Gehele punten onder een groepswerking

Zij $K \subset L$ een lichaamsuitbreiding met L algebraïsch afgesloten en zij $R \subset K$ een deelring. Zij G een groep met een linkse werking van G op $L \times L \times \cdots \times L = L^n$. Het zou interessant zijn om iets algemeens te zeggen over de volgende kwestie: gegeven een punt $\mathbf{x} \in L^n$, wanneer is $G \cdot \mathbf{x} \cap R^n \neq \varnothing$?
Denk hierbij eens aan het volgende voorbeeld (zie [2]). Veronderstel $\mathrm{char}(K) \neq 2, 3$ en bekijk de kromme in $L \times L$ gegeven door

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

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

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

waarbij $A' = u^{-4}A, B' = u^{-6}B$. Hierbij hoort de linkse werking van L^* op $L \times L$ gegeven door $u \cdot (A, B) = (u^{-4}A, u^{-6}B)$. Het is niet moeilijk om functies te maken die invariant zijn op een baan onder L^*; gebruikelijk is bijvoorbeeld

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

zolang $A^3 - 27B^2 \neq 0$. Het belang van deze functie ligt in het feit dat $j(A, B) = j(A', B') \Leftrightarrow A = u^4 A', B = u^6 B'$ voor zekere $u \in L^*$. Met andere woorden, de j-invariant geeft een bijectie

$$L^* \setminus \{(A, B) \in L \times L \,:\, A^3 - 27B^2 \neq 0\} \xrightarrow{\sim} L$$

en levert dus een goed kenmerk om bovenstaande banenverzameling in kaart te brengen, en dus om krommen van de vorm (*) te classificeren.
Echter, merk op dat in het algemeen de lichaamsuitbreiding

$$K(j) \subset K(A, B)$$

enorm kan variëren als (A, B) door een baan onder L^* loopt. Zijn er in een baan altijd (A, B) zodat $K(j) \subset K(A, B)$ algebraïsch is en een kleine graad heeft? Het antwoord hier is bevestigend: men kan zelfs (A, B) vinden zodat $K(j) = K(A, B)$. Bewijs dit ! De vraag is echter, of iets dergelijks ook geldt met R in plaats van K: zijn er in een baan altijd (A, B) zodat $A, B \in S$ met S een eindig moduul over $R[j]$ van kleine rang ? Lukt het altijd om A, B te vinden met $R[j] = R[A, B]$? Deze vraag lijkt veel lastiger te zijn om in zijn algemeenheid te beantwoorden. Misschien kunnen eerst wat voorbeelden uitgewerkt worden, of kan gegeken worden of variaties op de j-invariant niet beter zijn. Een bevredigend antwoord voor $R = \mathbb{Z}, K = \mathbb{Q}$ en $L = \mathbb{C}$ wordt besproken in [1], maar dit bewijs gebruikt nogal wat complex analytische middelen. Probeer dit bewijs te begrijpen ! Kan het bewijs meer “algebraïsch” worden gemaakt ? Kun je variaties op bovenstaand thema bedenken ?

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.