Weil pairing and the Drinfeld modular curve

van der Heiden, Gerrit

Samenvatting

In 1974 verscheen er van de hand van de Oekraïnse wiskundige Vladimir Gershonovich Drinfeld een baanbrekend artikel getiteld 'Elliptic modules'. Met deze elliptische modulen, die tegenwoordig *Drinfeld modulen* worden genoemd, voegde de toen 19-jarige Drinfeld een nieuw en belangwekkend onderwerp toe aan de arithmetische theorie van functielichamen. Eén van de mooiste resultaten binnen deze theorie is voor een groot deel verkregen dankzij Drinfelds werk. Samen met de resultaten verkregen in zijn artikel uit 1974 weet hij in 1977 een bewijs te geven van een speciaal geval van het zogenaamde *Langlands' vermoeden*.
Dit nogal technische vermoeden staat nog steeds in het centrum van de belangstelling, omdat het nogal verreikende consequenties heeft. Zo sluit bijvoorbeeld het bewijs dat de Engelse wiskundige Andrew Wiles in 1994 geeft van de laatste stelling van Fermat naadloos aan bij pogingen meer over dit vermoeden (voor getallenlichamen) te bewijzen. De bewijsstrategie die Drinfeld uiteenzet blijkt conceptueel zo goed te zijn dat de Franse wiskundige Laurent Lafforgue deze strategie in 2000 kan generaliseren tot een indrukwekkend bewijs van Langlands' vermoeden voor functielichamen in het algemeen. Door deze fundamentele ontwikkelingen heeft de functielichamentheorie zich een belangrijke plaats weten te verwerven binnen de hedendaagse wiskunde. De waardering voor deze resultaten is navenant. In 1990 wordt aan Drinfeld de Fields medal, een prestigieuze prijs voor wiskundigen, uitgereikt en hetzelfde overkomt Lafforgue twaalf jaar later.

Ondanks deze heftige ontwikkelingen bevat de literatuur over Drinfeld modulen en Drinfeld modulaire krommen nog een aantal gaten. Er is en wordt veel werk verricht om deze op te vullen en de theorie expliciet te maken. Dit proefschrift neemt een deel van dit werk voor z'n rekening.
De verwantschap tussen de theorie van elliptische krommen en de theorie van Drinfeld modulen vormt een belangrijke leidraad voor de werkwijze in dit proefschrift. Deze analogie heeft Drinfeld geïnspireerd tot de naam die hij koos voor de objecten die hij introduceerde in 1974: de naam 'elliptisch moduul' suggereert een verband met de theorie van elliptische krommen.
In dit proefschrift wordt de Weil paring ontwikkeld voor Drinfeld modulen. Deze Weil paring is klassiek bekend voor elliptische krommen en is daar behulpzaam bij het beschrijven van klassieke modulaire krommen. Zo ook hier. Na de constructie van de Weil paring wordt deze paring benut om de Drinfeld modulaire krommen te bestuderen. Alvorens iets over deze modulaire krommen te zeggen wil ik hier een eenvoudig voorbeeld geven van de Weil paring.

Laat ik beginnen met een voorbeeld van een functielichaam. In de definitie van Drinfeld

modulen worden functielichamen van krommen over een eindig lichaam gebruikt. Een eenvoudig voorbeeld van een *eindig lichaam* is de verzameling $\mathbb{F}_2 = \{0, 1\}$ voorzien van een optelling en een vermenigvuldiging. De elementen 0 en 1 van $\mathbb{F}_2$ kun je op de gebruikelijke manier optellen en vermenigvuldigen; er is één uitzondering: we definiëren $1 + 1 = 0$.
Vervolgens beschouwen we de *polynoomring* $\mathbb{F}_2[T]$. Dit is een verzameling bestaande uit alle polynomen met coëfficiënten in $\mathbb{F}_2$, d.w.z. de elementen uit $\mathbb{F}_2[T]$ zijn van de vorm $a_0 + a_1T + \ldots + a_nT^n$ met a_i is of 0 of 1. En deze elementen kun je weer optellen en vermenigvuldigen. Het bijbehorende *functielichaam* noteren we als $\mathbb{F}_2(T)$. Deze bestaat uit alle quotiënten $\frac{f_1}{f_2}$ waarbij f_1 en f_2 elementen uit $\mathbb{F}_2[T]$ zijn en bovendien geldt $f_2 \neq 0$.
Het kwadrateren van elementen uit $\mathbb{F}_2(T)$ noteren we met de afbeelding

$$\tau : \mathbb{F}_2(T) \longrightarrow \mathbb{F}_2(T), \quad f \mapsto f^2.$$

De functie τ heeft een speciale plaats in deze theorie, omdat τ *lineair* is, d.w.z. voor alle elementen g_1, g_2 in $\mathbb{F}_2(T)$ geldt $\tau(g_1 + g_2) = \tau(g_1) + \tau(g_2)$. (Dit is makkelijk na te rekenen als je bedenkt dat '$2 = 0$' in $\mathbb{F}_2$.) Een *Drinfeld moduul* φ over $\mathbb{F}_2(T)$ is een afbeelding

$$\varphi : \mathbb{F}_2[T] \longrightarrow \mathbb{F}_2(T)[\tau]$$

met een aantal specifieke eigenschappen: φ is een ringhomomorfisme. Aan de rechterkant van de bovenstaande pijl staat een (scheve) polynoomring. De polynomen zijn $g_0 + g_1\tau + \ldots + g_n\tau^n$ waarbij elke g_i een element van $\mathbb{F}_2(T)$ is. De optelling in deze ring gaat zoals gebruikelijk. De vermenigvuldiging wordt gegeven door de vermenigvuldiging in $\mathbb{F}_2(T)$ en de regel $\tau \cdot g = \tau(g) \cdot \tau = g^2 \cdot \tau$. Van deze regel komt het scheve karakter van de polynoomring. In deze regel zie je ook het dubbele gebruik van τ: als afbeelding op $\mathbb{F}_2(T)$ en als 'variabele' van de polynoomring.
We schrijven $\varphi(T) = T + c_1\tau + \cdots + c_r\tau^r$. Deze r noemen we de *rang* van φ. Dat de constante van $\varphi(T)$ alleen T mag zijn volgt uit de 'specifieke eigenschappen' van een Drinfeld moduul.
Je kunt $\varphi(T)$ zien als een afbeelding $\varphi(T) : \mathbb{F}_2(T) \longrightarrow \mathbb{F}_2(T)$ gegeven door

$$y \mapsto \varphi(T)(y) = Ty + c_1\tau(y) + \cdots + c_r\tau^r(y) = Ty + c_1y^2 + \cdots + c_ry^{2^r}.$$

Met $\ker(\varphi(T))$ noteren we de verzameling die bestaat uit de elementen y waarvoor geldt $\varphi(T)(y) = 0$. Dit betekent dat $\ker(\varphi(T))$ bestaat uit alle elementen y met

$$\varphi(T)(y) = Ty + c_1y^2 + \cdots + c_ry^{2^r} = 0.$$

Als we bijvoorbeeld $\varphi(T) = T - \tau$ nemen, dan geldt

$$\varphi(T)(y) = (T - \tau)(y) = T \cdot y - y^2.$$

En dus bestaat $\ker(\varphi(T))$ uit de elementen $y = 0$ en $y = T$.

Stel dat φ een Drinfeld moduul van rang 2 is, zeg $\varphi(T) = T + c_1\tau + c_2\tau^2$. De constructie van de Weil paring maakt bij φ een Drinfeld moduul ψ van rang 1. In dit speciale geval kunnen we de formule uitrekenen voor $\psi(T)$; die is $\psi(T) = T - c_2\tau$.
De Weil paring is de volgende afbeelding, die we expliciet kunnen geven:

$$w : \ker(\varphi(T)) \times \ker(\varphi(T)) \longrightarrow \ker(\psi(T)), \quad (y_1, y_2) \mapsto w_f(y_1, y_2) = y_1y_2^2 - y_1^2y_2.$$

In hoofdstuk 4 wordt de constructie van deze Weil paring gegeven. Deze constructie is min of meer een gevolg van het artikel 'T-motives' van de Amerikaanse wiskundige Greg Anderson uit 1985. Een groot deel van dit hoofdstuk is gewijd aan het generaliseren van delen van Andersons artikel naar willekeurige globale functielichamen.
Met deze Weil paring wordt de *Drinfeld modulaire kromme* bestudeerd. Een Drinfeld modulaire kromme van niveau f classificeert (isomorfie klassen van) Drinfeld modulen van rang 2 met een niveau f-structuur. (Deze niveaustructuur is een technisch hulpmiddel: als je alleen isomorfie klassen van Drinfeld modulen classificeert, dan krijg je niet de prettige algebraïsche eigenschappen die je wilt. Het toevoegen van niveau f-structuren lost dit probleem op.) Classificeren betekent hier dat elk punt op de modulaire kromme correspondeert met een Drinfeld moduul met niveaustructuur en, omgekeerd, dat elk Drinfeld moduul met niveaustructuur correspondeert met een punt op deze kromme. De precieze formulering is te vinden in hoofdstuk 1.

In hoofdstuk 5 wordt deze Drinfeld modulaire kromme bestudeerd. Eerst laat ik zien dat de Weil paring aanleiding geeft tot een afbeelding van de Drinfeld modulaire kromme naar de punten die de Drinfeld modulen van rang 1 met niveau f-structuur classificeren. Daarnaast bestudeer ik de compactificatie van deze kromme. Er is een meetkundige eigenschap die *compactheid* of *compleetheid* wordt genoemd. De Drinfeld modulaire kromme blijkt niet compact te zijn, maar deze kromme kan wel compact gemaakt worden door een paar extra punten toe te voegen. Zulke toegevoegde punten heten *spitsen*, in het Engels *cusps*.
De vraag is wat deze toegevoegde punten betekenen. Zo'n spits correspondeert niet met een Drinfeld moduul met niveaustructuur. Immers, zo'n Drinfeld moduul met niveaustructuur correspondeert met een punt op de originele kromme, en dus niet met een toegevoegd punt. Door eigenschappen van de compactificatie is er echter wel wat over te zeggen. In hoofdstuk 5 worden de spitsen beschreven aan de hand van het zogenaamde *Tate-Drinfeld moduul*.
Een gevolg van deze beschrijving is dat het aantal samenhangscomponenten van de Drinfeld modulaire kromme kan worden berekend. Het blijkt dat de Weil paring, net zoals in het klassieke geval, deze samenhangscomponenten labelt.

In hoofdstuk 6 wil ik een eerste aanzet geven tot een antwoord op de vraag of de gecompactificeerde Drinfeld modulaire kromme ook gezien kan worden als de classificerende ruimte van een meetkundig zinvol object. Daarvoor wordt dus eigenlijk gezocht naar een generalisatie van het begrip 'Drinfeld moduul met niveaustructuur'. In hoofdstuk 6 wordt het schema beschreven dat daarvoor nodig is. Boven de spitsen blijkt dit schema te corresponderen met het *Néron model* van het Tate-Drinfeld moduul. Hiermee wordt een beschrijving gegeven die in het analoge geval van de klassieke modulaire krommen de eerste stap is naar de classificatie van zogenaamde gegeneraliseerde elliptische krommen.

Tenslotte worden in hoofdstuk 2 en 3 twee onafhankelijke, getaltheoretische onderwerpen behandeld. In hoofdstuk 2 worden Drinfeld modulen gebruikt om een algorithme te ontwikkelen voor het factoriseren van polynomen in $\mathbb{F}_q[T]$. In hoofdstuk 3 wordt een 'Hasse-principe' voor Drinfeld modulen en elliptische krommen bestudeerd.