

Werk

Titel: 2. Elliptische und hyperelliptische Kurven

Jahr: 1975

PURL: https://resolver.sub.uni-goettingen.de/purl?301416052_0004|log25

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 $(f)_\infty = f^{-1}(\infty) = P_1 + \dots + P_n$ beliebig verschieben kann (bis auf eine dünne Menge im Raum $M^{(m)}$ aller Divisoren vom Grade m , in der $P_1 + \dots + P_n$ nicht liegen darf) und zweitens bei gegebenem Polardivisor $P_1 + \dots + P_n$ die zugehörigen Funktionen f einen $(n + p - 1)$ -dimensionalen Vektorraum $L = L(P_1 + \dots + P_n)$ 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 $E \rightarrow \mathbf{P}^2$ (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 $f: E \rightarrow \mathbf{P}^1$ (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 $\frac{\lambda}{\lambda - 1}$.

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

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

also hat E nach einer Koordinatentransformation die Gleichung

$$Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3, \quad a \neq 0. \quad (1)$$

Eine leichte Rechnung zeigt

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

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 $M = \text{Spec } k[t]$.
- (ii) Ist $(E_s)_{s \in S}$ eine algebraische Familie elliptischer Kurven, so daß ein Schnitt $\varepsilon: S \rightarrow E$, $\varepsilon(s) \in E_s$, existiert, dann wird $s \mapsto j(s)$ durch einen Morphismus $S \rightarrow M$ 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

$$\begin{array}{ccc} E & & \\ \sigma \downarrow \wr & \searrow & \mathbf{P}^2 \\ E' & \nearrow & \end{array}$$

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

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

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 d 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 $E \rightarrow \mathbf{P}^2 \times S$, 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 τ ($=: \pm \frac{w_2}{w_1}$) erzeugt werde, wobei τ in der oberen Halbebene von $\mathbf{C}$ liegt.

Die elliptischen Funktionen mit den Perioden 1, τ 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

$$\begin{aligned} f(z+1) &= f(z), \\ f(z+\tau) &= \varepsilon \left(-m \left(z + \frac{\tau}{2} \right) \right) f(z) \quad (\varepsilon(t) \stackrel{\text{def}}{=} \exp(2\pi i t)). \end{aligned}$$

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

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

(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 $\mathbf{C}/\Gamma \rightarrow \mathbf{P}^2$ 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.

$$\begin{aligned} f_0 &= \vartheta\left(z + \frac{1}{2} + \frac{\tau}{2}\right)^3, \\ f_1 &= \vartheta\left(z + \frac{1}{2} + \frac{\tau}{2}\right) \cdot \vartheta\left(z + \frac{\tau}{2}\right)^2, \\ f_2 &= \varepsilon(-z) \cdot \vartheta(z) \cdot \vartheta\left(z + \frac{1}{2}\right) \cdot \vartheta\left(z + \frac{\tau}{2}\right) \quad (\vartheta(z) =: \vartheta(z, \tau)). \end{aligned}$$

(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 Fourierreihe jeweils das i -te und $-(i+1)$ -te Glied zusammenfaßt für $i = 0, 1, 2, \dots$).

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-

rechnet, erhält man

$$a = c = \frac{\vartheta(0)^2 \cdot \vartheta\left(\frac{1}{2}\right)^2}{\vartheta\left(\frac{\tau}{2}\right)^4}, \quad b = \frac{\vartheta(0)^4 + \vartheta\left(\frac{1}{2}\right)^4}{\vartheta\left(\frac{\tau}{2}\right)^4}.$$

Die Wurzeln von $ax^3 + bx^2 + cx = 0$ sind daher

$$e_1 = 0, \quad e_2 = \frac{\vartheta(0)^2}{\vartheta\left(\frac{1}{2}\right)^2}, \quad e_3 = \frac{\vartheta\left(\frac{1}{2}\right)^2}{\vartheta(0)^2}.$$

Hieraus folgt, daß die absolute Invariante durch

$$j(\tau) = 2^8 \frac{\left[\vartheta(0, \tau)^8 + \vartheta\left(\frac{1}{2}, \tau\right)^8 - \vartheta(0, \tau)^4 \cdot \vartheta\left(\frac{1}{2}, \tau\right)^4 \right]^3}{\vartheta(0, \tau)^8 \vartheta\left(\frac{1}{2}, \tau\right)^8 \cdot \left[\vartheta\left(\frac{1}{2}, \tau\right)^4 - \vartheta(0, \tau)^4 \right]^2}$$

gegeben ist.

Daher ist $j(\tau)$ Quotient der Nullwerte zweier Thetafunktionen der Ordnung 24 zu dem Gitter $\Gamma = \mathbf{Z} + \mathbf{Z}\tau$.

Es sei umgekehrt eine Kurve E durch $y^2 = x^3 - ax - b$ gegeben (d. h. als zwei-blättrige Überlagerung von $\mathbf{P}^1$ mit den Verzweigungspunkten e_1, e_2, e_3, ∞).

Indem man $\frac{dx}{y}$ auf der zugehörigen Riemannschen Fläche längs der Fundamental-

zyklen γ_1, γ_2 integriert, erhält man Perioden w_1, w_2 , und $E \xrightarrow{u} (\mathbf{Z}w_1 + \mathbf{Z}w_2)$ wird durch

$$(x, y) \mapsto \left(\int_{(x_0, y_0)}^{(x, y)} \frac{dx}{y} \right) \bmod (\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2)$$

gegeben. Das topologische Bild zeigt Abb. 5 (vgl. S. 106).

Insbesondere sind die Perioden (lokal) stetig von dem Doppelverhältnis

$\lambda = (e_1 : e_2 : e_3 : \infty)$ abhängig.

2.2. Kurven vom Geschlecht 2 (vgl. J. IGUSA [1] und P. SAMUEL [1])

Für singularitätenfreie komplette Kurven $\mathbf{C}$ vom Geschlecht 2 sind die Verhältnisse besonders einfach; zu jeder solchen Kurve gibt es nämlich eine kanonische Überlagerung $f: \mathbf{C} \rightarrow \mathbf{P}^1$, da es genau zwei linear unabhängige Abelsche Differentiale w_1, w_2 auf $\mathbf{C}$ gibt; es ist $f(x) = (w_1(x) : w_2(x))$, und f hat sechs Verzweigungspunkte. Bezüglich der kanonischen Abbildung gilt allgemein folgendes: Wir setzen wieder der Einfachheit halber voraus, daß die Charakteristik des Grundkörpers $\neq 2$ ist.

2.2.1. Satz. Ist C eine singularitätenfreie Kurve vom Geschlecht $p \geq 2$ und ω_C die Garbe der 1-Formen, so hat das lineare System $|\omega_C|$ keine Basispunkte, und die zugehörige

kanonische Abbildung $f: C \rightarrow \mathbb{P}^1$ ist entweder eine abgeschlossene Einbettung oder $f(C) \cong \mathbb{P}^1$ und $C \rightarrow f(C)$ ist eine zweiblättrige Überlagerung mit $2p + 2$ Verzweigungspunkten (hyperelliptischer Fall).

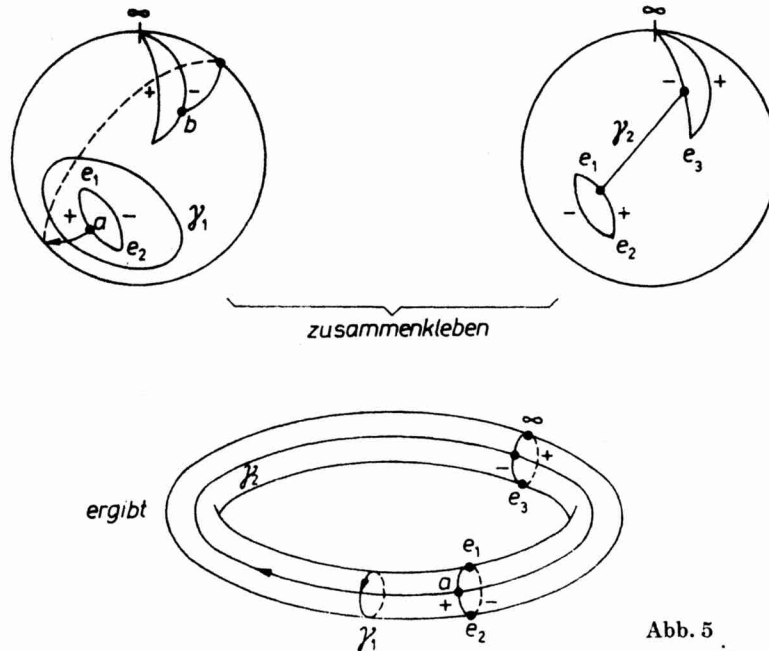


Abb. 5

Beweis. Ist $|\omega_C \otimes \mathcal{O}_C(-P)| = |\omega_C|$ (d. h. P Basispunkt), so ist $\dim |\mathcal{O}(P)| = 1$ (Satz von RIEMANN-ROCH), d. h., es gibt eine rationale Funktion f mit einem einfachen Pol in P , d. h., C ist vom Geschlecht 0. Also hat $|\omega_C|$ für $p \geq 2$ keine Basispunkte.

Wenn f keine Einbettung ist, gibt es zwei (nicht notwendig verschiedene) Punkte P, Q , so daß $|\omega_C(-P - Q)| = |\omega_C(P)|$, also

$$|\mathcal{O}_C(P)| \not\subseteq |\mathcal{O}_C(P + Q)|$$

ist, und es gibt eine rationale Funktion g mit dem Poldivisor $P + Q$; g ist daher eine zweiblättrige Überlagerung $g: C \rightarrow \mathbb{P}^1$. Bei geeigneter Wahl von y ist dann C in affinen Koordinaten durch

$$y^2 = F(x), \quad \deg F(x) = 2p + 1 \text{ oder } 2p + 2 \quad (3)$$

definiert, wobei $F(x)$ nur einfache Nullstellen hat. Man rechnet für jede durch eine Gleichung (3) definierte Kurve direkt nach:

a) $\frac{dx}{y}, x \frac{dx}{y}, \dots, x^{p-1} \frac{dx}{y}$ ist eine Basis der abelschen Differentiale (also ist $g(x, y) = x$ bis auf Isomorphie die kanonische Abbildung).

b) Die Verzweigungspunkte liegen über den Nullstellen von $F(x)$ (und über ∞ , wenn $\deg F = 2p + 1$ ist).

Wir kehren jetzt zu Kurven C vom Geschlecht 2 und der kanonischen Überlagerung $f: C \rightarrow \mathbf{P}^1$ zurück; offensichtlich ist $f: C \rightarrow \mathbf{P}^1$ durch die Bilder der sechs Verzweigungspunkte auf $\mathbf{P}^1$, d. h. durch eine Form sechsten Grades (binäre Sextik)

$$u_0 X^6 + u_1 X^5 Y + u_2 X^4 Y^2 + \dots + u_6 Y^6 = u(X, Y)$$

eindeutig bestimmt, und die Isomorphieklassen der Kurven vom Geschlecht 2 entsprechen den Punkten des Orbitraums

$$M = U/PGL(2), \quad (u\sigma)(X, Y) = u(aX + bY, cX + dY) \text{ für } \sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL(2).$$

($U \subset \mathbf{P}^6$ Unterraum der binären Sextiken, Menge aller $(u_0 : u_1 : \dots : u_6)$, deren Diskriminante $D(u_0, \dots, u_6) \neq 0$ ist).

Ist $j(C)$ der entsprechende Punkt aus M , so gilt wieder:

2.2.2. Satz

- (i) Ist $\mathfrak{M}$ die Menge aller Isomorphieklassen von Kurven vom Geschlecht 2, so ist $\mathfrak{M} \rightarrow M, C \mapsto j(C)$ eine Bijektion.
- (ii) Ist $(C_s)_{s \in S}$ eine beliebige algebraische Familie von Kurven vom Geschlecht 2, so wird $s \mapsto j(s)$ durch einen Morphismus $S \rightarrow M$ induziert, der durch $C|S$ eindeutig bestimmt ist. (Dabei wird vorausgesetzt, daß 2 auf S umkehrbar ist.)
- (iii) (j, M) mit den Eigenschaften (i) und (ii) ist universell.

Die Konstruktion des Raumes der Invarianten der binären Sextiken über C als Grundkörper ist seit dem vorigen Jahrhundert bekannt (A. CLEBSCH [1]). Eine Beschreibung von M erhält man z. B. wie folgt:

Es sei $\mathfrak{M}$ das System aller Isomorphieklassen von 7-Tupeln $(C, P_1, \dots, P_6)$, C eine Kurve vom Geschlecht 2, $P_i \in \mathbf{P}^1$ seien die Bildpunkte der Verzweigungspunkte der kanonischen Abbildung. Es sei $\tilde{M} \subset \mathbf{A}^3$ die Menge aller Punkte $(\lambda_1, \lambda_2, \lambda_3) \in \mathbf{A}^3$, $\lambda_i \neq 0, 1$; dann erhält man eine Bijektion $\tilde{j}: \mathfrak{M} \rightarrow \tilde{M}$ durch

$$(C, P_1, \dots, P_6) \rightarrow (\lambda_1, \lambda_2, \lambda_3) \quad \text{mit} \quad \lambda_i = (P_4 : P_5 : P_6 : P_i)$$

(Doppelverhältnis).

Die symmetrische Gruppe S_6 operiert in kanonischer Weise auf $\mathfrak{M}$, und diese Operation überträgt sich auf $\tilde{M}$, so daß S_6 algebraisch auf $\tilde{M}$ operiert. Daher induziert $\tilde{j}$ eine Bijektion

$$j: \mathfrak{M} = \mathfrak{M}/S_6 \rightarrow \tilde{M} = \tilde{M}/S_6;$$

insbesondere ist M ein dreidimensionales normales affines Schema.

Es ist klar, wie man algebraische Familien $(C|S, \sigma_1, \dots, \sigma_6)$, $\sigma_i: S \rightarrow \mathbf{P}^1 \times S$ aus $\mathfrak{M}$ zu definieren hat. Für algebraische Familien aus $\mathfrak{M}$ mit dem Parameterschema S induziert die Abbildung

$$S \rightarrow \mathfrak{M} \xrightarrow{\tilde{j}} \tilde{M}, \quad s \mapsto \tilde{j}(s)$$

einen Morphismus $S \rightarrow M$.

Ist $C|S$ eine algebraische Familie, so wollen wir zeigen, daß $s \mapsto j(s)$ einen Morphismus $S \rightarrow M$ induziert. Da die Frage lokal bezüglich S ist, können wir annehmen, daß S zusammenhängend und $p_* \omega_{C|S}$ frei ist ($p: C \rightarrow S$ Strukturmorphismus); durch die globalen Schnitte wird also ein S -Morphismus $C \rightarrow \mathbf{P}^1 \times S$ induziert. Es sei $D = D_{C|S} \subset C$ der Verzweigungsdivisor (Differente) von $C|S$ über $\mathbf{P}^1 \times S/S$; dann ist $D \rightarrow S$ eine sechsblättrige Etalüberlagerung, die eventuell in mehrere Zusammenhangskomponenten zerfällt. Ist $S' = D \times_S \dots \times_S D$ (6mal), so ist $S' \rightarrow S$ ebenfalls eine Etalüberlagerung und $S'/S_6 \cong S$.

Die induzierte Familie $C' = C \times_S S'$ besitzt sechs Schnitte $S' \rightarrow D \times_S S' \subset C'$; durch Festlegung einer Reihenfolge dieser Schnitte erhält man also einen Morphismus $\tilde{j}: S' \rightarrow \tilde{M}$ mit $\tilde{j}(s') = j(C'_s) = j(C_s)$ (wenn s' über $s \in S$ liegt), und $S' \xrightarrow{\tilde{j}} \tilde{M} \rightarrow M$ ist ein S_6 -äquivarianter Morphismus (triviale Operation auf M). Also induziert j einen eindeutig durch $C|S$ bestimmten Morphismus $j: S \rightarrow M$ mit $j(s) = j(C_s)$. Zur genaueren Bestimmung von M müssen wir ein Erzeugendensystem für die Invarianten binärer Sextiken ausrechnen. Das ist mit erheblichem Rechenaufwand verbunden und war einer der Höhepunkte der klassischen Invariantentheorie. Wir betrachten die kanonische Abbildung

$$(\mathbf{P}^1)^6 \rightarrow (\mathbf{P}^1)^6/S_6 = \mathbf{P}^6,$$

$$((u_1 : v_1), \dots, (u_6 : v_6)) \mapsto \prod_{i=1}^6 (u_i X + v_i Y);$$

eine rationale Invariante auf $\mathbf{P}^6$ bezüglich $GL(2)$ ist umkehrbar eindeutig durch eine symmetrische rationale Funktion $f(P_1, \dots, P_6)$ auf $(\mathbf{P}^1)^6$ bestimmt, so daß $f(\sigma P_1, \dots, \sigma P_6) = \det(\sigma) g f(P_1, \dots, P_6)$ (g Gewicht der Invarianten) für alle $\sigma \in GL(2)$ gilt.

Die Funktion f ist Quotient zweier eindeutig bestimmter 6-homogener Formen $F = F(u_1, v_1, \dots, u_6, v_6)$ und $G = G(u_1, \dots, u_6)$, die symmetrisch in den (u_i, v_i) sind, also insbesondere denselben Grad m bezüglich jeder Variablenreihe $w_i = (u_i, v_i)$ haben. Wenn die Charakteristik 0 ist, gilt:

Ist m der Grad von F in jeder Variablenreihe w_i , so ist F von der Form $P(w_1, w_2, \dots, w_6; w_1, \dots, w_6; w_1, \dots, w_6)$ (m -mal), wobei I eine symmetrische $(6m)$ -Linearform in $w_1, \dots, w_6, w_7, \dots, w_{6m}$ ist (P gewinnt man durch m -fache Polarisierung von F).

Wir bezeichnen mit $[w_i, w_j]$ die Determinante von w_i, w_j . Nach dem ersten Hauptsatz der klassischen Invariantentheorie gilt (vgl. etwa J. B. CARRELL und J. DIEUDONNÉ [1]): Es sei p eine natürliche Zahl. Es gibt p -lineare Invarianten $P(w_1, \dots, w_p)$ bezüglich der Operation von $GL(2)$ auf dem Raum $\otimes^p E$ ($E = C^2$) nur dann, wenn $p = 2g$ ($2 = \dim E$) ist; jede solche Invariante ist eine Linearkombination von Invarianten der Form

$$[\omega_{\pi(1)}, \omega_{\pi(2)}] [\omega_{\pi(3)}, \omega_{\pi(4)}] \cdots [\omega_{\pi(2g-1)}, \omega_{\pi(2g)}], \quad \pi \in S_p.$$

Wir müssen für unser Problem unter diesen Invarianten P die symmetrischen aussuchen ($p = 6m$) und dann $w_1 = w_7 = w_{13} = \dots$, $w_2 = w_8 = w_{14} = \dots$ usw. einsetzen; auf diese Weise erhält man alle Invarianten $F(w_1, \dots, w_6)$ vom Grade m in jedem w_i . Da die Formen $[w_i, w_j]^2$ Faktoren sind, die in die Diskriminante derjenigen binären Formen $F(x, y)$ eingehen, die w_i, w_j als Nullstellen besitzen, erhält man z. B. für

$$F = u_0 x^6 + u_1 x^5 y + u_2 x^4 y^2 + \cdots + u_6 y^6$$

die folgenden Invarianten:

$$\text{Gewicht 6. } A(u) = \sum_{\substack{G_1 G_2 G_3 = F \\ \deg G_i = 2}} \Delta_2(G_1) \Delta_2(G_2) \Delta_2(G_3)$$

($\Delta_2(ax^2 + bxy + cy^2) = b^2 - 4ac$, Diskriminante für Formen zweiten Grades. Summiert wird über alle 15 wesentlich verschiedenen Zerlegungen von F in drei quadratische Formen).

$$\text{Gewicht 12. } B(u) = \sum_{\substack{F=H_1 H_2 \\ \deg H_i=3}} \Delta_3(H_1) \Delta_3(H_2)$$

(10 Summanden, $\Delta_3(ax^3 + bx^2y + cxy^2 + fy^3) = (bc)^2 - 4ac^3 - 4b^3d - 27(ad)^2 + 18abcd$, Diskriminante kubischer Formen).

$$\text{Gewicht 18. } C(u) = \sum_{\substack{F=H_1 H_2 \\ G_i \nmid H_j}} \Delta_3(H_1) \Delta_3(H_2) \Delta_2(G_1) \Delta_2(G_2) \Delta_2(G_3)$$

(60 Summanden, H_i kubische Formen, G_j quadratische Formen).

$$\text{Gewicht 30. } D(u) = \Delta_6(F)$$

Diskriminante von F).

IGUSA hat gezeigt, daß man mittels dieser vier Invarianten die Mannigfaltigkeit M und die Abbildung j beschreiben kann (vgl. auch P. SAMUEL [1]).

Wir wollen hier eine andere Methode zur Herleitung dieser Resultate angeben, wir schließen dabei der Einfachheit halber die Fälle der Charakteristik 2, 3, 5 aus, die einige gesonderte Betrachtungen erfordern.

Eine andere Möglichkeit, Invarianten $J(u_0, \dots, u_6) = J(u)$ direkt auszurechnen, besteht darin, daß man die Eigenschaften

$$\left. \begin{aligned} J(h^6 u_0, h^6 u_1, \dots, h^6 u_6) &= h^{20} J(u_0, \dots, u_6), \\ J(u_6, u_5, \dots, u_0) &= (-1)^g J(u_0, u_1, \dots, u_6), \\ J(h^6 u_0, h^6 u_1, \dots, h u_5, u_6) &= h^g J(u_0, \dots, u_6) \end{aligned} \right\} \quad (g \text{ Gewicht von } J)$$

benutzt (die aus der Invarianz bezüglich $\begin{bmatrix} h & 0 \\ 0 & h \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} h & 0 \\ 0 & 1 \end{bmatrix}$ folgen), und die Differentialgleichung

$$6u_0 \frac{\partial J}{\partial u_1} + 5u_1 \frac{\partial J}{\partial u_2} + 4u_2 \frac{\partial J}{\partial u_3} + \dots + u_5 \frac{\partial J}{\partial u_6} = 0$$

(die aus der Invarianz von J bezüglich $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ folgt) benutzt. Das liefert z. B. für $g = 6$

$$A(u) = -2(120u_0u_6 - 20u_1u_5 + 8u_2u_4 - 3u_3^2).$$

Hilfssatz 1. $A(u) = B(u) = C(u) = D(u) = 0$ gilt genau dann, wenn F eine mindestens vierfache Nullstelle hat, d. h. auf den Orbits der Formen $x^6, x^5y, x^4y^2, x^4y(x-y)$. Ferner gilt $A = B = D = 0$ außer auf den obigen Formen noch genau auf den Orbits von $F = xy^2(x-y)(x^2 - 3xy + 3y^2)$ und $xy^2(x^3 - y^3)$.

Beweis. Daß die Invarianten auf den angegebenen Formen verschwinden, rechnet man unmittelbar nach.

Es sei jetzt umgekehrt $F = u_0x^6 + u_1x^5y + \dots$ eine Form, für die $D(u) = 0$ ist (F hat also eine zweifache Wurzel); wir nehmen o. B. d. A. an, daß F mindestens zwei verschiedene Wurzeln hat, so daß man F in die Gestalt

$$F = xy^2G, \quad G \text{ eine kubische Form,}$$

bringen kann (also $u_0 = u_1 = u_6 = 0$). Eine leichte Rechnung zeigt, daß in diesem Fall

$$B = (u_4^2 - 3u_3u_5)u_2^2, \quad A = 3u_3^2 - 8u_2u_4$$

gilt (bis auf den Faktor 2).

Die Gleichungen $A = B = 0$ haben die folgenden Lösungen:

1. $u_2 = u_3 = 0$, entspricht den Formen xy^4L , L linear (also o. B. d. A. $L = x$, $L = y$ oder $L = x - y$).
2. $u_2 = 1$, $u_3 = u_4 = 0$, entspricht den Formen $xy^2(x^3 - \alpha y^3)$.
3. $u_2 = 1$, $u_3 \neq 0$, dann ist die allgemeine Lösung von $A = B = 0$ gleich $(u_3, u_4, u_5) = (4\alpha, 6\alpha^2, 3\alpha^3)$, $\alpha \neq 0$; diese entsprechen den Formen

$$xy^2(x^3 + 4\alpha x^2y + 6\alpha^2xy^2 + 3\alpha^3y^3) = xy^2(x + y)(x^2 + 3\alpha xy + 3\alpha^2y^2).$$

Der Rest der Behauptung ist klar.

Folgerung. Sind A, B, C, D Unbestimmte vom Grad 1, 2, 3, 5, so ist

$$\begin{aligned} \mathbf{P}^6 &\rightarrow \bar{M} =: \text{Proj}(k[A, B, C, D]), \\ (u_0 : \dots : u_6) &\mapsto [A(u), B(u), C(u), D(u)] \end{aligned}$$

eine rationale Abbildung von $\mathbf{P}^6$ auf $\bar{M}$. Das Schema M ist normal.

Beweis. Es ist $\dim \bar{M} = 3$ und z. B. die Dimension der Faser $[A, B, C, D] = [0, 0, 1, 0]$ gleich 3; also hat die allgemeine Faser ebenfalls die Dimension 3, und die Abbildung ist rational. Da A, B, C, D algebraisch unabhängig sind, ist $\bar{M}$ normal.

Ist M_D bzw. $(\mathbf{P}^6)_D$ die offene Menge mit $D \neq 0$, so erhält man einen Morphismus

$$\begin{array}{ccc} (\mathbf{P}^6)_D & \xrightarrow{\quad} & \bar{M}_D \\ & \searrow j & \nearrow \\ & M & \end{array}$$

und wir wollen zeigen, daß $M \cong \bar{M}_D$ ist, d. h.

$$M = \text{Spec}(k[x^5, xy, x^2z, xy^2, yz, y^5, xz^3, z^5])$$

$$\text{mit } x^5D = A^5, x^2yD = A^3B, x^2zD = A^2C, \dots, z^5D = C^5.$$

Hilfssatz 2. Es gibt eine $PGL(2)$ -stabile offene Menge $U \subseteq (\mathbf{P}^6)_D$, auf der $PGL(2)$ frei operiert (d. h., für die $U \times PGL(2) \rightarrow U \times U$, $(u, \sigma) \mapsto (u\sigma, u)$ eine abgeschlossene Einbettung ist).

Beweis. Wir haben ein kommutatives Diagramm

$$\begin{array}{ccc} (\mathbf{P}^1)_D^6 & \xrightarrow{\quad} & (\mathbf{P}^6)_D \\ \downarrow & & \downarrow j \\ (\mathbf{P}^1)_D^3 & \xrightarrow{\quad} & M \end{array}$$

wobei die vertikalen Pfeile Quotienten bezüglich $PGL(2)$ sind ($(\mathbb{P}^1)_D^6 \rightarrow (\mathbb{P}^1)_D^3$ ist die Abbildung

$$(x_1, \dots, x_6) \mapsto ((x_4 : x_5 : x_6 : x_1), (x_4 : x_5 : x_6 : x_2), (x_4 : x_5 : x_6 : x_3))^1,$$

und $(\mathbb{P}^1)_D^3$ ist die Menge aller Tripel (y_1, y_2, y_3) mit $y_i \neq y_j \neq 0, 1, \infty$.

Die horizontalen Pfeile sind Quotienten bezüglich S_6 , und $(\mathbb{P}^1)_D^3 \rightarrow M$ ist etal über einer offenen Menge $U_0 \subset M$ (die Zerlegungsgruppe

$$\text{Stab}(y_1, y_2, y_3) = \{s \in S_6 : s(y_1, y_2, y_3) = (y_1, y_2, y_3)\}$$

ist nur auf einer abgeschlossenen Teilmenge von M verschieden). Die Fasern von j über U_0 sind dann reduzierte Schemata, und in $j^{-1}(U_0)$ gibt es eine nichtleere, stabile offene Menge U , so daß für $u \in U$ gilt:

$$PGL(2) \rightarrow U, \quad \sigma \mapsto u\sigma \text{ ist injektiv.}$$

(Denn ist $u\sigma = u$ für ein $\sigma \in PGL(2)$, so permutiert σ die sechs Wurzeln der zu u gehörigen Form sechsten Grades, hat also endliche Ordnung, und daher ist bei geeigneten Koordinaten σ die Abbildung $(x : y) \rightarrow (\varepsilon x : y)$, ε eine zweite, dritte, vierte, fünfte oder sechste Einheitswurzel. Die Formen, die bei diesen Transformationen invariant bleiben, sind in einer echten abgeschlossenen Teilmenge von $(\mathbb{P}^6)_D$ enthalten.)

Man erhält dann

$$PGL(2) \times U \xrightarrow{\sim} U \times_{U_0} U,$$

$$(\sigma, u) \mapsto (u\sigma, u),$$

q. e. d.

Es sei jetzt $L \subset \mathbb{P}^6$ der Unterraum der Formen vom Grade 6, die in $(1 : 0)$, $(0 : 1)$ und $(1 : 1)$ verschwinden, d. h., L ist der durch $F(1, 0) = F(0, 1) = F(1, 1) = 0$ definierte lineare Unterraum der Formen sechsten Grades.

Jedes $PGL(2)$ -Orbit von Punkten aus $(\mathbb{P}^6)_D$ schneidet L (da man durch eine projektive Transformation drei der sechs Nullstellen der Form F , die dem Punkt aus $(\mathbb{P}^6)_D$ entspricht, in die Punkte $\infty, 0, 1$ überführen kann).

Da es 120 Möglichkeiten gibt, unter sechs verschiedenen Punkten drei auszuwählen, und da durch drei Punkte und ihre Bilder genau eine projektive Transformation bestimmt wird, schneiden die Fasern von $j : U \rightarrow j(U) \subseteq M$ den Unterraum L in genau 120 Punkten.

Hilfssatz 3. $L_D \rightarrow \overline{M}_D, u \mapsto (A(u), B(u), C(u), D(u))$ ist ein ganzer Morphismus vom Grade 120, und $M \rightarrow \overline{M}_D$ ist ein Isomorphismus.

Beweis. Die Einschränkung von $\mathbb{P}^6 \rightarrow \overline{M}$ auf L ist in den endlich vielen Punkten, die den Formen $xy(x - y)G$, $G = x^3, y^3$ oder $(x - y)^3$ entsprechen, nicht definiert. Hieraus folgt leicht, daß $L_D \rightarrow \overline{M}_D$ ein eigentlicher, rationaler Morphismus ist, also insbesondere endlich (da L_D offen ist).

Die Faser in einem Punkt aus $\overline{M}_D$, in dem $B = t_1 A^2, C = t_2 A^3, D = t_3 A^5$ gilt, ist im Schnittprodukt der drei Flächen in L mit den Gleichungen

$$B(u) - t_1 A^2(u) = C(u) - t_2 A^3(u) = D(u) - t_3 A^5(u) = 0$$

¹⁾ Mit $(a:b:c:d)$ wird das Doppelverhältnis der Punkte a, b, c, d auf $\mathbb{P}^1$ bezeichnet.

enthalten, und nach dem Satz von BÉZOUT ist (für allgemeine t_1, t_2, t_3) dieses Schnittprodukt ein Zyklus vom Grad $4 \cdot 6 \cdot 10 = 240$.

Da beispielsweise $x^4y(x-y)$ ein Punkt dieses Zyklus ist, der nicht zur Faser gehört, hat der Morphismus $L_D \rightarrow \bar{M}_D$ einen Grad $d < 240$, und wegen der Faktorisierung $L_D \rightarrow M \rightarrow \bar{M}_D$ ist der Grad $[L_D : M]$ ein Teiler von d .

Es genügt zu zeigen, daß $[L_D : M] = 120$ ist, denn dann ist $d = 120$ und $M \rightarrow \bar{M}_D$ birational (und endlich, also biregulär, da $\bar{M}_D$ normal ist).

Da jede Faser von $U \rightarrow j(U) \subset M$ den Unterraum in 120 Punkten schneidet und isomorph zu $PGL(2)$ ist, genügt zu zeigen, daß L diese Fasern transversal schneidet, bzw. folgenden

Hilfssatz 4. Für $u \in (\mathbf{P})_D^6$ ist

$$PGL(2) \times_{\mathbf{P}} L = \{(\sigma, v) \mid \sigma \in PGL(2), v \in L, u\sigma = v\}$$

reduziert und diskret.

Beweis. Ohne Beschränkung der Allgemeinheit sei $u \in L$, $(\sigma, v) = (\text{id}, u)$. Ist $F = \sum_{v=0}^6 u x^6-v y^v$, dann ist $PGL(2) \times_{\mathbf{P}} L$ im wesentlichen das algebraische Schema

$$\left\{ \sigma = \begin{bmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{bmatrix} \in PGL(2) \mid F^\sigma(1, 0) = F^\sigma(0, 1) = F^\sigma(1, 1) = 0 \right\},$$

d. h. das durch

$$F(\xi_1, \xi_2) = F(\eta_1, \eta_2) = F(\xi_1 + \eta_1, \xi_2 + \eta_2) = 0, \quad \xi_1\eta_2 - \xi_2\eta_1 = 1$$

definierte Schema.

Berechnung der Funktionaldeterminante Δ in $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ergibt

$$\Delta = 2 \frac{\partial F}{\partial x}(1, 0) \frac{\partial F}{\partial y}(0, 1) \frac{\partial F}{\partial x}(1, 1) \neq 0$$

(da F keine mehrfachen Wurzeln hat), q. e. d.

Alle diese Funktionen sind definiert über dem Ring $\Lambda = \mathbf{Z}\left[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}\right]$, und alle Betrachtungen gelten über diesem Ring. Zusammenfassend gilt also:

2.2.3. Satz. Es sei M das Λ -Schema

$$\text{Spec}(\Lambda[x^5, x^3y, x^2z, xy^2, yz, y^5, xz^3, z^5]).$$

(a) Die geometrischen Punkte $M(k)$ (k ein algebraisch abgeschlossener Körper der Charakteristik $\neq 2, 3, 5$) entsprechen umkehrbar eindeutig den Isomorphieklassen von Kurven vom Geschlecht 2 über k .

(b) Ist S ein Λ -Schema, $(C_s)_{s \in S}$ eine algebraische Familie von Kurven vom Geschlecht 2, so gibt es einen eindeutig bestimmten Λ -Morphismus $j: S \rightarrow M$, so daß $j(s)$ der zu C_s gehörige Punkt ist.

(c) (j, M) ist universell mit (a) und (b).

(d) Sind die Verzweigungswerte der kanonischen Überlagerung $C_s \rightarrow \mathbf{P}^1$ die Nullstellen von $u_0x^6 + u_1x^5y + \dots$, so ist $j(s)$ durch die Funktion von Hilfssatz 3 definiert.