Überlagerungen von elliptischen Kurven über der projektiven Gerade $\mathbb{P}^1_k$

Jürgen Böhm *

24. August 2024

1 Einleitung

Es sei E/k eine elliptische Kurve, definiert über dem Körper k, und $\pi : E \to \mathbb{P}^1_k = Y$ eine Überlagerungsabbildung vom Grad n

Von der Abbildung π sei bekannt, daß es genau K Punkte $R_1, \ldots, R_K$ in Y gibt, über denen π verzweigt.

Dabei seien S_{ij} die Punkte über R_j, der Verzeigungsindex in S_{ij} sei e_{ij}. Es sei bekannt, welche e_{ij} über jedem R_j auftreten.

Die Gesamtanzahl der Punkte S_{ij} sei M.

Das Geschlecht von E ist $g_E = 1$, das von Y gleich $g_Y = 0$. Nach der Hurwitzformel gilt

$$2g_E - 2 = n(2g_Y - 2) + \sum_{ij}(e_{ij} - 1) \tag{1}$$

also

$$\sum_{ij}(e_{ij} - 1) = 2n \tag{2}$$

oder auch

$$\sum_{ij} e_{ij} = 2n + \sum_{ij} 1 \tag{3}$$

Da $\sum_{ij} e_{ij} = Kn$ und $\sum_{ij} 1 = M$ ist, bedeutet dies

$$\sum_{ij} e_{ij} = Kn = 2n + M \tag{4}$$

2 Problemstellung

Es seien nun für einen uniformisierenden Parameter z in Y die Werte $z(R_j)$ sämtlich bekannt. Gesucht ist

1. Eine Weierstraßgleichung
$$y^2 = x^3 + ax + b \tag{5}$$
für zwei Erzeuger x und y aus dem Funktionenkörper $K(E)$.

2. Ein Ausdruck der rationalen Funktion $z \circ \pi \in K(E)$ als explizit bekannte rationale Funktion
$$z = \frac{\sum c_\alpha x^p y^q}{\sum d_\alpha x^p y^q} \tag{6}$$
also die Kenntnis der c_α, d_α. Das Symbol α stehe dabei für pq, der Bereich der zu durchlaufenden (p,q) wird weiter unten bestimmt werden.

*jboehm@gmx.net

Proposition 1 *Die c_α, d_α, a, b in* (5) *und* (6) *lassen sich durch Lösen eines polynomiellen Gleichungsystems eindeutig bis auf*

i) 2 *kontinuierliche Freiheitsgrade*

ii) eine endliche Zahl von diskreten Freiheitsgraden bestimmen.

3 Lösung

Zunächst seien die Punkte von E über $z=0$ mit $P_1,\dots,P_n$ und diejenigen über $z=\infty$ mit $Q_1,\dots,Q_n$ bezeichnet. Wir nehmen an, daß $z=0$ und $z=\infty$ keine Verzweigungsstellen von f, also $z(R_j)\neq 0,\infty$ ist.

Wir ziehen nun zwei willkürlich gewählte Weierstraßkoordinaten x, y heran. Diese mögen ihren Pol der Ordnung 2 beziehungsweise 3 in einem Punkt $Z\in E$ haben, der in bezug auf die S_{ij} sowie die P_i, Q_i generisch gewählt ist.

Betrachtet man nun den Divisor

$$D=-P_1-\cdots-P_n+(n+1)Z \tag{7}$$

so folgt aus dem Satz von Riemann-Roch

$$l(D)-l(K-D)=\deg D+1-g_E \tag{8}$$

daß $l(D)=1$ ist. Es gibt also eine nicht identisch verschwindende Funktion

$$f=\sum c_\alpha x^p y^q \tag{9}$$

mit $f(P_i)=0$ und einem Pol höchstens $(n+1)$–ter Ordnung in Z. Man kann die zu durchlaufenden (p,q) so wählen, daß

$$0\leqslant 2p+3q\leqslant (n+1) \tag{10}$$

$$0\leqslant q\leqslant 1 \tag{11}$$

ist, das heißt man wählt eine Basis

$$1,x,x^2,\dots,x^{\lfloor\frac{n+1}{2}\rfloor}$$

$$y,yx,yx^2,\dots,yx^{\lfloor\frac{n-2}{2}\rfloor}$$

des Linearsystems $\Gamma(E,\mathcal{O}_E((n+1)Z))$ der Dimension $(n+1)$. Im folgenden sei $L=(n+1)$ gesetzt.

Für die Q_i setzt man nun analog eine Funktion

$$g=\sum d_\alpha x^p y^q \tag{12}$$

an, für die $g(Q_i)=0$ gilt.

Da f und g einen Pol $(n+1)$-ter Ordnung in Z haben, hat f neben den P_i noch eine weitere Nullstelle W_1 und ebenso g neben den Q_i noch eine Nullstelle W_2. Wir verlangen $W=W_1=W_2$ und erhalten die wählbaren Parameter $x(W),y(W)$ und die Bedingung $y(W)^2=x(W)^3+ax(W)+b$. Außerdem natürlich $f(W)=0$ und $g(W)=0$, also zwei Freiheitsgrade und drei Bedingungen.

Es ist dann

$$z\circ\pi=\frac{f}{g} \tag{13}$$

Man hat also bis jetzt folgende Freiheitsgrade

i) 2 von a, b.

ii) $2(n+1) = 2L$ von den c_α, d_α.

iii) $4n$ von den $x(P_i)$, $y(P_i)$, $x(Q_i)$, $y(Q_i)$.

iv) 2 von den $x(W)$, $y(W)$.

Nebenbedingungen werden durch die Gleichungen $y(P_i)^2 = x(P_i)^3 + ax(P_i) + b$ und $y(Q_i)^2 = x(Q_i)^3 + ax(Q_i) + b$ sowie $y(W)^2 = x(W)^3 + ax(W) + b$ gegeben, es handelt sich um $2n+1$ Nebenbedingungen.

Ein weiterer Freiheitsgrad kann durch Normierung des Bruchs f/g getilgt werden.

Es verbleiben also $1+2L+2n+1$ Freiheitsgrade.

Davon muß man natürlich die $2n+2$ Nebenbedingungen

$$\begin{aligned}\sum c_\alpha x(P_i)^p y(P_i)^q &= 0\\ \sum d_\alpha x(Q_i)^p y(Q_i)^q &= 0\\ \sum c_\alpha x(W)^p y(W)^q &= 0\\ \sum d_\alpha x(W)^p y(W)^q &= 0\end{aligned}$$

abziehen, so daß $1+2L-1 = 2L$ Freiheitsgrade verbleiben.

Nun bringt man die Verzweigungstellen ins Spiel:

Gemäß den obigen Überlegungen über Divisoren gibt es für jedes R_j ein

$$h^{(j)} = \sum c_\alpha^j x^p y^q \tag{14}$$

so daß $h^{(j)}(S_{ij}) = 0$ mit Vielfachheit e_{ij} ist.

Nun gilt aufgrund der Gleichheit der Divisoren rechts und links

$$\frac{f}{g} - z(R_j) = \frac{h^{(j)}}{g} \tag{15}$$

oder auch

$$f - z(R_j)g = h^{(j)} \tag{16}$$

also ausgeschrieben

$$\sum c_\alpha x^p y^q - z(R_j) \sum d_\alpha x^p y^q = \sum c_\alpha^j x^p y^q \tag{17}$$

Damit sind die c_α^j alle durch die c_α, d_α linear ausgedrückt, es treten also keine neuen Freiheitsgrade hinzu.

Um die Bedingung zu formulieren, daß $h^{(j)}$ bei S_{ij} mit Vielfachheit e_{ij} verschwindet, benötigen wir die $x(S_{ij})$, $y(S_{ij})$. Sie bringen $2M$ Freiheitsgrade, aber, durch die sie bindenden Weierstraßgleichungen auch M Bedingungen hinein, also eine Bilanz von jetzt $2L+M$ Freiheitsgraden.

Bei generischer Wahl der Polstelle Z von x und y kann angenommen werden, daß x in jedem S_{ij} ein uniformisierender Parameter ist. Man erhält also die Bedingungen

$$\frac{dh^{(j)}}{dx^\nu}(x(S_{ij}), y(S_{ij})) = 0 \text{ für } \nu = 0, \ldots, e_{ij} - 1 \tag{18}$$

Führt man

$$D_x = \frac{d}{dx} = \frac{\partial}{\partial x} + \frac{\partial}{\partial y}\frac{dy}{dx} \tag{19}$$

ein und beachtet

$$2y\,dy = (3x^2 + a)\,dx \tag{20}$$

also

$$(*) \quad 2y\frac{dy}{dx} - (3x^2 + a) = \Psi_1(x, y, \frac{dy}{dx}) = 0$$

so kann $\frac{dh^{(j)}}{dx}$ als Polynom

$$\frac{dh^{(j)}}{dx} = \frac{\partial h^{(j)}}{\partial x} + \frac{\partial h^{(j)}}{\partial y}\frac{dy}{dx}$$

in $x, y, \frac{dy}{dx}$ geschrieben werden, wobei für $\frac{dy}{dx}$ noch das Polynom Ψ_1 zur Bestimmung hinzutritt.

Bildet man, weiter fortschreitend $\frac{d^2h^{(j)}}{dx^2}$, so kann man auch dies als ein Polynom, jetzt in $x, y, \frac{dy}{dx}, \frac{d^2y}{dx^2}$ ausdrücken, wobei ein weiteres Polynom Ψ_2 in $x, y, \frac{dy}{dx}, \frac{d^2y}{dx^2}$ analog zu $(*)$ hinzutritt, das durch zweifache Ableitung von $y^2 = x^3 + ax + b$ nach x gewonnen wird.

Man hat also für $\nu = 0, \ldots, e_{ij} - 1$

$$D_x^\nu h^{(j)} \left(x(S_{ij}), y(S_{ij}), \ldots, \frac{d^\nu y}{dx^\nu}(S_{ij}) \right) = 0 \tag{21}$$

plus die Polynome $\Psi_\nu(x, y, \ldots, \frac{d^\nu y}{dx^\nu}) = 0$ die die neu hinzutretenden Unbekannten $\frac{d^\nu y}{dx^\nu}$ festlegen.

Für jeden der M Punkte S_{ij} treten also e_{ij} Bedingungen auf. Dies sind insgesamt, wie oben ausgerechnet, $2n + M$ Bedingungen.

Die Bilanz ergibt also

$$2L + M - (2n + M) = 2(n+1) + M - 2n - M = 2 \tag{22}$$

Freiheitsgrade.

Bemerkung 1 *Der erste Freiheitsgrad kommt von der Wahl der Polstelle Z auf E, der zweite davon, daß E nur bis auf Isomorphie bestimmt ist, also nur $j = j(a,b)$ feststeht, aber die a, b innerhalb dieser Vorgabe variiert werden können.*

Fixiert man durch geeignete Nebenbedingungen diese 2 kontinuierlichen Freiheitsgrade, so definieren die sämtlich polynomiellen Bedingungen ein nulldimensionales Polynomideal, dessen endliche Lösungsgesamtheit für die möglicherweise existierenden diskreten Freiheitsgrade verantworlich ist.

4 Zusammenfassung

Man hat also folgendes polynomielle System

$$\begin{aligned}
y(P_i)^2 &= x(P_i)^3 + ax(P_i) + b \\
y(Q_i)^2 &= x(Q_i)^3 + ax(Q_i) + b \\
y(W)^2 &= x(W)^3 + ax(W) + b \\
y(S_{ij})^2 &= x(S_{ij})^3 + ax(S_{ij}) + b \\
\sum c_\alpha x(P_i)^p y(P_i)^q &= 0 \\
\sum d_\alpha x(Q_i)^p y(Q_i)^q &= 0 \\
\sum c_\alpha x(W)^p y(W)^q &= 0 \\
\sum d_\alpha x(W)^p y(W)^q &= 0 \\
c_\alpha^j &= c_\alpha - z(R_j) d_\alpha \\
D_x^\nu h^{(j)} \left(x(S_{ij}), y(S_{ij}), \ldots, \frac{d^\nu y}{dx^\nu}(S_{ij}) \right) &= 0, \quad \nu = 0, \ldots, e_{ij} - 1 \\
\Psi_\nu \left(x(S_{ij}), y(S_{ij}), \ldots, \frac{d^\nu y}{dx^\nu}(S_{ij}) \right) &= 0, \quad \nu = 1, \ldots, e_{ij} - 1
\end{aligned}$$

in den Unbestimmten a, b, $x(P_i)$,$y(P_i)$,$x(Q_i)$,$y(Q_i)$,$x(W)$, $y(W)$, $x(S_{ij})$,$y(S_{ij})$, $\frac{d^\nu y}{dx^\nu}(S_{ij})$, c_α, d_α, c_α^j, wobei

$$h^{(j)} = \sum c_\alpha^j x^p y^q$$

ist.

5 Bewertung

Mathematisch interessant könnte möglicherweise eine Anwendung dieses Verfahrens im Fall von Modulkurven $E = \mathfrak{H}^*/\Gamma$, die zugleich elliptische Kurven sind, sein. Hier besteht eine Überlagerung

$$E = \mathfrak{H}^*/\Gamma \to \mathfrak{H}^*/\mathrm{SL}_2(\mathbb{Z}) = \mathbb{P}^1_{\mathbb{C}}$$

deren Verzweigungsstruktur sich aus der Struktur der Untergruppe $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ ergibt.

Die $j(R_j)$ sind für die Wahl des kanonischen Parameters j in $\mathbb{P}^1_{\mathbb{C}}$ bekannt, es gilt $j(R_j) \in \{0, 1728, \infty\}$. Damit ist natürlich die Bedingung $j(R_j) \neq 0, \infty$ von oben verletzt.

Man kann dies aber durch Wahl eines anderen Parameters $j' = (aj+b)/(cj+d)$ umgehen, oder auch das obige Verfahren entsprechend modifizieren.

Die aufzustellenden Gleichungssysteme sind sehr groß, und mit Gröbnerbasismethoden vermutlich derzeit nicht zu lösen (Supercomputeranwendung?). Man könnte allerdings versuchen, sie numerisch mit hoher Genauigkeit zu lösen und in der Kenntnis des maximalen Grades der Körpererweiterung über $\mathbb{Q}$, in der die Lösungen als ganze Zahlen zu liegen haben, diese dann mit den üblichen Verfahren (LLL–Reduktion) exakt aufzufinden.