De Riemann-hypothese voor elliptische krommen over een eindig lichaam

Bachelorscriptie door Lars van den Berg
Onder begeleiding van prof. dr. Gunther Cornelissen en prof. dr. Frans Oort

Universiteit Utrecht

22 juli 2015

Inhoudsopgave

Dankwoord

Allereerst ben ik zeer veel dank verschuldigd aan Frans Oort. Van niemand heb ik zo veel geleerd als van hem, op wiskundig vlak en op persoonlijk vlak. Met een grote dosis geduld en enthousiasme heeft hij me jaren onder zijn hoede gehad om me wegwijs te maken in het schone maar moeilijke landschap van de wiskunde. Ik dank hem voor al het vertrouwen, de gastvrijheid en de gulheid die hij me heeft geschonken. Het spijt me dat ik door omstandigheden dit project niet onder zijn begeleiding af kon ronden.

Ik ben blij en dankbaar dat Gunther Cornelissen bereid was de begeleiding over te nemen, en ondanks zijn ongelooflijk volle agenda tijd wilde vrijmaken om mijn scriptie aandachtig te lezen en van constructief commentaar te voorzien. Zijn enthousiasme en fris-kritische blik hebben een stimulerende uitwerking op me gehad. Ik wil Gunther, samen met Carel Faber en Valentijn Karemaker, verder hartelijk bedanken voor het leiden van een seminarium over de aritmetische theorie van krommen. Ik heb veel van het seminarium geleerd en heb er veel ideeën opgedaan voor mijn scriptie.

Ik wil Pol van Hoften bedanken voor de zinvolle discussies over onderwerpen gerelateerd aan dat van mijn scriptie. Tenslotte bedank ik mijn vrienden en kennissen, met name Claudia, Marianne, mijn huisgenoten en mijn ouders, voor hun geduld, voor hun hulp en begrip als vanwege drukte allerlei taken erbij in schoten, en voor hun liefde en vertrouwen.

Inleiding

Een van de grootste onopgeloste problemen in de wiskunde is de in 1859 door Bernhard Riemann geformuleerde 'klassieke' Riemann-hypothese (KRH). In dit werkstuk bestuderen niet dit maar een analoog probleem, dat in de jaren '30 door Helmut Hasse werd opgelost. We noemen dit probleem hier *de Riemann-hypothese voor elliptische krommen over een eindig lichaam*, of afgekort pERH.[1] In deze inleiding proberen we slechts een indruk te geven van de context van dit probleem, voor definities en details verwijzen we naar de hoofdtekst.

De pERH geeft een omschrijving van de zogenaamde Zetafunctie van een elliptische kromme E over een eindig lichaam $\mathbb{F}_q$. Deze Zetafunctie codeert, voor elk geheel getal $n \geq 1$, het aantal $\#E(\mathbb{F}_{q^n})$ van punten op E met coördinaten in $\mathbb{F}_{q^n}$. Een gevolg van de pERH is dat we een expliciete formule krijgen voor $\#E(\mathbb{F}_{q^n})$. Zodoende geeft de pERH volledig antwoord op de vraag naar het aantal oplossingen van een stelsel diophantische vergelijkingen over een eindig lichaam – mits de het stelsel vergelijkingen aanleiding geeft tot een elliptische kromme – en doet dit simultaan voor alle eindige lichamen van dezelfde karakteristiek.

De pERH staat niet op zichzelf. Eind jaren '40 formuleerde André Weil een pakket van vermoedens die bekend zijn geworden als de Weil-vermoedens. Zij vormen een generalisatie van Hasse's resultaat naar willekeurige projectieve variëteiten over een eindig lichaam, in plaats van alleen elliptische krommen. De variant van de Riemann-hypothese die onderdeel is van de Weil-vermoedens, en waar de pERH een speciaal geval van is, korten we hier af met pRH. De pRH geeft volledig antwoord op de vraag naar het aantal oplossingen van een *willekeurig* stelsel diophantische vergelijkingen over een eindig lichaam.

De Weil-vermoedens zijn sinds 1974 geen vermoedens meer maar een stelling, dankzij werk van onder anderen Grothendieck en Deligne – het was Deligne die in 1974 pRH bewees. Het bewijs daarvan, dat intensief op de leer van ℓ-adische cohomologie voortbouwt, gaat echter boven het bestek van dit werkstuk. Het hoofddoel van dit werkstuk is een bewijs geven van de pERH. Dat is een hele opgave, maar het is fraai dat al het materiaal (tegenwoordig) tot het basispakket aan kennis behoort dat een student geïnteresseerd in elliptische krommen zou moeten kennen. Het schrijven van deze scriptie was daarom niet alleen een gelegenheid om een mooi bewijs van een mooie stelling te begrijpen, maar ook om mijn basiskennis van elliptische krommen te verstevigen: de scriptie al opstapje naar moeilijkere theorie.

In Hoofdstuk 8 presenteren we het daadwerkelijke bewijs van de pERH. De andere hoofdstukken zijn er om de nodige fundering te leggen. Deze fundering is geen samenraapsel van allerlei feiten. De onderlinge afhankelijkheid van de stellingen is zelfs zo groot dat er weinig aan de volgorde van de presentatie te veranderen valt. Het is mijn hoop dat dit werkstuk erin slaagt deze samenhang helder te maken.

We schetsen kort de inhoud van dit werkstuk, en daarmee de strategie van het bewijs van de pERH.

[1] De p voor positieve karakteristiek, de E voor elliptische kromme. Deze notatie is niet standaard.

Het korte Hoofdstuk 1 gaat over de separabiliteitsgraad en inseparabiliteitsgraad van een lichaamsuitbreiding. Dit is hier relevant omdat morfismen van krommen kunnen worden gerepresenteerd door inbeddingen van functielichamen, en studie van de zo verkregen lichaamsuitbreidingen, met name wat betreft separabiliteit, geeft informatie over het morfisme. Omdat de pERH gaat over krommen over eindige karakteristiek, zijn de verkregen uitbreidingen niet in het algemeen separabel.

Hoofdstuk 2 behandelt de basale algebraïsche meetkunde die we nodig hebben alleen al om elliptische krommen te definiëren. De nadruk ligt op concepten die specifiek zijn voor krommen, of in elk geval die wij hier alleen definiëren voor krommen, zoals de vertakkingsindex, divisoren en differentialen. Aan het eind definiëren we wat elliptische kromme zijn.

In Hoofdstuk 3 bekijken we een paar opzichten waarin elliptische krommen bijzonder zijn onder de krommen. De meest fundamentele bijzonderheid is dat een elliptische kromme op een natuurlijke manier een abelse groep is. Verder komt het van pas dat we een elliptische kromme kunnen representeren met een Weierstrass-vergelijking, zodat we concrete berekeningen kunnen doen.

De meeste theorie die in dit werkstuk aan bod komt, gaat op voor willekeurige karakteristiek. Centraal in de theorie die specifiek is voor *eindige* karakteristiek, is het Frobenius-morfisme. Deze onderzoeken we in Hoofdstuk 4. De theorie daar gaat op voor willekeurig krommen, niet alleen elliptische krommen, en er is wat voor te zeggen om de volgorde van de hoofdstukken 3 en 4 te verwisselen. De belangrijkste reden voor de gekozen volgorde is om zo vroeg mogelijk aan elliptische krommen toe te komen.

De hoofdstukken 5, 6 en 7 vormen het technische hart van dit werkstuk. De afbeeldingen tussen elliptische krommen waarin we het meest geïnteresseerd zijn, zijn de isogeniën, en we starten hun studie in Hoofdstuk 5, waar we krachtige Galois-theoretische eigenschappen van isogeniën bewijzen. Daarna introduceren we de duale van een isogenie. De wisselwerking tussen een isogenie en zijn duale speelt een centrale rol in de rest van de theorie.

In Hoofdstuk 6 construeren we (onder bepaalde restricties) de Weilparing op een torsieondergroep van een elliptische kromme. De Weilparing is een belangrijk technisch hulpmiddel, en we gebruiken het onder andere om isogeniën te bestuderen. De definitie van de Weilparing lijkt bij eerste kennismaking misschien ingewikkeld en moeilijk bruikbaar, maar we zullen zien dat hij juist flexibel is. Aan het eind van hoofdstuk 6 komt de kracht van de Weilparing tot uitdrukking als we bewijzen dat de isogenie 'vermenigvuldigen met m', graad m^2 heeft. In het wat technische Hoofdstuk 7 bundelen we een reeks van Weilparingen tot een nieuwe paring, de ℓ-adische Weilparing op het Tatemoduul. Belangrijk is dat deze paring in karakteristiek nul 'leeft', in tegenstelling tot de in het hoofdstuk daarvoor bestudeerde paring.

Hoofdstuk 8 bevat het daadwerkelijke bewijs van de pERH. Al het voorgaande materiaal komt hier samen. Vooral de aan het eind van Hoofdstuk 7 bewezen formule, die de graad van een endomorfisme van een elliptische kromme verbindt met de determinant van het geïnduceerde endomorfisme van het Tatemoduul, speelt een belangrijke rol doordat het in staat stel lineaire algebra toe te passen waar dit niet voor de hand ligt.

Het materiaal van deze scriptie is diep ingebed in de literatuur. Voor het schrijven hiervan heb met name gebruik gemaakt van de uitstekende expositie in [Sil09]. Ondank haar schoonheid heb ik weleens wat spijt gehad van de keuze van dit onderwerp, omdat de bestaande exposities eigenlijk niet verbeterd kunnen worden. Ik heb in elk geval geprobeerd, en hoop dat ik daarin voor een deel geslaagd ben, om mijn expositie helder en precies te maken en details uit te werken.

Hoofdstuk 1

Inseparabiliteit van lichaamsuitbreidingen

In dit korte hoofdstuk definiëren we de separabiliteitsgraad en de inseparabiliteitsgraad van een eindige lichaamsuitbreiding, en bewijzen we de eigenschappen die we nodig gaan hebben. Dit materiaal is redelijk standaard. Ik noem een paar redenen om het hier toch op te nemen. Ten eerste is het niet aan bod te gekomen in onze bacheloropleiding. Ten tweede zou het weglaten van de bewijzen het verhaal niet veel korter maken, en volgens mij niet leesbaarder, want de bewijzen zijn verhelderend. Ten derde speelt het onderwerp van dit werkstuk zich af tegen een achtergrond van lichamen van positieve karakteristiek, waardoor inseparabiliteit een cruciale rol speelt, bijvoorbeeld in het bewijs dat het q-de machts Frobenius-morfisme graad q heeft (4.1.3).

Definitie 1.0.1. Als $k \subset l$ een eindige lichaamsuitbreiding is, en $\overline{k}$ een algebraïsche afsluiting van k, dan is de *separabiliteitsgraad* van de uitbreiding $k \subset l$, notatie $[l : k]_s$, het aantal verschillende inbeddingen $l \to \overline{k}$ dat op k de identiteit is. Kortom,

$$[l : k]_s = \#\mathrm{Hom}_k(l, \overline{k}).$$

Dit aantal is eindig vanwege (1.0.2b), en het is welgedefinieerd, want als $\overline{k}'$ een andere algebraïsche afsluiting van k is, dan bestaat er een isomorfisme $\psi \in \mathrm{Hom}_k(\overline{k}, \overline{k}')$, en dan is de functie $\mathrm{Hom}_k(l, \overline{k}) \to \mathrm{Hom}_k(l, \overline{k}') : \theta \mapsto \psi \circ \theta$ een bijectie.

De meest basale eigenschappen van de separabiliteitsgraad, die we in het vervolg gebruiken zonder dat altijd te vermelden, sommen we op in

Propositie 1.0.2. *Zij $k \subset l \subset m$ een toren van eindige uitbreidingen.*

(a) Net als de gewone graad gedraagt de separabiliteitsgraad zich multiplicatief:

$$[m : l]_s[l : k]_s = [m : k]_s.$$

(b) Er geldt $[l : k]_s \leq [l : k]$, met gelijkheid precies dan als de uitbreiding $k \subset l$ separabel is.

Bewijs. Zie bijvoorbeeld [Ste15, 23.4], of [Lan02, V.4.1] □

Definitie 1.0.3. Zij k een lichaam met karakteristiek $p > 0$, en zij $l \supset k$ een algebraïsche uitbreiding. Een element $\alpha \in l$ heet *puur inseparabel over* k als er een geheel getal $n \geq 0$ bestaat zo dat

$$\alpha^{p^n} \in k.$$

De uitbreiding $l \supset k$ heet *puur inseparabel* als elk element van l puur inseparabel over k is. Als conventie noemen we een uitbreiding $l' \supset k'$ van lichamen van karakteristiek 0 puur inseparabel precies dan als $l' = k'$.

Propositie 1.0.4. *Zij $k \subset l \subset m$ een toren van lichamen, zo dat de uitbreiding $k \subset m$ eindig is.*

(a) De eigenschappen 'separabel' en 'puur inseparabel' zijn transitief, in de zin dat

$$k \subset m \text{ is separabel} \iff k \subset l \text{ en } l \subset m \text{ zijn separabel,}$$

$$k \subset m \text{ is puur inseparabel} \iff k \subset l \text{ en } l \subset m \text{ zijn puur inseparabel.}$$

Veronderstel dat de lichamen karakteristiek $p > 0$ hebben.

(b) Zij $\alpha \in l$ puur inseparabel over k, en zij $n \geq 0$ het kleinste gehele getal met de eigenschap dat $\alpha^{p^n} \in k$. Zij $f_\alpha \in k[X]$ het minimumpolynoom van α over k. Dan is

$$f_\alpha = X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}.$$

(c) Als $k \subset l$ puur inseparabel is, dan is $[l : k]$ een macht van p.

Bewijs. (a) De bewering met 'puur inseparabel' volgt direct uit de definities, die met 'separabel' volgt bijvoorbeeld uit (1.0.2ab).

(b) Omdat α een nulpunt is van het polynoom $X^{p^n} - \alpha^{p^n} \in k[X]$, is f_α er een deler van. Er zijn dus gehele getallen $r \geq 1$ en $t \geq 0$ met $\text{ggd}(r, p) = 1$ zo dat

$$f_\alpha = (X - \alpha)^{rp^t},$$

waarbij $rp^t \leq p^n$. Dan is

$$f_\alpha = (X^{p^t} - \alpha^{p^t})^r = X^{rp^t} - r\alpha^{p^t} X^{(r-1)p^t} + \text{ termen van lagere orde.}$$

De coëfficiënten van f_α, waaronder $r\alpha^{p^t}$, liggen in k. Dus $\alpha^{p^t} \in k$, want r is niet nul in k. Wegens minimaliteit van n is $t \geq n$, en omdat $rp^t \leq p^n$, volgt dat $t = n$ en $r = 1$.

(c) Neem $\alpha_1, \ldots, \alpha_n \in l$ zo dat $l = k(\alpha_1, \ldots, \alpha_n)$, dat kan want $l \supset k$ is eindig. Elke enkelvoudige uitbreiding in de toren

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n) = l$$

heeft volgens (b) als graad een macht van p, want α_i is puur inseparabel over $k(\alpha_1, \ldots, \alpha_{i-1})$, voor $i = 1, \ldots, n$. Er volgt dat $[l : k]$ een product van machten van p is. □

Ons volgende doel is het definiëren en bestuderen van de inseparabiliteitsgraad van een lichaamsuitbreiding. Dit doen we aan de hand van zijn separabele afsluiting.

Definitie 1.0.5. Als $k \subset l$ een eindige lichaamsuitbreiding is, dan is de *separabele afsluiting van k in l* het tussenlichaam k_s van $k \subset l$ gegeven door

$$k_s = \{x \in l : x \text{ is separabel over } k\}.$$

Dat k_s inderdaad een deellichaam van l is, zien we zo: Als $x, y \in l$ separabel zijn over k, dan zijn de uitbreidingen $k \subset k(x)$ en $k(x) \subset k(x)(y)$ separabel, dus volgens (1.0.4a) is $k \subset k(x, y)$ separabel. In het bijzonder hebben we $x + y, -x, xy, x^{-1} \in k_s$.

De volgende stelling laat zien dat elke eindige uitbreiding $l \supset k$ factoriseert als een separabele gevolgd door een puur inseparabele uitbreiding, waarbij de graad van de separabele uitbreiding gelijk is aan de separabiliteitsgraad van $l \supset k$.

Stelling 1.0.6. *Zij $l \supset k$ een eindige uitbreiding van lichamen van karakteristiek p, waarbij we niet uitsluiten dat $p = 0$. Zij k_s de separabele afsluiting van k in l, dus we hebben $l \supset k_s \supset k$.*

(a) De uitbreiding $l \supset k_s$ is puur inseparabel, en $k_s \supset k$ is separabel.

(b) $[l : k]_s = [k_s : k]$.

(c) $[l : k]_s = 1 \iff l \supset k$ is puur inseparabel.

(d) Als $l \supset k$ separabel en puur inseparabel is, dan is $l = k$.

(e) Stel dat $l \supset k$ puur inseparabel is met graad $[l : k] = q$. Dan hebben we $l^q \subset k$.

Bewijs. (a) De tweede bewering is duidelijk, we bewijzen de eerste. Als $p = 0$, dan is $l \supset k$ separabel, dus $k_s = l$, dus $l \supset k_s$ is puur inseparabel. Veronderstel dat $p > 0$. Zij $\alpha \in l$, en zij $f \in k[X]$ het minimumpolynoom van α over k. Zij $a \geq 0$ het grootste gehele getal met de eigenschap dat $f \in k[X^{p^a}]$, dus er is een polynoom $g(X) \in k[X]$ zo dat

$$f(X) = g(X^{p^a}).$$

Omdat α^{p^a} nulpunt is van $g(X)$, is het minimumpolynoom van α^{p^a} over k een deler van g. Wegens maximaliteit van a is $g \notin k[X^p]$, zodat g separabel is. Er volgt dat α^{p^a} separabel is over k, kortom, $\alpha^{p^a} \in k_s$. We concluderen dat $l \supset k_s$ puur inseparabel is.

(c '$\Longleftarrow$') Veronderstel dat $l \supset k$ puur inseparabel is. Als $p = 0$, dan is $l = k$, en dan is de bewering triviaal. Stel $p > 0$. Neem $\alpha_1, \ldots, \alpha_n \in l$ zo dat $l = k(\alpha_1, \ldots, \alpha_n)$. Elk homomorfisme

$$\psi \in \mathrm{Hom}_k(l, \overline{k}) = \mathrm{Hom}_k(k(\alpha_1, \ldots, \alpha_n), \overline{k})$$

beeldt, voor $i = 1, \ldots, n$, het element α_i af naar een nulpunt van diens minimumpolynoom over k, maar omdat α_i over k puur inseparabel is, zegt (1.0.4b) dat α_i het enige nulpunt is. Kortom, $\psi(\alpha_i) = \alpha_i$ voor alle i, dus ψ is de identiteit op l. We concluderen dat

$$[l : k]_s = \#\mathrm{Hom}_k(l, \overline{k}) = 1.$$

(b) Dit is een gevolg de vorige onderdelen:

$$\begin{aligned} [l : k]_s &= [l : k_s]_s [k_s : k]_s \\ &= [l : k_s]_s [k_s : k] && (a) \\ &= [k_s : k]. && (a), (c\ \text{'}\Longleftarrow\text{'}) \end{aligned}$$

(c '$\Longrightarrow$') Als $[l : k]_s = 1$, dan is $[k_s : k] = 1$ volgens (b), dus $k_s = k$, en (a) zegt dan dat l puur inseparabel is over $k_s = k$.

(d) Vanwege (c) is dan $[l : k] = [l : k]_s = 1$.

(e) Het is triviaal als $p = 0$, stel $p > 0$. Als f het minimumpolynoom van $\alpha \in l$ over k is, dan zegt (1.0.4b) dat $\alpha^{\deg f} \in l$. Bovendien is $\deg f$ een deler van q, dus $\alpha^q \in l$. □

Definitie 1.0.7. Zij $l \supset k$ een eindige lichaamsuitbreiding, en zij k_s de separabele afsluiting van k in l, we hebben dus $l \supset k_s \supset k$. De *inseparabiliteitsgraad* van l over k is

$$[l : k]_i = [l : k_s].$$

Vanwege (1.0.6b) wordt $[l : k]_i$ gekarakteriseerd door de identiteit

$$[l : k] = [l : k]_s[l : k]_i. \tag{1.1}$$

Bovendien geven (1.0.6a) en (1.0.4c) het

Gevolg 1.0.8. *Als $l \supset k$ een eindige uitbreiding is van lichamen van karakteristiek $p > 0$, dan is $[l : k]_i$ een macht van p.*

Tenslotte een eenvoudig lemma dat we in het volgende hoofdstuk gebruiken om eigenschappen van de graad van een morfisme van projectieve krommen te bewijzen.

Lemma 1.0.9. *Zij $k \subset l$ een eindige uitbreiding, en $\alpha : l \to l'$ een homomorfisme van lichamen.*

(a) $[k : l] = [\alpha k : \alpha l]$.

(b) $[k : l]_s = [\alpha k : \alpha l]_s$.

Bewijs. (a) Het is duidelijk dat als B een basis is van l als k-vectorruimte, dan is αB een basis van αl als αk-vectorruimte, want α is injectief.

(b) Zij m, m' algebraïsche afsluitingen van l resp. αl. Het is een algemeen feit over lichamen dat het isomorfisme $\alpha : l \to \alpha l$ een (in het algemeen niet unieke) voortzetting heeft tot een isomorfisme $\alpha : m \to m'$ van algebraïsche afsluitingen. Het is duidelijk dat de functie

$$\mathrm{Hom}_k(l, m) \to \mathrm{Hom}_{\alpha k}(\alpha l, \alpha m) : \quad \sigma \mapsto \alpha\sigma\alpha^{-1}$$

inverteerbaar is, waarbij α^{-1} de inverse is van het isomorfisme $\alpha : m \to \alpha m$. Er volgt dat

$$[k : l]_s = \#\mathrm{Hom}_k(l, m) = \#\mathrm{Hom}_{\alpha k}(\alpha l, \alpha m) = [\alpha k : \alpha l]_s. \qquad \square$$

Hoofdstuk 2

Projectieve krommen

We fixeren in dit hoofdstuk deze notatie:
K is een perfect lichaam,
L is een algebraïsche afsluiting van K.

Elliptische krommen vormen een speciale klasse van projectieve krommen. Een aantal stellingen en constructies voor elliptische krommen gaan al op voor projectieve krommen, vandaar dit hoofdstuk. Voor de meeste stellingen in dit hoofdstuk verwijzen we naar de literatuur, omdat ze tamelijk standaard zijn en omdat de scriptie anders te lang zou worden. Een groot deel van het materiaal staat in hoofdstuk 1 en 4 van [Har77]. Alleen al in onze definitie van elliptische krommen gebruiken we de stelling van Riemann–Roch, waarvan het bewijs een scriptie op zichzelf zou kunnen zijn.

2.1 Projectieve variëteiten

Deze paragraaf bestaat uit definities en stellingen uit de algebraïsche meetkunde die de basis vormen voor de rest van dit werkstuk. Verder geven we voorbeelden ter illustratie, waarvan sommigen verderop een belangrijke rol spelen.

Affiene en projectieve ruimte

Als k een lichaam is, en n een niet-negatief geheel getal, dan heet de verzameling k^n de *affiene ruimte over* k, notatie $\mathbb{A}^n_k$. Op de verzameling k^{n+1} krijgen we een equivalentierelatie door te zeggen dat twee elementen $(x_0, \ldots, x_n)$ en $(x'_0, \ldots, x'_n)$ equivalent zijn precies dan als er een $\lambda \in k$ bestaat met $(x'_0, \ldots, x'_n) = (\lambda x_0, \ldots, \lambda x_n)$. De equivalentieklasse van een element $(x_0, \ldots, x_n)$ onder deze relatie noteren we als $[x_0, \ldots, x_n]$. De verzameling van alle equivalentieklassen *behalve* die van $(0, \ldots, 0)$, heet de *projectieve n-ruimte over* k, notatie $\mathbb{P}^n_k$. De elementen van $\mathbb{P}^n_k$ noemen we 'punten'. Als $l \subset k$ een deellichaam is, dan vatten we $\mathbb{P}^n_l$ op de natuurlijke manier op als deelverzameling van $\mathbb{P}^n_k$.

Projectieve variëteiten over K

Als $f \in L[X_0, \ldots, X_n]$ een *homogeen* polynoom is, dat wil zeggen dat alle monomen in f van dezelfde graad zijn, dan geeft f aanleiding tot een functie $\mathbb{P}^n_L \to \{0, 1\}$ door te zeggen dat

$f[x_0, \ldots, x_n] = 0$ indien $f(x_0, \ldots, x_n) = 0$, en $f[x_0, \ldots, x_n] = 1$ anders. Omdat f homogeen is, is dit welgedefinieerd. Zodoende kunnen we het hebben over de *nulpunten* van f in $\mathbb{P}^n_L$.

Als $S \subset L[X_0, \ldots, X_n]$ een verzameling homogene polynomen is, dan heet de verzameling

$$\mathcal{Z}(S) = \{P \in \mathbb{P}^n_L : f(P) = 0 \text{ voor alle } f \in S\}$$

de *nulpuntenverzameling* van S. Een deelverzameling $V \subset \mathbb{P}^n_L$ heet een *algebraïsche verzameling* als er een verzameling homogene polynomen S is zo dat $V = \mathcal{Z}(S)$. Het is eenvoudig te zien dat de algebraïsche verzamelingen de gesloten verzamelingen van een topologie op $\mathbb{P}^n_L$ zijn [Har77, I.2.1], de *Zariski-topologie* op $\mathbb{P}^n_L$.

Een niet-lege topologische ruimte X heet *irreducibel* als X niet de vereniging is van twee gesloten echte deelverzamelingen van X. (Als we het hebben over een irreducibele deelverzameling, bedoelen we irreducibel met betrekking tot de deelruimte-topologie.) De *dimensie* van een topologische ruimte X is het supremum van de verzameling van lengtes van ketens van irreducibele gesloten deelverzamelingen van X, waarbij de lengte van een keten het aantal echte inclusies in de keten is. Zie bijvoorbeeld [Eis04] voor achtergrond bij deze begrippen.

Definitie 2.1.1. Zij n een niet-negatief geheel getal, en zij $S \subset K[X_0, \ldots, X_n]$ een verzameling homogene polynomen. Als de algebraïsche verzameling $V := \mathcal{Z}(S) \subset \mathbb{P}^n_L$, uitgerust met de topologie geïnduceerd door de Zariski-topologie op $\mathbb{P}^n_L$, irreducibel is, dan heet V een *projectieve variëteit over* K. Als V bovendien dimensie 1 heeft, dan heet V een *projectieve kromme over* K. Als k een tussenlichaam van $K \subset L$ is, schrijven we $V(k) = V \cap \mathbb{P}^n_k$ voor de verzameling van *k-rationale punten* op V.

Opmerking over taalgebruik: We hebben het over 'de projectieve variëteit V/K' om aan te duiden of te benadrukken dat V een projectieve variëteit over K is.

De topologie op V zoals hierboven heet de Zariski-topologie op V. Als we in dit werkstuk spreken over open of gesloten verzamelingen, bedoelen we dit altijd met betrekking tot de Zariski-topologie.

Voorbeeld 2.1.2. Neem $n = 2$, we spreken dan van het *projectieve vlak* $\mathbb{P}^2_L$ en het *affiene vlak* $\mathbb{A}^2_L$ over L, en we schrijven X, Y, Z in plaats van X_0, X_1, X_2. Een deelverzameling $C \subset \mathbb{P}^2_L$ is een projectieve kromme over K precies dan als er een homogeen polynoom $f \in K[X, Y, Z]$ is, irreducibel in $L[X, Y, Z]$, zo dat $C = \mathcal{Z}(f)$. Zie [Har77, exc. 2.8]. Omdat C in het projectieve vlak ligt, noemen we het een vlakke projectieve kromme. Als f graad 1 heeft, dan noemen we C een lijn.

Zij $N = \mathcal{Z}(Z)$, met andere woorden, N is 'de lijn $Z = 0$'. De functie $\mathbb{P}^2_L - N \to \mathbb{A}^2_L : [x, y, z] \mapsto [x/z, y/z]$ is welgedefinieërd en is een bijectie, en induceert een bijectie tussen de verzameling punten van C buiten de lijn $Z = 0$, en de verzameling C' van nulpunten in het affiene vlak van het polynoom $f(X, Y, 1) \in K[X, Y]$. We noemen C' de affiene voorstelling van C. Aan deze procedure kennen we hier geen theoretische betekenis toe, maar we gebruiken het om in concrete gevallen de notatie te vereenvoudigen. De affiene voorstelling van C kunnen we terugvertalen naar C: als $g = f(X, Y, 1) \in K[X, Y]$ het polynoom is waar C' de nulverzameling van is, zeg met graad $d := \deg g$, dan is $f = Z^d g(X/Z, Y/Z)$ als $d \geq 1$, en $f = Z$ als $d = 0$.

Een concreet voorbeeld, dat we ter illustratie verschillende keren laten terugkomen: neem $K = \mathbb{F}_3$ en een algebraïsche afsluiting L van $\mathbb{F}_3$, en beschouw de projectieve kromme $C/\mathbb{F}_3$ gegeven door

$$C: \quad Y^2 = X^3 + X + 1.$$

Hiermee bedoelen we dat de affiene voorstelling van C de verzameling nulpunten in $\mathbb{A}^2_L$ is van het polynoom $Y^2 - X^3 - X - 1 \in \mathbb{F}_3[X, Y]$. We hebben dus $C = \mathcal{Z}(f) \subset \mathbb{P}^2_L$, waarbij

$$f = Y^2 Z - X^3 - XZ^2 - Z^3 \in \mathbb{F}_3[X, Y, Z].$$

De verzameling $\mathbb{A}^2_{\mathbb{F}_3}$ bestaat uit slechts 9 punten, en $\mathbb{P}^2_{\mathbb{F}_3}$ uit slechts 13 punten (want de lijn $Z = 0$ heeft er 4). Het is eenvoudig om de deelverzameling $C(\mathbb{F}_3) \subset \mathbb{P}^2_{\mathbb{F}_3}$ te bepalen. Een nulpunt $[x, y, z]$ van f met $z = 0$ voldoet ook aan $x = 0$, dus $O := [0, 1, 0]$ is het enige punt van C op de lijn $Z = 0$, en het ligt in $C(\mathbb{F}_3)$. De andere punten in $C(\mathbb{F}_3)$ zijn de $[x, y, 1]$ waarvoor $(x, y) \in \mathbb{A}^2_{\mathbb{F}_3}$ een oplossing is van de vergelijking $Y^2 = X^3 + X + 1$. Invullen van $X = 0, 1, -1$ en de vergelijking in Y oplossen, levert dat

$$C(\mathbb{F}_3) = \{[0, 1, 1], [0, -1, 1], [1, 0, 1], O\}.$$

Het wordt minder eenvoudig om $C(\mathbb{F}_{3^m})$ te bepalen naarmate m groeit. Voor het *aantal* punten $\#C(\mathbb{F}_{3^m})$ bestaat echter een eenvoudige formule. Hier komen we later op terug.

Opmerking 2.1.3. De Zariski-topologie op een projectieve kromme C/K heeft een eenvoudige karakterisering: de gesloten verzamelingen zijn, naast C zelf, de eindige deelverzamelingen. Namelijk, volgens [Har77, I.1.5] is elke gesloten deelverzameling $Y \subset C$ te schrijven als een eindige vereniging van irreducibele gesloten deelverzamelingen van Y, en omdat C dimensie 1 heeft, zijn deze irreducibele delen ofwel punten, ofwel gelijk aan C. Dus $Y = C$ of Y is eindig. Omgekeerd is duidelijk dat elke éénpuntsverzameling in $\mathbb{P}^n_L$, en dus elke eindige deelverzameling van C, gesloten is.

De enige eindige irreducibele deelverzamelingen van $\mathbb{P}^n_L$ zijn de éénpuntsverzameling, en zij hebben dimensie 0, dus C is oneindig. In het bijzonder volgt dat elke niet-lege open deelverzameling van C, dicht ligt in C, en dat de intersectie van twee niet-lege open deelverzamelingen niet-leeg is.

Voorbeeld 2.1.4. Neem $n = 1$, we spreken dan van de *projectieve lijn* $\mathbb{P}^1_L$. Analoog als in het vorige voorbeeld, hebben we een bijectie $b : \mathbb{P}^1_L - N \to \mathbb{A}^1_L : [x, y] \mapsto x/y$, in dit geval bestaat $N = \{[1, 0]\}$ uit het unieke punt met als tweede coördinaat nul. Uiteraard is $\mathbb{P}^1_L = \mathcal{Z}(0)$ zelf een algebraïsche verzameling. De enige echte deelverzamelingen $V \subset \mathbb{P}^1_L$ die een algebraïsche verzameling zijn, zijn de eindige verzamelingen, want $b(V - N)$ kan worden gezien als de nulverzameling in L van een polynoom in één variabele en is dus eindig, terwijl ook $V \cap N$ eindig is. Er volgt dat $\mathbb{P}^1_L$ irreducibel is en dimensie 1 heeft, want $\mathbb{P}^1_L$ zelf is oneindig. Dus $\mathbb{P}^1_L$ is een projectieve kromme over K.

Reguliere functies

Als $h, h' \in L[X_0, \ldots, X_n]$ homogene polynomen van dezelfde graad zijn, en $U \subset \mathbb{P}^n_L$ een open deelverzameling waarop h' nergens nul is, dan geeft het quotiënt $h/h' \in L(X_0, \ldots, X_n)$ aanleiding tot een functie $U \to L$, die we ook aanduiden met h/h', gegeven door

$$\frac{h}{h'} : U \to L : \quad \frac{h}{h'}[x_0, \ldots, x_n] = \frac{h(x_0, \ldots, x_n)}{h'(x_0, \ldots, x_n)}.$$

Merk op dat het welgedefinieerd is of h' nul is op U omdat h' homogeen is, en omdat ook h homogeen is en van dezelfde graad, is de functie h/h' welgedefinieerd.

Definitie 2.1.5. Een functie $g : U \to L$ op een open deelverzameling U van een projectieve variëteit $V \subset \mathbb{P}^n_L$ over K, heet *regulier bij het punt* $P \in U$ als er een omgeving $W \subset U$ van P is, en homogene polynomen $h, h' \in L[X_0, \ldots, X_n]$ van dezelfde graad zo dat h' nergens nul is op W, en zo dat $g|_W = (h/h')|_W$. We noemen de functie g regulier als g regulier is bij elk punt van U. Als bovendien voor elk punt P de bijbehorende W, h, h' zo gekozen kunnen worden dat $h, h' \in K[X_0, \ldots, X_n]$, dan zeggen we dat g *gedefinieerd is over* K.

Functielichaam, lokale ring bij een punt

Zij V/K een projectieve variëteit. Op de verzameling van paren (U, g), met U een niet-lege open deelverzameling van V, en g een reguliere functie op U, krijgen we een equivalentierelatie [Har77, p16] door te zeggen dat twee elementen (U, g) en (W, h) equivalent zijn precies dan als $g_{|U\cap W} = h_{|U\cap W}$. De equivalentieklasse van (U, g) duiden we aan met $\langle U, g\rangle$. Als we in dit werkstuk $\langle U, g\rangle$ schrijven, bedoelen we dit altijd in deze context, kortom dat U een open deel is van de variëteit waar we mee werken en dat g een reguliere functie op U is.

Op de verzameling van equivalentieklassen onder de relatie van boven, definiëren we een optelling en vermenigvuldiging door middel van

$$\langle U, g\rangle + \langle W, h\rangle = \langle U \cap W, g + h\rangle \qquad \text{en} \qquad \langle U, g\rangle\langle W, h\rangle = \langle U \cap W, gh\rangle.$$

Volgens [Har77, p16] zijn deze operaties welgedefinieerd, en maken ze de collectie tot een lichaam.

Definitie 2.1.6. Als V/K een projectieve variëteit is, dan is $L(V)$ het lichaam bestaande uit de equivalentieklassen $\langle U, g\rangle$ onder de zojuist omschreven equivalentierelatie, uitgerust met de operaties 'plus' en 'keer' van hierboven. We vatten L op als deellichaam van $L(V)$ via de inbedding $L \to L(V) : \lambda \mapsto \langle V, \lambda\rangle$ waarbij de tweede 'λ' de constante functie λ op V is. Zodoende is $L(V)$ een L-algebra. Het deellichaam van $L(V)$ bestaande uit de elementen $\langle U, g\rangle$ waarbij g gedefinieerd is over K, heet het *functielichaam* van V/K, notatie $K(V)$. Via de inbedding $K \to K(V) : \kappa \mapsto \langle V, \kappa\rangle$ vatten we K op als deellichaam van $K(V)$, en $K(V)$ als K-algebra.

Als $P \in V$ een punt is, dan is de *lokale ring van P op V* de deelring

$$\mathcal{O}_{P,V} = \{\langle U, g\rangle \in L(V) : P \in U\}$$

van $L(V)$. Dit is een lokale ring, met als maximaal ideaal

$$\mathfrak{m}_{P,V} = \{\langle U, g\rangle \in \mathcal{O}_{P,V} : g(P) = 0\}$$

(zie [Har77, p16]).

Als duidelijk is wat V is, schrijven we wel eens $\mathcal{O}_P := O_{P,V}$ en $\mathfrak{m}_P := \mathfrak{m}_{P,V}$.

De elementen van $f \in L(V)$ worden informeel 'functies' genoemd. Ze representeren functies op een niet-lege open deelverzameling van V, maar niet per se op heel V. Namelijk, zij U de vereniging van de open delen $W \subset V$ waarvoor er een reguliere functie g_W op W bestaat met $f = \langle W, g_W\rangle$. Dan is duidelijk dat we een welgedefinieerde functie $f : U \to L$ krijgen door $f(P) = g_W(P)$ te stellen, als $P \in W$. We zeggen dat f *gedefinieerd is in* P als $P \in U$, met andere woorden, als $f \in \mathcal{O}_{P,V}$, en dat f gedefinieerd is op de open deelverzameling $X \subset V$ als f gedefinieerd is in elk punt van X.

Opmerking 2.1.7. Het is duidelijk uit de definitie dat een element van het functielichaam 'globaal vastligt als hij lokaal vastligt', in de zin die we nu precies opschrijven. Zij V/K een projectieve variëteit, en zij $f, g \in L(V)$ twee functies. Stel dat er een open deelverzameling $U \subset V$ bestaat zo f en g beide gedefinieerd zijn op U, en zo dat $f|_U = g|_U$. Dan is $f = g$. Namelijk, neem willekeurige representanten van f en g, zeg $\langle W, f'\rangle = f$ en $\langle X, g'\rangle = g$. Dan is

$$f = \langle W \cap X \cap U, f'\rangle = \langle W \cap X \cap U, g'\rangle = g.$$

Niet-singuliere punten

Zij $\mathfrak{m}_P$ het maximaal ideaal van de lokale ring $\mathcal{O}_P$ bij een punt P op een projectieve variëteit V/K. We kunnen het ideaal $\mathfrak{m}_P/\mathfrak{m}_P^2$ van $\mathcal{O}_P/\mathfrak{m}_P^2$ opvatten als vectorruimte over het lichaam $k := \mathcal{O}_P/\mathfrak{m}_P \cong L$, namelijk met scalaire vermenigvuldiging gegeven door $(x + \mathfrak{m}_P)(y + \mathfrak{m}_P^2) := xy + \mathfrak{m}_P^2$ voor $x \in \mathcal{O}_P$ en $y \in \mathfrak{m}_P$ (dit is welgedefinieerd).

Definitie 2.1.8. In de notatie van boven zeggen we dat het punt $P \in V$ *niet-singulier* is op V als $\dim_k \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim V$, en anders dat P *singulier* is op V. We zeggen dat V niet-singulier is als elk van zijn punten niet-singulier is op V, en anders dat V singulier is.

Voorbeeld 2.1.9. Een vlakke projectieve kromme $C \subset \mathbb{P}^2_L$ over K kunnen we volgens (2.1.2) schrijven als $C = \mathcal{Z}(f)$, met $f \subset K[X,Y,Z]$ een homogeen polynoom irreducibel in $L[X,Y,Z]$. Er is een alternatieve karakterisering van de singuliere punten op C, die concrete berekeningen vaak eenvoudiger maakt. We schrijven f_X voor de formele partiële afgeleide van f naar X. Omdat f_X een homogeen polynoom is, kunnen we spreken van de nulpunten van f_X op $\mathbb{P}^2_L$. Analoog hebben we f_Y, f_Z. Volgens [Har77, exc. I.5.8] is een punt $P \in C$ singulier op C precies dan als

$$(f_X(P), f_Y(P), f_Z(P)) = (0,0,0).$$

We passen dit toe op de kromme $C/\mathbb{F}_3$ van voorbeeld (2.1.2), dat wil zeggen $C = \mathcal{Z}(f)$ met $f = Y^2Z - X^3 - XZ^2 - Z^3$. Een punt $[x,y,z] \in C$ is singulier op C precies dan als

$$(-z^2, 2yz, y^2 - 2xz) = (0,0,0).$$

Maar dan moet $z = y = 0$ zijn, terwijl $[0,1,0]$ het enige punt van C is op de lijn $Z = 0$. We concluderen dat C niet-singulier is.

Morfismen

Een *morfisme* $\varphi : V_1 \to V_2$ tussen twee projectieve variëteiten over K, is een continue functie $\varphi : V_1 \to V_2$ (zoals altijd met betrekking tot de Zariski-topologie) met de eigenschap dat als $g : U \to L$ een over K gedefinieerde reguliere functie is op een open deelverzameling $U \subset V_2$, dan is $g \circ \varphi : \varphi^{-1}(U) \to L$ een over K gedefinieerde reguliere functie.[1] Het is duidelijk dat de samenstelling van twee morfismen een morfisme is. Zodoende hebben we een categorie van projectieve variëteiten over K. Diens volle deelcategorie met als objecten de projectieve krommen, is hier altijd wat bedoelen als we het hebben over 'de categorie van projectieve krommen over K'.

Feit 2.1.10. *Als $\varphi : V_1 \to V_2$ een morfisme is van projectieve variëteiten over K, en als k een tussenlichaam is van $K \subset L$, dan induceert φ een functie $\varphi : V_1(k) \to V_2(k)$.*

Bewijs. Zij $P \in V_1(k)$, zeg $P = [x_0, \ldots, x_m]$ met $x_0, \ldots, x_m \in k$, en schrijf $\varphi(P) = [y_0, \ldots, y_n]$ met $y_0, \ldots, y_n \in L$, zeg met $y_j \neq 0$. Voor $i = 1, \ldots, n$ bekijken we de over K gedefinieerde reguliere functie

$$g_i = \frac{X_i}{X_j} : \quad U_i \to L,$$

waarbij U_i het complement in V_2 is van $\mathcal{Z}(X_i)$. Per definitie van een morfisme is de functie $g_i \circ \varphi : \varphi^{-1}(U_i) \to L$ een reguliere functie gedefinieerd over K, en we hebben $P \in \varphi^{-1}(U_i)$, dus er zijn polynomen h_i, h_i' met coëfficiënten in $K \subset k$ zo dat $g \circ \varphi$ lokaal bij P gegeven wordt door h_i/h_i'. Dan is

$$\frac{y_i}{y_j} = g_i(\varphi(P)) = (g_i \circ \varphi)(P) = \frac{h_i(x_0, \ldots, x_m)}{h_i'(x_0, \ldots, x_m)} \in k,$$

voor alle i. Conclusie: het punt $\varphi(P) = [y_0/y_j, \ldots, y_n/y_j]$ ligt in $V_2(k)$, zoals gewenst. □

[1] In de terminologie van [Sil09] is φ een *morfisme gedefinieerd over K*.

Voorbeeld 2.1.11. Als $C_1 \subset \mathbb{P}_L^m$ en $C_2 \subset \mathbb{P}_L^n$ twee projectieve krommen over K zijn, en $f_0, \ldots, f_n \in K[X_0, \ldots, X_m]$ zijn homogene polynomen van dezelfde graad zonder gezamenlijk nulpunt in $L^{n+1} - \{0\}$ zo dat het beeld van de (duidelijk welgedefinieerde) functie

$$\varphi : C_1 \to \mathbb{P}_L^n : \quad [x_0, \ldots, x_m] \mapsto [f_0(x_0, \ldots, x_m), \ldots, f_n(x_0, \ldots, x_m)]$$

in C_2 ligt, dan is $\varphi : C_1 \to C_2$ een morfisme. Bewijs: Als $[y_0, \ldots, y_n] = P \in C_2$ een punt is, zeg met $y_i \neq 0$, dan is het eenvoudig te zien dat

$$\varphi^{-1}\{[y_0, \ldots, y_n]\} = \mathcal{Z}(y_0 f_i - y_i f_0, \ldots, y_n f_i - y_i f_n).$$

Dit betekent dat het inverse beeld onder φ van een gesloten verzameling gesloten is, want de gesloten echte deelverzamelingen van C_2 zijn eindig. Dus φ is continu. Stel dat $g : U \to L$ een reguliere functie is op een open deel $U \subset C_2$. Als $Q \in \varphi^{-1}(U)$, neem dan homogene polynomen $h, h' \in K[X_0, \ldots, X_n]$ van dezelfde graad zo dat g op een omgeving W van $\varphi(Q)$ gegeven wordt door h/h'. Dan wordt $g \circ \varphi$ op de omgeving $\varphi^{-1}(W)$ van Q gegeven door

$$g \circ \varphi|_{\varphi^{-1}(W)} = \frac{h'(f_0, \ldots, f_n)}{h(f_0, \ldots, f_n)},$$

en dit is het quotiënt van homogene polynomen van dezelfde graad. Kortom, $g \circ \varphi$ is regulier in Q, en dit geldt voor alle $Q \in \varphi^{-1}(U)$, dus de functie $g \circ \varphi : \varphi^{-1}(U) \to L$ is regulier. Dit voltooit het bewijs dat φ een morfisme is.

Voorbeeld 2.1.12 (Het Frobenius-morfisme)**.** Als concreet geval van voorbeeld (2.1.11) beschouwen we een projectieve kromme $C = \mathcal{Z}(S) \subset \mathbb{P}_L^n$ over K, waarbij zoals gebruikelijk $S \subset K[X_0, \ldots, X_n]$ een verzameling homogene polynomen is, en we veronderstellen dat $\mathrm{char} K =: p > 0$. Zij q een niet-negatieve gehele macht van p. Als f een polynoom is, dan schrijven we $f^{(q)}$ voor het polynoom dat uit f verkregen wordt door zijn coëfficiënten tot de macht q te verheffen. We beschouwen de kromme $C^{(q)} := \mathcal{Z}(S^{(q)})$ waarbij $S^{(q)} := \{f^{(q)} : f \in S\}$. Het beeld van de functie

$$C \to \mathbb{P}_L^n : \quad [x_0, \ldots, x_n] \mapsto [x_0^q, \ldots, x_n^q]$$

ligt in $C^{(q)}$, want als $f \in S$ en $[x_0, \ldots, x_n] \in C$, dan is

$$f^{(q)}(x_0^q, \ldots, x_n^q) = f(x_0, \ldots, x_n)^q = 0^q = 0$$

omdat $K \to K : x \mapsto x^q$ een homomorfisme is. We concluderen uit (2.1.11) dat de functie

$$\pi : C \to C^{(q)} : \quad [x_0, \ldots, x_n] \mapsto [x_0^q, \ldots, x_n^q]$$

een morfisme is, het *q-de machts Frobenius-morfisme op* C. In tegenstelling tot het Frobenius-automorfisme $K \to K : x \mapsto x^q$ van het perfecte lichaam K, is π geen isomorfisme, zoals we later zullen zien.

2.2 Eigenschappen van projectieve krommen

Terwijl de vorige paragraaf algemeen opgaat voor projectieve variëteteiten, richten we ons hier op eigenschappen en constructies die specifiek zijn voor projectieve krommen.

Lokale parameter bij een niet-singulier punt op een kromme

Zij P een niet-singulier punt op een projectieve kromme C/K. Dan zegt (2.1.8) dat

$$\dim_{\mathcal{O}_P/\mathfrak{m}_P} \mathfrak{m}_P/\mathfrak{m}_P^2 = 1,$$

en volgens [Kem11, §14.1] betekent dit dat $\mathcal{O}_P$ een discrete valuatiering is, dat wil zeggen een lokaal hoofdideaaldomein dat geen lichaam is. Er volgt eenvoudig dat een *lokale parameter t bij P*, dat wil zeggen een voortbrenger van het maximaal ideaal $\mathfrak{m}_P$, het (op vermenigvuldiging met eenheden van $\mathcal{O}_P$ na) unieke irreducibele element van $\mathcal{O}_P$ is. Elk niet-nul element van het breukenlichaam $L(C)$ van de ontbindingsring $\mathcal{O}_P$ heeft daarom een unieke schrijfwijze als ut^m, met $u \in \mathcal{O}_P^*$ en $m \in \mathbb{Z}$. Bovendien is m onafhankelijk van de keuze van t, want een andere lokale parameter t' bij P is gelijk aan t op een factor in $\mathcal{O}_P^*$ na. De functie

$$\mathrm{ord}_P : L(C)^* \to \mathbb{Z} : \quad ut^m \mapsto m \qquad (\text{waarbij } (t) = \mathfrak{m}_P \text{ en } u \in \mathcal{O}_P^* \text{ en } m \in \mathbb{Z})$$

is daarom welgedefiniëerd. Deze functie wordt de discrete valuatie geassocieerd met de discrete valuatiering $\mathcal{O}_P$ genoemd. Dat het een valuatie is wil zeggen dat

$$\begin{aligned} \mathrm{ord}_P(fg) &= \mathrm{ord}_P(f) + \mathrm{ord}_P(g), \\ \mathrm{ord}_P(f+g) &\geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}, \end{aligned} \tag{2.1}$$

als de betrokken elementen in $L(C)^*$ liggen. Deze formules zijn duidelijk uit de definitie. In het bijzonder is ord_P een homomorfisme van abelse groepen. 'Discreet' slaat op het feit dat het beeld in $\mathbb{Z}$ ligt. Als $f \in L(C)^*$, dan zeggen we dat $\mathrm{ord}_P(f)$ 'de orde van f bij het punt P op C' is.

Merk op dat als $f \in L(C)^*$, dan is $\mathrm{ord}_P(f) \geq 0$ precies dan als $f \in \mathcal{O}_P$, met andere woorden, precies dan als f gedefinieerd is in P. Bovendien, als $f \in \mathcal{O}_P$, dan is $\mathrm{ord}_P(f) > 0$ precies dan als $f \in \mathfrak{m}_P$, kortom als $f(P) = 0$.

Propositie 2.2.1. *Zij C/K een projectieve kromme.*

(a) Als P een niet-singulier punt op C is zo dat $P \in C(K)$, dan bestaat er een lokale parameter t bij P zo dat $t \in K(C)$.

(b) Als C niet-singulier is, en $f \in L(C)^*$ een functie, dan zijn er maar eindig veel punten $P \in C$ waarvoor $\mathrm{ord}_P(f) \neq 0$.

Bewijs. (a) [Sil09, II.1.1.1]. (b) We hebben $\mathrm{ord}_P(f) \geq 0$ precies dan als f gedefinieerd is in P, en zoals we zagen is f gedefinieerd op een niet-lege open deelverzameling van C. Het complement hiervan is eindig volgens (2.1.3). Er zijn dus maar eindig veel $P \in C$ met $\mathrm{ord}_P(f) < 0$. Omdat $\mathrm{ord}_P(1/f) = -\mathrm{ord}_P(f)$, zijn de punten $P \in C$ met $\mathrm{ord}_P(f) > 0$ precies de punten met $\mathrm{ord}_P(1/f) < 0$, en dat zijn er eindig veel. □

Voorbeeld 2.2.2. Zij $C \subset \mathbb{P}^m_L$ een projectieve krommen over K, en zij $g_0, \ldots, g_n \in L(C)^*$. We definiëren de functie $\varphi := [g_0, \ldots, g_n] : C \to \mathbb{P}^n_L$ als volgt. Zij $P \in C$, en zij t een lokale parameter bij P. We stellen

$$\varphi(P) = [(g_0 t^{-k})(P), \ldots, (g_n t^{-k})(P)], \qquad \text{waarbij} \qquad k := \min\{\mathrm{ord}_P(g_0), \ldots, \mathrm{ord}_P(g_n)\}.$$

Dit kan omdat $\mathrm{ord}_P(g_i t^{-k}) = \mathrm{ord}_P(g_i) - k \geq 0$ voor alle $i = 0, \ldots, n$, dus $g_i t^{-k}$ is gedefinieerd in P; en omdat k *gelijk* is aan het minimum, is er een j zo dat $\mathrm{ord}_P(g_j t^{-k}) = 0$, dat wil zeggen, $(g_j t^{-k})(P) \neq 0$, zodat het geval $\varphi(P) = [0, \ldots, 0]$ uitgesloten is. Het is verder duidelijk dat φ

welgedefinieerd is. Algemener, als $g_P \in L(C)^*$ een functie is zo dat $g_0 g_P, \ldots, g_n g_P$ gedefinieerd zijn in P en niet allemaal nul zijn in P, dan is

$$\varphi(P) = [(g_0 g_P)(P), \ldots, (g_n g_P)(P)].$$

Als het beeld van φ in de projectieve variëteit $V \subset \mathbb{P}^n_L$ ligt, dan volgt eenvoudig, en op soortgelijke manier als in (2.1.9) dat $\varphi : C \to V$ een morfisme is. We schetsen het idee erachter. Lokaal bij een punt $P \in C$ wordt φ gegeven door quotiënten van homogene polynomen, en door te vermenigvuldigen met de noemers, reduceren we lokaal bij P naar de situatie van (2.1.9). Met het argument aldaar volgt dat φ continu is, en dat de samenstelling van φ met een over K gedefinieerde reguliere functie weer een over K gedefinieerde reguliere functie is – dit alles lokaal bij P. Maar omdat de noties 'continu' en 'regulier' sowieso al lokaal gedefinieerd zijn, kunnen we de frase 'lokaal bij P' weglaten als het voor alle P geldt, en zodoende volgt dat φ een morfisme is.

Geïnduceerde afbeelding van functielichamen

Een van de belangrijkste bijzonderheden van projectieve krommen is

Stelling 2.2.3. *Een morfisme $\varphi : C_1 \to C_2$ van projectieve krommen over K is ofwel constant, ofwel surjectief.*

Bewijs. [Har77, II.6.8] □

Een niet-constant morfisme $\varphi : C_1 \to C_2$ van projectieve krommen over K geeft aanleiding tot een functie

$$\varphi^* : L(C_2) \to L(C_1) : \quad \langle U, g \rangle \mapsto \langle \varphi^{-1}(U), g \circ \varphi \rangle.$$

Merk op dat $\varphi^{-1}(U)$ niet leeg is, want φ is surjectief. Het is eenvoudig te zien dat φ^* welgedefinieerd is, en een homomorfisme van L-algebra's is. Bovendien is duidelijk dat als $\psi : C_2 \to C_3$ een ander niet-constant morfisme is, dan is

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*.$$

(Met andere woorden, we hebben een contravariante functor van de categorie van projectieve krommen over K naar, bijvoorbeeld, de categorie van L-algebra's.) Restrictie van φ^* tot $K(C_2)$ levert een homomorfisme

$$\varphi^* : K(C_2) \to K(C_1)$$

van K-algebra's. Voor elk punt $P \in C_1$ krijgen we door restrictie van φ^* tot $\mathcal{O}_{\varphi(P),C_2}$ een homomorfisme

$$\varphi^* : \mathcal{O}_{\varphi(P),C_2} \to \mathcal{O}_{P,C_1}$$

van L-algebra's.

Stelling 2.2.4. *Zij C_1, C_2 twee niet-singuliere projectieve krommen over K.*

(a) Als $\varphi : C_1 \to C_2$ een niet-constant morfisme is, dan is $K(C_1)$ een eindige lichaamsuitbreiding van $\varphi^* K(C_2)$.

(b) De functie

$$\mathrm{Hom}_{nc}(C_1, C_2) \to \mathrm{Hom}(K(C_2), K(C_1)) : \quad \varphi \mapsto \varphi^*$$

is bijectief, waarbij de eerste 'Hom$_{nc}$' niet-constante morfismen van projectieve krommen over K betekent, en de tweede tweede 'Hom' homomorfismen van K-algebra's.

Bewijs. (a) [Har77, II.6.8]. (b) volgt uit [Har77, I.4.4] en [Sil09, II.2.1]. □

We gaan (2.2.4b) zeker drie keer gebruiken, waarvan twee keer in de volgende gedaante.

Lemma 2.2.5. *Als $\varphi : C_1 \to C_2$ en $\psi : C_1 \to C_3$ twee niet-constante morfismen zijn van niet-singuliere projectieve krommen over K, met de eigenschap dat*

$$K(C_1) \supset \varphi^* K(C_2) \supset \psi^* K(C_3), \tag{2.2}$$

dan is er een uniek morfisme $\chi : C_2 \to C_3$ zo dat dit diagram commuteert:

$$\begin{array}{ccc} C_1 & & \\ \downarrow{\scriptstyle \varphi} & \searrow^{\psi} & \\ C_2 & \overset{\chi}{\dashrightarrow} & C_3. \end{array} \tag{2.3}$$

Bewijs. Zij $(\varphi^*)^{-1}$ de inverse van het isomorfisme $\varphi^* : K(C_2) \to \varphi^* K(C_2)$. We definiëren i als het K-algebra homomorfisme

$$i : K(C_3) \to K(C_2) : \quad i = (\varphi^*)^{-1} \circ \psi^*,$$

deze definitie wordt gerechtvaardigd door (2.2). Kortom, het diagram

$$\begin{array}{ccc} K(C_1) & & \\ \uparrow{\scriptstyle \varphi^*} & \nwarrow^{\psi^*} & \\ K(C_2) & \xleftarrow{\ i\ } & K(C_3). \end{array}$$

commuteert. Volgens (2.2.4b) bestaat er een niet-constant morfisme $\chi : C_2 \to C_3$ met $\chi^* = i$. Dus $\psi^* = \varphi^* \circ \chi^* = (\chi \circ \varphi)^*$, en opnieuw uit (2.2.4b) volgt $\psi = \chi \circ \varphi$. Kortom, ook het diagram (2.3) commuteert. Dat χ uniek is met deze eigenschap, volgt omdat φ surjectief is. □

Graad van een niet-constant morfisme

Als $\varphi : C_1 \to C_2$ een niet-constant morfisme van projectieve krommen over K is, dan zijn de *graad*, de *separabiliteitsgraad* en de *inseparabiliteitsgraad* van φ gedefinieerd als

$$\begin{aligned} \deg \varphi &= [K(C_1) : \varphi^* K(C_2)] \quad \text{resp.} \\ \deg_s \varphi &= [K(C_1) : \varphi^* K(C_2)]_s \quad \text{resp.} \\ \deg_i \varphi &= [K(C_1) : \varphi^* K(C_2)]_i. \end{aligned}$$

Het morfisme φ wordt separabel, inseparabel, puur inseparabel, ... genoemd als de lichaamsuitbreiding $K(C_1) \supset \varphi^* K(C_2)$ de betreffende eigenschap heeft. Met behulp van hoofdstuk 1 krijgen we de volgende identiteiten.

Feiten 2.2.6. *Zij $\varphi : C_1 \to C_2$ en $\psi : C_2 \to C_3$ twee niet-constante morfismen van projectieve krommen over K.*

(a) $\deg \varphi = \deg_s \varphi \deg_i \varphi$.

(b) $\deg(\psi \circ \varphi) = \deg \psi \deg \varphi$.

(c) $\deg_s(\psi \circ \varphi) = \deg_s \psi \deg_s \varphi$.

(d) $\deg_i(\psi \circ \varphi) = \deg_i \psi \deg_i \varphi$.

(e) $\deg_i \varphi = 1$ *als* $p := \mathrm{char} K = 0$, *en* $\deg_i \varphi$ *is een macht van* p *als* $p > 0$.

Bewijs. (a) is een vertaling van (1.1).

(b) We berekenen

$$\begin{aligned} \deg(\psi \circ \varphi) &= [K(C_1) : (\psi \circ \varphi)^* K(C_3)] \\ &= [K(C_1) : \varphi^* \psi^* K(C_3)] \\ &= [K(C_1) : \varphi^* K(C_2)][\varphi^* K(C_2) : \varphi^* \psi^* K(C_3)] \\ &= [K(C_1) : \varphi^* K(C_2)][K(C_2) : \psi^* K(C_3)] \qquad (1.0.9a) \\ &= \deg \varphi \deg \psi. \end{aligned}$$

(c) Dit volgt uit precies dezelfde berekening als bij (b), maar dan met graden vervangen door separabiliteitsgraden, en in plaats van (1.0.9a) passen we (1.0.9b) toe.

(d) volgt direct uit (a), (b) en (c).

(e) is triviaal als $p = 0$, en een vertaling van (1.0.8) als $p > 0$. □

Vertakkingsindex van een morfisme bij een punt

Als $\varphi : C_1 \to C_2$ een niet-constant morfisme van niet-singuliere projectieve krommen is, $P \in C_1$ een punt, en t', t twee lokale parameters bij $\varphi(P)$, dan hebben we

$$t' = ut \qquad \text{voor een } u \in \mathcal{O}^*_{\varphi(P),C_2},$$

en omdat $\varphi^* : \mathcal{O}_{\varphi(P),C_2} \to \mathcal{O}_{P,C_1}$ een ringhomomorfisme is, geldt dat $\varphi^* u \in \mathcal{O}^*_{P,C_1}$. Er volgt dat

$$\mathrm{ord}_P(\varphi^* t') = \mathrm{ord}_P((\varphi^* u)(\varphi^* t)) = \mathrm{ord}_P(\varphi^* u) + \mathrm{ord}_P(\varphi^* t) = \mathrm{ord}_P(\varphi^* t).$$

Daarom is de functie

$$e_\varphi : C_1 \to \mathbb{Z} : \quad P \mapsto \mathrm{ord}_P(\varphi^* t) \qquad \text{met } t \text{ een lokale parameter bij het punt } \varphi(P) \text{ op } C_2,$$

welgedefinieerd. Bovendien ligt het beeld van e_φ in $\mathbb{Z}_{\geq 1}$, want het beeld van $\mathfrak{m}_{\varphi(P),C_2}$ onder φ^* ligt in $\mathfrak{m}_{P,C_1}$. Het getal $e_\varphi(P)$ heet de *vertakkingsindex van* φ *bij* P, en φ *vertakt in* P als $e_\varphi(P) > 1$. Een paar belangrijke eigenschappen noemen we in

Propositie 2.2.7. *Zij* $\varphi : C_1 \to C_2$ *en* $\psi : C_2 \to C_3$ *twee niet-constante morfismen van niet-singuliere projectieve krommen over* K.

(a) Voor elk punt $P \in C_1$ *geldt*

$$e_{\psi \circ \varphi}(P) = e_\psi(\varphi P) e_\varphi(P).$$

(b) Voor elk punt $Q \in C_2$ *geldt*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi.$$

(c) Voor alle punten $Q \in C_2$, *op eindig veel na, is*

$$\#\varphi^{-1}(Q) = \deg_s \varphi.$$

(d) Stel dat φ een isomorfisme is. Dan vertakt φ nergens, en $\deg\varphi = 1$.

Bewijs. (a), (b), (c) [Sil09, II.2.6].
(d) Het morfisme $I : C_1 \to C_1 : P \mapsto P$ vertakt nergens, want volgens (a) voldoet het positieve gehele getal $e_I(P)$ aan

$$e_I(P) = e_{I\circ I}(P) = e_I(P)^2,$$

voor alle $P \in C_1$. Er volgt dat voor alle $P \in C_1$,

$$1 = e_I(P) = e_{\varphi^{-1}\varphi}(P) = e_{\varphi^{-1}}(\varphi P)e_\varphi(P),$$

en omdat rechts een product van positieve gehele getallen staat, moeten ze beide 1 zijn. Omdat bovendien φ bijectief is, zegt (b) dat $\deg\varphi = 1$. □

Opmerking 2.2.8. Een morfisme $\varphi : C_1 \to C_2$ van projectieve krommen over K kunnen we opvatten als morfisme van projectieve krommen over L. We proberen precies te zijn. We schrijven $C_i \otimes L$ voor de projectieve kromme C_i opgevat als kromme over L, voor $i = 1, 2$. Dat wil zeggen, we hebben $C_i = \mathcal{Z}(S) \subset \mathbb{P}^n_L$ voor een verzameling homogene polynomen $S \subset K[X_0, \ldots, X_n]$, en dus ook $S \subset L[X_0, \ldots, X_n]$, en L is een algebraïsche afsluiting van L; we kunnen daarom de deelruimte $\mathcal{Z}(S) \subset \mathbb{P}^n_L$ als projectieve kromme over L opvatten, en deze noteren we als $C_i \otimes L$. Omdat $C_i \otimes L$ als topologische ruimte gelijk is aan C_i, is het duidelijk dat de functie $\varphi : C_1 \to C_2$ ook als morfisme $C_1 \otimes L \to C_2 \otimes L$ kan worden opgevat, en we noteren dit morfisme als φ_L.

Het is duidelijk uit de definities, die 'meetkundig' van aard zijn en alleen van L afhangen, dat dat de functies $e_\varphi : C_1 \to \mathbb{Z}_{\geq 1}$ en $e_{\varphi_L} : C_1 \otimes L \to \mathbb{Z}_{\geq 1}$ aan elkaar gelijk zijn. Namelijk, als functie is φ gelijk aan φ_L, en als functie is $\mathrm{ord}_P : L(C)^* \to \mathbb{Z}$ gelijk aan $\mathrm{ord}_P : L(C \otimes L)^* \to \mathbb{Z}$, en bovendien is $\varphi^{-1}(Q) = \varphi_L^{-1}(Q)$ voor alle $Q \in C_2$. Conclusie: (2.2.7b) impliceert dat $\deg\varphi = \deg\varphi_L$. Dit is niet direct duidelijk uit de definitie van de graad. Met andere woorden, we vinden dat

$$[L(C_1) : \varphi^* L(C_2)] = \deg\varphi_L = \deg\varphi = [K(C_1) : \varphi^* K(C_2)].$$

2.3 Divisoren

De *divisorengroep* van een projectieve kromme kromme C/K, notatie $\mathrm{Div}(C)$, is de vrije abelse groep voortgebracht door de punten van C. De elementen van $\mathrm{Div}(C)$ heten divisoren. Om duidelijk te maken dat het om een divisor gaat, noteren we een punt $P \in C$, opgevat als divisor, als (P). Als we het hebben over 'de divisor $\sum_{P\in C} n_P(P) \in \mathrm{Div}(C)$', dan bedoelen we dat de n_P gehele getallen zijn, waarvan er slechts eindig veel niet nul zijn.

We introduceren een aantal bijbehorende constructies.

We hebben een groepshomomorfisme

$$\deg : \mathrm{Div}(C) \to \mathbb{Z} : \quad \sum_{P\in C} n_P(P) \mapsto \sum_{P\in C} n_P,$$

en we zeggen dat $\deg(D)$ de *graad* van de divisor $D \in \mathrm{Div}(C)$ is. De ondergroep van $\mathrm{Div}(C)$ van divisoren van graad nul schrijven we als $\mathrm{Div}^0(C)$.

We hebben een natuurlijke partiële orderelatie '$\leq$' op $\mathrm{Div}(C)$, namelijk, $\sum_{P\in C} m_P(P) \leq \sum_{P\in C} n_P(P)$ precies dan als $m_P \leq n_P$ voor alle P.

Veronderstel dat C niet-singulier is. Met elk element $f \in L(C)^*$ kunnen we vanwege (2.2.1b) een divisor $\sum_{P\in C} \mathrm{ord}_P(f)(P) \in \mathrm{Div}(C)$ associëren. Zodoende hebben we een functie

$$\mathrm{div} : L(C)^* \to \mathrm{Div}(C) : \quad f \mapsto \sum_{P\in C} \mathrm{ord}_P(f)(P).$$

Omdat ord_P een valuatie is, is div een homomorfisme van abelse groepen.

Een niet-constant morfisme $\varphi : C_1 \to C_2$ van niet-singuliere projectieve krommen over K geeft aanleiding tot een homomorfisme $\varphi^{\mathrm{Div}} : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ van abelse groepen, namelijk het homomorfisme dat wordt vastgelegd door het voorschrift

$$\varphi^{\mathrm{Div}} : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1) : \quad (Q) \mapsto \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)$$

voor $Q \in C_2$, met andere woorden, we breiden dit voorschrift $\mathbb{Z}$-lineair uit naar heel $\mathrm{Div}(C_2)$. Daarnaast hebben we een homomorfisme

$$\varphi_{\mathrm{Div}} : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2) : \quad \sum_{P \in C_1} n_P(P) \mapsto \sum_{P \in C_1} n_P(\varphi(P)).$$

Als $\psi : C_2 \to C_3$ nog een niet-constant morfisme is, dan hebben we

$$(\psi \circ \varphi)^{\mathrm{Div}} = \varphi^{\mathrm{Div}} \circ \psi^{\mathrm{Div}} \qquad \text{en} \qquad (\psi \circ \varphi)_{\mathrm{Div}} = \psi_{\mathrm{Div}} \circ \varphi_{\mathrm{Div}}.$$

De tweede formule is duidelijk, de eerste volgt eenvoudig met behulp van (2.2.7b). (De constructies geven zodoende aanleiding tot een contravariante resp. covariante functor – het is duidelijk hoe we dit precies kunnen maken.)

Propositie 2.3.1. *Zij C, C' niet-singuliere projectieve krommen over K.*

(a) Het beeld van $\mathrm{div} : L(C)^* \to \mathrm{Div}(C)$ *is bevat in* $\mathrm{Div}^0(C)$.

(b) De kern van $\mathrm{div} : L(C)^* \to \mathrm{Div}(C)$ *is gelijk aan* L^*.

Zij $\varphi : C \to C'$ een niet-constant morfisme.

(c) Het diagram

$$\begin{array}{ccc} \mathrm{Div}(C) & \xleftarrow{\varphi^{\mathrm{Div}}} & \mathrm{Div}(C') \\ \uparrow{\scriptstyle \mathrm{div}} & & \uparrow{\scriptstyle \mathrm{div}} \\ L(C)^* & \xleftarrow{\varphi^*} & L(C')^* \end{array}$$

commuteert. Analoog hebben we

$$\varphi_{\mathrm{Div}}(\mathrm{div} L(C)^*) \subset \mathrm{div} L(C')^*.$$

(d) Voor alle $D \in \mathrm{Div}(C')$ geldt dat $\deg(\varphi^{\mathrm{Div}} D) = \deg \varphi \cdot \deg D$.

Bewijs. (a,b,c) Zie [Sil09, II.3.4]. (d) Voor divisoren van de vorm (Q), met $Q \in P$, volgt de formule direct uit de definities en uit (2.2.7b): we hebben

$$\deg(\varphi^{\mathrm{Div}}(Q)) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi.$$

Voor willekeurige D volgt het omdat de afbeeldingen

$$\varphi^{\mathrm{Div}} : \mathrm{Div}(C') \to \mathrm{Div}(C) \qquad \text{en} \qquad \deg : \mathrm{Div}(C) \to \mathbb{Z}$$

additief zijn. □

Onderdeel (a) van (2.3.1) rechtvaardigt

Definitie 2.3.2. Zij C/K een niet-singuliere projectieve kromme. We definiëren de *Picardgroep* $\mathrm{Pic}(C)$ van C, en diens ondergroep $\mathrm{Pic}^0(C)$ ('de graad-nul-Picardgroep'), als

$$\mathrm{Pic}(C) = \frac{\mathrm{Div}(C)}{\mathrm{div}(L(C)^*)}, \qquad \mathrm{Pic}^0(C) = \frac{\mathrm{Div}^0(C)}{\mathrm{div}(L(C)^*)}.$$

Conventie 2.3.3. In de notatie van (2.3.2), schrijven we de projectie van een divisor $D \in \mathrm{Div}^0(C)$ in de groep $\mathrm{Pic}^0(C)$ als $\lceil D \rceil$, met andere woorden, $\lceil D \rceil = D + \mathrm{div}(L(C)^*) \in \mathrm{Pic}^0(C)$.

Als $\varphi : C_1 \to C_2$ een niet-constant morfisme van niet-singuliere projectieve krommen over K is, dan beelden de homomorfismen $\varphi^{\mathrm{Div}} : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ en $\varphi_{\mathrm{Div}} : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ divisoren van graad 0 naar divisoren van graad 0 af: voor φ_{Div} is dit duidelijk, voor φ^{Div} volgt het uit (2.3.1d). Zodoende krijgen we, door restrictie, homomorfismen

$$\varphi^{\mathrm{Div}} : \mathrm{Div}^0(C_2) \to \mathrm{Div}^0(C_1) \qquad \text{en} \qquad \varphi_{\mathrm{Div}} : \mathrm{Div}^0(C_1) \to \mathrm{Div}^0(C_2).$$

Bovendien zien we uit het diagram in (2.3.1b) dat $\varphi^{\mathrm{Div}}(\mathrm{div}L(C_2)^*) \subset \mathrm{div}L(C_1)^*$, dus de kern van het door φ^{Div} geïnduceerde homomorfisme $\mathrm{Div}^0(C_2) \to \mathrm{Pic}^0(C_1)$ omvat $\mathrm{div}L(C_2)^*$. Hetzelfde verhaal gaat volgens de tweede bewering in (2.3.1b) op voor φ_{Div}: de kern van het door φ_{Div} geïnduceerde homomorfisme $\mathrm{Div}^0(C_1) \to \mathrm{Pic}^0(C_2)$ omvat $\mathrm{div}L(C_1)^*$. Kortom, we hebben welgedefinieerde homomorfismen

$$\varphi^{\mathrm{Pic}} : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1) : \lceil D \rceil \mapsto \lceil \varphi^{\mathrm{Div}} D \rceil, \qquad \varphi_{\mathrm{Pic}} : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2) : \lceil D \rceil \mapsto \lceil \varphi_{\mathrm{Div}} D \rceil.$$

2.4 Differentialen

Zij C/K een projectieve kromme. Zij V de $L(C)$-vectorruimte voortgebracht door de formele symbolen Dx met $x \in L(C)$, en zij W de deelruimte van V voortgebracht door de deelverzameling

$$\begin{aligned} &\{D(x+y) - Dx - Dy : x, y \in L(C)\} \quad \cup \\ &\{D(xy) - xDy - yDx : x, y \in L(C)\} \quad \cup \\ &\{D(a) : a \in L\} \end{aligned}$$

van W. De quotiëntruimte V/W is de *ruimte van differentiaalvormen op* C, notatie Ω_C. Het element $Dx + W$ van V/W schrijven we voor het gemak als dx. (De notatie V, W, Dx was puur om de definitie concreet op te schrijven, we gebruiken het verder niet.) Als abstracte $L(C)$-vectorruimte is Ω_C eenvoudig: volgens [Sil09, II.4.2] hebben we

Propositie 2.4.1. *Als C/K een projectieve kromme is, dan is* $\dim_{L(C)} \Omega_C = 1$.

Een niet-constant morfisme $\varphi : C_1 \to C_2$ van projectieve krommen over K geeft aanleiding tot de fucntie

$$\varphi^{\Omega} : \Omega_{C_2} \to \Omega_{C_1} : \quad f_1 dx_1 + \ldots + f_m dx_m \mapsto (\varphi^* f_1) d(\varphi^* x_1) + \ldots + (\varphi^* f_m) d(\varphi^* x_m),$$

waarbij $f_1, \ldots, f_m, x_1, \ldots, x_m \in L(C_2)$. Het is eenvoudig te zien dat φ^{Ω} welgedefinieerd is.

Propositie 2.4.2. *Zij $\varphi : C_1 \to C_2$ een niet-constant morfisme van projectieve krommen over K, en beschouw de functie $\varphi^{\Omega} : \Omega_{C_2} \to \Omega_{C_1}$.*

(a) φ^Ω *is een homomorfisme van abelse groepen, en voor alle* $f \in L(C_2)$ *en* $\omega \in \Omega_{C_2}$ *geldt*

$$\varphi^\Omega(f\omega) = \varphi^*(f)\varphi^\Omega(\omega).$$

(b) De volgende condities zijn equivalent:

(i) φ *is separabel.*

(ii) φ^Ω *is niet de nulafbeelding.*

(iii) φ^Ω *is injectief.*

Bewijs. (a) volgt direct uit de definities. (c) Zie [Sil09, II.4.2] voor '(i) $\iff$ (ii)'. De bewering '(ii) $\iff$ (iii)' volgt uit het voorgaande. Stel namelijk dat φ^Ω niet de nulafbeelding is, en neem $\omega \in \Omega_{C_2}$ met $\varphi^\Omega\omega \neq 0$. In het bijzonder is $\omega \neq 0$, dus vanwege (2.4.1) zijn alle elementen van Ω_{C_2} te schrijven als $f\omega$, met $f \in L(C_2)$. Als $f, f' \in L(C_2)$ met $f \neq f'$, dan geeft (a) dat

$$\varphi^\Omega(f\omega) = \varphi^*(f)\varphi^\Omega(\omega) \neq \varphi^*(f')\varphi^\Omega(\omega) = \varphi^\Omega(f'\omega),$$

de ongelijkheid volgt omdat φ^* injectief is en omdat $\varphi^\Omega(\omega) \neq 0$. Conclusie: φ^Ω is injectief. □

Een punt $P \in C$ op een projectieve kromme C/K geeft aanleiding tot een functie $\mathrm{ord}_P : \Omega_C - \{0\} \to \mathbb{Z}$. Namelijk, als $\omega \in \Omega_C$ met $\omega \neq 0$, en als $t \in L(C)$ een lokale parameter bij P is, dan zegt [Sil09, II.4.3] dat er een unieke functie $g_\omega \in L(C)$ is zo dat $\omega = g_\omega\, dt$, en dat bovendien het gehele getal $\mathrm{ord}_P(g_\omega)$ alleen afhangt van ω, niet van de keuze van t. Daarom is de functie

$$\mathrm{ord}_P : \Omega_C - \{0\} \to \mathbb{Z} : \quad \omega \mapsto \mathrm{ord}_P(g_\omega),$$

met $g_\omega \in L(C)$ zoals boven, welgedefinieerd.

Als $\omega \in \Omega_C$, dan zijn er volgens [Sil09, II.4.3] slechts eindig veel punten $P \in C$ met $\mathrm{ord}_P(\omega) \neq 0$. Daarom kunnen we de functie

$$\mathrm{div} : \Omega_C \to \mathrm{Div}(C) : \quad \mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$$

definiëren. Als $D \in \mathrm{Div}(C)$ in het beeld van deze functie div ligt, dan noemen we D een *canonieke divisor op* C.

2.5 De stelling van Riemann–Roch en elliptische krommen

Als C/K een projectieve kromme is en $D \in \mathrm{Div}(C)$ een divisor, dan is volgens [Sil09, II.5.2] de verzameling

$$\mathcal{L}(D) = \{g \in L(C)^* : \mathrm{div}(g) \geq -D\} \cup \{0\}$$

een eindig-dimensionale L-vectorruimte. We schrijven $\ell(D) = \dim_L \mathcal{L}(D)$.

We zijn nu in staat de diepe stelling van Riemann–Roch te formuleren. We gebruiken de formulering zoals in [Sil09, II.5.4]. Een bewijs van de stelling staat bijvoorbeeld in [Har77, IV.1.3].

Stelling 2.5.1 (Riemann–Roch)**.** *Zij* C/K *een niet-singuliere projectieve kromme, zij* D_{can} *een canonieke divisor op* C*, en zij* $D \in \mathrm{Div}(C)$ *een willekeurige divisor. Het gehele getal*

$$\ell(D_{\mathrm{can}} - D) - \ell(D) + \deg D + 1$$

is niet-negatief, en is onafhankelijk van de keuze van D_{can} *en van* D*.*

Definitie 2.5.2. In de notatie van (2.5.1) noemen we het getal $\ell(D_{\mathrm{can}} - D) - \ell(D) + \deg D + 1 \in \mathbb{Z}_{\geq 0}$ het *geslacht van* C.

Definitie 2.5.3. Als C/K een niet-singuliere projectieve kromme van geslacht 1 is, en als $O \in C(K)$ een K-rationaal punt op C is, dan noemen we (C, O) een *elliptische kromme over* K.

In de praktijk zullen we vaak het punt O in de notatie onderdrukken, en het over 'de elliptische kromme C' hebben in plaats van het correctere 'de elliptische kromme (C, O)'.

Hoofdstuk 3

Elliptische krommen

We fixeren in dit hoofdstuk deze notatie:
K is een perfect lichaam,
L is een algebraïsche afsluiting van K.

Wat elliptische krommen tot een bijzondere klasse onder de krommen maakt, is dat ze op een natuurlijke manier een abelse groep zijn. In dit hoofdstuk introduceren we de groepswet. Een andere bijzonderheid is dat elke elliptische kromme te schrijven is in een eenvoudige vorm, namelijk met een Weierstrass-vergelijking. Dit helpt ons om concrete berekeningen te doen.

3.1 Isogeniën

We specificeren de afbeeldingen tussen elliptische krommen waarin we het meest geïnteresseerd zijn, zodat we een categorie hebben om mee te werken.

Omdat een elliptische kromme een projectieve kromme is met een gespecificeerd 'basispunt' daarop, is het natuurlijk om ons te beperken tot de afbeeldingen die het basispunt van de een naar dat van de ander afbeelden.

Definitie 3.1.1. Een *isogenie* $\varphi : E_1 \to E_2$ tussen elliptische krommen (E_1, O_1) en (E_2, O_2) over K, is een morfisme $\varphi : E_1 \to E_2$ van projectieve krommen over K zo dat $\varphi(O_1) = O_2$. Het is duidelijk dat de samenstelling van twee isogeniën een isogenie is, zodat we een categorie hebben. Een isogenie $\varphi : E_1 \to E_2$ waarvoor er een isogenie $\psi : E_2 \to E_1$ bestaat zo dat $\psi \circ \varphi$ en $\varphi \circ \psi$ de identiteit zijn op resp. E_1 en E_2, noemen we een *isomorfisme*.

We schrijven $\mathrm{Ign}(E_1, E_2)$ voor de verzameling van isogeniën $E_1 \to E_2$ (deze notatie is niet standaard), en we schrijven $\mathrm{End}(E) := \mathrm{Ign}(E, E)$ voor de verzameling van *endomorfismen* van E.

Conventie 3.1.2. Als we het over een isomorfisme of isomorfie van elliptische krommen hebben, bedoelen we dit, tenzij anders vermeld, met betrekking tot categorie van elliptische krommen met isogeniën. Met andere woorden, een isomorfisme is zoals beschreven in (3.1.1).

3.2 De groepswet op een elliptische kromme

Een elliptische kromme is op een natuurlijke manier een abelse groep. We introduceren de groepsstructuur aan de hand van een bijectie tussen de kromme en de graad-nul-Picardgroep.

Stelling 3.2.1. *Als (E, O) een elliptische kromme over K is, dan is de functie*

$$\kappa : E \to \mathrm{Pic}^0(E) : \quad P \mapsto \lceil (P) - (O) \rceil$$

bijectief.

Zie [Sil09, III.3.4] voor een bewijs. In essentie is het een gevolg van de stelling van Riemann-Roch. Omdat $\mathrm{Pic}^0(E)$ al een abelse groep is, induceert κ de structuur van een abelse groep op E, en omdat $\kappa(O) = 0$, is O is het neutrale element. Voor de duidelijkheid formuleren we dit in

Definitie 3.2.2. Zij (E, O) een elliptische kromme over K, en zij $\kappa : E \to \mathrm{Pic}^0(E)$ de bijectie van (3.2.1). We definiëren een operatie '+' op E door middel van

$$P_1 + P_2 = \kappa^{-1}(\kappa(P_1) + \kappa(P_2)).$$

voor $P_1, P_2 \in E$. Deze operatie maakt E tot een abelse groep met O als neutraal element, en per constructie is κ een isomorfisme van abelse groepen.

Een van de zinnen waarin deze groepswet 'natuurlijk' is, is dat het isogenieën tot groepshomomorfismen maakt.

Propositie 3.2.3. *Een isogenie $\varphi : E_1 \to E_2$ van elliptische krommen $(E_1, O_1), (E_2, O_2)$ over K is een homomorfisme van abelse groepen.*

Bewijs. Zij $\kappa_i : E_i \to \mathrm{Pic}^0(E_i) : P \mapsto \lceil (P) - (O_i) \rceil$ het groepsisomorfisme zoals in (3.2.1), voor $i = 1, 2$. Het diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E_2 \\ \downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_2} \\ \mathrm{Pic}^0(E_1) & \xrightarrow{\varphi_{\mathrm{Pic}}} & \mathrm{Pic}^0(E_2) \end{array}$$

commuteert, want voor $P \in E_1$ hebben we, vanwege $\varphi(O_1) = O_2$, dat

$$P \quad \overset{\kappa_1}{\longmapsto} \quad \lceil (P) - (O_1) \rceil \quad \overset{\varphi_{\mathrm{Pic}}}{\longmapsto} \quad \lceil \varphi(P) - (O_2) \rceil \quad \overset{\kappa_2^{-1}}{\longmapsto} \quad \varphi(P).$$

Omdat $\kappa_1, \varphi_{\mathrm{Pic}}, \kappa_2^{-1}$ groepshomomorfismen zijn, is hun samenstelling φ dat ook. □

Conventie 3.2.4. Als A een abelse groep is en m een geheel getal, dan schrijven we $[m]$ voor het endomorfisme van A dat vermenigvuldiging met m voorstelt, kortom, $A \to A : x \mapsto mx$ als $[m]$. We schrijven $A[m] := \ker[m]$. In het bijzonder passen we dit toe op $A = E$.

De afbeeldingen $[m] : E \to E$ spelen een belangrijke rol. De belangrijkste eigenschappen, die verderop aan de orde zullen komen, zijn dat $[m]$ een isogenie is, en dat $\deg[m] = m^2$. Uit dit laatste zullen we uiteindelijk het belangrijke resultaat afleiden dat, indien m niet nul is in K, de abelse groep $E[m]$ isomorf is met $\mathbb{Z}/m \times \mathbb{Z}/m$.

We kunnen een divisor op E, met andere woorden een 'formele' som van punten op E, opvatten als 'echte' som die we kunnen berekenen in E. Met andere woorden, we hebben een homomorfisme van abelse groepen

$$\mathrm{som} : \mathrm{Div}(E) \to E : \quad \sum_{P \in E} n_P(P) \mapsto \sum_{P \in E} [n_P]P.$$

Lemma 3.2.5. *Zij (E, O) een elliptische kromme over K. De inverse van het groepsisomorfisme $\kappa : E \to \mathrm{Pic}^0(E) : P \mapsto \lceil (P) - (O) \rceil$ wordt gegeven door*

$$\kappa^{-1} : \mathrm{Pic}^0(E) \to E : \quad \lceil D \rceil \mapsto \mathrm{som}(D), \qquad \textit{voor } D \in \mathrm{Div}^0(E).$$

Bewijs. Zij $D \in \mathrm{Div}^0(E)$, zeg $D = \sum_{P \in E} n_P(P)$. Dan is

$$D = \sum_{P \in E} n_P((P) - (O)),$$

want $\sum_{P \in E} n_P(O) = 0(O) = 0$ omdat $\deg D = 0$. Er volgt dat

$$\lceil D \rceil = \sum_{P \in E} n_P \lceil (P) - (O) \rceil, \qquad \text{zodat}$$
$$\kappa^{-1} \lceil D \rceil = \sum_{P \in E} [n_P] P = \mathrm{som}(D). \qquad \square$$

Het volgende gevolg is een echt werkpaard, dat we onder meer in onze studie van de Weilparing veelvuldig zullen gebruiken om te garanderen dat er een functie $f \in L(E)^*$ met een bepaalde gewenste eigenschap bestaat. Het is een variant van de 'Stelling van Abel'.

Gevolg 3.2.6. *Zij (E, O) een elliptische kromme over K en zij $D \in \mathrm{Div}^0(E)$ een divisor van graad nul. Er geldt*

$$D \in \mathrm{div}(L(E)^*) \iff \mathrm{som}(D) = O.$$

Bewijs. De volgende condities zijn equivalent:

$$\begin{aligned} D &\in \mathrm{div}(L(E)^*), && \\ \lceil D \rceil &= 0 && \text{per definitie van } \mathrm{Pic}^0(E), \\ \kappa^{-1} \lceil D \rceil &= O && \text{met } \kappa \text{ als in (3.2.1)}, \\ \mathrm{som}(D) &= O && \text{volgens (3.2.5).} \end{aligned}$$ $\square$

Voorbeeld 3.2.7. Als P een punt is op een elliptische kromme E/K, dan definiëren we τ_P, 'translatie over P', als de funcie

$$\tau_P : E \to E : \quad T \mapsto P + T.$$

Volgens [Sil09, III.3.6] is τ_P een morfisme van projectieve krommen, en zelfs een isomorfisme want hij heeft een inverse τ_{-P}. Het is echter duidelijk dat τ_P geen isogenie is, tenzij $P = O$. Niet-triviale voorbeelden van isogeniën zullen we straks zien.

3.3 Weierstrass-vergelijkingen

De theorie tot hier toe was vrij abstract. Het wordt concreter als we elliptische krommen bekijken die door een Weierstrass-vergelijkingen worden gegeven.

Zij C/K de vlakke projectieve kromme die, in affiene notatie, gegeven wordt door

$$C : \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{3.1}$$

waarbij $a_1, \ldots, a_4, a_6 \in K$. Met andere woorden, we hebben $C = \mathcal{Z}(f) \subset \mathbb{P}^2_L$, waarbij

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X, Y, Z].$$

Op dezelfde manier als in (2.1.2) zien we dat C de lijn $Z = 0$ alleen snijdt in het punt $[0, 1, 0]$. We hebben dus een bijectie $C - \{[0, 1, 0]\} \to C' : [x, y, z] \mapsto (x/z, y/z)$, waarbij C' de affiene voorstelling van C is, dat wil zeggen de verzameling wortels in $\mathbb{A}^2_L$ van de vergelijking (3.1).

De vergelijking (3.1) heet een *Weierstrass-vergelijking*. Als we zeggen 'zij C/K een kromme gegeven door een Weierstrass-vergelijking', dan bedoelen we dat C is als in (3.1), voor zekere $a_1 \ldots, a_4, a_6 \in K$.

De *discriminant van* C is het element

$$\Delta(C) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \in K, \tag{3.2}$$

waarbij

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, & b_6 &:= a_3^2 + 4a_6, \\ b_4 &:= 2a_4 + a_1 a_3, & b_8 &:= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned} \tag{3.3}$$

De belangrijkste feiten over krommen gegeven door een Weierstrass-vergelijking, sommen we op in

Stelling 3.3.1. *(a) Een kromme C/K als in* (3.1) *is singulier precies dan als $\Delta(C) = 0$.*

(b) Als $\Delta(C) \neq 0$, dan is $(C, [0, 1, 0])$ een elliptische kromme over K.

(c) Elke elliptische kromme E/K is isomorf met een elliptische kromme gegeven door een Weierstrass-vergelijking. Met andere woorden, er zijn (niet noodzakelijk unieke) elementen $a_1, \ldots, a_4, a_6 \in K$ zo dat $(C, [0, 1, 0])$ een elliptische kromme over K is, waarbij C is als in (3.1)*, en zo dat $E \cong C$.*

(d) Als in de situatie van (c) bovendien $\mathrm{char} K \neq 2$*, dan kunnen $a_1, \ldots, a_4, a_6$ zo gekozen worden dat $a_1 = a_3 = 0$.*

Bewijs. (a) [Sil09, III.1.4a]. (b) [Sil09, III.3.1c]. (c) [Sil09, III.3.1a]. (d) [Sil09, III.1]. □

Voorbeeld 3.3.2. Zij $C/\mathbb{F}_3$ de projectieve kromme van Voorbeeld 2.1.2, kortom, we hebben

$$C: \quad Y^2 = X^3 + X + 1.$$

Dus C wordt gegeven door een Weierstrass-vergelijking. We zagen in (2.1.9) al dat C niet-singulier is, dus uit (3.3.1ab) volgt dat $(C, [0, 1, 0])$ een elliptische kromme over $\mathbb{F}_3$ is. Dit wordt bevestigd door een berekening: in de notatie van (3.2) en (3.3) hebben we

$$a_1 = a_2 = a_3 = 0, \quad a_4 = a_6 = 1, \qquad b_2 = 0, \quad b_4 = -1, \qquad \Delta(E) = b_4^3 = -1.$$

Conventie 3.3.3. Als we het hebben over een elliptische kromme (E, O) gegeven door een Weierstrass-vergelijking, dan bedoelen we altijd dat $O = [0, 1, 0]$. Zoals we al opmerkten, hebben we een bijectie $a : E - \{O\} \to E' : [x, y, z] \mapsto (x/z, y/z)$, met E' de affiene voorstelling van E. Met misbruik van notatie spreken we van 'het punt $(x, y) \in E$' als we het punt $[x, y, 1] \in E$ bedoelen, met andere woorden, we hebben dan eigenlijk $(x, y) \in E'$ en we bedoelen het punt $a^{-1}(x, y) \in E$.

Vanwege (3.3.1c) is het normaal gesproken genoeg om een vraagstuk over elliptische krommen te beantwoorden voor elliptische krommen gegeven door een Weierstrass-vergelijking. Dit zullen we verderop een paar keer gebruiken.

De groepswet op een elliptische kromme E/K gegeven door een Weierstrass-vergelijking, heeft een concrete meetkundige interpretatie, die we hier alleen schetsen, zie [Sil09, III.2] voor details. Namelijk, het is een bijzonder geval van de stelling van Bézout [Har77, I.7.8] dat elke lijn $M \subset \mathbb{P}^2_L$ de elliptische kromme E in precies drie punten snijdt, mits de snijpunten met de juiste multipliciteit worden geteld (we definiëren dit begrip van multipliciteit hier niet). Als P, Q, R de snijpunten van M en E zijn (vanwege de multipliciteit zijn dit niet per se drie verschillende punten), dan geldt

$$P + Q + R = O.$$

Zie [Sil09, III.3.4e] voor een bewijs.

Het vinden van de snijpunten van M en C komt neer op het vinden van de nulpunten van een derdegraads polynoom. Door alles expliciet uit te schrijven, vindt men onder andere de volgende formules.

Feit 3.3.4. *Zij E/K een elliptische kromme gegeven door een Weierstrass-vergelijking zoals in* (3.1)*, en zij $P = (x, y) \in E$.*

(a) We hebben $-P = (x, -y - a_1x - a_3)$.

(b) Als $[2]P \neq O$, dan is $[2]P = (x', y')$ voor een zekere $y' \in L$ en met

$$x' = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} \in L, \tag{3.4}$$

waarbij $b_2, b_4, b_6, b_8 \in K$ de elementen zijn gegeven in (3.3)*.*

Bewijs. [Sil09, III.2.3] □

Opmerking 3.3.5. Zij (E, O) een elliptische kromme over K gegeven door een Weierstrass-vergelijking. Uit (3.3.4) volgt dat als k een tussenlichaam is van $K \subset L$, en als $P \in E(k)$, dan is ook $-P \in E(k)$ en $[2]P \in E(k)$. (We willen benadrukken dat $O = [0, 1, 0] \in E(k)$.) Algemenere formules (zie [Sil09, III.2.3]) laten zien dat als $P, Q \in E(k)$, dan is $P + Q \in E(k)$. Dus $E(k)$ is een ondergroep van E.

Voorbeeld 3.3.6. Zij E/K een elliptische kromme gegeven door een Weierstrass-vergelijking, en veronderstel dat $\mathrm{char}K =: p > 0$. Zij q een macht van p en zij $\pi : E \to E^{(q)}$ het q-de machts Frobenius-morfisme op E. Merk op dat ook de kromme $E^{(q)}/K$ gegeven wordt door een Weierstrass-vergelijking, namelijk door de coëfficiënten van de vergelijking van E tot de macht q te verheffen. Bovendien, omdat het Frobenius-automorfisme $K \to K : x \mapsto x^q$ de identiteit is op $\mathbb{F}_p$, blijkt uit de formules dat $\Delta(E^{(q)}) = \Delta(E)^q$. Volgens (3.3.1b) betekent dit dat $E^{(q)}/K$ een elliptische kromme is. Bovendien is $\pi[0, 1, 0] = [0, 1, 0]$, dus we hebben

$$\pi \in \mathrm{Ign}(E, E^{(q)}).$$

Als bovendien $K = \mathbb{F}_{q'}$ voor een macht $q' \leq q$ van p, dan is $E^{(q)} = E$, want de coëfficiënten van de vergelijking van E liggen dan in $\mathbb{F}_{q'}$, waarop het automorfisme $K \to K : x \mapsto x^q$ de identiteit is. Er volgt dat dan

$$\pi \in \mathrm{End}(E).$$

Zoals we al opmerkten, gaan we verderop bewijzen dat $\#E[m] = m^2$ als E/K een elliptische kromme is en als m niet nul is in K. We gaan dit in de volgende twee voorbeelden expliciet na voor het geval $m = 2$, en voor het geval $m = 3$ indien K karakteristiek 2 heeft. De voorbeelden dienen drie doelen. Ten eerste illustreren ze hoe er concreet gerekend kan worden aan elliptische

krommen. Ten tweede ontmoedigen ze ons om de gevallen $m > 3$ met soortgelijke methoden aan te pakken, zodat we de erop volgende theorie beter kunnen waarderen. Ten derde, en meest essentiële: in ons bewijs van de stelling dat $\#E[m] = m^2$ zodra m niet nul is in K, gebruiken we de Voorbeelden! Zij hebben hebben hier dus eerder de status van lemma's.

Voorbeeld 3.3.7. Dit voorbeeld behandelt de genoemde stelling voor het geval $m = 2$.

Veronderstel dat $\mathrm{char}K \neq 2$. Volgens (3.3.1d) is elke elliptische kromme over K isomorf met een elliptische kromme van de vorm

$$E: \quad Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

voor zekere $a_2, a_4, a_6 \in K$. We berekenen $E[2]$.[1]

Zij $P \in E$ een punt ongelijk aan O, zeg $P = (x, y)$ met $x, y \in L$. De volgende condities zijn equivalent:

$$\begin{aligned}
&P \in E[2], && \\
&P = -P, && \\
&(x, y) = (x, -y) && \text{wegens (3.3.4a)}, \\
&y = -y, && \\
&y = 0 && \text{want } \mathrm{char}K \neq 2, \\
&x^3 + a_2x^2 + a_4x + a_6 = 0 = y && \text{want } P \in E.
\end{aligned}$$

Kortom, de elementen van $E[2]$ zijn, naast O, precies de $(x, 0)$ waarbij $x \in L$ een nulpunt is van $g := X^3 + a_2X^2 + a_4X + a_6$. Berekening toont dat g en zijn formele afgeleide g_X copriem zijn in $L[X]$, namelijk

$$\frac{4a_2^3 - 15a_2a_4 + 27a_6 + 6a_2^2x - 18a_4x}{-\Delta(E)/16}g + \frac{-a_2^2a_4 + 4a_4^2 - 3a_2a_6 - 2a_2^3x + 7a_2a_4x - 9a_6x - 2a_2^2x^2 + 6a_4x^2}{-\Delta(E)/16}g_X = 1.$$

Dit betekent dat g separabel is. We concluderen dat als $x_1, x_2, x_3 \in L$ de drie verschillende nulpunten van g zijn, dan is

$$E[2] = \{(x_1, 0), (x_2, 0), (x_3, 0), O\}.$$

In het bijzonder is $\#E[2] = 4$.

Voorbeeld 3.3.8. Dit voorbeeld behandelt een speciaal geval van de genoemde stelling, namelijk het geval waarin $m = 3$ en $\mathrm{char}K = 2$.[2]

Veronderstel dat $\mathrm{char}K = 2$. Volgens (3.3.1c) is elke elliptische kromme over K isomorf met een elliptische kromme van de vorm

$$E: \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{3.5}$$

voor zekere $a_1, \ldots, a_4, a_6 \in K$. We berekenen $E[3]$.

[1] De reden dat we de restrictie $\mathrm{char}K \neq 2$ opleggen, is dat we willen dat het getal $m = 2$ niet nul is in K. Als $\mathrm{char}K = 2$, dan kan men $E[2]$ ook expliciet berekenen, maar dat hebben we niet nodig.

[2] Het ligt meer voor de hand om het voorbeeld algemener uit te werken voor $m = 3$ en $\mathrm{char}K \neq 3$. Maar meer dan wat we nu doen, hebben we later niet nodig, en de uitwerking wordt eenvoudiger door deze restrictie.

Zij $P \in E$ een punt met $P \neq O$ en $[2]P \neq O$, zeg $P = (x, y)$. Volgens (3.3.4) is $[2]P = (x', y')$ voor een zekere $y' \in L$ en met

$$x' = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}. \tag{3.6}$$

Stel dat $x' = x$. Er zijn hooguit twee verschillende $y'' \in L$ zo dat $(x, y'') \in E$, namelijk de nulpunten van de kwadratische vergelijking in Y die we krijgen door $X = x$ in te vullen in (3.5). De punten

$$[2]P = (x, y'), \qquad -P = (x, -y - a_1x - a_3), \qquad P = (x, y)$$

zijn dus niet alledrie verschillend, met andere woorden, er geldt $[2]P = -P$ of $[2]P = P$. Dus $P \in E[3]$. Omgekeerd, stel dat $P \in E[3]$. Dan is $[2]P = -P$, dus $(x', y') = (x, -y - a_1x - a_3)$, dus $x' = x$. Conclusie:

$$P \in E[3] \iff x' = x \iff g(x) = 0, \tag{3.7}$$

waarbij

$$g := X^4 + b_2X^3 + b_4X^2 + b_6X + b_8.$$

(De tweede ' $\iff$ ' volgt door $x' = x$ te substitueren in (3.6), en te gebruiken dat $\mathrm{char}K = 2$.)

We laten nu zien dat de aanname '$[2]P \neq O$' die we hadden gedaan, overbodig is in (3.7), met andere woorden, dat

$$\text{voor alle } (x, y) := Q \in E \text{ met } Q \neq O \text{ geldt:} \qquad Q \in E[3] \iff g(x) = 0. \tag{3.8}$$

'$\Longrightarrow$' is al bewezen, want als $Q \in E[3]$ dan is $[2]Q \neq O$. Voor '$\Longleftarrow$' moeten we nagaan dat als $g(x) = 0$, dan is $[2]Q \neq O$, want dan kunnen we (3.7) gebruiken. Stel dat $[2]Q = O$. Dan is $Q = -Q$, dat wil zeggen $(x, y) = (x, -y - a_1x - a_3)$. Dus

$$a_1x + a_3 = -2y = 0. \tag{3.9}$$

Als $a_3 = 0$, dan impliceren de formules (3.3, 3.2) de tegenspraak $\Delta(E) = 0$. Als $a_1 = 0$, dan zegt (3.9) dat $a_3 = 0$. Kortom, $a_1 \neq 0$ en $a_3 \neq 0$. We hebben

$$b_4 = a_1a_3 \neq 0 \qquad \text{en} \qquad b_6 = a_3^2 \neq 0,$$

en (3.9) geeft

$$x = -\frac{a_3}{a_1} = \frac{a_3}{a_1} = \frac{b_6}{b_4}.$$

We berekenen

$$\begin{aligned}
g(x) &= g(\frac{b_6}{b_4}) \\
&= \frac{b_6^4 + b_2b_6^3b_4 + b_4b_6^2b_4^2 + b_6b_6b_4^3 + b_8b_4^4}{b_4^4} \\
&= \frac{b_6^4 + b_2b_6^3b_4 + b_8b_4^4}{b_4^4} && \text{want } 2b_4^3b_6^2 = 0 \\
&= \frac{b_6^2(b_6^2 + b_2b_6b_4 + b_2^2b_8)}{b_4^4} && \text{want } b_4^2 = b_2b_6 \\
&= \frac{b_6^2\Delta(E)}{b_4^4} \neq 0.
\end{aligned}$$

Conclusie: als $[2]Q = O$, dan is $g(x) \neq 0$, zoals gewenst. Dit voltooit het bewijs van (3.8).

Het polynoom $g \in K[X]$ en zijn afgeleide g_X zijn relatief priem, een berekening toont namelijk dat

$$\frac{-b_2^2}{\Delta(E)}g + \frac{b_2b_4 - b_6 + b_2^2x + b_2x^2}{\Delta(E)}g_X = 1.$$

Dat wil zeggen dat g separabel is. Zij x_1, x_2, x_3, x_4 zijn vier verschillende nulpunten in L. Dan vertelt (3.8) dat $E[3] - \{O\}$ precies bestaat uit de punten op E met als eerste coördinaat x_i, met andere woorden, de punten van de vorm (x_i, y), voor $i = 1, \ldots, 4$. Voor elke i bevat E minstens één en hoogstens twee punten met als eerste coördinaat x_i, want zo'n punt ligt op E precies als $y \in L$ een nulpunt is van de kwadratische vergelijking in Y die wordt verkregen door $X = x_i$ in te vullen in (3.5). Omgekeerd zien we dat het er precies twee zijn, want als Q_i als eerste coördinaat x_i heeft, dan geldt dat ook voor $-Q_i$, en we hebben $Q_i \neq -Q_i$ aangezien $Q_i \in E[3]$. We concluderen dat

$$E[3] = \{Q_1, -Q_1, Q_2, -Q_2, Q_3, -Q_3, Q_4, -Q_4, O\}.$$

In het bijzonder is $\#E[3] = 9$, want het is duidelijk dat het om negen verschillende punten gaat.

Hoofdstuk 4

Het Frobenius-morfisme

We fixeren in dit hoofdstuk deze notatie:
p is een priemgetal,
K is een perfect lichaam met karakteristiek p,
L is een algebraïsche afsluiting van K.

De Frobenius-isogenie $\pi : E \to E^{(q)}$ van Voorbeeld 3.3.6, speelt een belangrijke rol in de bewijzen van de komende hoofdstukken. Een deel van de theorie gaat al op in de algemenere context van het Frobenius-morfisme $\pi : C \to C^{(q)}$ op een willekeurige projectieve kromme zonder dat de bewijzen anders zijn, daarom schrijven we dit hoofdstuk in deze algemenere context. De belangrijkste eigenschappen die we hier bewijzen, zijn dat $\deg \pi = \deg_i \pi = q$, en dat elk morfisme φ factoriseert via het Frobenius-morfisme van de grootst mogelijke graad (namelijk de inseparabiliteitsgraad van φ), gevolgd door een separabel morfisme.

4.1 De graad van het Frobenius-morfisme

Ter voorbereiding van het hoofdresultaat van deze paragraaf, bewijzen we

Propositie 4.1.1. *Als C/K een projectieve kromme is, $P \in C(K)$ een niet-singulier punt op C, en $t \in K(C)$ een lokale parameter bij P, dan is de uitbreiding $K(C) \supset K(t)$ eindig en separabel.*

Bewijs. Het element t is transcendent over K, want anders zou het maximaal ideaal (t) van $\mathcal{O}_{P,C}$ een element van K^* bevatten. Volgens [Har77, I.6.11] heeft $K(C)$ transcendentiegraad 1 over K. Er volgt dat de verzameling $\{t\}$ reeds een transcendentiebasis is voor $K(C)$ over K, dus $K(C)$ is algebraïsch over $K(t)$. Bovendien is $K(C)$ volgens [Sil09, I.2.9] eindig voortgebracht over K, en daarom ook over $K(t)$. Er volgt dat de uitbreiding $K(C) \supset K(t)$ eindig is. Ons rest te bewijzen dat hij bovendien separabel is.

Stel dat een element $x \in K(C)$ inseparabel is over $K(t)$, en zij $h_x \in K(t)[X]$ een minimumpolynoom van x over $K(t)$. Door de coëfficiënten te herschalen, kunnen we bereiken dat $h_x \in K[t][X]$. Bovendien, omdat x inseparabel is over $K(t)$, hebben we $h_x \in K[t][X^p]$, zeg

$$h_x(X) = \sum_{n \geq 0} \sum_{m \geq 0} a_{mn} t^m X^{pn}$$

waarbij slechts eindig veel van de $a_{mn} \in K$ ongelijk aan nul zijn. Omdat K perfect is, bestaat

er voor elk paar $m, n \geq 0$ een element $b_{mn} \in K$ zo dat $a_{mn} = b_{mn}^p$, dus

$$h_x(X) = \sum_{m\geq 0} \sum_{n\geq 0} b_{mn}^p X^{pn} t^m.$$

We 'splitsen h_x uit' naar de rest van de exponent van t bij deling door p, opdat we veelvouden van p in de exponenten krijgen en we kunnen gebruiken dat $K[t, X] \to K[t, X] : \alpha \mapsto \alpha^p$ een homomorfisme is:

$$\begin{aligned} h_x(X) &= \sum_{k=0}^{p-1} \sum_{l\geq 0} \sum_{n\geq 0} (b_{k+lp,n}^p X^{np} t^{lp}) t^k \\ &=: \sum_{k=0}^{p-1} \varphi_k(t, X)^p t^k, \end{aligned}$$

waarbij we

$$\varphi_k(t, X) = \sum_{n\geq 0} \sum_{l\geq 0} b_{k+lp,n} t^l X^n$$

hebben geschreven. Er volgt dat

$$0 = h_x(x) = \sum_{k=0}^{p-1} \varphi_k(t, x)^p t^k. \tag{4.1}$$

Als de k-de term van deze som niet nul is, dan is daar de orde bij P gelijk aan

$$\begin{aligned} \operatorname{ord}_P(\varphi_k(t,x)^p t^k) &= p \operatorname{ord}_P(\varphi_k(t,x)) + k \operatorname{ord}_P(t) && \text{want } \operatorname{ord}_P \text{ is een valuatie} \\ &= p \operatorname{ord}_P(\varphi_k(t,x)) + k && \text{want } t \text{ is een lokale parameter bij } P \\ &\equiv k \pmod p. \end{aligned}$$

Dit betekent dat de termen van de som in (4.1) die niet nul zijn, onderling verschillende ordes bij P hebben, want zelfs de restklassen modulo p daarvan zijn onderling verschillend. Volgens het onderstaande lemma (4.1.2) kan dit alleen als alle termen nul zijn, want ze sommeren tot nul. Kortom, $\varphi_k(t, x)^p t^k = 0$ en dus

$$\varphi_k(t, x) = 0, \qquad \text{voor } k = 0, \ldots, p-1.$$

Als we echter een k nemen zo dat $\varphi_k(t, X) \neq 0$, en zo'n k bestaat want $h_x \neq 0$, dan is de graad in X van $\varphi_k(t, X)$ strikt kleiner dan die van h_x, want als h_x graad pn heeft, dan is $a_{mt} = 0$ en daarmee $b_{mt} = 0$ voor alle $t > n$, dus $\varphi_k(t, X)$ heeft hooguit graad n. Maar x is een nulpunt van $\varphi_k(t, X) \in K(t)[X]$, in tegenspraak met de minimaliteit van h_x. □

In het bewijs gebruikten we

Lemma 4.1.2. *Zij C/K een projectieve kromme, en zij P een niet-singulier punt op C. Veronderstel dat er onder de functies $f_1, \ldots, f_n \in L(C)^*$ een unieke functie is met minimale orde bij P, zeg f_1; kortom,*

$$\operatorname{ord}_P(f_1) < \operatorname{ord}_P(f_i)$$

voor alle $1 < i$. Dan is $f_1 + \ldots + f_n \neq 0$.

Bewijs. Stel dat $f_1 + \ldots + f_n = 0$. Omdat ord_P een valuatie is, is

$$\begin{aligned}\mathrm{ord}_P(f_1) &= \mathrm{ord}_P(-f_1)\\ &= \mathrm{ord}_P(f_2 + \ldots + f_{n+1})\\ &\geq \min\{\mathrm{ord}_P(f_2), \ldots, \mathrm{ord}_P(f_n)\},\end{aligned}$$

in tegenspraak met de minimaliteit van $\mathrm{ord}_P(f_1)$. □

We zijn nu klaar voor het hoofdresultaat,

Stelling 4.1.3. *Zij C/K een projectieve kromme, zij q een macht van p, en zij $\pi : C \to C^{(q)}$ het q-de machts Frobenius-morfisme op C. Stel dat C een niet-singulier punt $P \in C(K)$ heeft. Dan geldt:*

(a) $\pi^* K(C^{(q)}) = K(C)^q$. In het bijzonder is π puur inseparabel.

(b) $\deg \pi = q$.

Bewijs. (a) Neem een element van $K(C^{(q)})$, zeg $\langle U, f\rangle$ waarbij U een open deelverzameling van $C^{(q)}$ is, en f een reguliere functie op U gedefinieerd over K. Dan is

$$\pi^*\langle U, f\rangle = \langle \pi^{-1}(U), f \circ \pi\rangle.$$

Voor elke $P \in \pi^{-1}(U)$ zijn er, per definitie van f, een omgeving $U_{\pi(P)} \subset U$ van $\pi(P)$, en homogene polynomen $g, h \in K[X_0, \ldots, X_n]$ van dezelfde graad zo dat

$$f = \frac{g}{h} \qquad \text{op } U_{\pi(P)}.$$

Omdat K perfect is, bestaan er polynomen $G, H \in K[X_0, \ldots, X_n]$ met $g = G^{(q)}$ en $h = H^{(q)}$. Daardoor is $f \circ \pi$ lokaal een q-de macht: voor $[x_0, \ldots, x_n] \in \pi^{-1}(U_{\pi(P)})$ hebben we

$$\begin{aligned}(f \circ \pi)[x_0, \ldots, x_n] &= \frac{g(x_0^q, \ldots, x_n^q)}{h(x_0^q, \ldots, x_n^q)}\\ &= \Big(\frac{G(x_0, \ldots, x_n)}{H(x_0, \ldots, x_n)}\Big)^q\\ &=: F^q[x_0, \ldots, x_n], \qquad (4.2)\end{aligned}$$

waarbij F per definitie de reguliere functie op $\pi^{-1}(U)$ is die lokaal bij $P \in \pi^{-1}(U)$, namelijk op diens omgeving $\pi^{-1}(U_{\pi(P)})$, gegeven wordt door G/H. Omdat dit voor alle P geldt, volgt dat $f \circ \pi = F^q$. Dus

$$\begin{aligned}\pi^*\langle U, f\rangle &= \langle \pi^{-1}(U), f \circ \pi\rangle\\ &= \langle \pi^{-1}(U), F\rangle^q \in K(C)^q.\end{aligned}$$

Conclusie: $\pi^* K(C^{(q)}) \subset K(C)^q$.

Omgekeerd, neem een element van $K(C)^q$, zeg $\langle V, F^q\rangle$, met V open in C, en F een over K gedefinieerde reguliere functie op V. Voor elk punt $P \in V$ zijn er een omgeving $V_P \subset V$, en polynomen $G, H \in K[X_0, \ldots, X_n]$, zo dat $F = G/H$ op V_P. Door (4.2) omgekeerd te lezen, nu met $[x_0, \ldots, x_n] \in V_P$ en met $g := G^{(q)}$ en $h := H^{(q)}$, en met $f := g/h$ op de open verzameling waar $h \neq 0$, en door op te merken dat het voor alle $P \in V$ geldt, zien we dat

$$F^q = f \circ \pi \qquad \text{op } V.$$

Omdat V als niet-lege open deelverzameling van C een eindig complement heeft, is het duidelijk dat er niet-lege open $U \subset C^{(q)}$ zijn met $\pi^{-1}(U) \subset V$, bijvoorbeeld $U = C^{(q)} - \pi(C - U)$ voldoet. Er volgt dat

$$\begin{aligned}\langle V, F^q\rangle &= \langle V, f \circ \pi\rangle \\ &= \langle \pi^{-1}(U), f \circ \pi\rangle \\ &= \pi^* \langle U, f\rangle \in \pi^* K(C^{(q)}).\end{aligned}$$

We concluderen dat ook de omgekeerde inclusie waar is, kortom, $\pi^* K(C^{(q)}) = K(C)^q$.

De uitbreiding $K(C) \supset K(C)^q$ is duidelijk puur inseparabel, dus π is puur inseparabel.

(b) Neem een lokale parameter $t \in K(C)$ bij het niet-singuliere punt $P \in C(K)$; het bestaan van zo'n t wordt gegarandeerd door (2.2.1a). Beschouw de torens van uitbreidingen

$$\begin{aligned} K(t) \subset K(C)^q(t) \subset K(C) \qquad &\text{en} \\ K(C)^q \subset K(C)^q(t) \subset K(C).&\end{aligned}$$

Volgens (4.1.1) is de uitbreiding $K(t) \subset K(C)$ separabel, dus $K(C)^q(t) \subset K(C)$ is separabel. Anderzijds is $K(C)^q \subset K(C)$ puur inseparabel, dus $K(C)^q(t) \subset K(C)$ is puur inseparabel. Er moet dan wel gelden dat

$$K(C)^q(t) = K(C),$$

zie (1.0.6d). Samen met de formule van (a), levert dit dat

$$\deg \pi = [K(C) : \pi^* K(C^{(q)})] = [K(C)^q(t) : K(C)^q] = \deg t,$$

waarbij we met $\deg t$ de graad van t over $K(C)^q$ bedoelen. Volgens (1.0.4b) is $\deg t$ gelijk aan de kleinste macht q' van p met de eigenschap dat $t^{q'} \in K(C)^q$. We hebben uiteraard $t^q \in K(C)^q$. Anderzijds, als a een natuurlijk getal is zo dat $t^a \in K(C)^q$, zeg $t^a = f^q$ met $f \in K(C)$, dan is

$$a = \operatorname{ord}_P(t^a) = \operatorname{ord}_P(f^q) = q \operatorname{ord}_P(f),$$

dus a is een veelvoud van q. We concluderen dat $q' = q$, zodat $\deg \pi = q$. □

4.2 Factorisatie via het Frobenius-morfisme

Het tweede hoofdresultaat van dit hoofdstuk is in essentie een gevolg van het eerste, en van (2.2.5).

Stelling 4.2.1. *Zij $\varphi : C_1 \to C_2$ een morfisme van niet-singuliere projectieve krommen over K. Er is een uniek morfisme ψ zo dat het diagram*

$$\begin{array}{ccc} C_1 & & \\ \downarrow{\scriptstyle \pi} & \searrow^{\varphi} & \\ C_1^{(q)} & \overset{\psi}{\dashrightarrow} & C_2 \end{array} \tag{4.3}$$

commuteert, waarbij $q = \deg_i \varphi$, en waarbij π het q-de machts Frobenius-morfisme $C_1 \to C_1^{(q)}$ is. Bovendien is ψ separabel.

Bewijs. Voor het gemak schrijven we $k := \varphi^* K(C_2)$, en k_s is de separabele afsluiting van k in $K(C_1)$, dus we hebben een toren

$$K(C_1) \supset k_s \supset k. \tag{4.4}$$

Omdat $q = \deg_i \varphi = [K(C_1) : k_s]$, vertelt (1.0.6e) dat $k_s \supset K(C_1)^q$. In de toren

$$K(C_1) \supset k_s \supset K(C_1)^q$$

hebben we $[K(C_1) : k_s] = q$, maar volgens (4.1.3ab) is reeds $[K(C_1) : K(C_1)^q] = q$. Kortom,

$$k_s = K(C_1)^q = \pi^* K(C_1^{(q)}),$$

dit laatste vanwege (4.1.3a). Dit resultaat substitueren in (4.4) levert de toren

$$K(C_1) \supset \pi^* K(C_1^{(q)}) \supset \varphi^* K(C_2). \tag{4.5}$$

Dit betekent volgens (2.2.5) dat er een een uniek morfisme ψ bestaat dat het diagram (4.3) commutatief maakt. Bovendien vertellen (2.2.6d) en (4.1.3ab) dat

$$q = \deg_i \varphi = \deg_i(\psi \circ \pi) = \deg_i(\psi) \deg_i(\pi) = \deg_i(\psi) q,$$

dus $\deg_i \psi = 1$, kortom, ψ is separabel. □

Hoofdstuk 5

Isogeniën van elliptische krommen

We fixeren in dit hoofdstuk deze notatie:
K is een perfect lichaam,
L is een algebraïsche afsluiting van K.

Hoewel het respecteren van de basispunten de enige aan een morfisme opgelegde eis is om een isogenie te zijn, vormen de isogeniën een bijzondere klasse van afbeeldingen. Zoals we al zagen is een isogenie een groepshomomorfisme, en dit stelt ons in staat om eigenschappen van de bij de isogenie horende lichaamsuitbreiding te bewijzen, zoals in de tweede paragraaf. Daarna richten we ons op *duale isogeniën*, zij spelen in dit werkstuk een hoofdrol.

5.1 De groep van isogeniën

De verzameling groepshomomorfismen tussen twee elliptische krommen (E_1, O_1) en (E_2, O_2) duiden we aan met $\mathrm{Hom}_{\mathrm{ab}}(E_1, E_2)$, en we schrijven $\mathrm{End}_{\mathrm{ab}}(E) := \mathrm{Hom}_{\mathrm{ab}}(E, E)$. (Deze notatie zullen we hierna niet mer gebruiken.) Het is een algemeen feit over abelse groepen dat we op $\mathrm{Hom}_{\mathrm{ab}}(E_1, E_2)$ de structuur van een abelse groep hebben, en op $\mathrm{End}_{\mathrm{ab}}(E)$ bovendien de structuur van een ring, waarbij samenstelling van afbeeldingen de rol van vermenigvuldiging heeft.

Propositie 5.1.1. *Zij E_1, E_2, E elliptische krommen over K.*

(a) De verzamelingen

$$\mathrm{Ign}(E_1, E_2) \subset \mathrm{Hom}_{\mathrm{ab}}(E_1, E_2) \qquad \textit{en} \qquad \mathrm{End}(E) \subset \mathrm{End}_{\mathrm{ab}}(E)$$

zijn respectievelijk een ondergroep van $\mathrm{Hom}_{\mathrm{ab}}(E_1, E_2)$ en een deelring van $\mathrm{End}_{\mathrm{ab}}(E)$. Met andere woorden, als $\varphi, \psi : E_1 \to E_2$ twee isogenieën zijn, dan zijn $\varphi + \psi$ en $-\varphi$ isogenieën, en als $\tau, \sigma : E \to E$ isogeniën zijn, dan is $\tau \circ \sigma$ een isogenie.

In het bijzonder is voor elke $m \in \mathbb{Z}$ de afbeelding $[m] \in \mathrm{End}(E)$ een isogenie.

(b) De abelse groep $\mathrm{Ign}(E_1, E_2)$ is torsievrij.

Bewijs. We geven slechts schetsen van bewijzen.

(a) In het geval dat de krommen worden gegeven door Weierstrass-vergelijkingen, kan men bewijzen dat $\varphi + \psi$ en $-\psi$ morfismen van projectieve krommen zijn door expliciete formules te gebruiken voor $P+Q$ en $-P$ in termen van de coördinaten van $P, Q \in E_2$. Deze formules worden

gegeven door rationale functies met coëfficiënten in K, en het bewijs volgt dan in essentie doordat morfismen gedefiniëerd zijn aan de hand van rationale functies met coëfficiënten in K. Zie [Sil09, III.3.6] voor details. Als we eenmaal weten dat $\varphi+\psi$ en $-\psi$ morfismen zijn, volgt direct dat het isogeniën zijn, want $(\varphi+\psi)(O_1) = O_2+O_2 = O_2$ en $(-\psi)(O_1) = -O_2 = O_2$. De bewering dat $\tau\circ\sigma$ een isogenie is, wisten we al, want we hadden al een categorie. Voor willekeurige E, E_1, E_2 volgen de beweringen uit het voorgaande door samen te stellen met isomorfismen van/naar elliptische krommen gegeven door een Weierstrass-vergelijking.

(b) Met expliciete formules kan men laten zien dat voor gehele getallen $m \in \mathbb{Z} - \{0\}$, de isogenie $[m] : E_2 \to E_2$ niet-constant is, kortom $[m] \neq [0]$. Dat betekent dat $[m]$ surjectief is. Als $\varphi : E_1 \to E_2$ een isogenie is met $\varphi \neq [0]$, dan is ook φ surjectief, dus $[m] \circ \varphi$ is dat ook en is dus ongelijk aan $[0]$. □

5.2 Lichaamstheoretische eigenschappen van isogeniën

Conventie 5.2.1. Als $\varphi : E_1 \to E_2$ een isogenie van elliptische krommen is, dan bedoelen we met $\ker\varphi$ de kern van φ als groepshomomorfisme. (In de algebraïsche meetkunde zijn er andere betekenissen van het begrip 'kern', die gebruiken we hier niet.)

Stelling 5.2.2. *Zij $\varphi : E_1 \to E_2$ een niet-constante isogenie van elliptische krommen over K. Voor alle $P \in E_1$ en $Q \in E_2$ geldt*

$$\deg_s \varphi = \#\varphi^{-1}(Q) \qquad \textit{en} \qquad \deg_i \varphi = e_\varphi(P).$$

Bewijs. Zij $Q, Q' \in E_2$ en neem een punt $R \in \varphi^{-1}(Q' - Q)$, zo'n R bestaat omdat φ surjectief is. Het is duidelijk dat de functie

$$\varphi^{-1}(Q) \to \varphi^{-1}(Q') : \quad P \mapsto R + P$$

bijectief is. Conclusie: de verzamelingen $\varphi^{-1}(Q)$, met $Q \in E_2$, zijn allemaal even groot. Volgens (2.2.7c) zijn er slechts eindig veel uitzonderingen $Q \in E_2$ op de regel $\varphi^{-1}(Q) = \deg_s \varphi$. Omdat E_2 oneindig is, volgt dat er geen zulke uitzonderingen zijn.

Dan de tweede identiteit. Zij $P \in E_1$ en zij $Q := \varphi(P)$. Zij P' nog een punt in $\varphi^{-1}(Q)$, en beschouw het translatie-morfisme

$$\psi := \tau_{P'-P} : E_1 \to E_1.$$

Omdat $P' - P \in \ker\varphi$, is $\varphi = \varphi \circ \psi$, en omdat ψ een isomorfisme van projectieve krommen is, is ψ volgens (2.2.7d) overal onvertakt. Er volgt dat

$$\begin{aligned} e_\varphi(P) &= e_{\varphi\circ\psi}(P) \\ &= e_\varphi(\psi(P))e_\psi(P) && (2.2.7a) \\ &= e_\varphi(\psi(P)) && (\text{want } \psi \text{ onvertakt}) \\ &= e_\varphi(P'). \end{aligned}$$

Er geldt daarom dat

$$\sum_{P' \in \varphi^{-1}(Q)} e_\varphi(P') = \#\varphi^{-1}(Q) e_\varphi(P).$$

Het rechterlid is, volgens de eerste formule van deze Stelling, gelijk aan $\deg_s(\varphi)e_\varphi(P)$. Het linkerlid is, volgens (2.2.7b), gelijk aan $\deg\varphi = \deg_s(\varphi)\deg_i(\varphi)$. Delen door $\deg_s(\varphi)$ voltooit het bewijs. □

Opmerking 5.2.3. De zojuist bewezen formules geven 'meetkundige' interpretaties van $\deg_s \varphi$ en $\deg_i \varphi$, die in zekere zin alleen afhangen van L, niet van K. Preciezer, op dezelfde manier en met dezelfde notatie als in (2.2.8) zien we dat $\deg_s(\varphi_L) = \deg_s(\varphi)$ en dat $\deg_i(\varphi_L) = \deg_i(\varphi)$. (We vatten $E_i \otimes L$ op als elliptische kromme over L met hetzelfde basispunt als E_i. Uit Riemann–Roch is duidelijk dat dit inderdaad elliptische krommen zijn, en het is duidelijk dat φ_L een isogenie is.) Met andere woorden, we hebben

$$[L(E_1) : \varphi^* L(E_2)]_s = [K(E_1) : \varphi^* K(E_2)]_s, \qquad [L(E_1) : \varphi^* L(E_2)]_i = [K(E_1) : \varphi^* K(E_2)]_i.$$

Ter voorbereiding op de volgende stelling: Zij E_1/K een elliptische kromme. Voor punten $T \in E_1$ bekijken we het translatie-morfisme $\tau_T : E_1 \to E_1 : P \mapsto P + T$, en het geïnduceerde homomorfisme $\tau_T^* : L(E_1) \to L(E_1)$. Als $T' \in E_1$ nog een punt is, dan is

$$\tau_{T+T'}^* = (\tau_{T'} \circ \tau_T)^* = \tau_T^* \circ \tau_{T'}^*.$$

Dus $\tau_T^* \in \mathrm{Aut}(L(E_1))$, want hij heeft een inverse τ_{-T}^*, en we hebben een groepshomomorfisme

$$F : \quad E_1 \to \mathrm{Aut}(L(E_1)) : \quad T \mapsto \tau_T^*.$$

Zij E_2/K nog een elliptische kromme en zij $[0] \neq \varphi : E_1 \to E_2$ een isogenie. Als $T \in \ker \varphi$ en $f \in L(E_2)$, dan is

$$F(T)(\varphi^* f) = \tau_T^* \varphi^* f = (\varphi \circ \tau_T)^* f = \varphi^* f,$$

dus $F(T)$ is de identiteit op $\varphi^* L(E_2) \subset L(E_1)$. We krijgen daarom door restrictie van domein en codomein van F, een homomorfisme

$$F_\varphi : \quad \ker \varphi \to \mathrm{Aut}_{\varphi^* L(E_2)}(L(E_1)) : \quad T \mapsto \tau_T^*.$$

We laten zien dat F_φ een isomorfisme is.

Stelling 5.2.4. *Zij $\varphi : E_1 \to E_2$ een niet-constant isogenie van elliptische krommen over K. We hebben een isomorfisme van groepen*

$$F_\varphi : \quad \ker \varphi \xrightarrow{\sim} \mathrm{Aut}_{\varphi^* L(E_2)}(L(E_1)) : \quad T \mapsto \tau_T^*.$$

Bewijs. We zagen al F_φ een homomorfisme is. We hebben

$$\begin{aligned} \#\mathrm{Aut}_{\varphi^* L(E_2)}(L(E_1)) &\leq [L(E_1) : \varphi^* L(E_2)]_s && \text{(basis Galoistheorie)} \\ &= \deg_s \varphi && (5.2.3) \\ &= \#\ker \varphi, && (5.2.2) \end{aligned}$$

dus als F_φ injectief is, dan moet hij wel surjectief zijn en dan zijn we klaar. Zij $T \in \ker F_\varphi$. Dan is $\tau_T^* = [1]^*$ op $L(E_1)$, waarbij we $[1] \in \mathrm{End}(E_1)$ bedoelen, en (2.2.4b) zegt dat dan $\tau_T = [1]$. Het is duidelijk dat dan $T = O$. Kortom, $\ker F_\varphi = \{O\}$, en dit voltooit het bewijs. □

Gevolg 5.2.5. *Zij $\varphi : E_1 \to E_2$ een separabele, niet-constante isogenie van elliptische krommen over K. Dan is φ onvertakt, en*

$$\#\ker \varphi = \deg \varphi,$$

en $L(E_1) \supset \varphi^* L(E_2)$ is een Galoisuitbreiding.

Bewijs. Als φ is separabel is, dan zegt (a) dat

$$e_\varphi(P) = \deg_i \varphi = 1$$

voor alle $P \in E_1$, kortom φ is onvertakt, en dat

$$\#\ker\varphi = \#\varphi^{-1}(O) = \deg_s \varphi = \deg\varphi.$$

Vervolgens gebruiken we (b) om te berekenen dat

$$\begin{aligned}[L(E_1) : \varphi^* L(E_2)] &= [K(E_1) : \varphi^* K(E_2)] \\ &= \deg\varphi \\ &= \#\ker\varphi \\ &= \#\mathrm{Aut}_{\varphi^* L(E_2)}(L(E_1)).\end{aligned} \tag{5.2.3}$$

De identiteit $[L(E_1) : \varphi^* L(E_2)] = \#\mathrm{Aut}_{\varphi^* L(E_2)}(L(E_1))$ betekent dat uitbreiding $L(E_1) \supset \varphi^* L(E_2)$ Galois is. □

5.3 Factorisatie via een isogenie met kleinere kern

Als toepassing van de stellingen in de vorige paragraaf, bewijzen we

Propositie 5.3.1. *Zij $\varphi : E_1 \to E_2$ en $\psi : E_1 \to E_3$ isogeniën van elliptische krommen over K. Als φ separabel is en*

$$\ker\varphi \subset \ker\psi,$$

dan is er een unieke isogenie $\chi : E_2 \to E_3$ zo dat dit diagram commuteert:

$$\begin{array}{ccc} E_1 & & \\ \downarrow{\scriptstyle\varphi} & \searrow^{\psi} & \\ E_2 & \overset{\chi}{\dashrightarrow} & E_3 \end{array} \tag{5.1}$$

Bewijs. We beschouwen de uitbreidingen

$$L(E_1) \supset \varphi^* L(E_2) \qquad \text{en} \qquad L(E_1) \supset \psi^* L(E_3).$$

De eerste is volgens (5.2.5) een Galoisuitbreiding, want φ is separabel. Neem willekeurige elementen van $\psi^* L(E_3)$ en van

$$G := \mathrm{Gal}(L(E_1)/\varphi^* L(E_2)),$$

laten we zeggen $\psi^* x \in \psi^* L(E_3)$ met $x \in L(E_3)$, en $g := \tau_T^* \in G$ met $T \in \ker\varphi$ – zo'n T bestaat volgens (5.2.4). Omdat $T \in \ker\varphi \subset \ker\psi$, is $\psi \circ \tau_T = \psi$. Er volgt dat

$$\begin{aligned} g(\psi^* x) &= \tau_T^* \psi^* x \\ &= (\psi \circ \tau_T)^* x \\ &= \psi^* x. \end{aligned}$$

Omdat g en $\psi^* x$ willekeurig zijn gekozen, wil dit zeggen dat $\psi^* L(E_3)$ bevat is in het invariantenlichaam $L(E_1)^G = \varphi^* L(E_2)$. Kortom,

$$L(E_1) \supset \varphi^* L(E_2) \supset \psi^* L(E_3).$$

Dit betekent volgens (2.2.5) dat er een uniek morfisme χ bestaat zo dat het diagram (5.1) commuteert. Omdat $\varphi(O) = O$ en $\psi(O) = O$, is ook $\chi(O) = O$, dus χ is een isogenie. □

We zullen dit resultaat onder meer gebruiken bij de constructie van de duale isogenie.

5.4 Lineaire combinaties van het Frobenius-endomorfisme

Als $E/\mathbb{F}_q$ een elliptische kromme is over een eindig lichaam, dan hebben we het q-de machts Frobenius-endomorfisme $\pi \in \mathrm{End}(E)$ en de vermenigvuldigingsafbeeldingen $[m] \in \mathrm{End}(E)$ bestudeerd, maar nog geen algemene lineaire combinaties $[m] + [n]\pi \in \mathrm{End}(E)$. In deze paragraaf laten we zien wanneer zo'n combinatie separabel is. We gebruiken eigenschappen van de ruimte van differentialen Ω_E, waarvoor we naar de literatuur verwijzen.

Propositie 5.4.1. *Zij E/K een elliptische kromme.*

(a) Er bestaat een differentiaal $\omega \in \Omega_E$ met $\omega \neq 0$, zo dat als E'/K een andere elliptische kromme is, de afbeelding

$$\mathrm{Ign}(E', E) \to \Omega_{E'} : \quad \varphi \mapsto \varphi^{\Omega}\omega$$

een homomorfisme van abelse groepen is. (Hier is $\varphi^{\Omega} : \Omega_E \to \Omega_{E'}$ zoals gedefinieerd bovens (2.4.2) indien φ niet-constant is, en als conventie is φ^{Ω} de nulafbeelding als φ de nulafbeelding is.)

(b) Zij $\omega \in \Omega_E$ een differentiaal zoals in (a), zij m een geheel getal, en beschouw de isogenie $[m] \in \mathrm{End}(E)$. Dan is

$$[m]^{\Omega}\omega = m\omega.$$

Bewijs. (a) [Sil09, III.5.2]. (b) Voor $m = 0$ is het duidelijk. Stel m is positief. Dan is

$$\begin{aligned} [m]^{\Omega}\omega &= ([1] + \ldots + [1])^{\Omega}\omega \\ &= [1]^{\Omega}\omega + \ldots + [1]^{\Omega}\omega && \text{volgens (a)} \\ &= m\omega && \text{want } [1]^{\Omega} \text{ is de identiteit op } \Omega_E, \end{aligned}$$

dus het is waar voor m. Bovendien, vanwege (a) is

$$[-m]^{\Omega}\omega = -[m]^{\Omega}\omega = -m\omega,$$

dus het is ook waar voor $-m$. □

Gevolg 5.4.2. *Als m een geheel getal is zo dat m niet nul is in K, dan is de isogenie $[m] \in \mathrm{End}(E)$ separabel.*

Bewijs. Neem een differentiaal $0 \neq \omega \in \Omega_E$ zoals in (5.4.1). Dan zegt (5.4.1b) dat

$$[m]^{\Omega}\omega = m\omega \neq 0,$$

dit laatste omdat $\omega \neq 0$ en omdat m niet nul is in K. In het bijzonder is $[m]^{\Omega} : \Omega_E \to \Omega_E$ niet de nulafbeelding, en daarom is $[m]$ volgens (2.4.2b) separabel. □

Stelling 5.4.3. *Zij p een priemgetal, q een macht van p, en $E/\mathbb{F}_q$ een elliptische kromme. Zij $\pi \in \mathrm{End}(E)$ het q-de machts Frobenius-endomorfisme, en zij $m, n \in \mathbb{Z}$. Het isogenie*

$$[m] + [n]\pi \in \mathrm{End}(E)$$

is separabel precies dan als $m \not\equiv 0 \pmod{p}$.

Bewijs. Zij $0 \neq \omega \in \Omega_E$ een differentiaal met de eigenschap van (5.4.1). Het morfisme $\pi : E \to E$ is inseparabel (4.1.3ab), zodat $\pi^\Omega : \Omega_E \to \Omega_E$ de nulafbeelding is (2.4.2). Dit gebruiken we om te berekenen dat

$$\begin{aligned}
([m] + [n]\pi)^\Omega\omega &= ([m] + \pi + \ldots + \pi)^\Omega\omega && (n \text{ termen } \pi)\\
&= [m]^\Omega\omega + \pi^\Omega\omega + \ldots + \pi^\Omega\omega && (5.4.1a)\\
&= m\omega + n\pi^\Omega\omega && (5.4.1b)\\
&= m\omega && \text{want } \pi^\Omega = 0.
\end{aligned}$$

We laten zien dat de volgende beweringen equivalent zijn:

1. $[m] + [n]\pi$ is separabel
2. $([m] + [n]\pi)^\Omega$ is de nulafbeelding
3. $([m] + [n]\pi)^\Omega\omega = 0$
4. $m\omega = 0$
5. $m \equiv 0 \pmod{p}$.

'1 $\iff$ 2' is een toepassing van (2.4.2b), en '2 $\iff$ 3' is waar omdat $\omega \neq 0$ reeds de 1-dimensionale $L(E)$-vectorruimte Ω_E opspant (2.4.2b). '3 $\iff$ 4' volgt uit bovenstaande berekening, en '4 $\iff$ 5' volgt omdat $m\omega = 0$ precies dan als m nul is in $\mathbb{F}_q$. □

5.5 De duale isogenie

Centraal in de leer van elliptische krommen, en in ons bewijs van de pERH, is het feit dat elke isogenie φ een zogenaamde 'duale' isogenie heeft die in de andere richting gaat, en die samengesteld met φ, 'vermenigvuldiging met $\deg\varphi$' oplevert. De definitie is in principe eenvoudig, maar bewijzen dat het een isogenie is, kost wat werk.

Definitie 5.5.1. Zij $\varphi : E_1 \to E_2$ een isogenie van elliptisch krommen (E_1, O_1) en (E_2, O_2) over K, en zij $\kappa_i : E_i \to \mathrm{Pic}^0(E_i) : P \mapsto \lceil (P) - (O_i) \rceil$ het isomorfisme zoals in (3.2.1), voor $i = 1, 2$. We definiëren de functie $\varphi^t : E_2 \to E_1$ door te eisen dat het diagram

$$\begin{array}{ccc}
E_1 & \xleftarrow{\varphi^t} & E_2\\
\downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_2}\\
\mathrm{Pic}^0(E_1) & \xleftarrow{\varphi^{\mathrm{Pic}}} & \mathrm{Pic}^0(E_2)
\end{array}$$

commuteert. Met andere woorden, $\varphi^t = \kappa_1^{-1} \circ \varphi^{\mathrm{Pic}} \circ \kappa_2$.

Merk op dat φ^t een groepshomomorfisme is, want $\kappa_1, \varphi^{\mathrm{Pic}}, \kappa_2$ zijn groepshomomorfismen. Expliciet wordt φ^t gegeven door het voorschrift

$$\varphi^t : E_2 \to E_1 : \quad P \mapsto \mathrm{som}\,\varphi^{\mathrm{Div}}((P) - (O_2)), \tag{5.2}$$

want wegens de definities en (3.2.5) hebben we

$$P \quad \overset{\kappa_2}{\longmapsto} \quad \lceil (P) - (O_2) \rceil \quad \overset{\varphi^{\mathrm{Pic}}}{\longmapsto} \quad \lceil \varphi^{\mathrm{Div}}((P) - (O_2)) \rceil \quad \overset{\kappa_1^{-1}}{\longmapsto} \quad \mathrm{som}\,\varphi^{\mathrm{Div}}((P) - (O_2)).$$

De functie φ^t is de bedoelde duale van φ, maar we moeten nog bewijzen dat φ^t een isogenie is. Het is fascinerend hoeveel van de voorgaande resultaten gebruikt worden in het bewijs.

Stelling 5.5.2. *Zij $\varphi : E_1 \to E_2$ een isogenie van elliptische krommen over K. Dan geldt:*

(a) $\varphi^t \circ \varphi = [\deg \varphi] \in \mathrm{End}(E_1)$.

(b) φ^t *is een isogenie, en het is de unieke isogenie met de eigenschap zoals in (a).*

Bewijs. (a) Zij $P \in E_1$. Per definitie van φ^{Div} hebben we

$$\begin{aligned}\varphi^{\mathrm{Div}}((\varphi(P)) - (O)) &= \sum_{P' \in \varphi^{-1}(\varphi(P))} e_\varphi(P')(P') - \sum_{R \in \ker \varphi} e_\varphi(R)(R) \\ &= \sum_{R \in \ker \varphi} e_\varphi(R+P)(R+P) - e_\varphi(R)(R),\end{aligned}$$

dit laatste omdat de functie $\ker \varphi \to \varphi^{-1}(\varphi(P)) : R \mapsto R + P$ een bijectie is. Omdat φ een isogenie is, zegt (5.2.2) dat $e_\varphi(Q) = \deg_i \varphi$ voor alle $Q \in E_1$, dus

$$\varphi^{\mathrm{Div}}((\varphi(P)) - (O)) = \deg_i \varphi \sum_{R \in \ker \varphi} (R+P) - (R). \tag{5.3}$$

Om $\varphi^t(\varphi(P))$ te berekenen, moeten we volgens (5.2) de 'som' van deze divisor nemen:

$$\begin{aligned}\varphi^t(\varphi(P)) &= \mathrm{som}\, \varphi^{\mathrm{Div}}((\varphi(P)) - (O)) \\ &= [\deg_i \varphi] \sum_{R \in \ker \varphi} P && \text{volgens (5.3)} \\ &= [\deg_i \varphi][\deg_s \varphi]P && \text{volgens (5.2.2)} \\ &= [\deg \varphi]P.\end{aligned}$$

Kortom, $\varphi^t \circ \varphi = [\deg \varphi]$.

(b) We gaan bewijzen:

$$\text{Er bestaat een isogenie } \varphi' : E_2 \to E_1 \text{ met de eigenschap dat } \varphi' \circ \varphi = [\deg \varphi]. \tag{5.4}$$

Dit is voldoende, want uit de identiteit $\varphi^t \circ \varphi = \varphi' \circ \varphi$ volgt dan, wegens surjectiviteit van φ, dat $\varphi^t = \varphi'$. We bewijzen (5.4) in stappen.

Geval 1: φ *is separabel.*
Volgens (5.2.5) is dan

$$\#\ker \varphi = \deg \varphi.$$

In het bijzonder wordt de abelse groep $\ker \varphi$ geannihileerd door vermenigvuldiging met het getal $\deg \varphi$. Dus

$$\ker \varphi \subset \ker[\deg \varphi],$$

waarbij we $[\deg \varphi] \in \mathrm{End}(E_1)$ bedoelen. Dit betekent volgens (5.3.1), omdat φ separabel is, dat er een uniek isogenie $\varphi' : E_2 \to E_1$ bestaat zo dat het diagram

$$\begin{array}{ccc} E_1 & & \\ \downarrow{\scriptstyle \varphi} & \searrow^{[\deg \varphi]} & \\ E_2 & \overset{\varphi'}{\dashrightarrow} & E_1 \end{array}$$

commuteert. Kortom, (5.4) is in dit geval waar.

Geval 2: *K heeft karakteristiek $p > 0$, en φ is het p-de machts Frobenius-morfisme:*

$$\varphi = \pi_p : E \to E^{(p)}.$$

We beschouwen de isogenie $[p] \in \mathrm{End}(E)$, en de bijbehorende functie $[p]^\Omega : \Omega_E \to \Omega_E$. Vanwege (5.4.1b) is er een differentiaal $0 \neq \omega \in \Omega_E$ zo dat

$$[p]^\Omega \omega = p\omega = 0,$$

dit tweede vanwege de karakteristiek p. Dus $[p]^\Omega$ is niet injectief, en daarom is $[p]$ volgens (2.4.2b) niet separabel. Zij $q = \deg_i[p]$. Volgens (4.2.1) is er een uniek morfisme $\psi : E^{(q)} \to E$ zo dat het diagram

$$\begin{array}{ccc} E & & \\ \downarrow{\scriptstyle \pi_q} & \searrow^{[p]} & \\ E^{(q)} & \xrightarrow{\psi} & E \end{array}$$

commuteert, met π_q het q-de machts Frobenius-morfisme $E \to E^{(q)}$. Bovendien is ψ een isogenie, want $[p]$ en π_q zijn dat, en $q > 1$, want $[p]$ is niet separabel. Daarom kunnen we π_q ontbinden als $\pi_q = \pi_{q/p} \circ \pi_p$, met $\pi_{q/p}$ de q/p-de machts Frobenius $E^{(p)} \to E^{(q)}$. We concluderen dat

$$\begin{aligned} (\psi \circ \pi_{q/p}) \circ \pi_p &= \psi \circ \pi_q \\ &= [p] \\ &= [\deg \pi_p] \qquad (4.1.3b). \end{aligned}$$

Kortom, (5.4) is ook in dit geval waar, want we kunnen $\pi'_p = \psi \circ \pi_{q/p} : E^{(p)} \to E$ nemen.

Geval 3: *Er geldt $\varphi = \lambda \circ \psi$ waarbij $\psi : E_1 \to E$ en $\lambda : E \to E_2$ isogenieën zijn van elliptische krommen over K waarvan we al weten dat* (5.4) *waar is, met andere woorden, er zijn isogeniën $\psi' : E \to E_1$ en $\lambda' : E_2 \to E$ zo dat $\psi' \circ \psi = [\deg \psi]$ en $\lambda' \circ \lambda = [\deg \lambda]$.*
We berekenen dat

$$\begin{aligned} (\psi' \circ \lambda') \circ (\lambda \circ \psi) &= \psi' \circ [\deg \lambda] \circ \psi \\ &= \psi' \circ \psi \circ [\deg \lambda] \\ &= [\deg \psi] \circ [\deg \lambda] \\ &= [\deg \lambda \deg \psi)] = [\deg(\lambda \circ \psi)]. \end{aligned} \tag{5.5}$$

Dit betekent dat (5.4) ook in dit geval waar is, want we kunnen $\varphi' = \psi' \circ \lambda'$ nemen.

Geval 4: *het algemene geval. Met andere woorden, $\varphi : E_1 \to E_2$ is een willekeurig isogenie.*
Zij $p^n := q = \deg_i(\varphi)$, en $\pi : E_1 \to E_1^{(q)}$ het q-de machts Frobenius-morfisme. Als $\psi : E_1^{(q)} \to E_2$ het separabele isogenie is zo dat $\varphi = \psi \circ \pi$, waarvan het bestaan wordt gegarandeerd door (4.2.1), dan kunnen we φ verder factoriseren als

$$\varphi = \psi \circ \pi_{p,n} \circ \cdots \circ \pi_{p,1},$$

waarbij $\pi_{p,i} : E_1^{(p^{i-1})} \to E_1^{(p^i)}$ het p-de machts Frobenius-morfisme is. We hebben ψ en de $\pi_{p,i}$ behandeld in Geval 1 resp. Geval 2, en door Geval 3 herhaald toe te passen, volgt het bestaan van φ' als in (5.4). We concluderen dat (5.4) waar is. □

Definitie 5.5.3. Zij $\varphi : E_1 \to E_2$ een isogenie van elliptisch krommen. De isogenie $\varphi^t : E_2 \to E_1$, die we in (5.5.1) gedefiniëerd hebben en waarvan we in de vorige stelling zagen dat het een isogenie is, noemen we de *duale isogenie* van φ, of de isogenie duaal aan φ.

Omdat 'duaal zijn' in andere contexten een symmetrische relatie is, suggereert de terminologie dat φ op zijn beurt de duale is van φ^t, kortom dat $((\varphi)^t)^t = \varphi$. Dit is inderdaad waar, maar we zijn pas in staat het te bewijzen aan het eind van het volgende hoofdstuk. Een paar andere eigenschappen kunnen we wel direct afleiden, namelijk

Gevolg 5.5.4. *Zij $\varphi : E_1 \to E_2$ een niet-constant isogenie.*

(a) Naast $\varphi^t \circ \varphi = [\deg \varphi] \in \mathrm{End}(E_1)$, geldt ook $\varphi \circ \varphi^t = [\deg \varphi] \in \mathrm{End}(E_2)$.

(b) Als $\lambda : E_2 \to E_3$ nog een niet-constant isogenie is, dan is

$$(\lambda \circ \varphi)^t = \varphi^t \circ \lambda^t \in \mathrm{Ign}(E_3, E_1).$$

Met andere woorden, als $\mathcal{E}$ de categorie is van elliptische krommen met isogenieën, dan hebben we een contravariante functor $D : \mathcal{E} \to \mathcal{E}$, die op objecten de identiteit is, en die een isogenie $\varphi \in \mathrm{Ign}(E_1, E_2)$ naar zijn duale $\varphi^t \in \mathrm{Ign}(E_2, E_1)$ afbeeldt.

Bewijs. (a) We berekenen dat

$$\begin{aligned}(\varphi \circ \varphi^t) \circ \varphi &= \varphi \circ (\varphi^t \circ \varphi) \\ &= \varphi \circ [\deg \varphi] \\ &= [\deg \varphi] \circ \varphi.\end{aligned}$$

(Hier is de eerste '$[\deg \varphi]$' bevat in $\mathrm{End}(E_1)$, en de tweede in $\mathrm{End}(E_2)$.) Als niet-constant isogenie is φ surjectief, en er volgt $\varphi \circ \varphi^t = [\deg \varphi]$.

(b) Dit hebben we in essentie al gezien: de berekening (5.5), met accenten vervangen door 't', toont dat $(\varphi^t \circ \lambda^t) \circ (\lambda \circ \varphi) = [\deg(\lambda \circ \varphi)]$, zodat wegens uniciteit $\varphi^t \circ \lambda^t = (\lambda \circ \varphi)^t$. □

Voordat we meer eigenschappen van de duale isogenie bewijzen, hebben we meer theorie nodig, en die ontwikkelen we in het volgende hoofdstuk.

Hoofdstuk 6

De Weilparing op $E[m]$

We fixeren in dit hoofdstuk deze notatie:
K is een lichaam,
L is een algebraïsch afsluiting van K.
$\boldsymbol{\mu}_m$ is de ondergroep van m-de machts eenheidswortels van L^*, indien $m \in \mathbb{Z}_{\geq 1}$.

Het 'einddoel' van dit hoofdstuk is het bepalen van de structuur van de groep $E[m]$ voor gehele getallen m die niet nul zijn in K, en het bewijzen van de verwante stelling dat de isogenie $[m] \in \mathrm{End}(E)$ graad m^2 heeft indien $m \in \mathbb{Z}_{\neq 0}$. Deze stelling is een gevolg van het feit dat $[m]$ zelfduaal is, en dit is op zijn beurt een gevolg van de stelling dat 'de duale nemen' een groepshomomorfisme $\mathrm{Ign}(E_1, E_2) \to \mathrm{Ign}(E_2, E_1)$ is. Om dit laatste te bewijzen, introduceren we de Weilparing $e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m$. De definitie is vrij ingewikkeld, maar zeer bruikbaar, en de Weilparing respecteert in allerlei opzichten de structuur van E. In het bijzonder zullen we zien dat een isogenie en zijn duale geadjungeerd zijn met betrekking tot de Weilparing.

We zijn alleen in staat om de Weilparing e_m op E te definiëren in het geval dat $\#E[m] = m^2$. Als gevolg van het genoemde 'einddoel', zullen we aan het eind van het hoofdstuk zien dat dit waar is zodra m niet nul is in K. Dat resultaat hebben we echter nog niet, vandaar dat we de voorwaarde $\#E[m] = m^2$ steeds moeten vermelden. Dat we ondanks dit 'voorwaardelijke' toch wat kunnen bereiken, komt doordat we speciale gevallen al expliciet hebben doorgerekend.

6.1 Constructie van de Weilparing

Het kost aardig wat werk om de Weilparing goed te definiëren. Ter voorbereiding een paar lemma's, die bijna triviaal zijn maar toch handig om op te schrijven omdat we ze vaker gebruiken.

Lemma 6.1.1. *Zij m een geheel getal dat niet nul is in K. Als $Q \in E$, en als $Q' \in E$ een punt is met $[m]Q' = Q$, dan is*

$$[m]^{\mathrm{Div}}(Q) = \sum_{R \in E[m]} (Q' + R).$$

Bewijs. Per definitie hebben we

$$[m]^{\mathrm{Div}}(Q) = \sum_{P \in [m]^{-1}(Q)} e_{[m]}(P)(P). \tag{6.1}$$

Omdat m niet nul is in K, is $[m]$ separabel (5.4.2) en daarom onvertakt (5.2.5). Dus (6.1) leest

$$[m]^{\mathrm{Div}}(Q) = \sum_{P \in [m]^{-1}(Q)} (P).$$

De gewenst formule volgt door op te merken dat de functie $[m]^{-1}(O) \to [m]^{-1}(Q) : R \mapsto Q' + R$ een bijectie is. □

Lemma 6.1.2. *Als $f \in L(E)^*$ zo dat $f^m \in L^*$, dan is $f \in L^*$.*

Bewijs. Het polynoom $X^m - f^m \in L(E)[X]$ ligt al in $L[X]$, en ontbindt in $L[X]$ in lineaire factoren want L is algebraïsch afgesloten. Dus al zijn nulpunten, waaronder f, liggen reeds in L. Bovendien is $f \neq 0$, want $f^m \neq 0$. □

Het volgende propositie construeert eigenlijk de Weilparing op $E[m]$, zie de definitie daarna.

Propositie 6.1.3. *Zij E/K een elliptische kromme en zij $m \in \mathbb{Z}_{\geq 1}$ een getal met $\#E[m] = m^2$.*

(a) Zij $T \in E[m]$. Er bestaan $f, g \in L(E)^*$ met

$$\mathrm{div}(f) = m(T) - m(O) \qquad \text{en} \qquad g^m = [m]^* f. \tag{6.2}$$

Bovendien zijn f en g uniek modulo L^*, of met andere woorden, als ook $f', g' \in L(E)^*$ voldoen aan (6.2), dan geldt $f'/f \in L^*$ en $g'/g \in L^*$.

(b) Zij T, f, g zoals in (a), en zij $S \in E[m]$ nog een punt. Als $X \in E$ een punt is zo dat g regulier is in X en in $X + S$, en met $g(X) \neq 0$, dan geldt

$$\frac{g(X+S)}{g(X)} \in \boldsymbol{\mu}_m,$$

en de waarde van $g(X+S)/g(X)$ hangt alleen af van S en T, niet van de keuze van f, g of X.

Bewijs. (a) Omdat de divisor $D := m(T) - m(O) \in \mathrm{Div}(E)$ graad 0 heeft, en omdat $\mathrm{som}(D) = [m]T - [m]O = O$, zegt (3.2.6) dat er een $f \in L(E)^*$ bestaat met $\mathrm{div} f = D$.

De divisor

$$D' = [m]^{\mathrm{Div}}(T) - [m]^{\mathrm{Div}}(O) \in \mathrm{Div}(E)$$

kunnen we volgens (6.1.1) herschrijven als

$$D' = \sum_{R \in E[m]} (T' + R) - (R),$$

waarbij $T' \in E$ een willekeurig punt is met $[m]T' = T$. Het is duidelijk dat $\deg D' = 0$, en bovendien is

$$\mathrm{som}(D') = \sum_{R \in E[m]} T' = [m^2]T' = [m]T = 0,$$

vanwege de aanname dat $\#E[m] = m^2$. Kortom, ook in dit geval zegt (3.2.6) dat er een functie $h \in L(C)^*$ bestaat met

$$\mathrm{div}(h) = D'.$$

De functie h is zo geconstrueerd dat hij, op een constante na, aan de aan g gestelde eis voldoet, zoals deze berekening laat zien:

$$\begin{aligned}
\operatorname{div}([m]^*f) &= [m]^{\mathrm{Div}}\operatorname{div} f && \text{(2.3.1c)}\\
&= [m]^{\mathrm{Div}}\big(m(T) - m(O)\big)\\
&= m[m]^{\mathrm{Div}}\big((T) - (O)\big) && \text{want } [m]^{\mathrm{Div}} \text{ is een groepshomomorfisme}\\
&= m\operatorname{div}(h)\\
&= \operatorname{div}(h^m) && \text{want div is een groepshomomorfisme.}
\end{aligned}$$

Dit zegt namelijk dat er een een $c \in L^*$ bestaat met

$$[m]^*f = ch^m,$$

want het groepshomomorfisme $\operatorname{div} : L(E)^* \to \operatorname{Div}(E)$ heeft L^* als kern, zie (2.3.1b). Omdat L algebraïsch afgesloten is, bestaat er een $d \in L^*$ met $d^m = c$, en als we $g := dh$ stellen, dan krijgen we

$$[m]^*f = d^m h^m = g^m,$$

zoals gewenst.

Tenslotte de uniciteitsuitspraak. Als $f', g' \in L(E)^*$ ook aan (6.2) voldoen, dan is $\operatorname{div}(f') = \operatorname{div}(f)$, en wederom zegt (2.3.1b) dat $f'/f \in L^*$. Dan is

$$(\frac{g'}{g})^m = \frac{[m]^*f'}{[m]^*f} \in L^*,$$

dus volgens (6.1.2) is ook $g'/g \in L^*$.

(b) Wegens de aan f, g, S gestelde eisen, hebben we

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m,$$

dus

$$(\frac{g(X+S)}{g(X)})^m = 1,$$

dat wil zeggen

$$\frac{g(X+S)}{g(X)} \in \boldsymbol{\mu}_m.$$

Er volgt dat het morfisme $\varphi := [\tau_S^* g, g] : E \to \mathbb{P}^1_L$ van projectieve krommen over L, zoals gedefinieerd in (2.2.2), maar eindig veel waarden aanneemt. Namelijk, buiten de eindige verzameling van punten Y waarvoor g niet gedefinieerd is in Y of in $Y + S$, of nul is in Y, wordt φ gegeven door $Y \mapsto [g(Y+S)/g(Y), 1]$, en daarvoor zijn maar $\#\boldsymbol{\mu}_m = m$ mogelijkheden. In het bijzonder is φ niet surjectief, dus als morfisme van projectieve krommen moet φ wel constant zijn. Conclusie: de waarde van $g(X+S)/g(X)$ hangt niet af van X. De onafhankelijkheid van f en g volgt uit de tweede bewering in (a). □

Definitie 6.1.4. Zij E/K een elliptische kromme, en zij $m \in \mathbb{Z}_{\geq 1}$ een getal zo dat $\#E[m] = m^2$. We definiëren de functie

$$e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m,$$

genaamd de *Weilparing op* $E[m]$, als volgt. Als $S, T \in E[m]$, dan nemen we bij T horende functies $f, g \in L(E)^*$ zoals in (6.2), en een punt $X \in E$ zoals in (6.1.3b), en we definiëren

$$e_m(S,T) := \frac{g(X+S)}{g(X)}.$$

Volgens (6.1.3) is dit welgedefinieerd.

6.2 Eigenschappen van de Weilparing

Ondanks (of waarschijnlijk moeten we 'dankzij' zeggen) zijn ingewikkelde definitie, voldoet de Weilparing aan een aantal eenvoudige en handige eigenschappen.

Propositie 6.2.1. *Zij E/K een elliptische kromme, en zij m een positief geheel getal met de eigenschap dat m niet nul is in K, en dat $\#E[m] = m^2$. De Weilparing e_m op $E[m]$ heeft de volgende eigenschappen, voor alle $S, T, S_1, S_2, T_1, T_2 \in E[m]$:*

(a) 'Bilineair':

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T),$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

(b) 'Alternerend':

$$e_m(T, T) = 1,$$
$$e_m(T, S) = e_m(S, T)^{-1}.$$

(c) 'Niet-ontaard': Veronderstel dat $e_m(P, T) = 1$ voor alle $P \in E[m]$. Dan is $T = O$.

Bewijs. (a) Neem f, g behorende bij T zoals in (6.1.3), met andere woorden, waarvoor $\mathrm{div}(f) = m(T) - m(O)$ en $g^m = [m]^* f$. Zij $S_1, S_2 \in E[m]$, en neem een 'geschikte' $X \in E$, met andere woorden, g moet regulier zijn in de punten $X, X + S_1 + S_2, X + S_1$, en $g(X)$ en $g(X + S_1)$ mogen niet nul zijn. Zo'n X bestaat omdat er maar eindig veel 'X' zijn die niet aan deze eisen voldoen, terwijl E oneindig is. Direct uit de definitie van e_m volgt dat

$$\begin{aligned} e_m(S_1 + S_2, T) &= \frac{g(X + (S_1 + S_2))}{g(X)} \\ &= \frac{g((X + S_1) + S_2)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} \\ &= e_m(S_2, T)e_m(S_1, T), \end{aligned}$$

waarbij we gebruiken dat zowel X als $X + S_1$ geschikte 'X-en' zijn voor g. Dit bewijst lineariteit in de eerste variabele.

Voor lineariteit in de tweede variabele moeten we wat meer doen, want in tegenstelling tot daarnet hebben we met verschillende 'T' en daardoor met verschillende 'f' en 'g' te maken. Zij $f_1, g_1, f_2, g_2, f_3, g_3 \in L(E)^*$ functies 'horende bij' resp. $T_1, T_2, T_3 := T_1 + T_2$, met andere woorden, zo dat $\mathrm{div}(f_i) = m(T_i) - m(O)$ en $g_i^m = [m]^* f_i$ voor $i = 1, 2, 3$. Neem een 'geschikt' punt $X \in E$, met andere woorden, zo dat g_i regulier is in X en in $X + S_i$, en niet nul is in X, voor $i = 1, 2, 3$. Dit zijn eindig veel eisen aan X en voor elke eis zijn er maar eindig veel punten die niet voldoen, dus omdat E oneindig is, bestaat zo'n X. Per definitie is $e_m(S, T_i) = g_i(X + S)/g_i(X)$ voor elk van de i, dus bewijzen dat $e_m(S, T_1 + T_2) = e_m(S, T_2)e_m(S, T_2)$ komt neer op bewijzen dat

$$\frac{g_3(X + S)}{g_3(X)} = \frac{g_2(X + S)}{g_2(X)} \frac{g_1(X + S)}{g_1(X)}. \tag{6.3}$$

Om dit te bewijzen, gebruiken we weer (3.2.6), die garandeert dat er een functie $h \in L(E)^*$

bestaat zo dat

$$\begin{aligned}\operatorname{div}(\frac{f_3}{f_1 f_2}) &= \operatorname{div} f_3 - \operatorname{div} f_1 - \operatorname{div} f_2 \\ &= m\Big(\big((T_3)-(O)\big) - \big((T_1)-(O)\big) - \big((T_2)-(O)\big)\Big) \\ &= m \operatorname{div}(h) \\ &= \operatorname{div}(h^m).\end{aligned}$$

Dit betekent dat er een $c \in L^*$ bestaat zo dat $f_3/f_1 f_2 = ch^m$, want 'div' heeft L^* als kern. Dus

$$f_3 = c f_1 f_2 h^m,$$

en op beide kanten de afbeelding $[m]^*$ loslaten levert

$$\begin{aligned}g_3^m &= [m^*] f_3 \\ &= c \cdot [m]^* f_1 \cdot [m]^* f_2 \cdot ([m]^* h)^m \\ &= c g_1^m g_2^m ([m]^* h)^m,\end{aligned}$$

wat uit de verte al doet denken aan (6.3). De exponenten m kunnen we elimineren: omdat $(g_3/g_1 g_2([m]^* h))^m \in L^*$, zegt (6.1.2) dat er een $d \in L^*$ bestaat zo dat

$$g_3 = d g_1 g_2([m]^* h).$$

Invullen levert

$$\begin{aligned}\frac{g_3(X+S)}{g_3(X)} &= \frac{d g_1(X+S) g_2(X+S) h([m]X + [m]S)}{d g_1(X) g_2(X) h([m]X)} \\ &= \frac{g_1(X+S) g_2(X+S)}{g_1(X) g_2(X)},\end{aligned}$$

dit laatste omdat $S \in E[m]$, en dit bewijst (6.3), zoals gewenst.

(b) Als de eerste formule waar is, dan volgt uit (a) eenvoudig de tweede, want dan is

$$\begin{aligned}1 &= e_m(S+T, S+T) && \text{'eerste formule'} \\ &= e_m(S,S) e_m(S,T) e_m(T,S) e_m(T,T) && \text{(a)} \\ &= e_m(S,T) e_m(T,S) && \text{'eerste formule'}.\end{aligned}$$

We bewijzen de eerste formule. Neem weer $f, g \in L(E)^*$ met $\operatorname{div} f = m(T) - m(O)$ en $g^m = [m]^* f$. De kern van ons bewijs is de observatie dat

$$\prod_{k=0}^{m-1} \tau_{[k]T}^* f \in L^*. \tag{6.4}$$

We zullen (6.4) straks bewijzen, eerst laten we zien hoe eruit volgt dat $e_m(T,T) = 1$. Neem een punt $T' \in [m]^{-1}(T)$. Dan is, voor $0 \le k \le m-1$,

$$\begin{aligned}(\tau_{[k]T'}^* g)^m &= \tau_{[k]T'}^* g^m \\ &= \tau_{[k]T'}^* [m]^* f \\ &= ([m] \circ \tau_{[k]T'})^* f \\ &= (\tau_{[k]T} \circ [m])^* f && \text{want } [m][k]T' = [k]T \\ &= [m]^* \tau_{[k]T}^* f.\end{aligned}$$

We hebben daarom

$$\prod_{k=0}^{m-1}(\tau_{[k]T'}^* g)^m = \prod_{k=0}^{m-1}[m]^*\tau_{[k]T}^* f = [m]^*\prod_{k=0}^{m-1}\tau_{[k]T}^* f \in L^*,$$

dit laatste vanwege (6.4), en volgens (6.1.2) betekent dit dat

$$\prod_{k=0}^{m-1}\tau_{[k]T'}^* g \in L^*. \tag{6.5}$$

Neem een punt $X \in E$ zo dat g regulier en niet nul is in de punten $X+[k]T'$ met $k = 0, 1, \ldots, m$, zo'n X bestaat omdat slechts eindig veel 'X' niet voldoen terwijl E oneindig is. Evalueren we de functie (6.5) in de punten X en $X+T'$, dan zijn de uitkomsten gelijk want de functie is constant, kortom,

$$\begin{aligned} &g(X)g(X+T')g(X+[2]T')\cdots g(X+[m-1]T') \\ &\quad = g(X+T')g(X+[2]T')\cdots g(X+[m-1]T')g(X+[m]T'). \end{aligned}$$

Dus

$$\frac{g(X)}{g(X+T)} = \frac{g(X)}{g(X+[m]T')} = 1,$$

en per definitie van e_m betekent dit dat $e_m(T,T) = 1$, zoals gewenst.

We moeten (6.4) nog bewijzen. Als $\tau_Q : E \to E$ de translatie over Q is, voor een willekeurig punt $Q \in E$, dan is

$$\tau_Q^{\mathrm{Div}}(P) = (P-Q) \tag{6.6}$$

voor alle $P \in E$, want $P-Q$ is het enige punt in de vezel van P onder τ_Q, en bovendien is $e_{\tau_Q}(P) = 1$ omdat τ_Q een isomorfisme is (zie 2.2.7d). Dit passen we toe op onze situatie:

$$\begin{aligned} \mathrm{div}(\tau_{[k]T}^* f) &= \tau_{[k]T}^{\mathrm{Div}}\mathrm{div}(f) && (2.3.1c) \\ &= \tau_{[k]T}^{\mathrm{Div}}(m(T)-m(O)) \\ &= m([1-k]T) - m([-k]T) && \text{wegens (6.6).} \end{aligned}$$

Er volgt dat

$$\begin{aligned} \mathrm{div}(\prod_{k=0}^{m-1}\tau_{[k]T}^* f) &= \sum_{k=0}^{m-1}\mathrm{div}(\tau_{[k]T}^* f) \\ &= m\sum_{k=0}^{m-1}([1-k]T) - ([-k]T) \\ &= m((T) - ([1-m]T)) && \text{want binnenste termen heffen elkaar op} \\ &= 0 && \text{want } T = [1-m]T, \text{ omdat } T \in E[m]. \end{aligned}$$

Omdat 'div' als kern L^* heeft (2.3.1b), voltooit dit het bewijs van (6.4), en daarmee van (b).

(c) Neem, zoals gebruikelijk, functies $f, g \in L(E)^*$ met $\mathrm{div} f = m(T) - m(O)$ en $g^m = [m]^* f$. De belangrijkste observatie in ons bewijs is:

$$\text{Er bestaat een functie } h \in L(E)^* \text{ zo dat} \qquad g = [m]^* h. \tag{6.7}$$

We bewijzen dit straks, eerst leiden we hieruit (c) af. Uit (6.7) volgt dat $[m]^*f = g^m = [m]^*h^m$, en dus dat $f = h^m$, want $[m]^*$ is als homomorfisme van lichamen injectief. We hebben daarom

$$m(T) - m(O) = \operatorname{div} f = \operatorname{div} h^m = m \operatorname{div} h,$$

dus

$$(T) - (O) = \operatorname{div} h.$$

In de groep $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{div}(L(E)^*)$ geldt $\lceil \operatorname{div} h \rceil = 0$. Dus $\lceil (T)-(O) \rceil = 0 = \lceil (O)-(O) \rceil$, en vanwege de bijectie (3.2.1) volgt dat $T = O$, zoals gewenst.

We moeten (6.7) nog bewijzen. Omdat m niet nul is in K, is het isogenie $[m] \in \mathrm{End}(E)$ volgens (5.4.2) separabel, en omdat $m \neq 0$, is $[m]$ volgens (5.1.1) niet-constant. Daarmee zegt (5.2.5) dat de uitbreiding $L(E) \supset [m]^*L(E)$ Galois is, en (5.2.4) zegt dat de afbeelding

$$E[m] \xrightarrow{\sim} \mathrm{Gal}(L(E)/[m]^*L(E)) : \quad P \mapsto \tau_P^* \tag{6.8}$$

een isomorfisme van groepen is. Zij $P \in E[m]$, en zij U de niet-lege open deelverzameling van E bestaande uit de punten $X \in E$ zo dat g gedefinieerd is in X en $X + P$, en zo dat $g(X) \neq 0$. Bij aanname is $e(P, T) = 1$, dat wil zeggen $g(X + P)/g(X) = 1$ voor $X \in U$. Dus

$$(\tau_P^* g)(X) = g(X + P) = g(X) \qquad \text{voor alle } X \in U.$$

Omdat U open en niet-leeg is, concluderen we met (2.1.7) dat $\tau_P^* g = g$. Dit is waar voor alle $P \in E[m]$. Vanwege de bijectie (6.8) wil dit zeggen dat $g \in L(E)$ invariant is onder de werking van $\mathrm{Gal}(L(E)/[m]^*L(E))$, en omdat het een Galoisuitbreiding betreft, betekent dit dat $g \in [m]^*L(E)$. Dit bewijst (6.7), en voltooit het bewijs van (c). □

Tot nu toe was het verband tussen dit en het vorige hoofdstuk onduidelijk, maar hier komt een synthese: we bewijzen dat een isogenie geadjungeerd is met zijn duale isogenie ten opzichte van de Weilparing.

Stelling 6.2.2. *Zij E_1, E_2 elliptische krommen over K, en zij m een positief geheel getal zo dat m niet nul is in K, en zo dat $\#E_1[m] = \#E_2[m] = m^2$. Als $\varphi : E_1 \to E_2$ een isogenie is, en als $S \in E_1[m]$ en $T \in E_2[m]$, dan is*

$$e_m(S, \varphi^t T) = e_m(\varphi S, T).$$

Hier is de eerste 'e_m' de Weil-paring op $E_1[m]$, en de tweede die op $E_2[m]$.

Bewijs. Net als bij de tweede formule in (6.2.1b) moeten we wat werk verrichten, omdat we met verschillende 'T' te maken hebben. Neem f en g als in (6.1.3) behorende bij T, met andere woorden, zo dat $\operatorname{div}(f) = m(T) - m(O)$ en $g^m = [m]^*f$. De divisor

$$D := \varphi^{\mathrm{Div}}(T) - \varphi^{\mathrm{Div}}(O) - (\varphi^t T) + (O) \in \mathrm{Div}(E_1)$$

heeft graad $\deg(D) = \deg(\varphi) - \deg(\varphi) - 1 + 1 = 0$ volgens (2.3.1d), en wegens de definitie van φ^t is

$$\mathrm{som}(D) = \mathrm{som}(\varphi^{\mathrm{Div}}(T) - \varphi^{\mathrm{Div}}(O)) - \varphi^t T = \varphi^t T - \varphi^t T = O.$$

Daarom zegt (3.2.6) dat er een functie $h \in L(E_1)$ bestaat met $\operatorname{div}(h) = D$. We laten zien dat de functies

$$f' := \frac{\varphi^* f}{h^m} \qquad \text{en} \qquad g' := \frac{\varphi^* g}{[m]^* h}$$

de bij $\varphi^t T$ behorende 'f' en 'g' zijn:

$$\begin{aligned}\operatorname{div}(f') &= \operatorname{div}(\varphi^* f) - m\operatorname{div}(h)\\ &= \varphi^{\mathrm{Div}}\operatorname{div}(f) - mD \qquad (2.3.1d)\\ &= \varphi^{\mathrm{Div}}\big(m(T) - m(O)\big) - mD\\ &= m(\varphi^t T) - m(O),\end{aligned}$$

en

$$\begin{aligned}(g')^m &= \frac{\varphi^*(g^m)}{[m]^*(h^m)}\\ &= \frac{\varphi^*[m]^* f}{[m]^*(h^m)} = \frac{[m]^*\varphi^* f}{[m]^*(h^m)} \qquad \text{want } [m]\circ\varphi = \varphi\circ[m]\\ &= [m]^*\frac{\varphi^* f}{h^m}\\ &= [m]^* f'.\end{aligned}$$

Met deze kennis volgt de rest van het bewijs door invullen in de definitie van de Weil-paringen. Neem namelijk een 'geschikt' punt $X \in E$, dat wil zeggen zo dat g' regulier is in X en in $X+S$ en niet nul is in X, en zo dat g regulier is in φX en in $\varphi X + \varphi S$ en niet nul is in φX; er zijn maar eindig veel 'X' ongeschikt (want de vezels van φ zijn eindig), dus een geschikte X bestaat. Er volgt dat

$$\begin{aligned}e_m(S, \varphi^t T) &= \frac{g'(X+S)}{g'(X)}\\ &= \frac{g(\varphi X + \varphi S)}{g(\varphi X)}\frac{h([m]X)}{h([m]X + [m]S)} \qquad \text{per definitie van } g'\\ &= \frac{g(\varphi X + \varphi S)}{g(\varphi X)} \qquad \text{want } S \in E[m]\\ &= e_m(\varphi S, T),\end{aligned}$$

zoals gewenst. □

6.3 Meer over duale isogeniën, en de graad van $[m]$

Nu we een connectie hebben tussen duale isogeniën en de Weilparing, kunnen we eigenschappen van de Weilparing 'omzetten' naar eigenschappen van duale isogeniën.

Stelling 6.3.1. *Als E_1/K en E_2/K twee elliptische krommen zijn, dan is de afbeelding*

$$\operatorname{Ign}(E_1, E_2) \to \operatorname{Ign}(E_2, E_1): \quad \psi \mapsto \psi^t$$

een homomorfisme van abelse groepen.

Bewijs. Het gehele getal

$$a := \begin{cases} 2 & \text{als } \operatorname{char}(K) \neq 2 \\ 3 & \text{als } \operatorname{char}(K) = 2 \end{cases}$$

is niet nul in K, dus als E/K een elliptische kromme is, dan zegt (5.4.2) dat $[a] : E \to E$ separabel is. Volgens (5.2.5) is $\deg[a] = \#E[a]$, en vanwege de specifieke keus van a, weten we

uit Voorbeeld 3.3.7 resp. 3.3.8 dat $\#E[a] = a^2$, want E is isomorf aan een elliptische kromme met een Weierstrass-vergelijking zoals in die voorbeelden. Kortom,

$$\deg[a] = \#E[a] = a^2.$$

Als $n \geq 1$, dan volgt, omdat de graad multiplicatief is, en omdat ook a^n niet nul is in K, dat

$$\#E[a^n] = \deg[a^n] = \deg([a]^n) = (\deg[a])^n = (a^n)^2.$$

Dit stelt ons in staat het over de Weilparing op $E[a^n]$ te hebben. We schrijven $m := a^n$.

In het bijzonder hebben we Weilparingen op $E_1[m]$ en $E_2[m]$. Zij $\varphi, \psi \in \mathrm{Ign}(E_1, E_2)$ twee isogeniën. Als $T_1 \in E_1[m]$ en $T_2 \in E_2[m]$, dan is

$$\begin{aligned} e_m(T_1, (\varphi+\psi)^t T_2) &= e_m((\varphi+\psi)T_1, T_2) && (6.2.2)\\ &= e_m(\varphi T_1, T_2) + e_m(\psi T_1, T_2) && (6.2.1\text{ 'bilineair'})\\ &= e_m(T_1, \varphi^t T_2) + e_m(T_1, \psi^t T_2) && (6.2.2)\\ &= e_m(T_1, (\varphi^t + \psi^t)T_2) && (6.2.1\text{ 'bilineair'}). \end{aligned}$$

Omdat dit, voor vaste $T_2 \in E_2[m]$, waar is voor alle $T_1 \in E_1[m]$, zegt (6.2.1 'niet-ontaard') dat

$$(\varphi+\psi)^t T_2 = (\varphi^t + \psi^t)T_2.$$

Bovendien is dit waar met $m = a^n$ voor alle $n \geq 1$. Kortom,

$$\bigcup_{n\geq 1} E[a^n] \subset \ker\big((\varphi+\psi)^t - (\varphi^t+\psi^t)\big).$$

Omdat $\#E[a^n] = a^{2n}$, is de kern van de isogenie $(\varphi+\psi)^t - (\varphi^t+\psi^t)$ oneindig, dus vanwege (5.2.2) is dit het nul-isogenie. Kortom,

$$(\varphi+\psi)^t = (\varphi^t + \psi^t),$$

zoals gewenst. □

Gevolg 6.3.2. *Als E/K een elliptische kromme is en $m \in \mathbb{Z}_{\neq 0}$, dan is*

$$\deg[m] = m^2,$$

en als m niet nul is in K, dan is bovendien

$$\#E[m] = m^2.$$

Bewijs. We laten zien dat $[m]^t = [m]$. Het is eenvoudig voor $m = \pm 1$. Namelijk, omdat $[1]$ en $[-1]$ isomorfismen zijn, hebben ze graad 1 (zie 2.2.7d), zodat

$$[1]\circ[1] = [1] = [\deg[1]] \qquad \text{en} \qquad [-1]\circ[-1] = [1] = [\deg[-1]],$$

en de karakterisering 5.5.2 van de duale isogenie zegt dat $[1]^t = [1]$ en $[-1]^t = [-1]$. Als m positief is, dan volgt

$$\begin{aligned} [m]^t &= ([1] + \ldots + [1])^t && (m\text{ termen})\\ &= [1]^t + \ldots + [1]^t && (6.3.1)\\ &= [1] + \ldots + [1] = [m], \end{aligned}$$

zoals gewenst. Door in deze berekening $[m]$ en $[1]$ door $[-m]$ resp. $[-1]$ te vervangen, zien we dat het ook voor negatieve m geldt.

Uit dit resultaat leiden we af dat

$$\begin{aligned}[m^2] &= [m] \circ [m] \\ &= [m]^t \circ [m] \\ &= [\deg[m]].\end{aligned}$$

Omdat de abelse groep $\mathrm{End}(E)$ torsievrij is (5.1.1b), volgt dat $m^2 = \deg[m]$. Als bovendien m niet nul is in K, dan is $[m]$ separabel (5.4.2), dus wegens (5.2.5) hebben we dan $\#E[m] = \deg[m]$. □

In het bijzonder zien we dat de Weilparing op $E[m]$ is gedefinieerd zodra m niet nul is in K.

Zoals eerder opgemerkt, suggereert de term 'duaal' een symmetrische relatie, en we kunnen nu laten zien dat dat zo is.

Gevolg 6.3.3. *Als $\varphi : E_1 \to E_2$ een isogenie van elliptische krommen over K is, dan is $(\varphi^t)^t = \varphi$. Met andere woorden, de contravariante functor $D : \mathcal{E} \to \mathcal{E}$ van (5.5.4b) is een involutie.*

Bewijs. We hebben

$$\begin{aligned}(\varphi^t)^t \circ \varphi^t &= (\varphi \circ \varphi^t)^t && (5.5.4b) \\ &= [\deg \varphi]^t && (5.5.4a)] \\ &= [\deg \varphi && (6.3.2)] \\ &= \varphi \circ \varphi^t. && (5.5.4a)\end{aligned}$$

Als niet-constant isogenie is φ^t surjectief, zodat $(\varphi^t)^t = \varphi$. □

Uit (6.3.2) kunnen we de structuur van de abelse groep $E[m]$ afleiden, in het geval dat m niet nul is in K. Het kost geen extra moeite, en maakt het idee helderder, om het bewijs te schrijven in de algemenere context van

Lemma 6.3.4. *Zij A een abelse groep van orde n^r, waarbij $n, r \in \mathbb{Z}_{\geq 1}$. Stel dat $\#A[d] = d^r$, voor elke deler d van n. Dan is*

$$A \cong (\mathbb{Z}/n)^r.$$

Bewijs. Een variant van de structuurstelling voor Abelse groepen, zegt dat er een getal $t \in \mathbb{Z}_{\geq 1}$ en getallen $a_1, \ldots, a_t \in \mathbb{Z}_{\geq 2}$ bestaan zo dat

$$A \cong \mathbb{Z}/a_1 \oplus \ldots \oplus \mathbb{Z}/a_t, \tag{6.9}$$

en zo dat a_i deler is van a_{i+1}, voor $i = 1, \ldots, t-1$. (Zie bijvoorbeeld [Arm87, 21.1].) Als d een deler is van n, dan is eenvoudig te zien dat

$$A[d] \cong (\mathbb{Z}/a_1)[d] \oplus \ldots \oplus (\mathbb{Z}/a_t)[d]. \tag{6.10}$$

Als a, d', x gehele getallen zijn, dan geldt $d'x \equiv 0 \pmod{a}$ precies dan als x een veelvoud is van $a/\mathrm{ggd}(a, d')$. Omdat $\mathbb{Z}/a$ zelf a element heeft, betekent dit dat

$$\#(\mathbb{Z}/a)[d'] = \mathrm{ggd}(a, d'). \tag{6.11}$$

Uit (6.11) en (6.10) en uit de aanname dat $d^r = \#A[d]$, volgt dat

$$d^r = \mathrm{ggd}(a_1, d) \cdots \mathrm{ggd}(a_t, d). \tag{6.12}$$

Als we $d = n$ invullen, krijgen we

$$\begin{aligned} \mathrm{ggd}(a_1, n) \cdots \mathrm{ggd}(a_t, n) &= n^r \\ &= \#A && \text{bij aanname} \\ &= a_1 \cdots a_t && \text{wegens (6.9).} \end{aligned}$$

Omdat $\mathrm{ggd}(a_i, n) \leq a_i$ voor elke i, met gelijkheid precies dan als a_i deler is van n, concluderen we dat elk van de getallen $a_1, \ldots, a_t$ een deler is van n. In het bijzonder kunnen we $d = a_1$ invullen in (6.12). Dit levert

$$a_1^r = a_1^t,$$

want a_1 deelt bij aanname elk van de a_i. Dus $r = t$. Invullen van $r = t$ in (6.9), levert

$$a_1 \cdots a_r = n^r.$$

Omdat $a_i \leq n$ voor elke i, betekent dit dat $a_i = n$ voor $i = 1, \ldots, r$. Dit substitueren in (6.9), en gebruiken dat $t = r$, levert $A \cong (\mathbb{Z}/n)^r$. □

Gevolg 6.3.5. *Zij m een geheel getal dat niet nul is in K. Dan hebben we een isomorfie van groepen*

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

Bewijs. Volgens (6.3.2) heeft de groep $E[m]$ orde m^2. Algemener is elke deler d van m niet nul in K, dus (6.3.2) zegt dat $\#E[d] = d^2$. Dan vertelt (6.3.4) dat $E[m] \cong (\mathbb{Z}/m)^2$. □

Hoofdstuk 7

De ℓ-adische Weilparing op het Tatemoduul

We fixeren in dit hoofdstuk deze notatie:
K is een lichaam,
L is een algebraïsch afsluiting van K,
$\boldsymbol{\mu}_m$ is de ondergroep van m-de machts eenheidswortels van L^*, indien $m \in \mathbb{Z}_{\geq 1}$,
$\boldsymbol{\mu}$ is de ondergroep van alle eenheidswortels van L^*, dus $\boldsymbol{\mu} = \bigcup_{m \geq 1} \boldsymbol{\mu}_m$.

In het vorige hoofdstuk hebben we voorbeelden gezien van hoe de Weilparing op $E[m]$ iets kan zeggen over isogeniën. In dit hoofdstuk gaan we dit verder uitdiepen. Concreet gesproken: we nemen een priemgetal ℓ dat niet nul is in K, en beschouwen alle Weilparingen e_{ℓ^n} op $E[\ell^n]$ met $n \geq 0$. We 'bundelen' deze Weilparingen 'op een structuur-respecterende manier' tot een nieuwe paring 'e' op het zogenaamde Tatemoduul $T_\ell(E)$ van E, zodat we via e in zekere zin alle paringen e_{ℓ^n} tegelijk bestuderen. Een isogenie kunnen we representeren als afbeelding van Tatemodulen, en de Weilparingen op deze Tatemodulen helpen om de isogenie te onderzoeken.

7.1 Het ℓ-adische Tatemoduul

Het idee van het 'bundelen' van Weilparingen kan precies worden gemaakt met het concept *inverse limiet*.

Definitie 7.1.1. Als een $\{X_n\}_{n\geq 0}$ een verzameling van groepen resp. ringen is, en als voor elke $n \geq 0$ een homomorfisme $f_n : X_{n+1} \to X_n$ gegeven is, dan definiëren we de *inverse limiet van de familie* $\{(X_n, f_n)\}_{n\geq 0}$ als de ondergroep resp. deelring

$$\varprojlim_n (X_n, f_n) = \{(x_n)_{n\geq 0} \in \prod_{n\geq 0} X_n \,:\, f_n(x_{n+1}) = x_n \text{ voor alle } n\}$$

van het product $\prod_{n\geq 0} X_n$.

Dat het inderdaad om een ondergroep gaat (of deelring in het geval van ringen), is eenvoudig te zien: als $(x_n)_n, (y_n)_n \in \varprojlim(X_n, f_n)$, dan $f_n(x_{n+1}y_{n+1}) = x_n y_n$ want f_n is een homomorfisme, dus ook het product $(x_n)_n(y_n)_n = (x_n y_n)_n$ ligt in $\varprojlim(X_n, f_n)$. (We laten om typografische redenen de 'n' onder de pijl weg, evenals '≥ 0' in de index.)

Het standaardvoorbeeld van een inverse limiet is de ring van ℓ-adische getallen.

Definitie 7.1.2. Zij ℓ een priemgetal. De ring van *ℓ-adische getallen*, notatie $\mathbb{Z}_\ell$, is de inverse limiet

$$\mathbb{Z}_\ell = \varprojlim_n (\mathbb{Z}/\ell^n, \pi_n),$$

waarbij $\pi_n : \mathbb{Z}/\ell^{n+1} \to \mathbb{Z}/\ell^n$, voor $n \geq 0$, de projectie $a \pmod{\ell^{n+1}} \mapsto a \pmod{\ell^n}$ is.

Via de inbedding $\mathbb{Z} \to \mathbb{Z}_\ell : a \mapsto (a \mod \ell^n)_n$ vatten we $\mathbb{Z}$ op als deelring van $\mathbb{Z}_\ell$.

Conventie 7.1.3. Als we het hebben over 'het element $(x_n)_n \in \varprojlim(X_n, f_n)$', dan bedoelen we dat $x_n \in X_n$, en uiteraard dat $f_n(x_{n+1}) = x_n$, voor alle $n \geq 0$. Bovendien, als we het hebben over 'het element $(\overline{x_n})_n$ van $\mathbb{Z}_\ell$', dan bedoelen we dat $x_n \in \mathbb{Z}$ en dat $\overline{x_n}$ zijn projectie is in $\mathbb{Z}/\ell^n$, kortom $\overline{x_n} = x_n \bmod \ell^n$.

In tegenstelling tot zijn bouwstenen $\mathbb{Z}/\ell^n$ met $n \geq 2$, is $\mathbb{Z}_\ell$ een domein. Stel namelijk dat $(\overline{x_n}), (\overline{y_n}) \in \mathbb{Z}_\ell$ beide niet nul zijn, dan zijn er $t, u \geq 0$ zo dat $x_t \not\equiv 0 \pmod{\ell^t}$ en $y_u \not\equiv 0 \pmod{\ell^u}$. Per definitie van de afbeeldingen π_n is dan, voor willekeurige $n \geq u + t$, ook $x_n \not\equiv 0 \pmod{\ell^t}$ en $y_n \not\equiv 0 \pmod{\ell^u}$, kortom ℓ^t deelt niet x_n en ℓ^u deelt niet y_n. Omdat ℓ priem is, volgt dat $x_n y_n \not\equiv 0 \pmod{\ell^{t+u}}$, dus $\overline{x_n y_n} \neq \overline{0} \in \mathbb{Z}/\ell^n$, dus $(\overline{x_n})_n (\overline{y_n})_n = (\overline{x_n y_n})_n \neq (\overline{0})_n$.
Een ander voorbeeld van een inverse limiet is het Tatemoduul.

Definitie 7.1.4. Zij A een (additief geschreven) abelse groep, en ℓ een priemgetal. De abelse groep

$$T_\ell(A) = \varprojlim_n (A[\ell^n], [\ell]_n),$$

waarbij $[\ell]_n : A[\ell^{n+1}] \to A[\ell^n]$ de restrictie van de afbeelding $[\ell] : A \to A$ is, kunnen we opvatten als $\mathbb{Z}_\ell$-moduul, namelijk via de 'coördinaatsgewijze' operatie van $\mathbb{Z}_\ell$ op $T_\ell(A)$ gegeven door

$$(\overline{x_n})_n (a_n)_n = (x_n a_n)_n,$$

die welgedefinieerd is omdat $A[\ell^n]$ een $\mathbb{Z}/\ell^n$-moduul is voor $n \geq 0$. Het $\mathbb{Z}_\ell$-moduul $T_\ell(A)$ heet het *ℓ-adische Tatemoduul van A*.

Als E/K een elliptische kromme is, dan krijgen we uit de onderliggende abelse groep van E het *ℓ-adische Tatemoduul van E*,

$$T_\ell(E) = \varprojlim_n (E[\ell^n], [\ell]).$$

Opmerking 7.1.5. Zij E/K een elliptische kromme, $\ell \neq \mathrm{char} K$ een priemgetal en $m \geq 0$. Als $T \in E[\ell^m]$, dan bestaat er een element $(T_n)_n \in T_\ell(E)$ met $T_m = T$. Namelijk, we kunnen $T_k := [\ell^{m-k}] T_m$ nemen voor $k \leq m$, en voor $k \geq m$ kiezen we inductief een element T_{k+1} uit de niet-lege vezel van T_k onder de afbeelding $[m]$.

Zoals gezegd willen we de paringen $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \boldsymbol{\mu}_{\ell^n}$ bundelen tot een nieuwe paring. Dit wordt een paring $T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu})$, waarbij $T_\ell(\boldsymbol{\mu})$ het Tatemoduul is van de abelse groep $\boldsymbol{\mu}$ van eenheidswortels in L^*. Omdat de groepsoperatie van $\boldsymbol{\mu}$ multiplicatief geschreven wordt, wordt de werking van $\mathbb{Z}$ op $\boldsymbol{\mu}$ als $\mathbb{Z}$-moduul niet als 'vermenigvuldiging', maar als 'exponentiatie' geschreven. Zodoende hebben we

$$T_\ell(\boldsymbol{\mu}) = \varprojlim_n (\boldsymbol{\mu}_{\ell^n}, m_\ell), \qquad \text{waarbij } m_\ell : \boldsymbol{\mu}_{\ell^{n+1}} \to \boldsymbol{\mu}_{\ell^n} : \zeta \mapsto \zeta^\ell.$$

(De notatie m_ℓ zullen we verder niet gebruiken.) Voor de consistentie schrijven we ook de werking van $\mathbb{Z}_\ell$ op het $\mathbb{Z}_\ell$-moduul $T_\ell(\boldsymbol{\mu})$ als 'exponentiatie' in plaats van 'vermenigvuldiging': het beeld van $(\zeta_n)_n \in T_\ell(\boldsymbol{\mu})$ onder de werking van $(\overline{z_n})_n \in \mathbb{Z}_\ell$ is

$$(\zeta_n)_n^{(\overline{z_n})_n} = (\zeta_n^{z_n})_n.$$

Omdat $E[\ell^n]$ als $\mathbb{Z}/\ell^n$-moduul isomorf is aan $\mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$, ligt het voor de hand dat $T_\ell(E)$ als $\mathbb{Z}_\ell$-moduul isomorf is aan $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Dit is inderdaad waar, en volgt uit basale, abstracte eigenschappen van inverse limieten die we onderbrengen in

Lemma 7.1.6. *(a) Als voor elke $n \geq 0$ een groep X_{in} en een homomorfisme $f_{in} : X_{i,n+1} \to X_{i,n}$ gegeven is, en dit voor elke i in een indexverzameling I, dan is de afbeelding*

$$\prod_{i\in I} \varprojlim_n (X_{in}, f_{in}) \xrightarrow{\sim} \varprojlim_n (\prod_{i\in I} X_{in}, \prod_{i\in I} f_{in}) : \quad ((x_{in})_n)_i \mapsto ((x_{in})_i)_n$$

een isomorfisme van groepen, waarbij we met $\prod_{i\in I} f_{in}$ het product-homomorfisme $\prod_{i\in I} X_{i,n+1} \to \prod_{i\in I} X_{in} : (x_{i,n+1})_i \mapsto (f_i(x_{i,n+1}))_i$ bedoelen. Analoog voor 'ringen' in plaats van 'groepen'. Met andere woorden, het nemen van producten commuteert met het nemen van inverse limieten.

(b) Als voor elke $n \geq 0$ groepen X_n, Y_n en homomorfismen $f_n : X_{n+1} \to X_n$ en $g_n : Y_{n+1} \to Y_n$ gegeven zijn, en bovendien homomorfismen $\tau_n : X_n \to Y_n$ die hiermee compatibel zijn in de zin dat het diagram

$$\begin{array}{ccccccc} \cdots & \xrightarrow{f_2} & X_2 & \xrightarrow{f_1} & X_1 & \xrightarrow{f_0} & X_0 \\ \vdots & & \downarrow{\scriptstyle \tau_2} & & \downarrow{\scriptstyle \tau_1} & & \downarrow{\scriptstyle \tau_0} \\ \cdots & \xrightarrow{g_2} & Y_2 & \xrightarrow{g_1} & Y_1 & \xrightarrow{g_0} & Y_0 \end{array}$$

commuteert, dan is de afbeelding

$$\tau : \varprojlim(X_n, f_n) \to \varprojlim(Y_n, g_n) : \quad (x_n)_n \mapsto (\tau_n x_n)_n$$

een homomorfisme van groepen. Als alle τ_n isomorfismen zijn, dan is τ een isomorfisme. Analoog voor 'ringen' in plaats van 'groepen'.

Bewijs. (a) Het is duidelijk dat de 'grotere' afbeelding

$$\prod_{i\in I} \prod_{n\geq 0} X_{in} \xrightarrow{\sim} \prod_{n\geq 0} \prod_{i\in I} X_{in} : \quad ((x_{in})_n)_i \mapsto ((x_{in})_i)_n$$

een isomorfisme is, en het is eenvoudig na te gaan dat restrictie van deze afbeelding een bijectie tussen de beoogde ondergroepen induceert.

(b) Dat het beeld van τ inderdaad in $\varprojlim(Y_n, g_n)$ ligt, volgt omdat het diagram commuteert: als $(x_n)_n \in \varprojlim(X_n, f_n)$, dan is

$$g_n(\tau_{n+1}x_{n+1}) = \tau_n(f_n(x_{n+1})) = \tau_n x_n$$

voor alle $n \geq 0$, dus $(\tau_n x_n)_n \in \varprojlim(Y_n, g_n)$, zoals gewenst. Een rechtstreekse berekening toont dat τ een homomorfisme is. Als elke τ_n een inverse homomorfisme τ_n^{-1} heeft, dan is duidelijk dat τ een inverse homomorfisme heeft, namelijk $\tau^{-1} : \varprojlim(Y_n, g_n) \to \varprojlim(X_n, f_n) : (y_n)_n \mapsto (\tau_n^{-1} y_n)_n$, dus τ is een isomorfisme. $\square$

Stelling 7.1.7. *Als E/K een elliptische kromme is en $\ell \neq \mathrm{char}K$ een priemgetal, dan hebben we een isomorfie van $\mathbb{Z}_\ell$-modulen*

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Bewijs. Zij $n \geq 0$ willekeurig. Volgens (6.3.5) hebben we een isomorfie $E[\ell^n] \cong \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$ van abelse groepen, met andere woorden $E[\ell^n]$ is een vrij $\mathbb{Z}/\ell^n$-moduul van rang 2. Neem een basis $\{P_n, Q_n\}$ van dit $\mathbb{Z}/\ell^n$-moduul. Neem punten $P_{n+1}, Q_{n+1} \in E[\ell^{n+1}]$ zo dat $[\ell]P_{n+1} = P_n$ en $[\ell]Q_{n+1} = Q_n$. We beweren dat $\{P_{n+1}, Q_{n+1}\}$ een basis is van het $\mathbb{Z}/\ell^{n+1}$-moduul $E[\ell^{n+1}]$. Stel namelijk dat a, b gehele getallen zijn met $[a]P_{n+1} + [b]Q_{n+1} = O$. We willen bewijzen dat $a, b \equiv 0 \pmod{\ell^{n+1}}$, want dan zijn P_{n+1} en Q_{n+1} lineair onafhankelijk. Door beide kanten met ℓ te vermenigvuldigen, krijgen we

$$[a]P_n + [b]Q_n = [\ell][a]P_{n+1} + [\ell][b]Q_{n+1} = O,$$

en omdat $\{P_n, Q_n\}$ een basis is van $E[\ell^n]$ over $\mathbb{Z}/\ell^n$, volgt dat $a, b \equiv 0 \pmod{\ell^n}$. Dit is net niet genoeg, maar het betekent wel dat a en b veelvouden van ℓ zijn, zeg $a = \ell a'$ en $b = \ell b'$, en we kunnen nu hetzelfde doen als net behalve dat we de factor ℓ al hebben:

$$[a']P_n + [b']Q_n = [\ell][a']P_{n+1} + [\ell][b']Q_{n+1} = [a]P_{n+1} + [b]Q_{n+1} = O.$$

Zoals daarnet volgt dat $a', b' \equiv 0 \pmod{\ell^n}$, zodat $a, b \equiv 0 \pmod{\ell^{n+1}}$, zoals gewenst. Omdat P_{n+1} en Q_{n+1} lineair onafhankelijk zijn over $\mathbb{Z}/\ell^{n+1}$, spannen zij reeds $(\ell^{n+1})^2 = \#E[\ell^{n+1}]$ elementen van $E[\ell^{n+1}]$ op, dus $\{P_{n+1}, Q_{n+1}\}$ is inderdaad een basis van $E[\ell^{n+1}]$.

De isomorfismen

$$\begin{aligned} \tau_n : E[\ell^n] \to \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n : &\qquad [a]P_n + [b]Q_n \mapsto (a \bmod \ell^n, b \bmod \ell^n), \\ \tau_{n+1} : E[\ell^{n+1}] \to \mathbb{Z}/\ell^{n+1} \times \mathbb{Z}/\ell^{n+1} : &\qquad [a]P_{n+1} + [b]Q_{n+1} \mapsto (a \bmod \ell^{n+1}, b \bmod \ell^{n+1}) \end{aligned}$$

maken het diagram

$$\begin{array}{ccc} E[\ell^{n+1}] & \xrightarrow{[\ell]} & E[\ell^n] \\ \downarrow{\scriptstyle \tau_{n+1}} & & \downarrow{\scriptstyle \tau_n} \\ (\mathbb{Z}/\ell^{n+1})^2 & \xrightarrow{\pi_n^2} & (\mathbb{Z}/\ell^n)^2 \end{array}$$

commutatief, met $\pi_n : \mathbb{Z}/\ell^{n+1} \to \mathbb{Z}/\ell^n : a \bmod \ell^{n+1} \mapsto a \bmod \ell^n$, en π_n^2 de productafbeelding hiervan zoals in (7.1.6a). Omdat dit voor alle $n \geq 0$ geldt, is voldaan aan de compatibiliteitseis, zodat (7.1.6b) een isomorfisme van groepen $T_\ell(E) \to \varprojlim((\mathbb{Z}/\ell^n)^2, \pi_n^2)$ geeft. Vervolgens geeft (7.1.6a) een isomorfisme $T_\ell(E) \to \varprojlim((\mathbb{Z}/\ell^n)^2, \pi_n^2) \to \mathbb{Z}_\ell^2$. Uit de formules aldaar is duidelijk dat dit isomorfismen van $\mathbb{Z}_\ell$-modulen zijn. □

7.2 De Weilparing op het Tatemoduul

Om de beoogde bundeling van Weilparingen voor elkaar te krijgen, hebben we nodig dat de verschillende paringen 'compatibel' zijn, in de zin van

Lemma 7.2.1. *Zij m_1, m_2 twee positieve gehele getallen die beide niet nul zijn in K. Zij e_{m_1} en $e_{m_1 m_2}$ de Weil-paringen op $E[m_1]$ resp. $E[m_1 m_2]$. Als $U \in E[m_1 m_2]$ en $T \in E[m_1] \subset E[m_1 m_2]$, dan is*

$$e_{m_1 m_2}(U, T) = e_{m_1}([m_2]U, T).$$

Bewijs. Neem $f, g \in L(E)$ behorende bij (m_1, T), dat wil zeggen met

$$\mathrm{div} f = m_1(T) - m_1(O) \qquad \text{en} \qquad g^{m_1} = [m_1]^* f.$$

Dan zijn

$$f_2 := f^{m_2} \qquad \text{en} \qquad g_2 := [m_2]^* g$$

corresponderende functies behorende bij $(m_1 m_2, T)$, want

$$\mathrm{div} f_2 = m_2 \,\mathrm{div} f = m_2 m_1(T) - m_2 m_1(O),$$

en

$$\begin{aligned} g_2^{m_1 m_2} &= [m_2]^* g^{m_1 m_2} \\ &= [m_2]^* ([m_1]^* f)^{m_2} \\ &= [m_2]^* [m_1]^* f_2 \\ &= [m_1 m_2]^* f_2 \qquad\qquad \text{want } [m_2]^*[m_1]^* = ([m_1] \circ [m_2])^*. \end{aligned}$$

Neem een geschikte $X \in E$, dat wil zeggen zo dat g_2 regulier is in de punten $X, X+U$ en niet nul in X, en zo dat g regulier is in $[m_2]X, [m_2]X + [m_2]U$ en niet nul is in $[m_2]X$. Zoals gebruikelijk zijn er slechts eindig veel 'X' die niet zouden kunnen. Uit de definitie van de betrokken Weilparingen volgt dat

$$\begin{aligned} e_{m_1 m_2}(U, T) &= \frac{g_2(X+U)}{g_2(X)} \\ &= \frac{g([m_2]X + [m_2]U)}{g([m_2]X)} = e_{m_1}([m_2]U, T). \end{aligned}$$ □

We zijn nu bijna (dat wil zeggen in 7.2.3) in staat de Weilparingen e_{ℓ^n} te bundelen tot een nieuwe paring 'e'. Het volgende lemma, waarvan het bewijs berust op de compatibiliteitseis (7.2.1), rechtvaardigt de keuze van het codomein van e.

Lemma 7.2.2. *Zij E/K een elliptische kromme, zij ℓ een priemgetal ongelijk aan de karakteristiek van K, en zij $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \boldsymbol{\mu}_{\ell^n}$ de Weil-paringen op $E[\ell^n]$, voor $n \geq 0$. Het beeld van de functie*

$$T_\ell(E) \times T_\ell(E) \to \prod_{n \geq 0} \boldsymbol{\mu}_{\ell^n} : \big((P_n)_n, (Q_n)_n\big) \mapsto \big(e_{\ell^n}(P_n, Q_n)\big)_n$$

ligt in $T_\ell(\boldsymbol{\mu})$.

Bewijs. Zij $(P_n)_n, (Q_n)_n \in T_\ell(E)$. De te bewijzen conditie komt erop neer dat $e_{\ell^{n+1}}(P_{n+1}, Q_{n+1})^\ell = e_{\ell^n}(P_n, Q_n)$ voor alle $n \geq 0$. Dit volgt direct uit reeds bewezen eigenschappen:

$$\begin{aligned} e_{\ell^{n+1}}(P_{n+1}, Q_{n+1})^\ell &= e_{\ell^{n+1}}(P_{n+1}, [\ell]Q_{n+1}) && \text{(6.2.1) 'bilineair'} \\ &= e_{\ell^n}([\ell]P_{n+1}, [\ell]Q_{n+1}) && \text{(7.2.1)} \\ &= e_{\ell^n}(P_n, Q_n) && \text{want } (P_n)_n, (Q_n)_n \in T_\ell(E). \end{aligned}$$ □

Definitie 7.2.3. Zij E/K een elliptische kromme, zij ℓ een priemgetal ongelijk aan de karakteristiek van K, en zij $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \boldsymbol{\mu}_{\ell^n}$ de Weilparing op $E[\ell^n]$, voor $n \geq 0$. De *ℓ-adische Weilparing op $T_\ell(E)$* is de functie

$$\begin{aligned} e : T_\ell(E) \times T_\ell(E) &\to T_\ell(\boldsymbol{\mu}) : \\ \big((P_n)_n, (Q_n)_n\big) &\mapsto \big(e_{\ell^n}(P_n, Q_n)\big)_n. \end{aligned}$$

Met andere woorden, de 'ℓ^n-coördinaat' van $e(x,y)$ wordt verkregen door de Weilparing e_{l^n} toe te passen op de 'ℓ^n-coördinaten' van x en y.

Onze opmerking in de introductie van dit hoofdstuk dat het bundelen van de Weilparingen e_{ℓ^n} 'op een structuur-respecterende manier' gebeurt, zien we terug in het volgende propositie: de basiseigenschappen van de e_{ℓ^n} worden direct overgevoerd naar die van e.

Propositie 7.2.4. *Zij E/K een elliptische kromme en $\ell \neq \mathrm{char}K$ een priemgetal. De Weilparing $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu})$ heeft de volgende eigenschappen, voor alle $v, w, v', w' \in T_\ell(E)$ en $a, b \in \mathbb{Z}_\ell$:*

(a) 'Bilineair':

$$\begin{aligned} e(v+v', w) &= e(v,w)e(v',w), \\ e(v, w+w') &= e(v,w)e(v,w'), \\ e(av, bw) &= e(v,w)^{ab}. \end{aligned}$$

(b) 'Alternerend':

$$\begin{aligned} e(w,w) &= 1, \\ e(w,v) &= e(v,w)^{-1}. \end{aligned}$$

(c) 'Niet-ontaard': Veronderstel dat $e(u,v) = 1$ voor alle $u \in T_\ell(E)$. Dan is $v = 0$.

Bewijs. De bewijzen zijn berekeningen rechtstreeks uit de definities en uit de analoge formules in (6.2.1). We schrijven

$$v = (P_n)_n, \quad v' = (P'_n)_n, \quad w = (Q_n)_n, \quad w' = (Q'_n)_n.$$

(a) De eerste formule volgt uit de berekening

$$\begin{aligned} e(v+v', w) &= e\big((P_n + P'_n)_n, (Q_n)_n\big) \\ &= \big(e_{\ell^n}(P_n + P'_n, Q_n)\big)_n \\ &= \big(e_{\ell^n}(P_n, Q_n) e_{\ell^n}(P'_n, Q_n)\big)_n \qquad \text{(6.2.1a)} \\ &= \big(e_{\ell^n}(P_n, Q_n)\big)_n \big(e_{\ell^n}(P'_n, Q_n)\big)_n \\ &= e(v_1, w)e(v_2, w), \end{aligned}$$

en de tweede gaat op analoge manier. Het analogon van de derde formule staat niet vermeld in (6.2.1a) omdat die direct uit de eerste twee formules daar volgt, maar hier gaat het om $\mathbb{Z}_\ell$-lineariteit in plaats van $\mathbb{Z}$-lineariteit. We berekenen

$$\begin{aligned} e(av, bw) &= e\big((a_n P_n)_n, (b_n Q_n)_n\big) \\ &= \big(e_{l^n}(a_n P_n, b_n Q_n)\big)_n \\ &= \big(e_{l^n}(P_n, Q_n)^{a_n b_n}\big)_n \qquad \text{(6.2.1a)} \\ &= \big(e_{l^n}(P_n, Q_n)\big)_n^{\overline{(a_n b_n)_n}} \qquad \text{per definitie van de werking van } \mathbb{Z}_l \text{ op } T_l(\boldsymbol{\mu}) \\ &= e(v,w)^{ab}, \end{aligned}$$

zoals gewenst.

(b) De eerste formule volgt direct uit de analoge formule in (6.2.1b):

$$e(w,w) = (e_{\ell^n}(Q_n,Q_n))_n = (1)_n = 1.$$

Net als in (6.2.1b) volgt de tweede formule direct uit de eerste en uit bilineariteit.

(c) Zij $m \geq 0$ willekeurig, en zij $S \in E[\ell^m]$ willekeurig. Neem een element $u := (S_n)_n \in T_\ell(E)$ met $S_m = S$, zo'n element bestaat volgens (7.1.5). Bij aanname hebben we

$$(1)_n = e(u,v) = \big(e_{\ell^n}(S_n,P_n)\big)_n,$$

dus

$$1 = e_{\ell^m}(S_m,P_m) = e_{\ell^m}(S,P_m).$$

Omdat dit voor alle $S \in E[\ell^m]$ geldt, zegt (6.2.1c) dat $P_m = 0$. Dit geldt weer voor alle $m \geq 0$, dus $v = 0$. □

Gevolg 7.2.5. *Zij $v_1, v_2 \in T_l(E)$ en zij $a,b,c,d \in \mathbb{Z}_l$. Dan is*

$$e(av_1+bv_2, cv_1+dv_2) = e(v_1,v_2)^{ad-bc}.$$

Bewijs. Dit is een directe berekening:

$$\begin{aligned} e(av_1+bv_2,cv_1+dv_2) &= e(av_1,cv_1)e(av_1,dv_2)e(bv_2,cv_1)e(bv_2,dv_2) && \text{(7.2.4a)}\\ &= e(v_1,v_1)^{ac}e(v_1,v_2)^{ad}e(v_2,v_1)^{bc}e(v_2,v_2)^{bd} && \text{(7.2.4}a\text{)}\\ &= 1^{ac}\cdot e(v_1,v_2)^{ad}(e(v_1,v_2)^{-1})^{bc}\cdot 1^{bd} && \text{(7.2.4}b\text{)}\\ &= e(v_1,v_2)^{ad-bc}. \end{aligned}$$

De laatste gelijkheid volgt omdat de 'exponentiatie' eigenlijk de werking van $\mathbb{Z}_\ell$ voorstelt op het $\mathbb{Z}_\ell$-moduul $T_\ell(\boldsymbol{\mu})$. □

7.3 Isogenieën bestuderen via het Tatemoduul

Nu we een paar eigenschappen van de Weilparing op het Tatemoduul kennen, is de volgende stap om een verbinding te maken met isogeniën.

Als E_1, E_2 twee elliptische krommen zijn over K, en $\ell \neq \mathrm{char}K$ een priemgetal, dan geeft een isogenie $\varphi : E_1 \to E_2$ aanleiding tot een functie

$$\varphi_\ell : T_\ell(E_1) \to T_\ell(E_2) : \quad (P_n)_n \mapsto (\varphi(P_n))_n.$$

Het beeld van φ_ℓ ligt inderdaad in $T_\ell(E_2)$, want als $P_n \in E_1[\ell^n]$, dan is $\varphi(P_n) \in E_2[\ell^n]$, en

$$[\ell]\varphi(P_n) = \varphi([\ell]P_n) = \varphi(P_{n-1}).$$

Bovendien is φ_ℓ niet zomaar een functie, het is een homomorfisme van $\mathbb{Z}_\ell$-modulen, zoals een rechtstreekse berekening toont: voor $(\overline{x_n})_n \in \mathbb{Z}_\ell$ en $(P_n)_n, (Q_n)_n \in T_\ell(E_1)$ hebben we

$$\begin{aligned} \varphi_\ell\big((\overline{x_n})_n(P_n)_n + (Q_n)_n\big) &= \varphi_\ell\big((x_nP_n+Q_n)_n\big) = (\varphi(x_nP_n+Q_n))_n\\ &= (x_n\varphi(P_n)+\varphi(Q_n))_n = (\overline{x_n})_n\varphi_\ell((P_n)_n)+\varphi_\ell((Q_n)_n). \end{aligned}$$

Een net zo rechtstreekse berekening toont dat als $\psi : E_1 \to E_2$ en $\chi : E_2 \to E_3$ nog twee isogeniën zijn van elliptische krommen over K, dan is $(\psi+\varphi)_\ell = \varphi_\ell + \psi_\ell$, en $(\chi\circ\varphi)_\ell = \chi_\ell \circ \varphi_\ell$. We vatten deze observaties samen in

Feit 7.3.1. *Zij $\ell \neq \mathrm{char}K$ een priemgetal. We hebben een functor van de categorie van elliptische krommen over K met isogeniën naar de categorie van $\mathbb{Z}_\ell$-modulen, namelijk '$E \mapsto T_\ell(E)$' wat betreft objecten en '$\varphi \mapsto \varphi_\ell$' wat betreft morfismen. Bovendien is voor elk paar objecten E_1, E_2 in de eerste categorie, de afbeelding*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) : \quad \varphi \mapsto \varphi_\ell$$

een homomorfisme van abelse groepen. Indien $E_1 = E_2 =: E$, dan is deze afbeelding, die we dan schrijven als

$$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E)) : \quad \varphi \mapsto \varphi_\ell,$$

bovendien een ringhomomorfisme.

Net als de eerdere basiseigenschappen van de Weilparing, kan de eigenschap dat duale isogeniën geadjungeerd ten opzichte van de Weilparing op $E[\ell^n]$, direct vertaald worden naar de ℓ-adische context.

Stelling 7.3.2. *Als $\varphi : E_1 \to E_2$ en $\psi : E_2 \to E_1$ isogenieën zijn van elliptische krommen over K is, en als $v \in T_\ell(E_1)$ en $x \in T_\ell(E_2)$, dan hebben we*

$$e(v, (\varphi^t)_\ell x) = e(\varphi_\ell v, x),$$
$$e((\psi^t)_\ell v, x) = e(v, \psi_\ell x).$$

Hier is de linker 'e' de Weil-paring op $T_\ell(E_1)$, en de rechter die op $T_\ell(E_2)$.

Bewijs. We schrijven $x = (X_n)_n$. De eerste formule volgt rechtstreeks uit de analoge formule in (6.2.2):

$$\begin{aligned} e(v, (\varphi^t)_\ell x) = e\big((P_n)_n, (\varphi^t X_n)_n\big) &= \big(e_{\ell^n}(P_n, \varphi^t X_n)\big)_n \\ &= \big(e_{\ell^n}(\varphi P_n, X_n)\big)_n = e\big((\varphi P_n)_n, (X_n)_n\big) = e(\varphi_\ell v, x). \end{aligned}$$

De tweede formule volgt direct uit de eerste en omdat 'duale nemen' een involutie is, zie (6.3.3):

$$e((\psi^t)_\ell v, x) = e(v, ((\psi^t)^t)_\ell x) = e(v, \psi_\ell x). \qquad \square$$

We zagen in (7.1.7) dat $T_\ell(E)$ een vrij $\mathbb{Z}_\ell$-moduul van rang 2 is. Dat stelt ons in staat lineaire algebra toe te passen. We hebben bijvoorbeeld groepshomomorfismen $\det : \mathrm{End}(T_\ell(E))^* \to \mathbb{Z}_\ell^*$ en $\mathrm{tr} : \mathrm{End}(T_\ell(E)) \to \mathbb{Z}_\ell$. Expliciet kunnen we determinant en spoor van een element $\sigma \in \mathrm{End}(T_\ell(E))$ berekenen door een $\mathbb{Z}_\ell$-basis van $T_\ell(E)$ te kiezen en σ als matrix ten opzichte van deze basis te representeren. Uiteraard zijn determinant en spoor onafhankelijk van de keuze van de basis.

Voorbeeld 7.3.3. Zij E/K een elliptische kromme, $\ell \neq \mathrm{char}K$ een priemgetal, en $m \in \mathbb{Z}$, en beschouw het isogenie $[m] \in \mathrm{End}(E)$. Dan is $[m]_\ell(P_n)_n = ([m]P_n)_n = m(P_n)_n$, voor $(P_n)_n \in T_\ell(E)$. Met andere woorden, de geïnduceerde afbeelding $[m]_\ell \in \mathrm{End}(T_\ell(E))$ wordt gegeven door

$$[m]_\ell x = mx,$$

voor $x \in T_\ell(E)$. Er volgt dat als $\{v, w\}$ een basis is van $T_\ell(E)$ over $\mathbb{Z}_\ell$, dan is de matrix van $[m]_\ell$ ten opzichte van deze basis gelijk aan

$$\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) \subset \mathrm{Mat}_2(\mathbb{Z}_\ell).$$

In het bijzonder is $\det[m]_\ell = m^2 = \deg[m]$.

Het resultaat van (7.3.3) is een bijzonder geval van de volgende stelling. De stelling speelt een hoofdrol in ons bewijs van pERH in het volgende hoofdstuk, doordat het ons in staat stelt om lastige vragen over isogeniën te vertalen naar eenvoudige lineaire algebra.

Stelling 7.3.4. *Zij E/K een elliptische kromme en $\ell \neq \mathrm{char}K$ een priemgetal. Als $\varphi \in \mathrm{End}(E)$ een isogenie is, en $\varphi_\ell \in \mathrm{End}(T_\ell(E))$ de geïnduceerde afbeelding op het Tate-moduul, dan is*

$$\det(\varphi_\ell) = \deg(\varphi).$$

In het bijzonder ligt $\det(\varphi_\ell)$ *niet alleen in $\mathbb{Z}_\ell$ maar zelfs in $\mathbb{Z}$, en is zijn waarde onafhankelijk van de keuze van ℓ.*

Bewijs. Neem een basis $\{v_1, v_2\}$ van $T_\ell(E)$ als $\mathbb{Z}_\ell$-moduul, zo'n basis bestaat volgens (7.1.7). Zij

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$$

de matrix van φ_ℓ ten opzichte van deze basis, dat wil zeggen, de ℓ-adische getallen $a, b, c, d \in \mathbb{Z}_\ell$ zijn zo dat $\varphi_\ell(v_1) = av_1 + bv_2$ en $\varphi_\ell(v_2) = cv_1 + dv_2$. Een berekening toont dat het element $e(v_1, v_2)$ van het $\mathbb{Z}_\ell$-moduul $T_\ell(\boldsymbol{\mu})$, hetzelfde beeld heeft onder de werking van $\deg\varphi \in \mathbb{Z} \subset \mathbb{Z}_\ell$ als onder die van $\det\varphi_\ell \in \mathbb{Z}_\ell$:

$$\begin{aligned}
e(v_1, v_2)^{\deg\varphi} &= e((\deg\varphi)v_1, v_2) && \text{(7.2.4a)}\\
&= e([\deg\varphi]_\ell v_1, v_2) && \text{(7.3.3)}\\
&= e((\varphi^t\varphi)_\ell v_1, v_2) && \text{(5.5.2)}\\
&= e((\varphi^t)_\ell \varphi_\ell v_1, v_2) && \text{(7.3.1)}\\
&= e(\varphi_\ell v_1, \varphi_\ell v_2) && \text{(7.3.2)}\\
&= e(av_1 + bv_2, cv_1 + dv_2)\\
&= e(v_1, v_2)^{ad-bc} && \text{(7.2.5)}\\
&= e(v_1, v_2)^{\det\varphi_\ell}.
\end{aligned}$$

Vanwege $\mathbb{Z}_\ell$-lineariteit (7.2.4a), betekent dit dat

$$e((\deg\varphi - \det\varphi_\ell)v_1, v_2) = e(v_1, v_2)^{\deg\varphi - \det\varphi_\ell} = 1. \tag{7.1}$$

We laten zien dat dit laatste ook geldt met een willekeurige $w \in T_\ell(E)$ gesubstitueerd voor v_2, zeg $w = \alpha v_1 + \beta v_2$ met $\alpha, \beta \in \mathbb{Z}_\ell$. Namelijk,

$$\begin{aligned}
e((\deg\varphi - \det\varphi_l)v_1, w) &= e((\deg\varphi - \det\varphi_l)v_1, \alpha v_1 + \beta v_2)\\
&= e(v_1, v_1)^{(\deg\varphi - \det\varphi_l)\alpha} e((\deg\varphi - \det\varphi_l)v_1, v_2)^{\beta} && \text{(7.2.4}a\text{)}\\
&= 1. && \text{(7.2.4}b\text{), (7.1)}
\end{aligned}$$

Omdat dit voor alle $w \in T_\ell(E)$ geldt, vertelt (7.2.4c) dat $(\deg\varphi - \det\varphi_\ell)v_1 = 0$. Omdat $\{v_1, v_2\}$ een $\mathbb{Z}_\ell$-basis is, volgt dat $\deg\varphi - \det\varphi_\ell = 0$. □

Hoofdstuk 8

De Riemann-hypothese voor elliptische krommen over $\mathbb{F}_q$

We fixeren in dit hoofdstuk deze notatie:
p is een priemgetal,
q is een macht van p,
$\mathbb{F}_q$ is het lichaam met q elementen,
$\mathbb{F}_q^c$ is een algebraïsche afsluiting van $\mathbb{F}_q$,
(E, O) is een elliptische kromme over $\mathbb{F}_q$ gegeven door een Weierstrass-vergelijking,
$\pi \in \mathrm{End}(E)$ is het q-de machts Frobenius-endomorfisme,
ℓ is een priemgetal ongelijk aan p.

Het materiaal van de vorige hoofdstukken culmineert hier in een bewijs van de pERH, de hoofdstelling van dit werkstuk. De strategie is om steeds verdere formules voor $\#E(\mathbb{F}_{q^n})$ af te leiden, totdat we een formule hebben die direct vertaalt naar de gewenste formule voor de Zeta-functie. Concreet gesproken, de reeks van formules die we bewijzen is

$$\begin{aligned} \#E(\mathbb{F}_q) &= \deg([1] - \pi) && (8.1)\\ &= \det(1 - \pi_\ell) && (8.2)\\ &= 1 - \mathrm{tr}(\pi_\ell) + \det(\pi_\ell) && (8.3)\\ &= 1 - a + q && (8.4)\\ &= (1-\alpha)(1-\beta) = q + 1 - \alpha - \beta, && (8.5) \end{aligned}$$

waarbij $\pi \in \mathrm{End}(E)$ het q-de machts Frobenius-morfisme is, a een zeker geheel getal, en α, β zekere complex geconjungeerde getallen met modulus $\sqrt{q}$. (Zie de tekst voor verdere notatie en details.) Kortom, we vertalen het naar een probleem (8.1) over de graad van een isogenie, en dit pakken we aan door de betrokken isogeniën te bestuderen via de afbeeldingen van Tatemodulen die zij induceren (8.2), zodat we lineaire algebra, specifiek karakteristieke polynomen, kunnen gebruiken (8.3). Met behulp van onze kennis van het Frobenius-endomorfisme laten we zien (8.4) dat de ℓ-adische getallen $\mathrm{tr}(\pi_\ell)$ en $\det(\pi_\ell)$ in feite geheel zijn, en onafhankelijk van ℓ. Een slimme truc levert de factorisatie (8.5). We hebben dan formules voor alle $\#E(\mathbb{F}_{q^n})$, want q^n is ook een macht van p, en met hulp van lineaire algebra schrijven deze formules in termen van α en β.

8.1 Bewijs van de pERH

De eerste stap is dus het herschrijven van $\#E(\mathbb{F}_q)$ als in

Stelling 8.1.1. *Er geldt*

$$\#E(\mathbb{F}_q) = \deg([1] - \pi).$$

Bewijs. De elementen van $\mathbb{F}_q$ zijn precies de nulpunten in $\mathbb{F}_q^c$ van het polynoom $T^q - T$; kortom, voor $x \in \mathbb{F}_q^c$ geldt

$$x^q = x \iff x \in \mathbb{F}_q. \tag{8.6}$$

Dit gebruiken we om te zien dat voor punten $P \in E - \{O\}$, zeg $P = (x, y)$ in affiene notatie, de volgende beweringen equivalent zijn:

$$\begin{aligned} &P \in \ker([1] - \pi), \\ &(x^q, y^q) = (x, y), \\ &x \in \mathbb{F}_q \quad \text{en} \quad y \in \mathbb{F}_q, \\ &P \in E(\mathbb{F}_q). \end{aligned}$$

Verder, het punt O ligt zowel in $\ker([1] - \pi)$ als in $E(\mathbb{F}_q)$. Conclusie:

$$E(\mathbb{F}_q) = \ker([1] - \pi).$$

Omdat $1 \not\equiv 0 \pmod{p}$, vertelt (5.4.3) dat $[1] - \pi$ een separabel isogenie is, en dan zegt (4.1.3) dat

$$\#\ker([1] - \pi) = \deg([1] - \pi).$$

Dit voltooit het bewijs. □

Als M een vrij R-moduul van dimensie twee is, met R een ring, dan is het karakteristiek polynoom van een R-moduul-endomorfimse $m \in \mathrm{End}(M)$ gelijk aan

$$\det(T - m) = T^2 - \mathrm{tr}(m)T + \det(m). \tag{8.7}$$

Dit is uiteraard een bijzonder geval ('$n = 2$') van een bekende formule, en volgt direct door een basis van M te kiezen en m ten opzichte daarvan als 2×2-matrix te schrijven. Door $T = 1$ te substitueren, krijgen we de formule

$$\mathrm{tr}(m) = 1 + \det(m) - \det(1 - m). \tag{8.8}$$

Dit passen we toe op onze situatie.

Propositie 8.1.2. *Het karakteristiek polynoom van $\pi_\ell \in \mathrm{End}(T_\ell(E))$ is*

$$\begin{aligned} \det(T - \pi_\ell) &= T^2 - \mathrm{tr}(\pi_\ell)T + \det(\pi_\ell) \\ &= T^2 - aT + q, \end{aligned}$$

waarbij

$$a := q + 1 - \#E(\mathbb{F}_q). \tag{8.9}$$

Bewijs. De eerste gelijkheid is een speciaal geval van (8.7). Om de tweede gelijkheid te krijgen, merken we op dat

$$\det(\pi_\ell) = \deg(\pi) = q,$$

zie (7.3.4) en (4.1.3b), en dat

$$\begin{aligned} \mathrm{tr}(\pi_\ell) &= 1 + \det(\pi_\ell) - \det(1 - \pi_\ell) && \text{zie (8.8)} \\ &= 1 + \deg(\pi) - \deg([1] - \pi) && (7.3.4, 7.3.1) \\ &= 1 + q - \#E(\mathbb{F}_q) = a && (4.1.3b, 8.1.1). \end{aligned}$$ □

Merk op dat $T = 1$ substitueren in (8.1.2) de formules (8.3) en (8.4) leveren.

Met de resultaten die we hebben, is het bewijs van de pERH niet moeilijk meer. De daadwerkelijke Riemann-hypothese is de combinatie van (b) en (d) in de volgende Stelling. We leiden hem af uit (a); omgekeerd volgt overigens eenvoudig (a) uit (b).

Definitie 8.1.3. Zij $V/\mathbb{F}_q$ een projectieve variëteit. De *Zetafunctie* van V is de formele machtreeks

$$Z(V,T) = \exp\big(\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n})\frac{T^n}{n}\big) \in \mathbb{Q}[[T]].$$

Stelling 8.1.4 (Hasse [Has36])**.** *Zij $\alpha, \beta \in \overline{\mathbb{Q}}$ de nulpunten van het polynoom $T^2 - aT + q \in \mathbb{Z}[T]$, waarbij $a \in \mathbb{Z}$ het 'spoor van Frobenius' is zoals in* (8.9)*. Dan is het volgende waar.*

(a) Voor alle $n \geq 1$ is

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

(b) 'Expliciete formule voor de Zeta-functie':

$$Z(E,T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.$$

(c) 'Functionaalvergelijking':

$$Z(E, \frac{1}{qT}) = Z(E,T).$$

(d) 'Riemann-hypothese voor E':

$$|\alpha| = \sqrt{q} = |\beta|.$$

Opmerking 8.1.5. We hebben zoals gebruikelijk $\overline{\mathbb{Q}}$ geschreven voor een algebraïsche afsluiting van $\mathbb{Q}$. De voor de hand liggende interpretatie, die we in (d) inderdaad hebben gebruikt, is om $\overline{\mathbb{Q}}$ als deellichaam van $\mathbb{C}$ op te vatten, zodat we een beroep kunnen doen op de modulus-functie op $\mathbb{C}$, en complexe conjugatie. We willen echter benadrukken dat α en β al in $\overline{\mathbb{Q}}$ liggen, zodat we ze ook kunnen opvatten als elementen van de algebraïsche afsluiting $\overline{\mathbb{Q}_\ell}$ van het quotiëntenlichaam $\mathbb{Q}_\ell$ van $\mathbb{Z}_\ell$.

Bewijs (van 8.1.4). (a) We kunnen (8.1.1) toepassen op q^n in plaats van q; het bijbehorende q^n-de machts Frobenius-endomorfisme is $\pi^n \in \mathrm{End}(E)$ in plaats van π. Kortom,

$$\#E(\mathbb{F}_{q^n}) = \det(1 - \pi_\ell^n). \tag{8.10}$$

Kies een basis van $T_\ell(E)$ en zij $A \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$ de matrix van π_ℓ ten opzichte van deze basis. We kunnen A als element van $\mathrm{Mat}_2(\overline{\mathbb{Q}_\ell})$ beschouwen. In deze grotere matrixring kunnen we A in

Jordan-normaalvorm zetten, omdat $\overline{\mathbb{Q}_\ell}$ algebraïsch afgesloten is (zie bijv. [Lan02, XIV.2.2.5]): er is een $B \in \mathrm{Mat}_2(\overline{\mathbb{Q}_\ell})$ zo dat $J := BAB^{-1}$ onderdriehoeksvorm heeft, zeg

$$J = \begin{pmatrix} x & 0 \\ \cdot & y \end{pmatrix}.$$

voor nader te bepalen $x, y \in \overline{\mathbb{Q}_\ell}$. We hebben

$$(T-x)(T-y) = \det(T-J) = \det(T-A) = \det(T-\pi_\ell) = (T-\alpha)(T-\beta).$$

We hebben $\alpha, \beta \in \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}_\ell}$; er staan dus twee ontbindingen over $\overline{\mathbb{Q}_\ell}$. Er volgt

$$x = \alpha \quad \text{en} \quad y = \beta \quad \text{of andersom.}$$

We concluderen dat

$$\det(T-\pi_\ell^n) = \det(T-A^n) = \det(T-J^n) = (T-\alpha^n)(T-\beta^n).$$

Als we dit invullen in (8.10), en opmerken dat (8.11) impliceert dat $\alpha\beta = q$, krijgen we

$$\#E(\mathbb{F}_{q^n}) = (1-\alpha^n)(1-\beta^n) = q^n + 1 - \alpha^n - \beta^n.$$

(b) Het resultaat van (a) invullen in de definitie van $Z(E,T)$, levert

$$\begin{aligned}
\log Z(E,T) &= \sum_{n=1}^{\infty} \frac{(q^n + 1 - \alpha^n - \beta^n)T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(qT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{n=1}^{\infty} \frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty} \frac{(\beta T)^n}{n} \\
&= -\log(1-qT) - \log(1-T) + \log(1-\alpha T) + \log(1-\beta T) \\
&= \log \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.
\end{aligned}$$

De formule volgt door van beide kanten ‘exp’ te nemen.

(c) We gebruiken (b) om te berekenen

$$\begin{aligned}
Z(E, \frac{1}{qT}) &= \frac{1 - \frac{a}{qT} + \frac{1}{qT^2}}{(1-\frac{1}{qT})(1-\frac{1}{T})} \\
&= \frac{qT^2 - aT + 1}{(qT-1)(T-1)} = Z(E,T).
\end{aligned}$$

(d) Vanwege (8.1.2), en per definitie van α, β, hebben we

$$\det(T-\pi_\ell) = T^2 - aT + q = (T-\alpha)(T-\beta). \tag{8.11}$$

Merk op dat het polynoom $\det(T-\pi_\ell)$ in eerste instantie in $\mathbb{Z}_\ell[T]$ ligt, maar omdat het zelfs in $\mathbb{Z}[T]$ ligt, kunnen we het ontbinden in $\mathbb{C}[T]$ zoals rechts. Bovendien, omdat de coëfficiënten van $T^2 - aT + q$ geheel zijn (reëel is al voldoende), zijn α en β complex geconjugeerd, of ze zijn beide reëel.

Zij $j, k \in \mathbb{Z}$ met $k \neq 0$. We hebben $\mathrm{tr}(\pi_\ell) = a$ en $\det(\pi_\ell) = q$, zie (8.1.2). Omdat 'het spoor nemen' additief is, hebben we

$$\mathrm{tr}(k\pi_\ell) = ka,$$

en omdat $T_\ell(E)$ rang 2 heeft over $\mathbb{Z}_\ell$, hebben we

$$\det(k\pi_\ell) = k^2 q.$$

Substitueren we $T = j/k$ in de rechter gelijkheid in (8.11), die simpelweg een gelijkheid van polynomen in $\mathbb{C}[T]$ is, dan vinden we zodoende dat

$$\begin{aligned}
(\frac{j}{k} - \alpha)(\frac{j}{k} - \beta) &= \frac{j^2 - kaj + k^2 q}{k^2} \\
&= \frac{j^2 - \mathrm{tr}(k\pi_l)j + \det(k\pi_l)}{k^2} \\
&= \frac{\det(j - k\pi_l)}{k^2} && \text{zie (8.7)} \\
&= \frac{\deg([j] - [k]\pi)}{k^2} && \text{zie (7.3.4)} \\
&> 0.
\end{aligned}$$

(De substitutie van j in (8.7) wordt gerechtvaardigd doordat $j \in \mathbb{Z} \subset \mathbb{Z}_\ell$.) Er volgt dat als α en β beide reëel zijn, dan is $\alpha = \beta$, want anders zou er een rationaal getal j/k bestaan die strikt tussen α en β ligt, en dan zou $(j/k - \alpha)(j/k - \beta) < 0$. We concluderen dat hoe dan ook $\beta = \overline{\alpha}$. Uit (8.11) lezen we af dat $\alpha\overline{\alpha} = \alpha\beta = q$, dus we hebben $|\alpha| = \sqrt{q}$. □

Opmerking 8.1.6. We hebben in dit hoofdstuk verondersteld dat E gegeven wordt door een elliptische kromme gegeven door een Weierstrass-vergelijking, zodat we weten dat het q-de machts Frobenius-morfisme op E een isogenie is. Er volgt echter dat (8.1.4) waar is voor elke elliptische kromme $E'/\mathbb{F}_q$. Namelijk, volgens (3.3.1c) is er een isomorfisme $\varphi : E' \to E$ naar een elliptische kromme gegeven door een Weierstrass-vergelijking, en volgens (2.1.10) induceert φ voor elke $n \geq 0$ een bijectie $E'(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$, dus $\#E'(\mathbb{F}_{q^n}) = \#E(\mathbb{F}_{q^n})$.

8.2 Voorbeelden, consequenties en generalisaties

De volgende afschatting wordt wel eens de stelling van Hasse genoemd:

Gevolg 8.2.1.

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Bewijs. Dit volgt direct uit (8.1.4ad). □

De 'fout' $2\sqrt{q}$ gaat redelijk snel naar nul ten opzichte van q, als $q \to \infty$.

We illustreren met twee voorbeelden hoe eenvoudig het is om in concrete gevallen formules op te schrijven voor $\#E(\mathbb{F}_{q^n})$.

Voorbeeld 8.2.2. Zij $C/\mathbb{F}_3$ de elliptische kromme die we al vaker bestudeerd hebben:

$$C: \quad Y^2 = X^3 + X + 1.$$

In (2.1.2) hebben we berekend dat $C(\mathbb{F}_3) = \{(0,1), (0,-1), (1,0), O\}$. Op dezelfde manier berekenen we $C(\mathbb{F}_9)$. Het lichaam $\mathbb{F}_9$ bestaat uit de nulpunten in $\mathbb{F}_3^c$ van $X^9 - X = X(X-1)(X+$

$1)(X^2+1)(X^4+1)$. Als j een nulpunt is van X^2+1, dan hebben we reeds $\mathbb{F}_9 = \mathbb{F}_3[j]$, want $\mathbb{F}_9$ heeft graad 2 over $\mathbb{F}_3$. De negen mogelijkheden voor $x = a + bj$ substitueren in $X^3 + X + 1$, en kijken of dit een kwadraat is, levert de lijst

$$\begin{aligned} C(\mathbb{F}_9) =&\{(-1-j,\pm j),(-1+j,\pm j),(-1,\pm j),(-j,\pm 1),(j,\pm 1),(0,\pm 1),\\ &(1,0),(1-j,0),(1+j,0),O\}. \end{aligned}$$

In het bijzonder hebben we $\#C(\mathbb{F}_3) = 4$ en $\#C(\mathbb{F}_9) = 16$. Voor grotere machten 3^n wordt een dergelijke berekening van $C(\mathbb{F}_{3^n})$ al snel tijdrovend. De Riemann-hypothese geeft echter een formule voor het aantal punten hierin. Namelijk, vanwege (8.1.4ad) met $n = 1$, hebben we

$$4 = \#C(\mathbb{F}_3) = 3 + 1 - \alpha - \beta,$$

dus $\alpha = -\beta$, zodat $-\alpha^2 = \alpha\beta = 3$, kortom $\alpha = \pm\sqrt{3}i$. Zodoende leest de formule (8.1.4a) in dit geval

$$\#C(\mathbb{F}_{3^n}) = 3^n + 1 - (\sqrt{3}i)^n - (-\sqrt{3}i)^n = \begin{cases} 3^n + 1 & \text{als } n \text{ oneven,} \\ (3^{n/2}+1)^2 & \text{als } n \equiv 2 \pmod 4, \\ (3^{n/2}-1)^2 & \text{als } n \equiv 0 \pmod 4. \end{cases}$$

De rij $(\#C(\mathbb{F}_{3^n}))_{n\geq 1}$ begint dus als $(4, 16, 28, 64, 244, 784, 2188, 6400, \ldots)$. Als $m|n$, dan is $\mathbb{F}_{3^m}$ deellichaam van $\mathbb{F}_{3^n}$ en dus $C(\mathbb{F}_{3^m})$ ondergroep van $C(\mathbb{F}_{3^n})$, en de expliciete formules hierboven bevestigen dat dan inderdaad $\#C(\mathbb{F}_{3^m})$ deler is van $\#C(\mathbb{F}_{3^n})$.

Voorbeeld 8.2.3. Beschouw de elliptische kromme

$$E: \quad Y^2 - Y = X^3 - X^2$$

over $\mathbb{F}_2$. Het is duidelijk dat $E(\mathbb{F}_2) = \mathbb{P}^2_{\mathbb{F}_2}$, kortom $\#E(\mathbb{F}_2) = 5$. We hebben

$$5 = \#E(\mathbb{F}_2) = 2 + 1 - \alpha - \beta,$$

dus naast $\alpha\beta = 2$ hebben we $\alpha + \beta = -2$, zodat $\alpha = -1 + i$ of $\alpha = -1 - i$, laten we zeggen $\alpha = -1 + i$ (wegens symmetrie maakt de keuze niet uit). Omdat α en β complex geconjugeerd zijn, zegt (8.1.4a) dat $\#E(\mathbb{F}_{q^n}) = q^n + 1 - 2\mathrm{Re}(\alpha^n)$. We hebben, als we $n = 2m + r$ schrijven met $r = 0, 1$,

$$\alpha^n = \alpha^{2m}\alpha^r = (-2i)^m(-1+i)^r.$$

Dus als n even is, dan is $\mathrm{Re}(\alpha^n) = 0$, en als $n = 2m+1$ oneven is, dan is $\alpha^n = 2^m(-i)^m(-1+i)$. We concluderen dat

$$\#E(\mathbb{F}_{2^n}) = 2^n + 1 - 2\mathrm{Re}(\alpha^n) = \begin{cases} 2^n + 1 & \text{als } n \text{ even,} \\ 2^n + 1 + 2^{\frac{n+1}{2}} & \text{als } n \equiv \pm 1 \pmod 8, \\ 2^n + 1 - 2^{\frac{n+1}{2}} & \text{als } n \equiv \pm 3 \pmod 8. \end{cases}$$

Tot slot geven we wat achtergrond over pERH. Het is niet meteen duidelijk uit (8.1.4) waar de naam Riemann-hypothese vandaan komt. Het wordt duidelijker als we in de formules q^{-S} substitueren voor T. We schrijven $\zeta_E(S) := Z(E, q^{-S})$. De expliciete formule in (b) luidt dan

$$\zeta_E(S) = \frac{1 - aq^{-S} + q^{1-2S}}{(1-q^{-S})(1-q^{1-S})} = \frac{(1-\alpha q^{-S})(1-\beta q^{-S})}{(1-q^{-S})(1-q^{1-S})}. \tag{8.12}$$

De functionaalvergelijking vertaalt naar de identiteit $\zeta_E(S) = \zeta_E(1-S)$:

$$\zeta_E(1-S) = \frac{1 - aq^{S-1} + q^{2S-1}}{(1-q^{S-1})(1-q^S)} = \frac{q^{1-2S} - aq^{-S} + 1}{(q^{1-S}-1)(q^{-S}-1)} = \zeta_E(S),$$

waarbij we voor de tweede gelijkheid teller en noemer met $q^{1-2S} = q^{1-S}q^{-S}$ hebben vermenigvuldigd. Dit is analoog aan de functionaalvergelijking voor de klassieke Riemann-zetafunctie. Bovendien kunnen we ζ_E opvatten als holomorfe functie op het deel van $\mathbb{C}$ waar de noemer niet nul is, dat wil zeggen, als functie

$$\zeta_E : \quad U := \mathbb{C} - \Big(\frac{2\pi i}{\log q}\mathbb{Z} \ \cup \ (1 + \frac{2\pi i}{\log q})\mathbb{Z} \Big) \ \longrightarrow \ \mathbb{C}.$$

Als $s \in U$ een nulpunt is van ζ_E, dan zegt (8.12) dat $q^{-s} = \alpha^{-1}$ of $q^{-s} = \beta^{-1}$. Omdat $|\alpha| = \sqrt{q} = |\beta|$, betekent dit dat

$$q^{\mathrm{Re}(-s)} = |q^{-s}| = |\alpha|^{-1} = q^{-1/2},$$

dus $\mathrm{Re}(s) = 1/2$. Dit is analoog aan de klassieke Riemann-hypothese.

Dit zijn niet slechts formele gelijkenissen. Er is namelijk een vermoeden, die we hier de ARH noemen (A voor aritmetisch), waarvan zowel de KRH als de pERH een speciaal geval zijn. Dit wordt wel de 'Riemann-hypothese voor de aritmetische zeta-functie van een regulier, samenhangend, equidimensionaal aritmetisch schema' genoemd. Wegens gebrek aan tijd en ruimte, gaan we hier niet op in. Wel willen we wat zeggen over de in de inleiding van dit werkstuk al genoemde pRH, die wat algemeenheid betreft 'tussen' de pERH en de ARH in zit. In plaats van elliptische krommen over eindige lichamen, gaat de pRH over willekeurige projectieve variëteiten over eindige lichamen. Het is onderdeel van de inmiddels bewezen Weil-vermoedens, in 1949 opgesteld door André Weil.

Stelling 8.2.4 (Weil-vermoedens)**.** *Zij $V/\mathbb{F}_q$ een projectieve variëteit van dimensie n.*

(b) 'Expliciete formule voor de Zeta-functie': Er zijn polynomen $P_i \in \mathbb{Z}[T]$, met $i = 1, \ldots, 2n$, zo dat

$$Z(V,T) = \frac{P_1 P_3 \cdots P_{2n-1}}{P_0 P_2 \cdots P_{2n}}.$$

Bovendien is $P_0 = 1 - T$ en $P_{2n} = 1 - q^n T$, en voor elke i is er een geheel getal b_i en complexe getallen $\alpha_{ij} \in \overline{\mathbb{Q}}$ zo dat

$$P_i = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T).$$

(c) 'Functionaalvergelijking': er is een geheel getal ε zo dat

$$Z(V, \frac{1}{q^n T}) = \pm q^{\varepsilon n/2}\, T^{\varepsilon}\, Z(V,T).$$

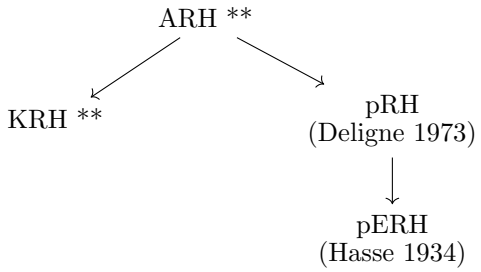
(d) 'Riemann-hypothese voor V', "pRH": Voor de complexe getallen α_{ij} zoals in (b) geldt

$$|\alpha_{ij}| = \sqrt{q}.$$

Opmerking 8.2.5. Hoewel we in (8.2.4) geen analogon van (8.1.4a) hebben vermeld, is het duidelijk dat uit de expliciete formule (b) een formule voor $\#V(\mathbb{F}_{q^n})$ af te leiden is in termen van de α_{ij}. Bovendien, als we $\#V(\mathbb{F}_{q^n})$ berekenen door bijvoorbeeld $V(\mathbb{F}_{q^n})$ expliciet op te schrijven, krijgen we een polynomiale vergelijking in de α_{ij}, en het lijkt me plausibel (maar ik ben het niet nagegaan) dat door eindig veel van de $\#V(\mathbb{F}_{q^n})$ te berekenen, zodoende de α_{ij} kunnen worden bepaald.

Hasse [Has36] bewees in 1934 de Weil-vermoedens (die toen nog niet waren geformuleerd) voor elliptische krommen, dat wil zeggen, pERH. Toen Weil [Wei49] de vermoedens in 1949 formuleerde, bewees hij ze voor projectieve krommen en abelse variëteiten. (We definiëren niet wat abelse variëteiten zijn, maar elliptische krommen vallen hieronder.) Grothendieck en anderen ontwikkelden de leer van ℓ-adische cohomologie, en bewezen daarmee de functionaalvergelijking. Voortbouwend op deze theorie van ℓ-adische cohomologie, bewees Deligne [Del74] in 1973 de Riemann-hypothese, dat wil zeggen (8.2.4bd). In 2013 won Deligne de Abelprijs, met name voor dit werk.

Voor de overzichtelijkheid zetten we de verschillende vormen van de Riemann-hypothese die we hebben benoemd, in een plaatje. Pijlen geven implicaties aan, asterisken een onopgelost vermoeden.



De waarheid van de pRH heeft geen enkele implicatie voor de waarheid van de KRH, en er lijkt ook geen manier te zijn om een bewijs van de pRH om te vormen zodat het iets zinnigs zegt over de KRH. Er is geen aanwijzing dat er een bewijs van de KRH (of ARH) in de lucht hangt, ook al vinden belangrijke ontwikkelingen op deze gebieden plaats.

Bibliografie

[Arm87] M.A. Armstrong. *Groups and Symmetry.* Springer, 1987.

[Del74] Pierre Deligne. La conjecture de Weil: I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974.

[Eis04] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in GTM. Springer, 2004.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Number 52 in GTM. Springer, 1977.

[Has36] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper; I, II & III. *Crelle's Journal*, 175, 1936.

[Kem11] Gregor Kemper. *A Course in Commutative Algebra.* Number 256 in GTM. Springer, 2011.

[Lan02] Serge Lang. *Algebra.* Number 211 in GTM. Springer, revised third edition, 2002.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Number 106 in GTM. Springer, 2nd edition, 2009.

[Ste15] Peter Stevenhagen. Algebra III. dictaat Universiteit Leiden, Te downloaden van websites.math.leidenuniv.nl/algebra, 2015.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.