Gehele punten onder een groepswerking

Zij L een algebraïsch afgesloten lichaam met $\mathrm{char}(L) \neq 2, 3$. Beschouw de kromme in $L \times L$ gegeven door:

$$(*) \qquad y^2 = 4x^3 - Ax - B\,.$$

Hierbij zijn A, B elementen van L die voldoen aan $\Delta = \Delta(A, B) = A^3 - 27B^2 \neq 0$ (wat betekent deze voorwaarde meetkundig?). Krommen van het type (*) worden veelvuldig bestudeerd in de wiskunde (zie bijvoorbeeld [2]) aangezien hun projectieve afsluiting voorzien kan worden van de structuur van een commutatieve groepvariëteit (een elliptische kromme). Deze structuur vormt de basis van enkele tegenwoordig veelvuldig toegepaste cryptografische protocollen.

Onder een coördinatentransformatie $x \mapsto u^2x, y \mapsto u^3y$ (met $0 \neq u \in L$) gaat de kromme (*) over in:

$$y^2 = 4x^3 - A'x - B'\,,$$

waarbij $A' = u^{-4}A, B' = u^{-6}B$. We zien hierin terug een linkswerking van L^* op $L \times L$ gegeven door $u \cdot (A, B) = (u^{-4}A, u^{-6}B)$. Het is nu niet moeilijk om functies te maken die invariant zijn op een baan onder L^*; een gebruikelijke functie is bijvoorbeeld:

$$j = j(A, B) = 1728 \cdot \frac{A^3}{A^3 - 27B^2}\,.$$

Men gaat eenvoudig na dat $j(A, B) = j(A', B') \Leftrightarrow A = u^4A', B = u^6B'$ voor zekere $u \in L^*$. Met andere woorden, de j-invariant geeft een bijectie

$$L^* \setminus \{(A, B) \in L \times L \,:\, \Delta \neq 0\} \xrightarrow{\sim} L$$

en helpt ons om bovenstaande banenverzameling in kaart te brengen, dat wil zeggen om krommen van de vorm (*) te classificeren.

Laat nu $K \subset L$ een deellichaam zijn, en stel nu eens dat we gegeven een $j \in L$, een kromme van de vorm (*) met j-invariant j willen construeren. Dit is niet zo moeilijk; maar we willen dit op een zuinige manier doen. Ook dat is niet lastig: we kunnen A, B vinden met $j(A, B) = j$ en zodat $K(j) = K(A, B)$.

Iets subtieler wordt het wanneer we K vervangen door een deelring R van L. Neem $j \in L$; is het dan mogelijk om A, B te vinden met $j(A, B) = j$ en $R[j, A, B]$ eindig van kleine 'graad' over $R[j]$? Met de zogenaamde λ-invariant kan hier een bevestigend antwoord worden gegeven. Een scherpere benadering is te vinden in [1] voor $R = \mathbb{Z}$ en $L = \mathbb{C}$. Probeer dit bewijs, dat van aardig wat complex analytische middelen gebruik maakt, te begrijpen. Kan het bewijs meer "algebraïsch" worden gemaakt ? Wat gebeurt er als we de voorwaarde $\mathrm{char}(L) \neq 2, 3$ weglaten ?

Literatuur

[1] J. Guàrdia, *Jacobi Thetanullwerte, periods of elliptic curves and minimal equations*, Mathematical Research Letters **11** (2004), pp. 115–123. (Online verkrijgbaar)
[2] J. Silverman, *The arithmetic of elliptic curves.* Graduate texts in Mathematics **106**, Springer-Verlag.

Begeleider: R.S. de Jong.