Werk

Titel: 2.1 Elliptische Kurven

Jahr: 1975

PURL: https://resolver.sub.uni-goettingen.de/purl?301416052_0004|log26

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Auf Grund von v kann man zeigen, daß $H_{n,m}$ eine komplexe Struktur der Dimension m besitzt (so daß v eine analytische Abbildung ist) (vgl. W. FULTON [1]). Die Fasern von σ, d. h. die Menge aller f, die auf M dieselbe konforme Struktur induzieren, sind $(2n + p - 1)$-dimensionale Mannigfaltigkeiten, da man erstens den Polardivisor $(f)_\infty = f^{-1}(\infty) = P_1 + \cdots + P_n$ beliebig verschieben kann (bis auf eine dünne Menge im Raum $M^{(m)}$ aller Divisoren vom Grade m, in der $P_1 + \cdots + P_n$ nicht liegen darf) und zweitens bei gegebenem Polardivisor $P_1 + \cdots + P_n$ die zugehörigen Funktionen f einen $(n + p - 1)$-dimensionalen Vektorraum $L = L(P_1 + \cdots + P_n)$ bilden (Satz von RIEMANN-ROCH). Alle Funktionen f aus L (bis auf eine dünne Menge) sind in $H_{n,m}$ enthalten. Also ist die Faser von σ ein offener Unterraum von $M^{(m)} \times \mathbf{C}^{n+p-1}$. Da

$$\begin{aligned} \dim H_{n,m} - \dim (M^{(n)} \times \mathbf{C}^{n+p-1}) &= 2(n + p - 1) - (n + n + p - 1) \\ &= 3p - 3 \end{aligned}$$

ist, schließt RIEMANN, daß es $3p - 3$ Parameter gibt, die die konformen Strukturen auf M festlegen.

2. Elliptische und hyperelliptische Kurven

2.1. Elliptische Kurven

Zur weiteren Illustration der Problematik betrachten wir den oben ausgeschlossenen Fall $p = 1$ (elliptische Kurven) und im Anschluß daran hyperelliptische Kurven, da hier die Verhältnisse eine explizite Beschreibung gestatten. Wir betrachten alles über einem beliebigen algebraisch abgeschlossenen Grundkörper k der Charakteristik $p \neq 2$.

Ist E eine elliptische Kurve, Q ein Punkt, so definiert das lineare System $|3Q|$ eine Einbettung $E \to \mathbf{P}^2$ (da $0 = \dim |3Q - P_1 - P_2| < \dim |3Q - P_1| < \dim |3Q| = 2$ ist für alle $P_1, P_2 \in E$); also ist E eine singularitätenfreie kubische Kurve. Projiziert man von Q aus auf eine beliebige Gerade, so erhält man eine zweiblättrige Überlagerung $f\colon E \to \mathbf{P}^1$ (da die Projektionsgerade außer Q noch zwei weitere Schnittpunkte mit E hat), und nach der Hurwitzschen Geschlechterformel erhält man außer Q noch drei weitere Verzweigungspunkte P_0, P_1, P_2. Man wähle auf $\mathbf{P}^1$ die Koordinaten so, daß $f(Q) = \infty$, $f(P_0) = 0$, $f(P_1) = 1$, $f(P_2) = \lambda$ (Doppelverhältnis auf $\mathbf{P}^1$) ist. Die komplexe Struktur wird also durch einen Parameter beschrieben. Hierbei ist zu beachten, daß λ nicht eindeutig der komplexen Struktur entspricht. Man kann z. B. noch eine Permutation der drei Punkte $f(P_0)$, $f(P_1)$, $f(P_2)$ betrachten. Entsprechend dem Transformationsverhalten des Doppelverhältnisses erhält man bei der Transposition $(0, 1)$ den Wert $1 - \lambda$ und bei der Transposition $(0, 2)$ den Wert $\dfrac{\lambda}{\lambda - 1}$.

Der Ring der Invarianten von $\mathbf{Z}\left[\lambda, \dfrac{1}{\lambda}, \dfrac{1}{1-\lambda}\right]$ bezüglich S_3 ist $\mathbf{Z}\left[\dfrac{(\lambda^2 - \lambda + 1)^3}{(\lambda - 1)^2 \lambda^2}\right]$, und die Größe

$$j(E) =: 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (1 - \lambda)^2}$$

heißt die *absolute Invariante* von E.

Wählt man die Koordinaten X, Y, Z in $\mathbf{P}^2$ so, daß Q der Punkt $(0:1:0)$ und $Z = 0$ die Tangente im Punkt Q ist, so genügt E der Gleichung

$$\begin{aligned} F(X, Y, Z) &= Y^2Z + 2(aX + bZ)\, YZ + G(X, Z) \\ &= (Y + aX + bZ)^2\, Z + H(X, Z) = 0; \end{aligned}$$

also hat E nach einer Koordinatentransformation die Gleichung

$$Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3, \qquad a \neq 0. \tag{1}$$

Eine leichte Rechnung zeigt

$$j(E) = 2^8 \frac{(b^2 - 3ac)^3}{a^2 \cdot \Delta}, \tag{2}$$

wobei Δ die Diskriminante von $aX^3 + bX^2 + cX + d$ ist.

Es gilt

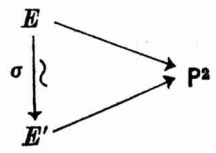
2.1.1. Satz

(i) *$E \mapsto j(E)$ ist eine Bijektion zwischen der Menge aller Isomorphieklassen elliptischer Kurven und den Punkten von $M = \operatorname{Spec} k[t]$.*

(ii) *Ist $(E_s)_{s \in S}$ eine algebraische Familie elliptischer Kurven, so daß ein Schnitt $\varepsilon: S \to E$, $\varepsilon(s) \in E_s$, existiert, dann wird $s \mapsto j(s)$ durch einen Morphismus $S \to M$ induziert.*

(iii) *(j, M) ist universell mit den Eigenschaften* (i), (ii).

Zu (i). Bekanntlich erhält die Kurve E durch Auszeichnung eines Punktes Q eine Gruppenstruktur (mit Q als Nullelement, drei Punkte haben die Summe 0, wenn sie bei der oben betrachteten Einbettung kollinear sind, der Punkt $-(X:Y:Z)$ hat die Koordinaten $(X:-Y:Z)$.
Ist $\sigma: (E, Q) \xrightarrow{\sim} (E', Q')$ ein Isomorphismus, so induzieren $|3Q|$ und $|3Q'|$ Einbettungen derart, daß



kommutativ ist, also ist $j(E) = j(E')$; nimmt man insbesondere $E = E'$, und $\sigma(P) = P + Q'$, so sieht man, daß j nicht von Q' abhängt.
Ist j gegeben, so kann man daraus λ und damit eine zu j gehörige Kurve bestimmen. Ist $\chi(k) \neq 3$, so ist

$$y^2 = x^3 - 3j(j - 12^3)c^2x - 2j(j - 12^3)^2c^3 \quad (c \in k^\times)$$

die affine Gleichung einer zu j gehörigen Kurve, falls $j \neq 0, \neq 12^3$ ist, und

$$\begin{aligned} y^2 &= x^3 + c \qquad (c \in k^\times) \qquad \text{für } j = 0, \\ y^2 &= x^3 + cx \qquad (c \in k^\times) \qquad \text{für } j = 12^3. \end{aligned}$$

Damit ist (i) bewiesen.

Zu (ii). Diese Behauptung ist unmittelbar klar, wenn die Familie durch eine Gleichung von der Form (1) gegeben ist, wobei a, b, c, d reguläre Funktionen auf S sind und a und Δ keine Nullstellen haben. Die Frage ist außerdem lokal bezüglich S. Der Schnitt $\varepsilon(S) = D$ ist ein relativer Cartierdivisor über S, und für hinreichend kleine S sind $p_*\mathcal{O}_E(D)$, $p_*\mathcal{O}_E(2D)$, $p_*\mathcal{O}_E(3D)$ frei vom Rang 1, 2 bzw. 3 über S (Basiswechsel, vgl. Kap. III).
Dann definiert $\mathcal{O}_E(3D)$ eine Einbettung $E \to \mathbf{P}^2 \times S$, die genau wie oben beschrieben bei geeigneter Wahl der Koordinaten durch eine Gleichung vom Typ (1) bestimmt ist, q. e. d.

Im folgenden nehmen wir $k = \mathbf{C}$ an; in diesem Fall entsprechen die elliptischen Kurven den komplexen Tori $\mathbf{C}/(\mathbf{Z}w_1 + \mathbf{Z}w_2)$ (w_1, w_2 Fundamentalperioden), da jede kompakte komplexe Liesche Gruppe ein komplexer Torus (man betrachte die Liesche Algebra und die Exponentialabbildung als universelle Überlagerung) und da jeder eindimensionale komplexe Torus algebraisch ist (vgl. D. Mumford [6]).
Konkreter läßt sich die Situation wie folgt beschreiben: Gegeben sei ein Periodengitter Γ, das bis auf Isomorphie durch die Fundamentalperioden 1 und $\tau \left(=: \pm\frac{w_2}{w_1}\right)$ erzeugt werde, wobei τ in der oberen Halbebene von $\mathbf{C}$ liegt.
Die elliptischen Funktionen mit den Perioden $1, \tau$ bilden einen eindimensionalen Funktionenkörper, und $\mathbf{C}/\Gamma$ ist komplex isomorph zu der zugehörigen singularitätenfreien kompletten Kurve.
Eine projektive Einbettung von $\mathbf{C}/\Gamma$ erhält man durch die Thetafunktionen. Unter einer Thetafunktion der Ordnung m mit dem Periodengitter Γ versteht man eine ganze Funktion f auf $\mathbf{C}$ mit den Eigenschaften

$$f(z+1) = f(z),$$
$$f(z+\tau) = \varepsilon\left(-m\left(z+\frac{\tau}{2}\right)\right) f(z) \qquad (\varepsilon(t) \underset{\text{def}}{=:} \exp(2\pi i t)).$$

Diese bilden einen Vektorraum der Dimension m, eine Basis bilden die durch Fourierreihen dargestellten Funktionen

$$\theta_m[n](z,\tau) = \sum_{\nu=-\infty}^{\infty} \varepsilon\left(\frac{\tau}{2m}(m\nu+n)^2\right)\varepsilon((m\nu+n)z) \quad (0 \leqq n < m).$$

(Gleichmäßige Konvergenz auf jeder kompakten Menge ergibt sich aus der Voraussetzung, daß τ in der oberen Halbebene liegt.)
Insbesondere ist folgende Bezeichnung üblich:

$$\vartheta(z,t) = \theta_1[0](z,\tau) = \sum_{\nu=-\infty}^{\infty} \varepsilon\left(\frac{\tau\nu^2}{2}\right)\varepsilon(\nu z).$$

Dann gilt (Koeffizientenvergleich!)

$$\theta_m[n](z,\tau) = \varepsilon\left(n\left(z+\frac{n\tau}{m}\right)\right)\vartheta(mz+n\tau, m\tau).$$

Integration der logarithmischen Ableitung um eine Grundmasche des Gitters Γ ergibt, daß eine Thetafunktion $f(z)$ modulo Γ genau m (= Ordnung (f)) Nullstellen hat (entsprechend den Vielfachheiten gezählt). Sind f, g Thetafunktionen der Ordnung m, die $m-1$ gemeinsame Nullstellen haben, so folgt aus dem Residuensatz

(Residuen von $\frac{f}{g}$ in einer Grundmasche haben die Summe 0), daß auch die letzten Nullstellen beider Funktionen übereinstimmen; insbesondere ist $\frac{f}{g} = c$ konstant, $f = gc$.
Mit diesen Bemerkungen erhält man leicht den folgenden

2.1.2. Satz. *Sind f_0, f_1, f_2 drei linear unabhängige Thetafunktionen der Ordnung 3, so liefert*

$$z \mapsto (f_0(z) : f_1(z) : f_2(z)) \in \mathbf{P}^2$$

eine komplexe Einbettung $\mathbf{C}/\Gamma \to \mathbf{P}^2$ auf eine kubische Kurve.

(Eine kubische Relation gilt wegen der Tatsache, daß es höchstens neun linear unabhängige Monome $f_0(z)^{i_0} f_1(z)^{i_1} f_2(z)^{i_2}$, $i_0 + i_1 + i_2 = 3$ (Thetafunktionen der Ordnung 9) gibt.)

Beispiel.

$$f_0 = \vartheta\left(z + \frac{1}{2} + \frac{\tau}{2}\right)^3,$$

$$f_1 = \vartheta\left(z + \frac{1}{2} + \frac{\tau}{2}\right) \cdot \vartheta\left(z + \frac{\tau}{2}\right)^2,$$

$$f_2 = \varepsilon(-z) \cdot \vartheta(z) \cdot \vartheta\left(z + \frac{1}{2}\right) \cdot \vartheta\left(z + \frac{\tau}{2}\right) \qquad (\vartheta(z) =: \vartheta(z, \tau)).$$

(Ersetzt man z durch $z + \tau$, so multiplizieren sich die drei Funktionswerte mit $-\varepsilon(-3(z + \tau))$; um Thetafunktionen im obigen Sinne zu erhalten, muß man noch eine unwesentliche Verschiebung der Variablen z durchführen.)
Man sieht leicht, daß $\frac{1+\tau}{2}$ Nullstelle von ϑ ist (indem man in der Fourierentwicklung jeweils das i-te und $(-(i+1))$-te Glied zusammenfaßt für $i = 0, 1, 2, \ldots$).
Also haben f_0, f_1, f_2 die Nullstellen $0, \left(0, \frac{1}{2}\right), \left(\frac{\tau+1}{2}, \frac{\tau}{2}, \frac{1}{2}\right)$, und F ist überall definiert; man erkennt ferner leicht, daß f_0, f_1, f_2 linear unabhängig sind und hieraus, daß F injektiv ist.
Weiterhin ist $\frac{f_1}{f_0}(z)$ eine gerade Funktion von z mit einem zweifachen Pol in $z = 0$; $\frac{f_2}{f_0}(z)$ ist ungerade und hat einen dreifachen Pol in $z = 0$. Somit genügen die Funktionen einer kubischen Relation

$$\left(\frac{f_2}{f_0}\right)^2 = a\left(\frac{f_1}{f_0}\right)^3 + b\left(\frac{f_1}{f_0}\right)^2 + c\left(\frac{f_1}{f_0}\right), \quad a \neq 0,$$

bzw. homogen:

$$f_2^2 f_0 = a f_1^3 + b f_1^2 f_0 + c f_1 f_0^2$$

(das konstante Glied ist Null, da $\frac{1}{2}$ eine gemeinsame Nullstelle von f_2 und f_1 ist).
Indem man durch f_0 bzw. f_1 dividiert und beide Seiten für $z = 0$ bzw. $z = \frac{1}{2}$ aus-