctheid van Algoritme VindPunt.* We bewijzen dat het algoritme met een geldige invoer altijd een oplossing geeft. We laten eerst zien dat een element uit de kern van $\phi$ inderdaad een nulpunt is van $f = aX^2 + bY^2 + cZ^2$, door een bovengrens te vinden voor de graad en te laten zien dat $f$ geëvalueerd in dat nulpunt deelbaar is door een polynoom van hogere graad. Vervolgens laten we zien dat $\ker \phi \neq 0$, omdat de dimensie van het domein van $\phi$ in alle gevallen groter is dan de dimensie van het codomein.

Voor $p \in S_a$, $\alpha$ een nulpunt van $f_a \bmod p$, en een element $(x, y, z) \in \ker \phi$ geldt $y \equiv \alpha z \pmod{p}$, dus $f(x, y, z) \equiv ax^2 + (b\alpha^2 + c)z^2 \equiv 0 \pmod{p}$. Op dezelfde manier is $f(x, y, z)$ deelbaar door alle $p \in S_a \cup S_b \cup S_c$, en omdat $abc$ kwadraatvrij is, is $f$ deelbaar door $s := \prod(S_a \cup S_b \cup S_c) = abc$.

Zij $D = \deg(abc)$. Stel eerst geval $= 1$, en stel zonder verlies van algemeenheid dat $d_b \equiv d_c \pmod 2$. Dan geldt

$$\begin{aligned}\deg(f(x, y, z)) &\leq \max\{d_a + 2A, d_b + 2B, d_c + 2C\} \\ &= \max\{d_a + d_b + d_c - 2, d_a + d_b + d_c - 1, d_a + d_b + d_c - 1\} \\ &= D - 1,\end{aligned}$$

maar $f(x, y, z)$ is deelbaar door een polynoom van graad $\deg(s) = D$, dus $f(x, y, z) = 0$. Als geval $= 0$, dan geldt $\deg(f(x, y, z)) \leq D = d_a + 2A = d_b + 2B = d_c + 2C$. De coëfficiënt van $t^D$ is wegens $\phi_\infty(x, y, z, w) = 0$ en vergelijking (2) gelijk aan $w^2(l_a l_x^2 + l_b l_y^2 + l_c l_c^2) = 0$, dus $\deg(f(x, y, z)) \leq D - 1$. Ook in dit geval is $f(x, y, z)$ deelbaar door een polynoom van hogere graad, dus $f(x, y, z) = 0$.

We moeten nu nog laten zien dat het de dimensie van het domein van $\phi$ groter is dan de dimensie van het codomein. Als geval $= 0$, dan geldt $A + B + C = D$ en de dimensie van het domein is $A + B + C + 3 + 1 = D + 4$. Voor $p \in S_a \cup S_b \cup S_c$ van graad $d$ heeft $L_p$ dimensie $d$ en $F^3$ heeft dimensie 3, dus de dimensie van het codomein is $D + 3$. Als geval $= 1$ geldt $A + B + C = D - 2$. De dimensie van het domein is $A + B + C + 3 = D + 1$ en de dimensie van het codomein is $D$.

Er volgt dat $\ker \phi \neq 0$. In geval 0 is verder nodig dat $\ker \phi \neq \{\mathbf{0}\} \oplus F$, en dit is duidelijk omdat $\phi_\infty(0, 0, 0, 1) \neq \mathbf{0}$. We concluderen dat het algoritme in alle gevallen een niet-triviale oplossing van vergelijking (1) vindt. □

*Bewijs van stelling 3.2.* De implicatie naar rechts is bewezen met lemma 3.4, en de andere implicatie met het bewijs van Algoritme VindPunt. □

Het blijkt dat er meerdere situaties zijn waarin we het simpelere geval kunnen toepassen, dat wil zeggen, waarin we vergelijking (2) niet hoeven op te lossen. Om het algoritme te verbeteren wijzigen we het gevalsonderscheid als volgt, waarmee we het algoritme van Van Hoeij en Cremona [1] krijgen.

$$\text{geval} := \begin{cases} 0, & \text{als } d_a \equiv d_b \equiv d_c \pmod 2 \text{ en } abc \text{ heeft geen nulpunt in } F; \\ 1, & \text{anders.} \end{cases}$$

Als $abc$ een nulpunt in $F$ heeft en $d_a \equiv d_b \equiv d_c \pmod 2$, dan verwijderen we voor het uitvoeren van het algoritme één element van graad 1 uit $\mathcal{S}_a, \mathcal{S}_b$ of $\mathcal{S}_c$ in het oplosbaarheidscertificaat.

We volgen de notatie van bewijs van Algoritme VindPunt en laten zien dat het algoritme nog steeds een oplossing geeft. Er geldt nu $\deg(s) = D - 1$, maar voor een element $(x, y, z) \in \ker \phi$ geldt $\deg(f(x, y, z)) \leq D - 2$. Om te laten zien dat $\ker \phi \neq 0$: er geldt nu $A + B + C = D - 3$. De dimensie van het domein is $\deg(S) + \dim_F(F) = D - 1 + 1 = D$ en de dimensie van het codomein is $D - 1$.

Laat Algoritme VindPunt* het Algoritme VindPunt zijn waarbij we in de laatste stap uit een basis van $\ker \phi \subset V \oplus F$ een maximale verzameling linear onafhankelijke oplossingen in $V$ als uitvoer

geven, in plaats van een enkele oplossing. De volgende propositie laat zien dat we alle oplossingen tot een bepaalde graad kunnen vinden als we Algoritme VindPunt* uitvoeren voor alle mogelijke oplosbaarheidscertificaten.

**Propositie 3.5.** *Zij* $(x, y, z) \in F(t)$ *een niet-triviale oplossing van vergelijking* (1) *zodat* $\deg(x) \leq A$, $\deg(y) \leq B$ *en* $\deg(z) \leq C$, *met* $A, B, C$ *zoals in Algoritme VindPunt. Dan bestaat er een oplosbaarheidscertificaat waarvoor* $(x, y, z)$ *een lineaire combinatie is van oplossingen in de uitvoer van Algoritme VindPunt*.*

*Bewijs.* Zij $(x, y, z) \in F(t)$ een niet-triviale oplossing van vergelijking (1) zodat $\deg(x) \leq A$, $\deg(y) \leq B$ en $\deg(z) \leq C$. De bewijzen van lemma 3.3 en lemma 3.4 geven een methode om een oplosbaarheidscertificaat te vinden, met nulpunten $(\frac{y}{z} \bmod p) \in L_p$ van $f_a \bmod p$ voor alle $p \in \mathcal{S}_a$, vergelijkbare nulpunten voor $\mathcal{S}_b$ en $\mathcal{S}_c$. Zie het bewijs van lemma 3.3 voor de constructie van een oplossing $(l_x, l_y, l_z) \in F$ van vergelijking (2), als geval $= 0$. We laten zien dat $(x, y, z) \in \ker \phi$, met $\phi$ zoals in Algoritme VindPunt en als invoer het bovengenoemde oplosbaarheidscertificaat, en dit bewijst de propositie.

Voor $p \in \mathcal{S}_a$ en $\phi_p$ als in Algoritme VindPunt geldt $\phi_p(x, y, z) = (y - \frac{y}{z} \cdot z \bmod p) = 0$, dus geldt $(x, y, z) \in \ker \phi_p$ voor alle $p \in \mathcal{S}_a \cup \mathcal{S}_b \cup \mathcal{S}_c$. Dus als geval $= 1$ geldt $(x, y, z) \in \ker \phi$. Als geval $= 0$ moeten we nog bewijzen dat $(x, y, z, w) \in \ker \phi_\infty$ voor een $w \in F$. Stel eerst $\deg(x) < A$, $\deg(y) < B$ en $\deg(z) < C$. Dan geldt $\phi_\infty(x, y, z, 0) = (0, 0, 0)$. Stel nu dat een van de graden van $x, y, z$ maximaal is (van graad $A$, $B$ respectievelijk $C$), en stel zonder verlies van algemeenheid $\deg(x) = A$.

Zij $d$ het maximum van de graden van $ax^2$, $by^2$ en $cz^2$, zoals in lemma 3.3. Stel dat deze polynomen alle dezelfde graad hebben. Uit $\deg(ax^2) = \deg(by^2)$ volgt $d_a + d_b + d_c = d_b + 2 \cdot \deg(y)$, dus $\deg(y) = B$. Met hetzelfde argument volgt $\deg(z) = C$, dus $\phi_\infty(x, y, z, 1) = (0, 0, 0)$. Stel nu dat een van de polynomen strikt lagere graad heeft. Er geldt $\deg(ax^2) = d_a + d_b + d_c$ is groter gelijk aan $\deg(by^2)$ en $\deg(cz^2)$, dus stel zonder verlies van algemeenheid $\deg(by^2) < d$. Nu geldt $\deg(ax^2) = \deg(cz^2)$, dus $\deg(z) = C$. Verder geldt $l_y = 0$ (zie het bewijs van lemma 3.3). Er volgt dat $\phi_\infty(x, y, z, 1) = (0, 0, 0)$. □

# 4 Implementatie en voorbeelden

Het algoritme zoals in deze scriptie beschreven (inclusief de verbetering aan het eind van paragraaf 3.3) is door de auteur geïmlementeerd in SageMath. Het algoritme zal in de standaardfunctionaliteit van SageMath worden opgenomen, en is reeds beschikbaar voor ontwikkelaars op `http://trac.sagemath.org/ticket/6881`. Van Hoeij en Cremona [1] hebben een implementatie geschreven voor Maple en Magma.

De implementatie kan gebruikt worden om kegelsneden over $\mathbb{Q}(t)$ op te lossen:

```
sage: K.<t> = FractionField(PolynomialRing(QQ, 't'))
sage: C = Conic(K, [t^2-2, 2*t^3, -2*t^3-13*t^2-2*t+18])
sage: C.has_rational_point(point=True)
(True, (-3 : (t + 1)/t : 1))
```

Het is ook mogelijk om kegelsneden over polynoomringen over eindige lichamen en eindige lichaamsuitbreidingen van $\mathbb{Q}$ op te lossen:

```
sage: R.<t> = FiniteField(23)[]
sage: C = Conic([2, t^2+1, t^2+5])
sage: C.has_rational_point(point = True)
(True, (5*t : 8 : 1))
sage: F.<i> = QuadraticField(-1)
sage: R.<t> = F[]
sage: C = Conic([1, i*t, -t^2+4])
sage: C.has_rational_point(point = True)
...
(True, (-t - 2*i : -2*i : 1))
```

Het is nog niet mogelijk om kegelsneden over $F(t)$ op te lossen waarbij $F$ weer een functielichaam is, omdat SageMath geen wortels kan trekken in eindige uitbreidingen van functielichamen.

Het is ook mogelijk om direct Algoritme VindPunt uit te voeren, met behulp van de functie `find_point(supports, roots, case, solution)`. Dit is handig omdat verschillende oplosbaarheidscertificaten verschillende punten kunnen geven, en we wegens propositie 3.5 alle oplossingen tot een bepaalde graad kunnen vinden door alle oplosbaarheidscertificaten te proberen. Zie het volgende voorbeeld:

```
sage: K.<t> = PolynomialRing(QQ, 't')
sage: C = Conic(K, [t^2-2, 2*t, -2*t^3-13*t^2-2*t+18])
sage: supp = [[t^2 - 2], [t], [t^3 + 13/2*t^2 + t - 9]]
sage: tbar1 = QQ.extension(supp[0][0], 'tbar').gens()[0]
sage: tbar2 = QQ.extension(supp[1][0], 'tbar').gens()[0]
sage: tbar3 = QQ.extension(supp[2][0], 'tbar').gens()[0]
sage: roots = [[tbar1 + 1], [1/3*tbar2^0], [2/3*tbar3^2 + 11/3*tbar3 - 3]]
sage: C.find_point(supp, roots, 1)
(3 : t + 1 : 1)
sage: roots = [[-tbar1 - 1], [-1/3*tbar2^0], [-2/3*tbar3^2 - 11/3*tbar3 + 3]]
sage: C.find_point(supp, roots, 1)
(3 : -t - 1 : 1)
```

## Referenties


[1] Mark van Hoeij en John Cremona. „Solving conics over function fields". In: *J. Théor. Nombres Bordeaux* 18.3 (2006), p. 595–606. ISSN: 1246-7405.

[2] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. 2de ed. Deel 58. Graduate Texts in Mathematics. Springer-Verlag, New York, 1984, p. xii+150. ISBN: 0-387-96017-1. DOI: 10.1007/978-1-4612-1112-9. URL: http://dx.doi.org/10.1007/978-1-4612-1112-9.

[3] Joachim Schwermer. „Minkowski, Hensel, and Hasse: on the beginnings of the local-global principle". In: *Episodes in the history of modern algebra (1800–1950)*. Deel 32. Hist. Math. Amer. Math. Soc., Providence, RI, 2007, p. 153–177.

[4] Jean-Pierre Serre. *A course in arithmetic*. Translated from the French, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973, p. viii+115.