STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1969-002

De vlakke kubische Kromme

Prof. Dr. F. van der Blij

Voordracht in de serie

"Elementaire onderwerpen vanuit hoger standpunt belicht"

1969

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
AFDELING ZUIVERE WISKUNDE

ZW 1969-002

Voordracht in de serie

"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof.Dr. F. van der Blij.

De vlakke kubische Kromme.

§1. Inleiding.

Laat k een lichaam zijn, V het projectieve vlak over k. Laat N een kubische vorm zijn in k^3. De bijbehorende trilineaire vorm geven we ook met N aan. De kubische vorm definieert een kubische kromme C in V. We veronderstellen verder dat deze kromme niet ontaard is, en niet birationaal equivalent is met de projectieve rechte. De kromme heeft dan geslacht 1, krommen van geslacht 1 noemt men wel elliptische krommen. Men kan bewijzen dat iedere elliptische kromme birationaal equivalent is met een kubische kromme.

De punten op een elliptische kromme vormen een groep. Om deze groep te beschrijven beschouwen we gemakshalve het geval dat de kromme C een over k gedefinieerd buigpunt $\mathcal{O}$ bezit.

We definieren een compositie $\ast$ door

$P \ast Q = R$ als $\ulcorner P,Q,T \urcorner$ en $\ulcorner R,\mathcal{O},T \urcorner$ collineaire tripels zijn, waarbij $T \in C$. We merken op dat $P \ast Q = Q \ast P$ en dat $P \ast \mathcal{O} = P$. De associativiteit volgt uit een klassieke stelling over bundels kubische krommen.

Gebruikmakende van de trilineaire vorm $N(P,Q,R)$ (we identificeren de namen van de punten met de tripels coördinaten) vinden we voor het met P en Q collineaire punt T op de kromme

$$T = N(P,P,Q)Q - N(P,Q,Q)P$$

Op deze manier kan R in coördinaten berekend worden en via berekeningen de associativiteit geverifieerd worden.
We merken op dat drie punten P, Q en R van C dan en slechts dan collineair zijn als $N(P,Q,R) = 0$.

Bovendien geldt voor drie collineaire punten P, Q en R dat $(P \ast Q) \ast R = \mathcal{O}$.

De expliciete schrijfwijze met de trilineaire vorm leent zich niet bizonder goed voor de bestudering van birationale invarianten. Daarom kiezen we een beschrijving door middel van de keuze van een speciaal coördinaten stelsel. Veelal bestuderen we de kromme verder in een affien vlak. De birationale eigenschappen van de kromme zijn te beschrijven in termen van het bijbehorende functielichaam $k(x,y)$. De groep van de kromme is uit de divisoren groep van $k(x,y)$ af te leiden.

§2. Speciale coördinaten.

Laten we aannemen dat C een over k gedefinieerd punt A bevat. Dan is ook de raaklijn in A over k gedefinieerd en deze snijdt de kromme verder nog in een over k gedefinieerd punt B. Als $B \neq A$ verondersteld wordt, voeren we coördinaten $A = (0,0,1)$ en $B = (0,1,0)$ in; de raaklijn in B zij $z = 0$. De vergelijking van de kromme wordt dan

$$\alpha y^2z + \beta xyz + \gamma x^2y + \delta x^3 + \varepsilon x^2z + \eta xz^2 = 0.$$

Is B een buigpunt dan is $\gamma = 0$. Is B geen buigpunt dan kunnen we het snijpunt van de raaklijn in B de coördinaten $(1,0,0)$ geven.

Na een birationale transformatie $x = \bar{x}^2$, $y = \bar{x}\bar{y}$, $z = \bar{y}\bar{z}$ wordt de vergelijking dan

$$\alpha y^2z + \beta xyz + \gamma x^3 + \varepsilon x^2z + \eta yz^2 = 0.$$

In het geval $\chi_k \neq 2,3$ kunnen we nog een eenvoudige birationale transformatie uitvoeren en de kromme een vergelijking in affiene coördinaten geven van de vorm:

$$y^2 = x^3 + ax + b.$$

Stelling. Iedere elliptische kromme over een lichaam met karakteristiek $\neq 2,3$ is birationaal equivalent met $y^2 = x^3 + ax + b$. Twee krommen $y^2 = x^3 + a_1x + b_1$ en $y^2 = x^3 + a_2x + b_2$ zijn birationaal equivalent dan en slechts dan als er een $m \in k$ bestaat met

$$a_1 = m^4 a_2, \quad b_1 = m^6 b_2.$$

Het bewijs kan b.v. elegant met de theorie van de functielichamen (Riemann-Roch) geleverd worden. We merken nog op dat a^3b^{-2} een birationale invariant van C is. Als regel introduceerd men

$$j = 2^8 \cdot 3^3 a^3 (4a^3 + 27b^2)^{-1}$$

als invariant. Bij iedere $j \in k$ behoort dan een elliptische kromme.

We beschrijven nog even de groepsoperaties in de nieuwe coördinaten. Laat $\mathcal{O} = (0,1,0)$. Laat verder $P + \bar{P} = \mathcal{O}$. Dan geldt

$$x_{\bar{P}} = x_P \quad , \quad y_{\bar{P}} = -y_P$$

$$x_{P+Q} = -x_P - x_Q + \left(\frac{y_P - y_Q}{x_P - x_Q} \right)^2$$

$$y_{P+Q} = y_P + y_Q - 3 \frac{x_Py_Q - x_Qy_P}{x_P - y_Q} - \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2$$

en evenzo

$$x_{P+P} = -2x_P + \frac{(3x^2_P + a)^2}{x^3_P + ax_P + b} \quad ,$$

$$y_{P+P} = \left\{ 2 + 3 \frac{x^2_P - 3x_P + b}{x^2_P + ax_P + b} - \frac{(3x_P + a)^3}{(x_P + ax_P + b)^2} \right\} y_P \, .$$

§3. Speciale lichamen.

Laat verder steeds $\chi_k \neq 2,3$. Laat k compleet zijn voor een al dan niet archimedische waardering. Voor $0 < |t| < 1$ definieren we een tweetal meromorfe funkties van w door

$$x_t(w) = \frac{1}{12} + \sum_{m=-\infty}^{+\infty} \frac{t^m w}{(1-t^m w)^2} - 2 \sum_{m=1}^{\infty} \frac{t^m}{(1-t^m)^2} \quad .$$

$$y_t(w) = \sum_{m=-\infty}^{+\infty} \frac{(t^m w)^2}{(1-t^m w)^3} + \frac{1}{2} \sum_{m=-\infty}^{\infty} \frac{t^m w}{(1-t^m w)^2} \quad .$$

Dan geldt

$y_t^2(w) = x_t^3(w) + a\, x_t(w) + b$, met

$$a = -\frac{1}{12} - 20 \sum_{m=1}^{\infty} \frac{m^3 t^m}{1-t^m} \quad ,$$

$$b = \frac{1}{216} - \frac{7}{3} \sum_{m=1}^{\infty} \frac{m^5 t^m}{1-t^m} \quad .$$

We merken op dat

$$x_t(w^{-1}) = x_t(w) \quad , \qquad y_t(w^{-1}) = -y_t(w) \quad ,$$

$$x_t(tw) = x_t(w) \quad , \qquad y_t(tw) = y_t(w) \quad .$$

Het geval k = $\mathbb{C}$, de complexe getallen is klassiek.
Schrijven we $t = e^{2\pi i\omega}$, $w = e^{2\pi iz}$, dan wordt de parameter voorstelling gegeven door

$$x(e^{2\pi iz}) = \wp(z)$$

$$y(e^{2\pi iz}) = \tfrac{1}{2}\wp'(z)$$

met $$\wp(z) = z^{-2} + \sum_{n,m}{}' \left[\frac{1}{(z+n+m\omega)^2} - \frac{1}{(n+m\omega)^2} \right] ,$$

$$\wp'(z) = -2z^{-3} + \sum_{n,m}{}' \frac{-2}{(z+n+m\omega)^3} ;$$

$$\wp(z+1) = \wp(z) \quad ; \quad \wp(z+\omega) = \wp(z) \quad .$$

§4. De endomorfismen ring van C.

Laat μ een rationale afbeelding zijn van C in C, die een groeps homomorfisme is. We hebben dan voor $A \in C$

$$x_{\mu A} = \frac{P_\mu(x_A)}{Q_\mu(x_A)} \quad ; \qquad y_{\mu A} = \frac{R_\mu(x_A)}{S_\mu(x_A)}\, y_A$$

met polynomen P_μ , Q_μ , R_μ , S_μ. We veronderstellen P_μ en Q_μ onderling ondeelbaar. We definieren $d(\mu)$ = graad van P_μ. De endomorfismen vormen een ring E, we definieren $(\mu + \nu)(A) = \mu(A) \dashv \nu(A)$,
$\mu(\bar{A}) = -\mu(A)$ als $A \dashv \bar{A} = \mathcal{O}$, en

$(\mu.\nu)(A) = \mu(\nu(A))$.

Voor d gelden de volgende regels:

$d(0) = 0$, $d(1) = 1$, $d(\mu.\nu) = d(\mu).d(\nu)$

$d(\mu + \nu) + d(\mu - \nu) = 2d(\mu) + 2d(\nu)$.

De laatste formule is te verifieren met de expliciete formule voor $A \dashv B$ in §2. We kunnen d voortzetten tot $E \otimes_{\mathbb{Z}} \mathbb{R}$. Deze laatste is een algebra over $\mathbb{R}$, die nuldelervrij is en een kwadratische norm d bezit.
Volgens een klassieke stelling geldt dan $E \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}$, $\mathbb{C}$ of $\mathbb{H}$
($\mathbb{H}$ = kwaternionen).

Omdat d geheel is op E vinden we voor E hetzij $\mathbb{Z}$, hetzij een ring van gehelen in een imaginair kwadratisch lichaam, hetzij een ring van gehele kwaternionen.

Stelling. Voor een k met $\chi_k = 0$, heeft een elliptische kromme een endomorfismen ring E, die isomorf is met $\mathbb{Z}$, behalve mogelijk voor speciale waarden van j, waarvoor de ring E isomorf is met een ring van gehele imaginair kwadratische getallen (singuliere j, dan complexe vermenigvuldiging). Als $\chi_k \neq 0$ kunnen er waarden van j zijn , super singuliere, waarvoor E isomorf is met een ring van gehele kwaternionen.

De afbeelding m: $A \longrightarrow A \dashv A \dashv A \dashv \ldots \dashv A$ (m factoren) is een element van E. Eenvoudige berekening leert $d(m) = m^2$. De punten A met $A \dashv A = \mathcal{O}$ zijn de vier raakpunten van de uit $\mathcal{O}$ aan de kromme getrokken raaklijnen.

De negen punten B met $B * B * B = \mathcal{O}$ zijn de negen buigpunten van de kromme. In het algemeen zijn er m^2 punten met de orde m. Deze punten zijn niet noodzakelijk over k gedefinieerd. Een klassieke stelling leert b.v. dat de 9 buigpunten van een kubische kromme nooit alle reëel kunnen zijn.

In het geval $k = \mathbb{C}$ kunnen we de parametrisering met $\wp$ gebruiken. Laat $P_1 = (\wp(z_1), \frac{1}{2}\wp'(z_1))$ en $P_2 = (\wp(z_2), \frac{1}{2}\wp'(z_2))$. Dan geldt $P_1 * P_2 = (\wp(z_1+z_2), \frac{1}{2}\wp'(z_1+z_2))$ en $\bar{P}_1 = (\wp(-z_1), \frac{1}{2}\wp'(-z_1))$. Verder $m(P_1) = (\wp(mz_1), \frac{1}{2}\wp'(mz_1))$. Verder $m(P_1) = (\wp(mz_1), \frac{1}{2}\wp'(mz_1))$.
Zelfs geldt voor "complexe endomorfismen" $\omega(P_1) = (\wp(\omega z_1), \frac{1}{2}\wp'(\omega z_1))$
Hieruit is opnieuw direct af te leiden dat ω geheel, imaginair kwadratisch moet zijn.

§5. Eindige lichamen.

Laat $k = \mathbb{F}_q$, dan is de frobenius $\phi(x,y) = (x^q, y^q)$ een endomorfisme van de kromme. Men rekent snel na dat $d(\phi) = q$. We beschouwen nu $\phi - 1$. Voor $A = (x,y)$ geldt $(\phi - 1)A = (x^q, y^q) * (x, -y) = (x_1, y_1)$

$$x_1 = -x^q - x + \frac{y^2(y^{q-1}+1)^2}{(x^q-x)^2} \quad ,$$

$$x_1 = -x^q - x + \frac{(x^3+ax+b)(y^{q-1}+1)^2}{(x^q-x)^2} \quad .$$

Hieruit volgt na enige berekening $d(\phi - 1) = 2q + 1 - 2m - n$, waarbij

$$m = \#\{\lambda \in k \mid (\lambda^3 + a\lambda + b)^{\frac{q-1}{2}} = -1\}$$

$$n = \#\{\lambda \in k \mid \lambda^3 + a\lambda + b = 0\}$$

Verder geldt

$$N_q \underset{\text{def}}{=\!=} \#\{\lambda, \mu \in k \mid \mu^2 = \lambda^3 + a\lambda + b\} + 1 = 2q + 1 - 2m - n.$$

Als nu $d(\phi + \psi) = d(\phi) + d(\psi) + \langle\phi,\psi\rangle$, dan

$$\langle\phi, 1\rangle = d(\phi-1) - d(\phi) - d(1) = N_q - q - 1.$$

Uit de ongelijkheid van Cauchy volgt $|\langle\phi,1\rangle| \leq 2q^{\frac{1}{2}}$.

Stelling. Het aantal punten over $k = \mathbb{F}_q$ van een elliptische kromme is gelijk aan

$$N_q = q + 1 + \langle\phi,1\rangle \qquad \text{met} \qquad |\langle\phi,1\rangle| \leq 2q.$$

Als q een priem getal is geldt:

$$\langle\phi,1\rangle = \sum_{x \bmod q} \left(\frac{x^3 + ax + b}{q}\right).$$

§6. De structuur van de groep G van een elliptische kromme.

Als $k = \mathbb{C}$ leiden we direct uit de parametervoorstelling van C af dat $G \cong \mathbb{C}^+/\mathbb{Z}+\omega\,\mathbb{Z}$; dat wil zeggen G is een torusgroep.

Als $k = \mathbb{R}$ leiden we uit de parametervoorstelling af dat òf

$$G \cong \mathbb{T} = \mathbb{R}/\mathbb{Z}$$

òf dat T een ondergroep met index 2 in G is.

Als $k = \mathbb{Q}_p$, een p-adisch lichaam, geldt

$$G \cong k^*/_t\,\mathbb{Z} \qquad \text{(zie §4)}$$

Als k een globaal lichaam is geldt de stelling van Mordell-Weil: G is eindig voortgebracht.

Voor het geval $k = \mathbb{Q}$ en $y^2 = (x - e_1)(x - e_2)(x - e_3)$ met rationale e_1, e_2 en e_3 is deze stelling elementair te bewijzen. Zie S. Chowla: The Riemann Hypothesis and Hilbert's Tenth Problem, 1965, New York, chapter VI. (The proof is nothing beyond the capacity or ability of a ten-year old).

§7. De Zetafunctie van C. Laat $N_q = \#\{\text{punten op C, over } \mathbb{F}_q \text{ gedefinieerd}\}$, waarbij $q = p^m$. We definieren

$$\log Z_p(t) = 1 + \sum_{m=1}^{\infty} N_{p^m} \frac{t^m}{m}.$$

We merken terloops op dat we ook $Z_p(t)$ hadden kunnen definieren als

$\prod_P (1 - N(P)^{b_{\log t}})^{-1}$, waarin het product uitgestrekt wordt over alle punten van C in de algebraïsche afsluiting van $\mathbb{F}_p$ en $N(P) = p^{\text{graad}(P)}$

$$Z_p(t) = (1-t)^{-1} (1-pt)^{-1} (1 - (p+1-N_p)t + pt^2).$$

We definieren nog

$$\zeta_p(s) = (1-p^{-s})^{-1} (1-p^{1-s})^{-1} (1 - (p+1-N_p)p^{-s} + p^{1-2s}).$$

En tenslotte

$$\zeta_C(s) = \prod_p \zeta_P(s) = \zeta(s)\,\zeta(s-1) \prod_p (1 - (p+1-N_p)p^{-s} + p^{1-2s}).$$

We schrijven

$$L_C(s) = \prod_p (1 - (p+1-N_p)p^{-s} + p^{1-2s})^{-1}.$$

Men kan nu vragen naar de voortzetbaarheid van L, naar een functionaal vergelijking, naar arithmetische betekenis o.a. van $L_C(1)$. Vele vermoedens zijn geformuleerd, in het geval van een kromme met complexe vermenigvuldiging kan men enkele resultaten verkrijgen. In dit geval is $L_C(s)$ te schrijven als een dirichlet L-reeks met "Grösszencharakter", op een factor na, die van de z.g. slechte priemgetallen afhangt. Dat zijn die priemgetallen waarvoor de elliptische kromme over $\mathbb{F}_p$ beschouwd niet langer elliptisch blijft.

§8. Opmerkingen.

De meeste literatuur verwijzingen zijn te vinden in een uitvoerig overzichts artikel van J.W.S. Cassels:
Diophantine equations with special reference to elliptic curves.
Journal London Math. Soc. 41 (1966) 193-291.
Verder zijn recente resultaten te vinden in
G. Shimura: Automorphic functions and number theory Berlin, 1968.

ijzen nog op enkele artikelen:

eil: Über die Bestimmung Dirichletscher Reihen durch Funktional chungen. Math. Ann. 168 (1967), 149-156.

nara: Hecke polynomials as congruence ζ functions in elliptic modular case. Ann. of Math. 85 (1967) 267-295.

oeiend probleem is nog de vraag naar punten met gehele coördinaten; $^2 = x^3+1$ liggen er zo precies zes! Soms is een vierde graads ruimte ne een beter model voor een elliptische kromme b.v. $\lambda x^2 + y^2 = t^2$, $^2 + z^2 = T^{\frac{1}{2}}$, men parametriseert dan met Θ-functies.